Documentazione sulla classificazione BlueXP

BlueXP classification

NetApp
April 03, 2024

Sommario

Documentazione sulla classificazione BlueXP

Note di rilascio

Novità della classificazione BlueXP

Scopri le novità della classificazione BlueXP (Cloud Data Sense).

1 aprile 2024 (versione 1,30)

Supporto aggiunto per la classificazione RHEL v8,8 e v9,3 BlueXP

Questa versione fornisce il supporto per Red Hat Enterprise Linux v8,8 e v9,3 oltre a 9.x, che richiede Podman, anziché il motore Docker. Applicabile a qualsiasi installazione manuale on-premise della classificazione BlueXP.

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.

Scopri di più "Panoramica sulle implementazioni di classificazione BlueXP".

Opzione per attivare la raccolta del registro di controllo rimossa

L'opzione per attivare la raccolta del registro di controllo è stata disattivata.

Velocità di scansione migliorata

Le prestazioni di scansione sui nodi scanner secondari sono state migliorate. È possibile aggiungere ulteriori nodi scanner se è necessaria una potenza di elaborazione aggiuntiva per le scansioni. Per ulteriori informazioni, fare riferimento a. "Installare la classificazione BlueXP su un host con accesso a Internet".

Aggiornamenti automatici

Se hai implementato la classificazione BlueXP su un sistema con accesso Internet, il sistema si aggiorna automaticamente. In precedenza, l'aggiornamento si è verificato dopo un tempo specifico trascorso dall'ultima attività dell'utente. Con questa release, la classificazione BlueXP si aggiorna automaticamente se l'ora locale è compresa tra le 9:1:00 e le 9:5:00. Se l'ora locale è al di fuori di queste ore, l'aggiornamento avviene dopo un intervallo di tempo specifico trascorso dall'ultima attività dell'utente. Per ulteriori informazioni, fare riferimento a. "Installazione su un host Linux con accesso a Internet".

Se hai implementato la classificazione BlueXP senza accesso a Internet, dovrai eseguire l'aggiornamento manualmente. Per ulteriori informazioni, fare riferimento a. "Installare la classificazione BlueXP su un host Linux senza accesso Internet".

4 marzo 2024 (versione 1,29)

Ora è possibile escludere la scansione dei dati che risiedono in determinate directory di origine dati

Se si desidera che la classificazione BlueXP escluda la scansione dei dati che risiedono in determinate directory di origine dati, è possibile aggiungere questi nomi di directory a un file di configurazione elaborato dalla classificazione BlueXP. Questa funzione consente di evitare la scansione di directory non necessarie o che potrebbero generare risultati falsi positivi per i dati personali.

"Scopri di più".

Il supporto di istanze di grandi dimensioni è ora qualificato

Se hai bisogno della classificazione BlueXP per analizzare più di 250 milioni di file, puoi utilizzare un'istanza Extra Large nell'implementazione del cloud o nell'installazione on-premise. Questo tipo di sistema è in grado di eseguire la scansione di un massimo di 500 milioni di file.

"Scopri di più".

10 gennaio 2024 (versione 1,27)

I risultati della pagina di analisi ora visualizzano le dimensioni totali oltre al numero totale di elementi

I risultati filtrati nella pagina di analisi ora mostrano la dimensione totale degli elementi oltre al numero totale di file. Ciò può essere utile quando si spostano file, si eliminano file e altro ancora.

Configurare gli ID gruppo aggiuntivi come "aperti all'organizzazione"

Ora puoi configurare gli ID di gruppo in NFS in modo che siano considerati "aperti all'organizzazione" direttamente dalla classificazione BlueXP se il gruppo non era stato inizialmente impostato con tale autorizzazione. Tutti i file e le cartelle con questi ID di gruppo allegati verranno visualizzati come "Apri all'organizzazione" nella pagina Dettagli analisi. Scopri come "Aggiungere altri ID gruppo come "aperti all'organizzazione"".

14 dicembre 2023 (versione 1.26.6)

Questa versione includeva alcuni miglioramenti minori.

Inoltre, la versione ha temporaneamente rimosso le seguenti opzioni:

- L'opzione per attivare la raccolta del registro di controllo è stata disattivata. Fare riferimento a. "Monitorare e gestire gli eventi di accesso ai file".
- Durante l'analisi Directory, l'opzione per calcolare il numero di dati personali identificabili (PII) per directory non è disponibile. Fare riferimento a. "Esaminare i dati memorizzati nella propria organizzazione".
- L'opzione per integrare i dati utilizzando le etichette AIP (Azure Information Protection) è stata disattivata. Fare riferimento a. "Organizzare i dati privati".

6 novembre 2023 (versione 1.26.3)

In questa versione sono stati risolti i seguenti problemi

- È stata risolta un'incoerenza quando si presenta il numero di file sottoposti a scansione dal sistema nei dashboard.
- Miglioramento del comportamento di scansione mediante la gestione e la creazione di report su file e directory con caratteri speciali nel nome e nei metadati.

4 ottobre 2023 (versione 1,26)

Supporto per le installazioni on-premise della classificazione BlueXP su RHEL versione 9

Le versioni 8 e 9 di Red Hat Enterprise Linux non supportano il motore Docker, necessario per l'installazione della classificazione BlueXP. Ora supportiamo l'installazione della classificazione BlueXP su RHEL 9,0, 9,1 e 9,2 utilizzando Podman versione 4 o superiore come infrastruttura container. Se il tuo ambiente richiede

l'utilizzo delle versioni più recenti di RHEL, ora puoi installare la classificazione BlueXP (versione 1,26 o superiore) quando utilizzi Podman.

Al momento non supportiamo installazioni in siti oscuri o ambienti di scansione distribuiti (utilizzando nodi di scansione master e remoti) quando si utilizza RHEL 9.x.

5 settembre 2023 (versione 1,25)

Implementazioni di piccole e medie dimensioni temporaneamente non disponibili

Quando implementi un'istanza di classificazione BlueXP in AWS, al momento non è disponibile l'opzione per selezionare **implementa > Configurazione** e scegliere un'istanza di piccole o medie dimensioni. È comunque possibile distribuire l'istanza utilizzando le dimensioni dell'istanza di grandi dimensioni selezionando **distribuisci > distribuisci**.

Applicare le etichette su un massimo di 100.000 elementi dalla pagina risultati analisi

In passato, nella pagina dei risultati dell'analisi era possibile applicare tag a una singola pagina alla volta (20 elementi). Ora è possibile selezionare **tutti** elementi nelle pagine dei risultati dell'analisi e applicare tag a tutti gli elementi, fino a 100.000 elementi alla volta. "Scopri come".

Identificare i file duplicati con una dimensione minima di 1 MB

Classificazione BlueXP utilizzata per identificare i file duplicati solo quando avevano 50 MB o più. Ora è possibile identificare i file duplicati che iniziano con 1 MB. È possibile utilizzare i filtri della pagina di analisi "dimensione file" insieme a "duplicati" per vedere quali file di una certa dimensione sono duplicati nell'ambiente in uso.

17 luglio 2023 (versione 1.24)

Due nuovi tipi di dati personali tedeschi sono identificati dalla classificazione BlueXP

La classificazione BlueXP è in grado di identificare e classificare i file che contengono i seguenti tipi di dati:

- ID tedesco (Personalausweisnummer)
- Numero tedesco di previdenza sociale (Sozialversicherungsnummer)

"Scopri tutti i tipi di dati personali che la classificazione BlueXP può identificare nei tuoi dati".

La classificazione BlueXP è completamente supportata in modalità limitata e privata

La classificazione BlueXP è ora completamente supportata nei siti senza accesso a Internet (modalità privata) e con accesso Internet in uscita limitato (modalità limitata). "Scopri di più sulle modalità di implementazione di BlueXP per il connettore".

Possibilità di saltare le versioni durante l'aggiornamento di un'installazione in modalità privata della classificazione BlueXP

Ora è possibile eseguire l'aggiornamento a una versione più recente della classificazione BlueXP anche se non è sequenziale. Ciò significa che l'attuale limite di aggiornamento della classificazione BlueXP per una versione alla volta non è più necessario. Questa funzione è rilevante a partire dalla versione 1.24 in poi.

L'API di classificazione BlueXP è ora disponibile

L'API di classificazione BlueXP ti consente di eseguire azioni, creare query ed esportare informazioni sui dati che stai analizzando. La documentazione interattiva è disponibile utilizzando Swagger. La documentazione è suddivisa in più categorie, tra cui analisi, conformità, governance e configurazione. Ogni categoria è un riferimento alle schede nell'interfaccia utente di classificazione BlueXP.

"Scopri di più sulle API di classificazione BlueXP".

6 giugno 2023 (versione 1.23)

Il giapponese è ora supportato durante la ricerca dei nomi dei soggetti dei dati

I nomi giapponesi possono ora essere inseriti quando si cerca il nome di un soggetto in risposta a una richiesta di accesso soggetto a dati (DSAR). È possibile generare un "Report Data Subject Access Request" con le informazioni risultanti. È inoltre possibile immettere i nomi giapponesi in "Filtro "Data Subject" nella pagina Data Investigation" identificare i file che contengono il nome dell'oggetto.

Ubuntu è ora una distribuzione Linux supportata su cui è possibile installare la classificazione BlueXP

Ubuntu 22.04 è stato qualificato come sistema operativo supportato per la classificazione BlueXP. È possibile installare la classificazione BlueXP su un host Ubuntu Linux nella rete o su un host Linux nel cloud quando si utilizza la versione 1.23 del programma di installazione. "Scopri come installare la classificazione BlueXP su un host con Ubuntu installato".

Red Hat Enterprise Linux 8.6 e 8.7 non sono più supportati con le nuove installazioni di classificazione BlueXP

Queste versioni non sono supportate con le nuove implementazioni perché Red Hat non supporta più Docker, che è un prerequisito. Se si dispone di una macchina di classificazione BlueXP esistente in esecuzione su RHEL 8.6 o 8.7, NetApp continuerà a supportare la configurazione.

La classificazione BlueXP può essere configurata come FPolicy Collector per ricevere eventi FPolicy dai sistemi ONTAP

È possibile consentire la raccolta dei registri di controllo dell'accesso ai file nel sistema di classificazione BlueXP per gli eventi di accesso ai file rilevati sui volumi negli ambienti di lavoro. La classificazione BlueXP può acquisire i seguenti tipi di eventi FPolicy e gli utenti che hanno eseguito le azioni sui file: Creare, leggere, scrivere, eliminare, rinominare, Modificare il proprietario/le autorizzazioni e modificare SACL/DACL. "Scopri come monitorare e gestire gli eventi di accesso ai file".

Le licenze Data Sense BYOL sono ora supportate nei siti bui

Ora puoi caricare la tua licenza BYOL Data Sense nel portafoglio digitale BlueXP in un sito buio, in modo da ricevere una notifica quando la tua licenza sta per esaurirsi. "Scopri come ottenere e caricare la licenza BYOL Data Sense".

3 aprile 2023 (versione 1.22)

Nuovo report sulla valutazione del rilevamento dei dati

Il Data Discovery Assessment Report fornisce un'analisi di alto livello dell'ambiente sottoposto a scansione per evidenziare i risultati del sistema e mostrare le aree problematiche e le potenziali fasi di risoluzione dei problemi. L'obiettivo di questo report è aumentare la consapevolezza dei problemi di governance dei dati, delle

esposizioni alla sicurezza dei dati e delle lacune nella compliance dei dati del tuo set di dati. "Scopri come generare e utilizzare il Data Discovery Assessment Report".

Possibilità di implementare la classificazione BlueXP su istanze più piccole nel cloud

Quando si implementa la classificazione BlueXP da un connettore BlueXP in un ambiente AWS, è ora possibile scegliere tra due tipi di istanze più piccoli rispetto a quelli disponibili con l'istanza predefinita. Se si esegue la scansione di un ambiente di piccole dimensioni, questo può contribuire a risparmiare sui costi del cloud. Tuttavia, esistono alcune limitazioni quando si utilizza l'istanza più piccola. "Vedere i tipi di istanze e le limitazioni disponibili".

È ora disponibile uno script standalone per qualificare il sistema Linux prima dell'installazione della classificazione BlueXP

Se si desidera verificare che il sistema Linux soddisfi tutti i prerequisiti indipendentemente dall'esecuzione dell'installazione di classificazione BlueXP, è possibile scaricare uno script separato che esegue solo i prerequisiti. "Scopri come verificare se il tuo host Linux è pronto per installare la classificazione BlueXP".

7 marzo 2023 (versione 1.21)

Nuova funzionalità per aggiungere categorie personalizzate dall'interfaccia utente di classificazione BlueXP

La classificazione BlueXP consente ora di aggiungere le proprie categorie personalizzate in modo che la classificazione BlueXP identifichi i file che si adattano a tali categorie. La classificazione BlueXP è molto ampia "categorie predefinite", pertanto, questa funzionalità consente di aggiungere categorie personalizzate per identificare dove si trovano informazioni specifiche per l'organizzazione nei dati.

"Scopri di più".

Ora è possibile aggiungere parole chiave personalizzate dall'interfaccia utente di classificazione BlueXP

La classificazione BlueXP ha avuto la possibilità di aggiungere parole chiave personalizzate che la classificazione BlueXP identificherà per un certo periodo di tempo nelle scansioni future. Tuttavia, era necessario accedere all'host Linux di classificazione BlueXP e utilizzare un'interfaccia a riga di comando per aggiungere le parole chiave. In questa release, la possibilità di aggiungere parole chiave personalizzate è nell'interfaccia utente di classificazione di BlueXP, rendendo molto semplice aggiungere e modificare queste parole chiave.

"Scopri di più sull'aggiunta di parole chiave personalizzate dall'interfaccia utente di classificazione BlueXP".

Possibilità di eseguire la classificazione BlueXP non dei file di scansione quando verrà modificato l'ultimo tempo di accesso

Per impostazione predefinita, se la classificazione di BlueXP non dispone di permessi di "scrittura" adeguati, 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. Tuttavia, se non si ha alcun problema se l'ultimo tempo di accesso viene ripristinato all'ora originale nei file, è possibile ignorare questo comportamento nella pagina di configurazione in modo che la classificazione BlueXP scansiona i volumi indipendentemente dalle autorizzazioni.

In combinazione con questa funzionalità, è stato aggiunto un nuovo filtro denominato "Scan Analysis Event", che consente di visualizzare i file non classificati perché la classificazione BlueXP non ha potuto ripristinare l'ultimo accesso o i file classificati anche se la classificazione BlueXP non ha potuto ripristinare l'ultimo

accesso.

"Scopri di più su "Last Access Time timestamp" e sulle autorizzazioni richieste dalla classificazione BlueXP".

Tre nuovi tipi di dati personali sono identificati dalla classificazione BlueXP

La classificazione BlueXP è in grado di identificare e classificare i file che contengono i seguenti tipi di dati:

- Numero della carta d'identità del Botswana (Omang)
- Numero passaporto Botswana
- Singapore National Registration Identity Card (NRIC)

"Scopri tutti i tipi di dati personali che la classificazione BlueXP può identificare nei tuoi dati".

Funzionalità aggiornate per le directory

- L'opzione "Light CSV Report" (Report CSV leggero) per i report di analisi dei dati include ora le informazioni provenienti dalle directory.
- Il filtro dell'ora "ultimo accesso" ora mostra l'ora dell'ultimo accesso per file e directory.

Miglioramenti all'installazione

- Il programma di installazione della classificazione BlueXP per i siti senza accesso a Internet (siti oscuri) ora esegue un controllo preliminare per assicurarsi che i requisiti di sistema e di rete siano stati soddisfatti per un'installazione corretta.
- I file di log di audit dell'installazione vengono salvati ora e scritti in `/ops/netapp/install_logs`.

5 febbraio 2023 (versione 1.20)

Possibilità di inviare e-mail di notifica basate su policy a qualsiasi indirizzo e-mail

Nelle versioni precedenti della classificazione BlueXP, è possibile inviare avvisi e-mail agli utenti BlueXP del proprio account quando alcuni criteri critici restituiscono risultati. Questa funzione ti consente di ricevere notifiche per proteggere i tuoi dati quando non sei online. Ora puoi anche inviare avvisi e-mail dalle policy a qualsiasi altro utente (fino a 20 indirizzi e-mail) che non sia presente nel tuo account BlueXP.

"Scopri di più sull'invio di avvisi e-mail in base ai risultati della policy".

Ora è possibile aggiungere modelli personali dall'interfaccia utente di classificazione BlueXP

La classificazione BlueXP ha avuto la possibilità di aggiungere "dati personali" personalizzati che la classificazione BlueXP identificherà per un certo periodo di tempo nelle scansioni future. Tuttavia, era necessario accedere all'host Linux di classificazione BlueXP e utilizzare una riga di comando per aggiungere i modelli personalizzati. In questa release, la possibilità di aggiungere modelli personali utilizzando un regex è nell'interfaccia utente di classificazione BlueXP, rendendo molto semplice aggiungere e modificare questi modelli personalizzati.

"Scopri di più sull'aggiunta di modelli personalizzati dall'interfaccia utente di classificazione BlueXP".

Possibilità di spostare 15 milioni di file utilizzando la classificazione BlueXP

In passato era possibile che la classificazione BlueXP spostasse un massimo di 100,000 file di origine in

qualsiasi condivisione NFS. Ora puoi spostare fino a 15 milioni di file alla volta. "Scopri di più sullo spostamento dei file di origine utilizzando la classificazione BlueXP".

Possibilità di visualizzare il numero di utenti che hanno accesso ai file di SharePoint Online

Il filtro "numero di utenti con accesso" ora supporta i file memorizzati nei repository SharePoint Online. In passato erano supportati solo i file su condivisioni CIFS. Si noti che i gruppi SharePoint che non sono basati su Active Directory non verranno conteggiati in questo filtro al momento.

Il nuovo stato "Partial Success" (operazione riuscita parziale) è stato aggiunto al pannello Action Status (Stato azione)

Il nuovo stato "Partial Success" (successo parziale) indica che un'azione di classificazione BlueXP è terminata e che alcuni elementi hanno avuto esito negativo, ad esempio quando si spostano o si eliminano file 100. Inoltre, lo stato "Finished" (terminato) è stato rinominato "Success" (riuscito). In passato, lo stato "Finished" (terminato) potrebbe elencare le azioni riuscite e non riuscite. Ora lo stato "Success" significa che tutte le azioni sono riuscite su tutti gli elementi. "Vedere come visualizzare il pannello Actions Status (Stato azioni)".

9 gennaio 2023 (versione 1.19)

Possibilità di visualizzare un grafico di file che contengono dati sensibili e che sono eccessivamente permissivi

La dashboard di governance ha aggiunto una nuova area *dati sensibili e permessi estesi* che fornisce una mappa termica dei file che contengono dati sensibili (inclusi dati personali sensibili e sensibili) e che sono eccessivamente permissivi. In questo modo è possibile individuare i rischi associati ai dati sensibili. "Scopri di più".

Nella pagina Data Investigation sono disponibili tre nuovi filtri

Sono disponibili nuovi filtri per perfezionare i risultati visualizzati nella pagina Data Investigation (analisi dati):

- Il filtro "numero di utenti con accesso" mostra i file e le cartelle aperti a un determinato numero di utenti. Puoi scegliere un intervallo di numeri per perfezionare i risultati, ad esempio per vedere quali file sono accessibili da 51-100 utenti.
- I filtri "ora di creazione", "ora di rilevamento", "ultima modifica" e "ultima accesso" consentono ora di creare un intervallo di date personalizzato invece di selezionare semplicemente un intervallo di giorni predefinito. Ad esempio, è possibile cercare i file con un'ora di creazione "più vecchia di 6 mesi" o con una data "ultima modifica" negli ultimi 10 giorni.
- Il filtro "percorso file" consente ora di specificare i percorsi che si desidera escludere dai risultati delle query filtrate. Se si inseriscono percorsi per includere ed escludere determinati dati, la classificazione BlueXP individua prima tutti i file nei percorsi inclusi, quindi rimuove i file dai percorsi esclusi e visualizza i risultati.

"Consulta l'elenco di tutti i filtri che puoi utilizzare per analizzare i tuoi dati".

La classificazione BlueXP può identificare il numero individuale giapponese

La classificazione BlueXP è in grado di identificare e classificare i file che contengono il numero individuale giapponese (noto anche come My Number). Questo include sia il numero personale che il numero personale aziendale. "Scopri tutti i tipi di dati personali che la classificazione BlueXP può identificare nei tuoi dati".

Limitazioni note

Le limitazioni note identificano le funzioni non supportate da questa versione del prodotto o che non interagiscono correttamente con esso. Esaminare attentamente queste limitazioni.

Opzioni rimosse temporaneamente dalla release di classificazione BlueXP

La versione di dicembre 2023 (versione 1.26.6) ha temporaneamente rimosso le seguenti opzioni:

- L'opzione per attivare la raccolta del registro di controllo è stata disattivata.
- Durante l'analisi Directory, l'opzione per calcolare il numero di dati personali identificabili (PII) per directory non è disponibile.
- L'opzione per integrare i dati utilizzando le etichette AIP (Azure Information Protection) è stata disattivata.

Limiti di scansione per la classificazione BlueXP

La classificazione BlueXP esegue la scansione di una sola condivisione in un volume

Se si dispone di più condivisioni di file in un singolo volume, la classificazione BlueXP esegue la scansione della condivisione con la gerarchia più alta. Ad esempio, se si dispone di condivisioni come le seguenti:

- /A
- /A/B.
- /C.
- /D/E.

I dati in /A verranno quindi sottoposti a scansione. I dati in /C e /D non verranno sottoposti a scansione.

Soluzione alternativa

Esiste una soluzione per assicurarsi di eseguire la scansione dei dati da tutte le condivisioni del volume. Attenersi alla seguente procedura:

1. Nell'ambiente di lavoro, aggiungere il volume da sottoporre a scansione.
2. Dopo che la classificazione BlueXP ha completato la scansione del volume, accedere alla pagina *Data Investigation* e creare un filtro per vedere quale condivisione viene sottoposta a scansione:

   I dati verranno filtrati in base al nome dell'ambiente di lavoro e al tipo di directory = condivisione per visualizzare la condivisione sottoposta a scansione.

3. Ottenere l'elenco completo delle condivisioni presenti nel volume in modo da visualizzare le condivisioni non sottoposte a scansione.
4. "Aggiungere le condivisioni rimanenti a un gruppo di condivisione".

   È necessario aggiungere tutte le condivisioni singolarmente, ad esempio:

   ```
   /C
   /D
   ```

5. Eseguire questa procedura per ogni volume dell’ambiente di lavoro che dispone di più condivisioni.

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".

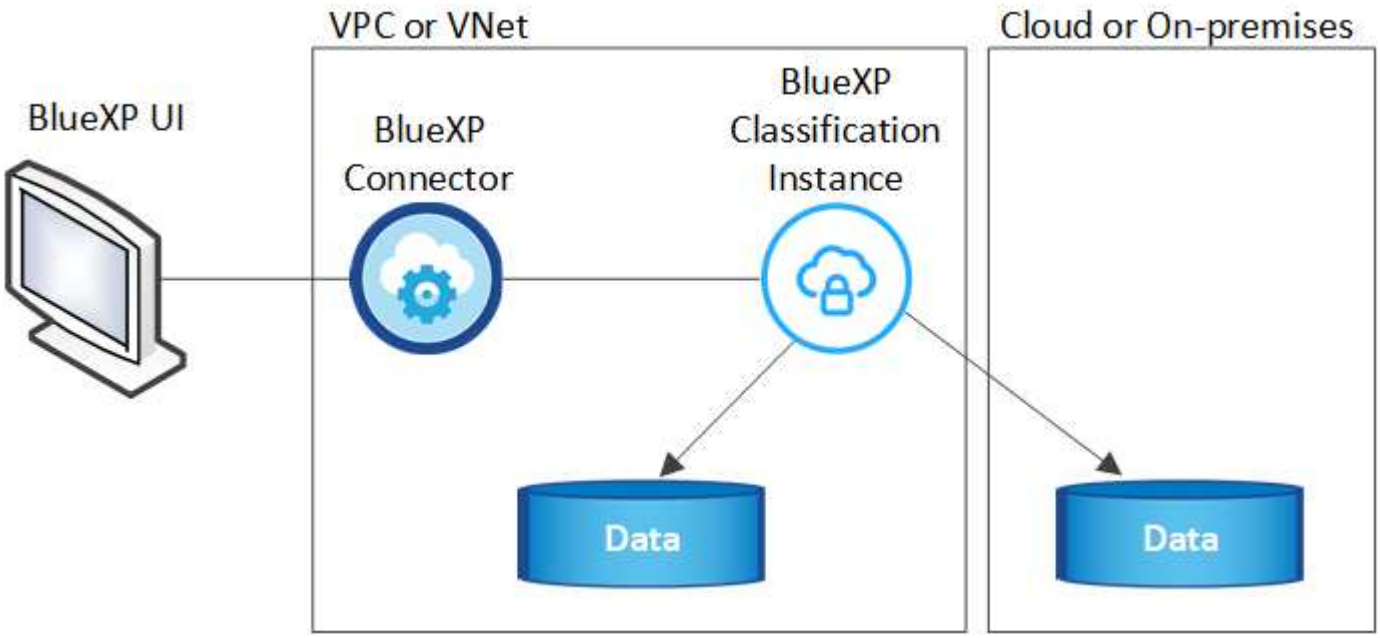
- L'installazione della classificazione BlueXP nel cloud richiede l'implementazione di un'istanza di cloud, con conseguente addebito da parte del provider di cloud in cui viene implementata. Vedere il tipo di istanza implementata per ciascun cloud provider. L'installazione della classificazione BlueXP 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

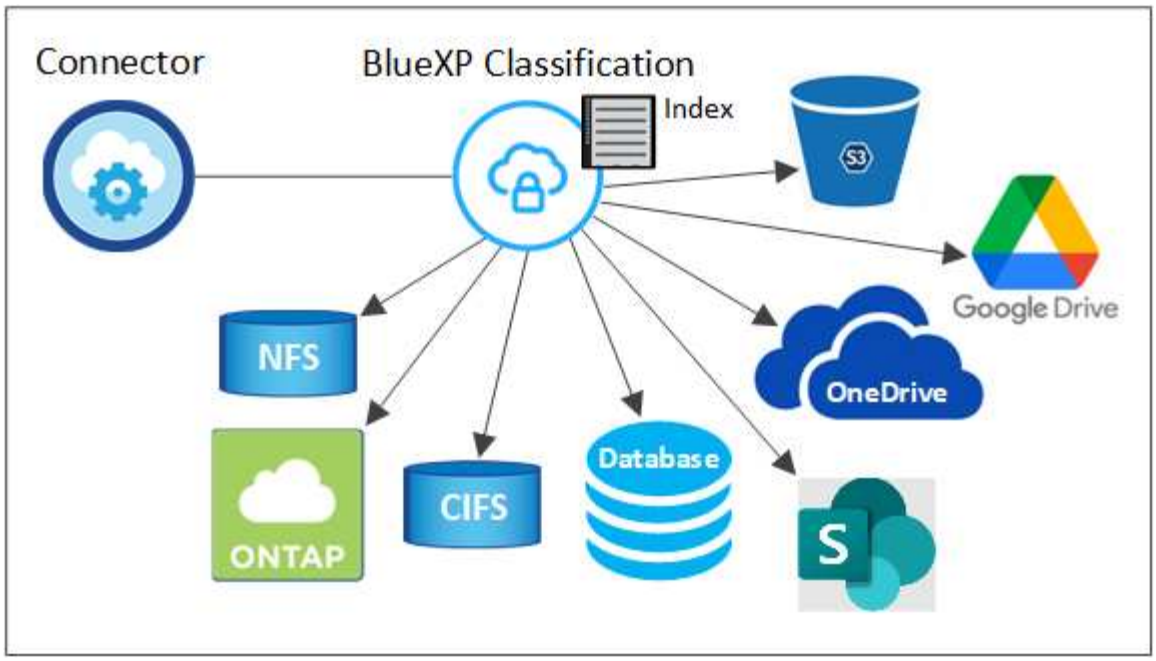
Ad alto livello, la classificazione BlueXP funziona come segue:

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

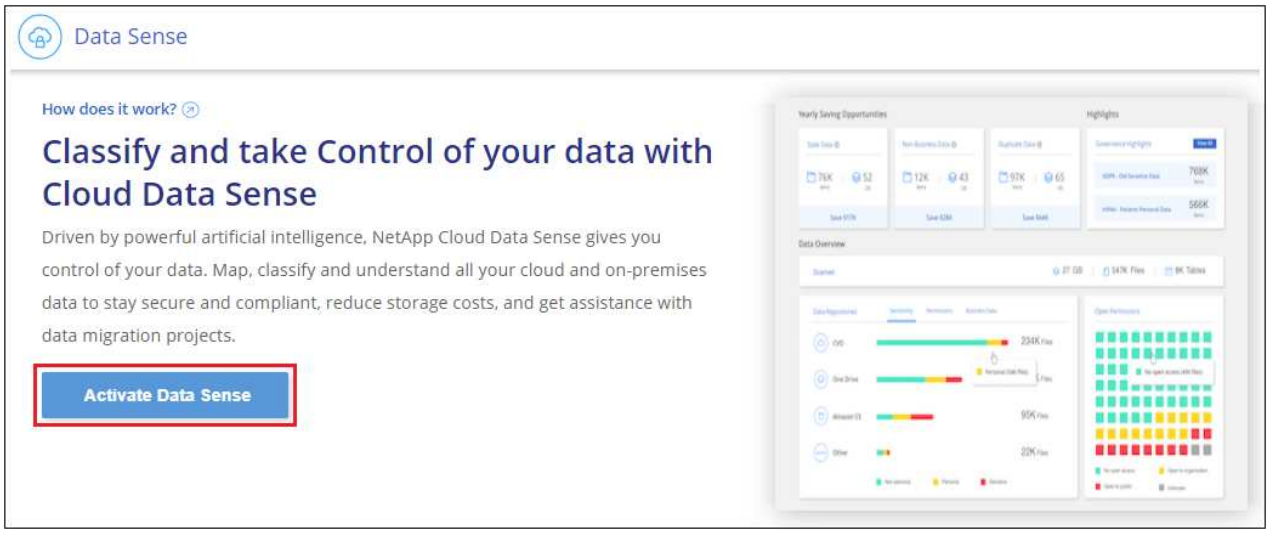
Seguire questi passaggi per implementare un'istanza della classificazione BlueXP nel cloud. Il connettore implementerà l'istanza nel cloud, quindi installerà il software di classificazione BlueXP su tale istanza.

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**.



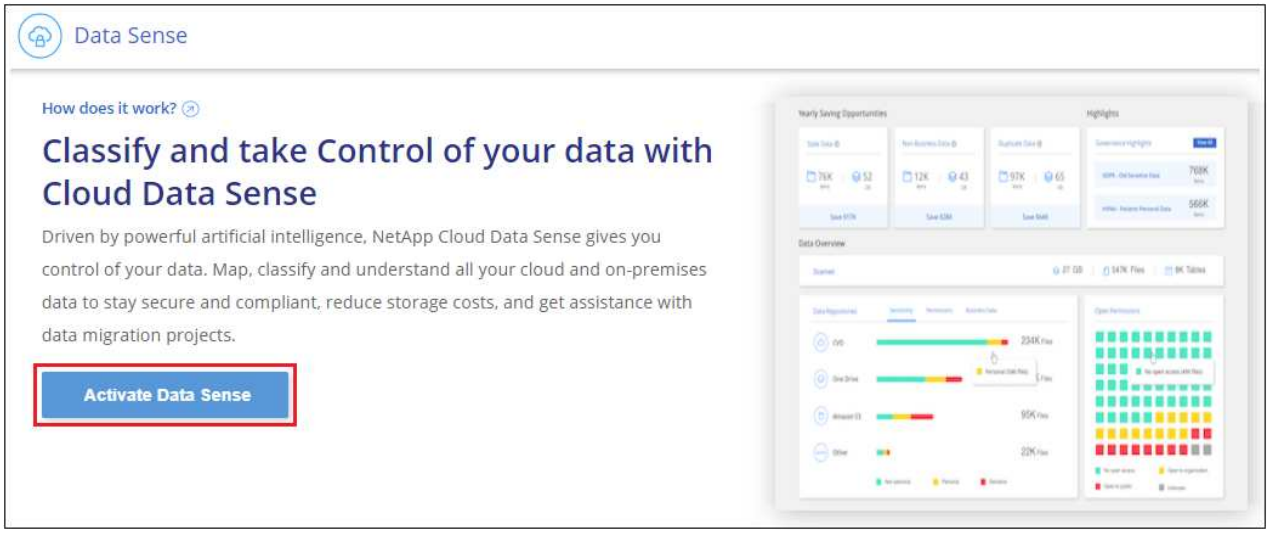
2. Fare clic su **Activate Data Sense** (attiva rilevamento dati).
3. Dalla pagina *Installation*, fare clic su **Deploy > Deploy** per utilizzare le dimensioni dell'istanza "Large" e avviare la procedura guidata di implementazione del cloud.
4. La procedura guidata visualizza lo stato di avanzamento 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).

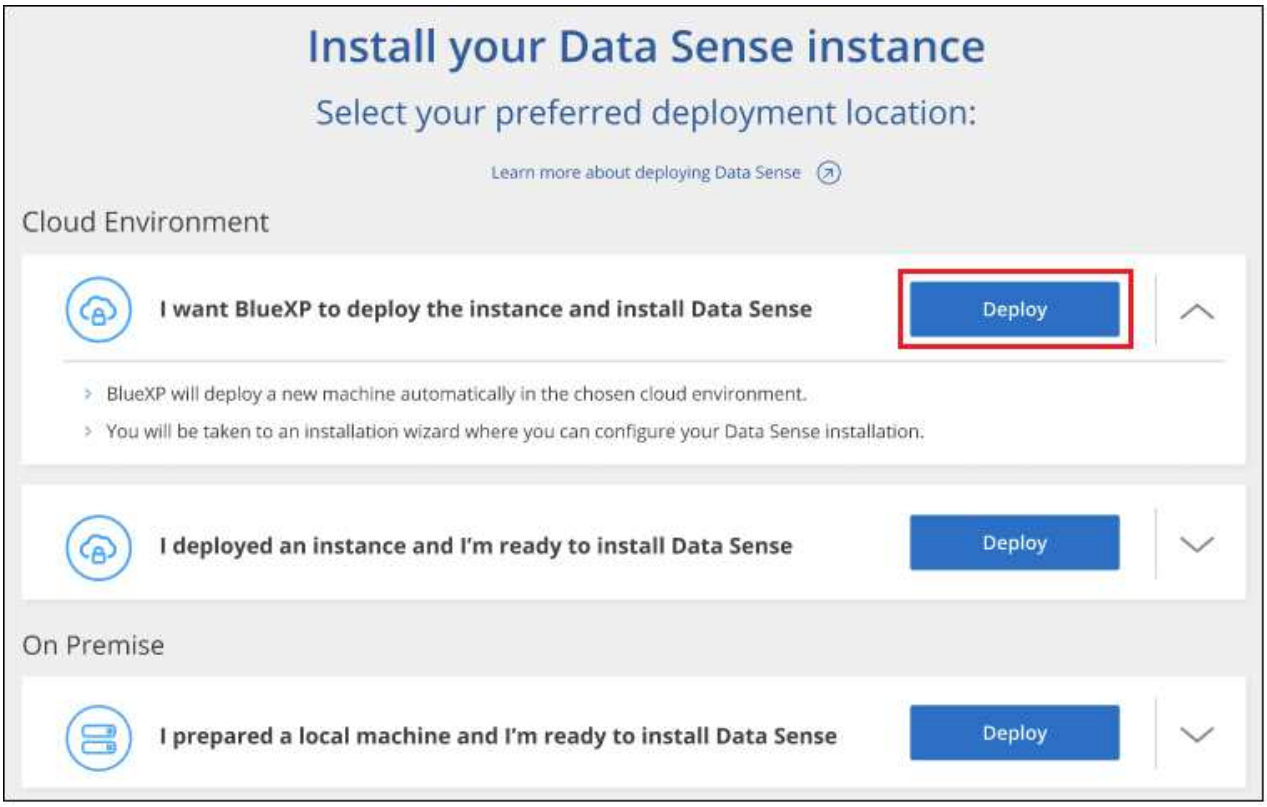
Implementazione in Azure

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.



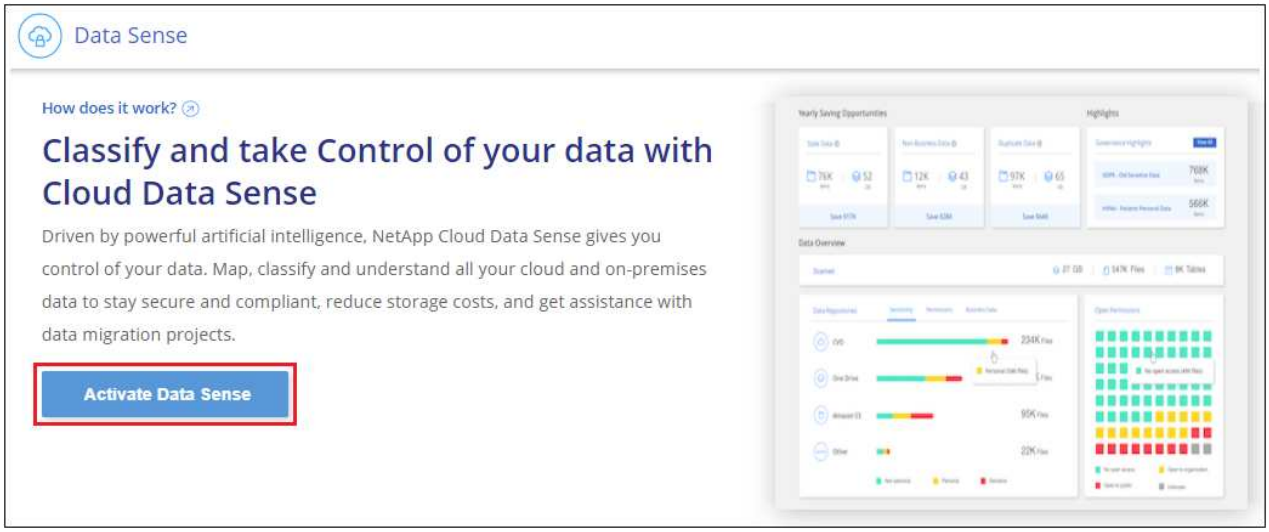
4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.

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).

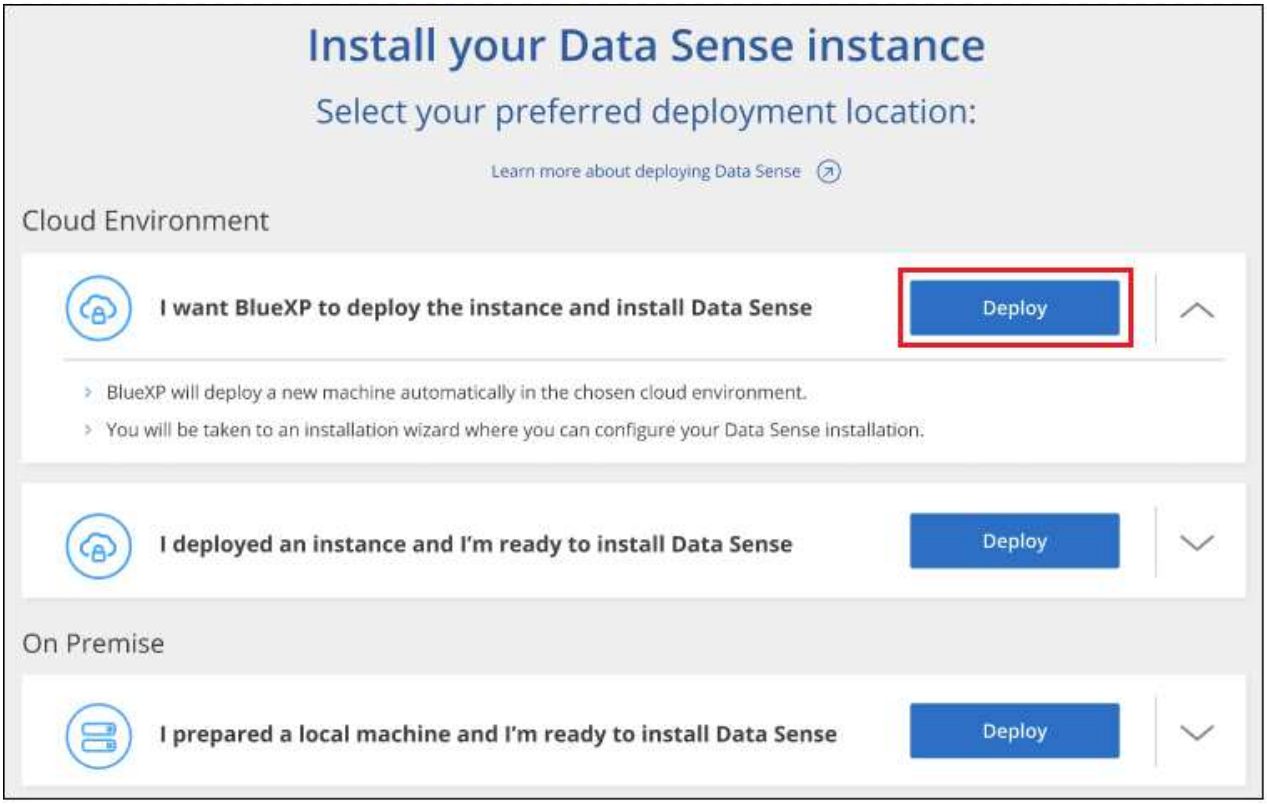
Implementazione in Google Cloud

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.

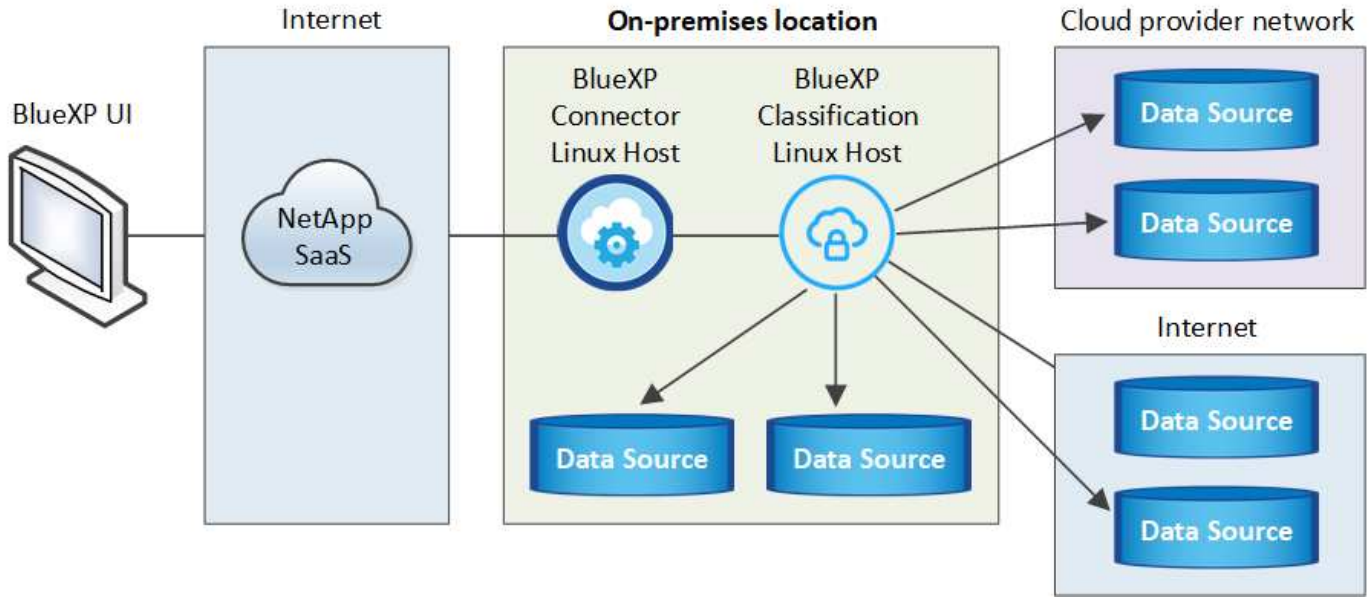
Installare la classificazione BlueXP su un host con accesso a Internet

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.

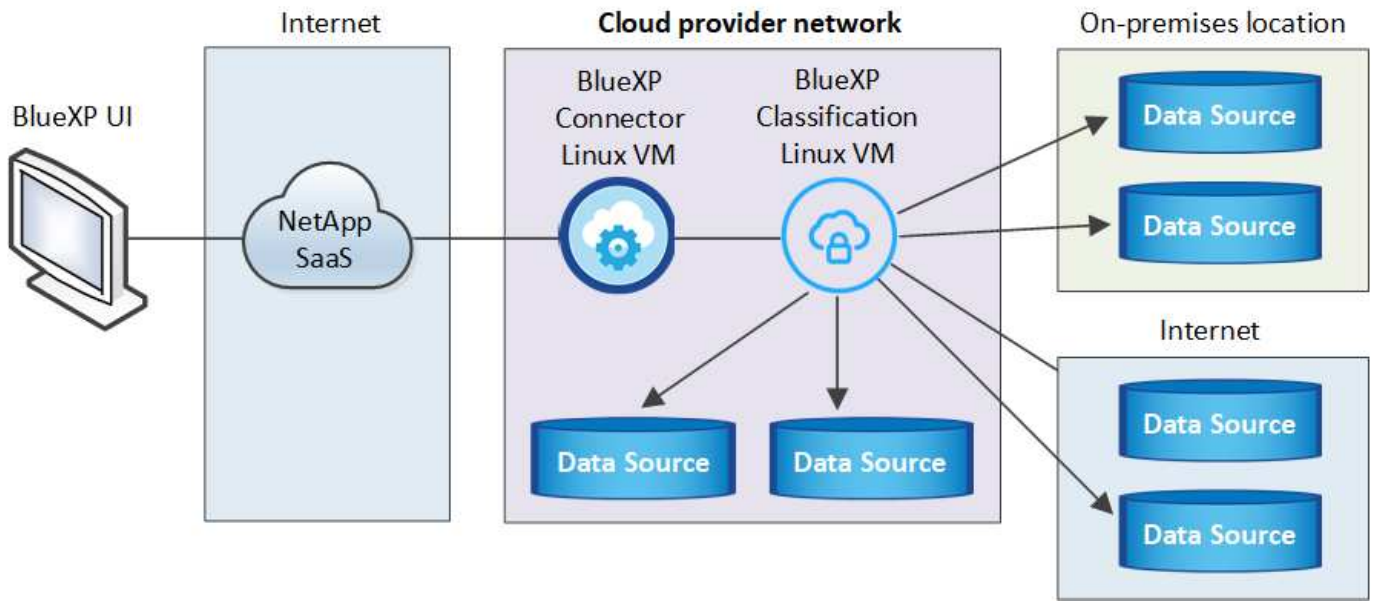
L'installazione on-premise potrebbe essere una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP on-premise utilizzando un'istanza di classificazione BlueXP che si trova anche on-premise, ma questo non è un requisito. Il software funziona esattamente allo stesso modo, indipendentemente 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.

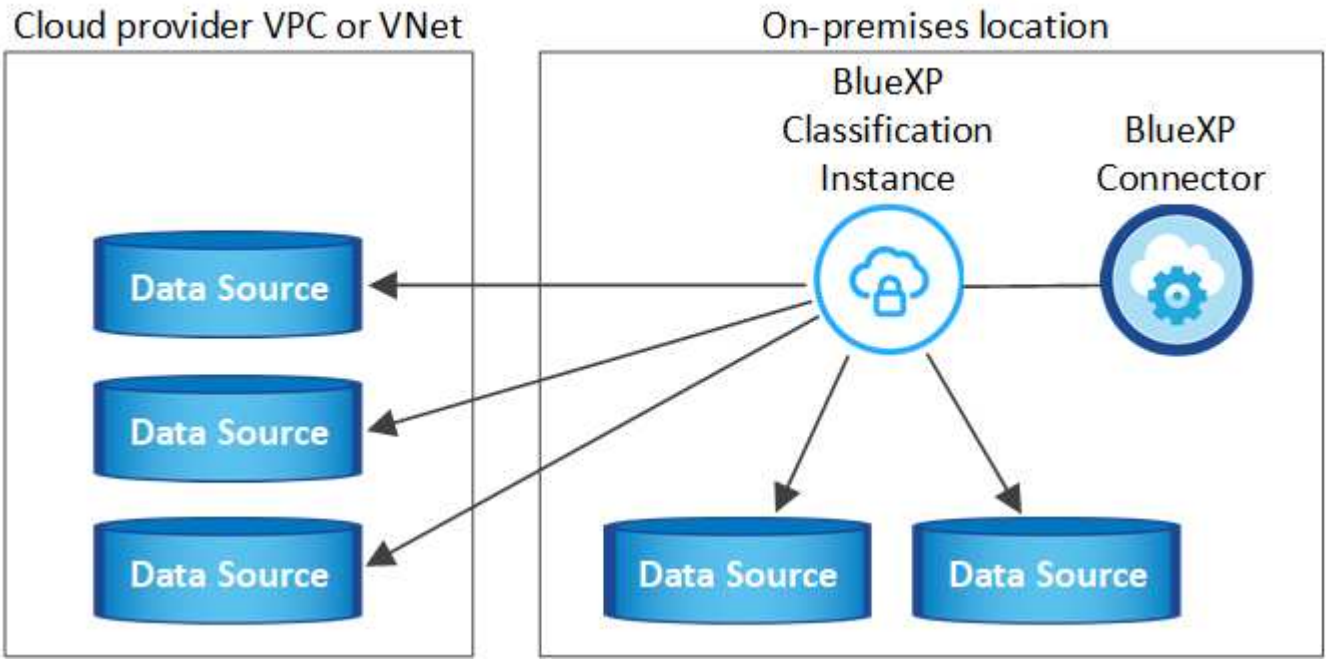
Tipo di connessione	Porte	Descrizione
Connettore <> classificazione BlueXP	8080 (TCP), 443 (TCP) e 80	Il firewall o le regole di routing per il connettore devono consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione BlueXP. Assicurarsi che la porta 8080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

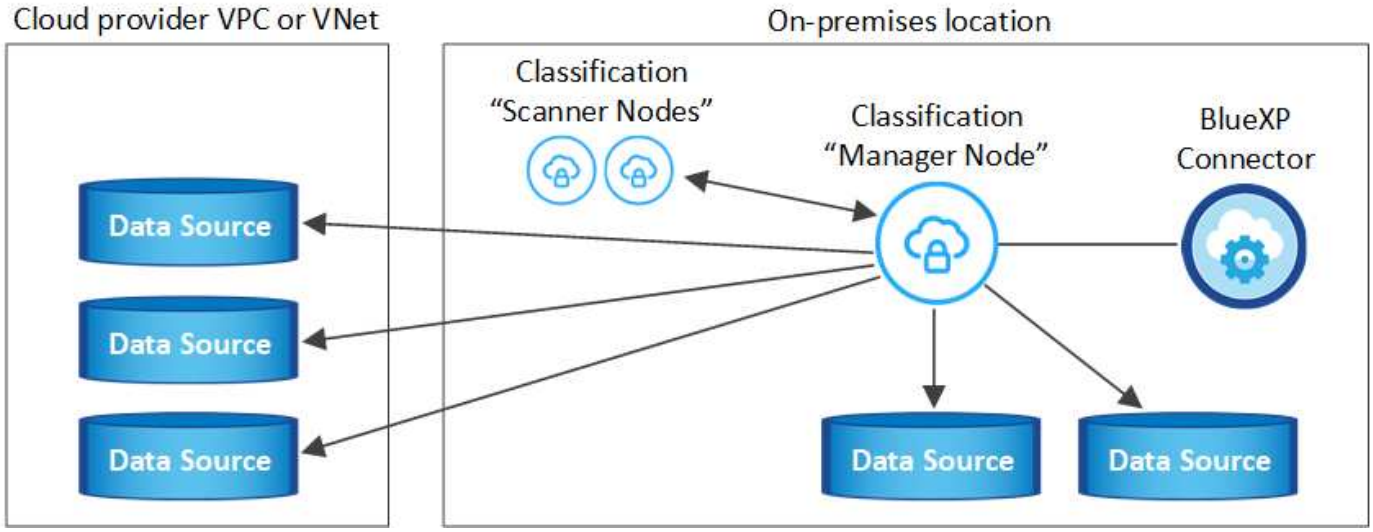
Se si utilizzano più host di classificazione BlueXP per fornire ulteriore potenza di elaborazione per eseguire la scansione delle origini dati, è necessario attivare porte/protocolli aggiuntivi. "Vedere i requisiti aggiuntivi per le porte".

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.

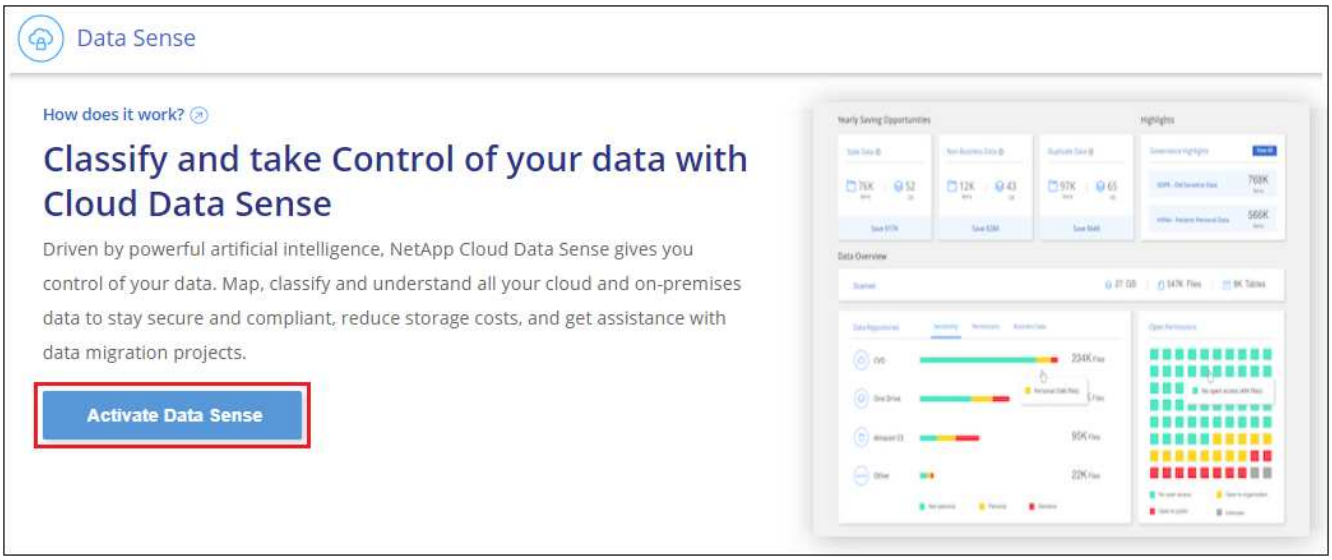
- Verificare che l'ambiente offline soddisfi i requisiti permessi e connettività.

Fasi

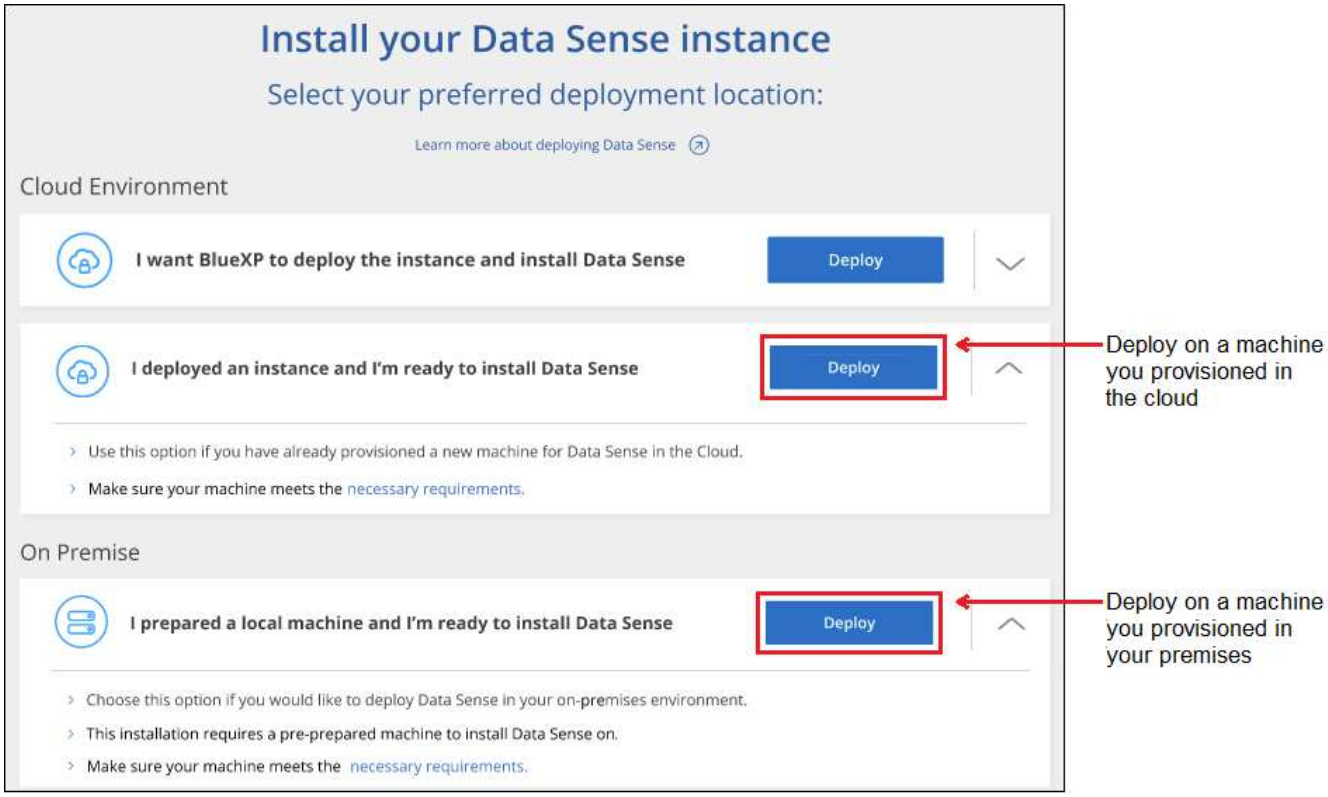
1. Scaricare il software di classificazione BlueXP dal "Sito di supporto NetApp". Il file da selezionare è **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copiare il file del programma di installazione sull'host Linux che si desidera utilizzare (utilizzando `scp` o qualche altro metodo).
3. Decomprimere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

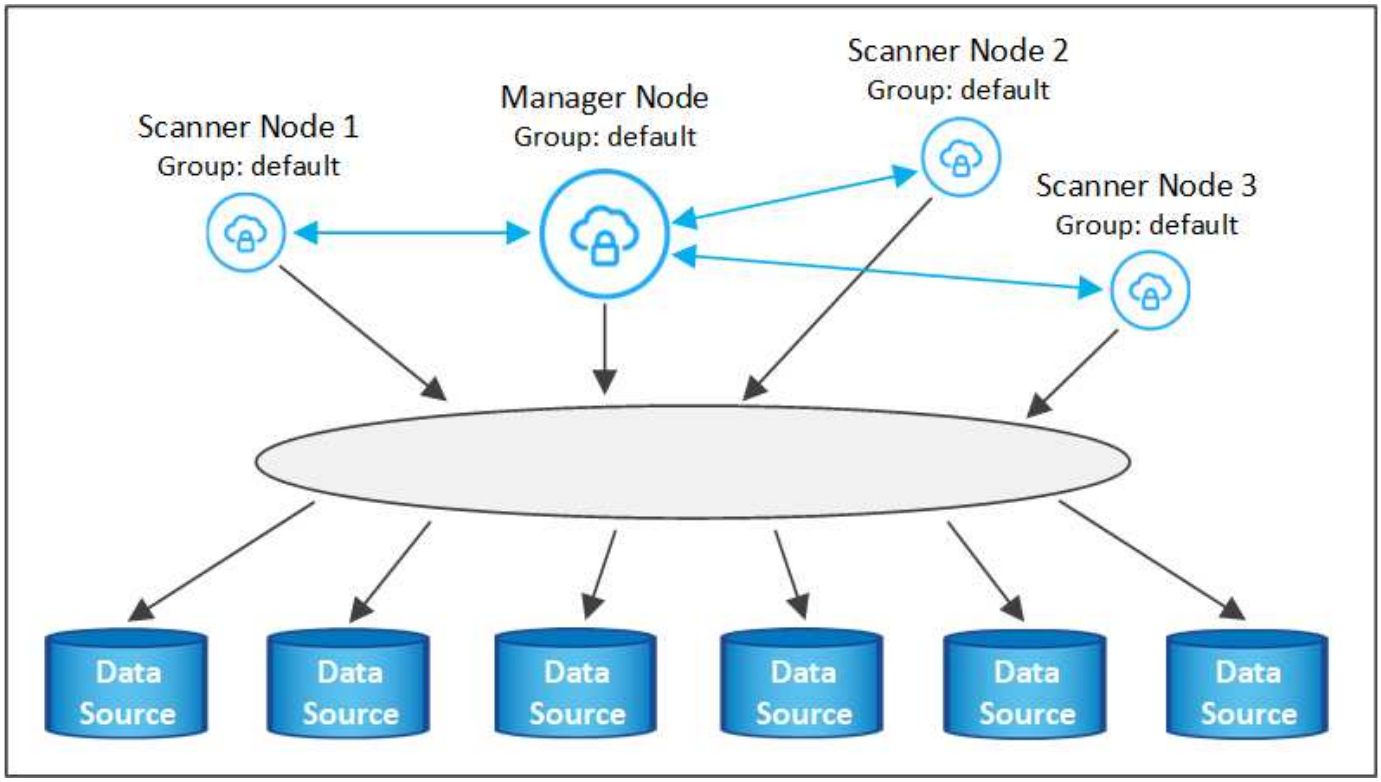
Aggiunta di nodi scanner a un'implementazione esistente

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:

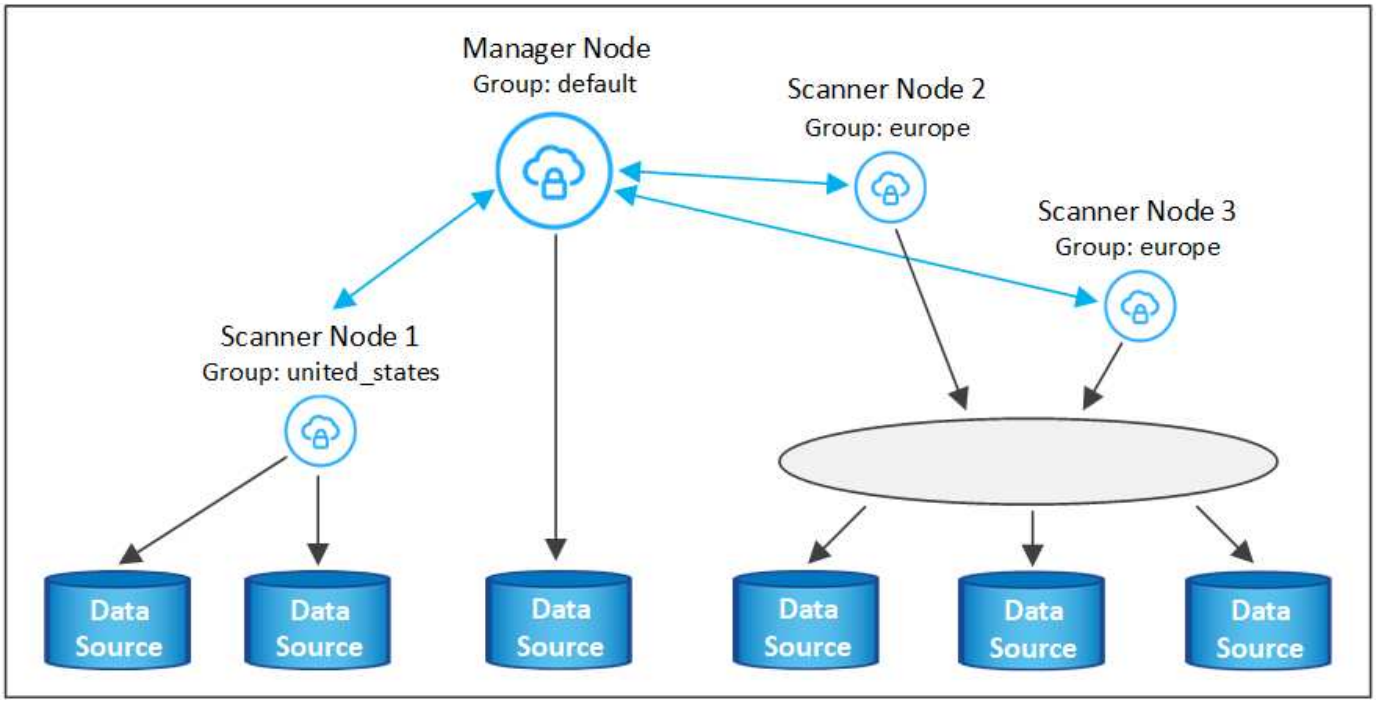
- aggiungere un nodo per facilitare la scansione di tutte le origini dati
- aggiunta di un nodo per agevolare la scansione di una specifica origine dati o di un gruppo specifico di origini dati (in genere in base alla posizione)

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:

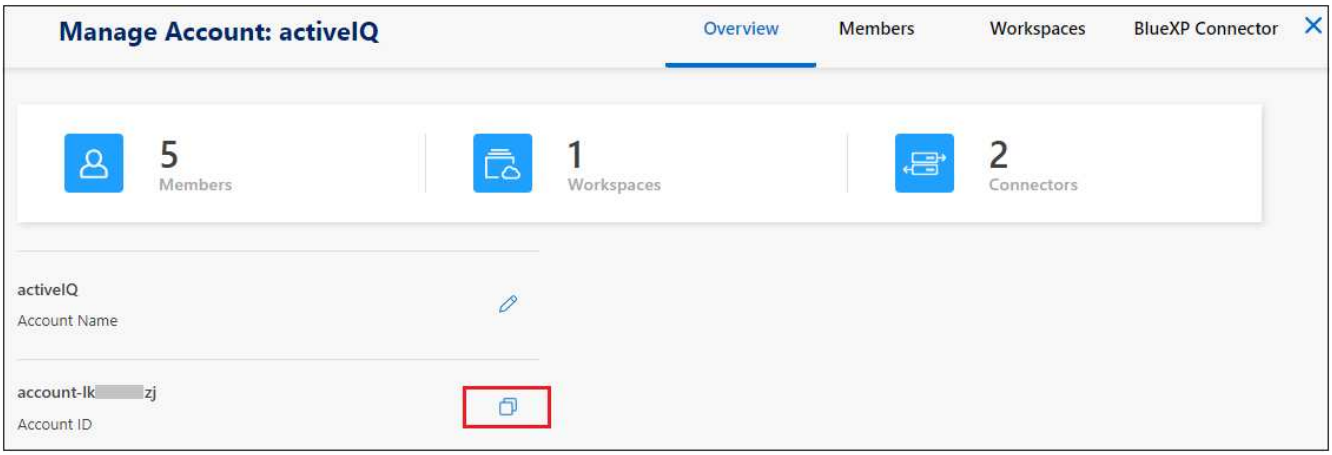
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp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

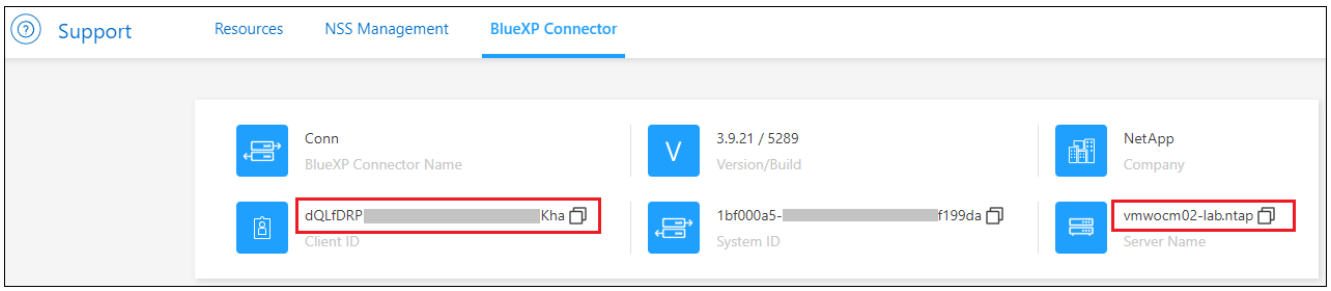
Fasi preliminari

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.

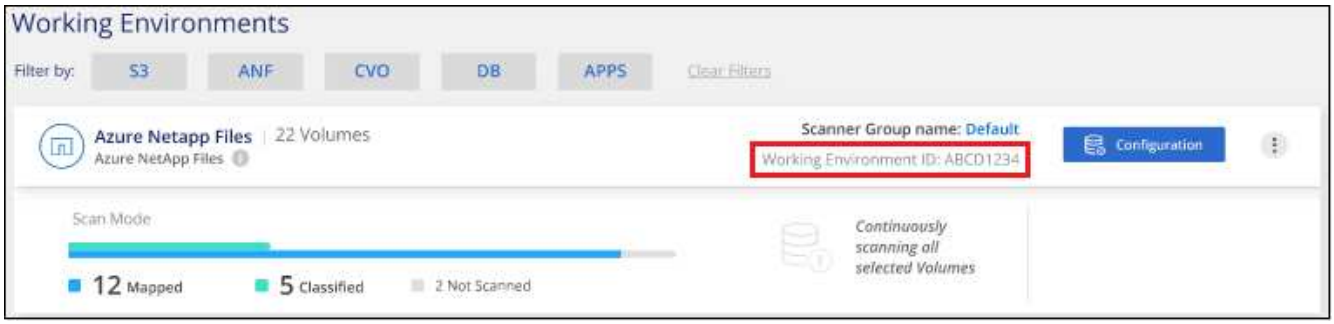
1. Dalla barra dei menu di BlueXP, fare clic su **account > Gestisci account**.



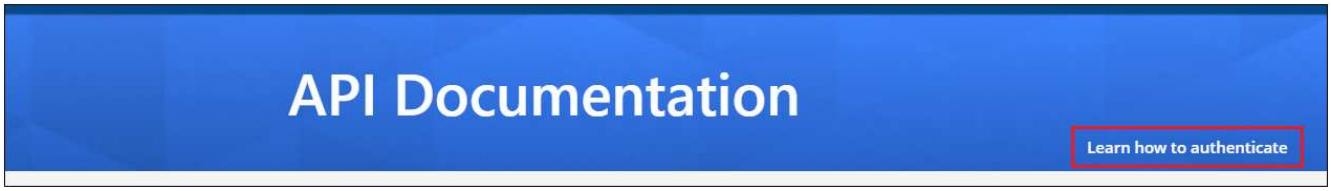
2. Copia l' *ID account*.
3. Dalla barra dei menu di BlueXP, fare clic su **Help > Support > BlueXP Connector**.



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`

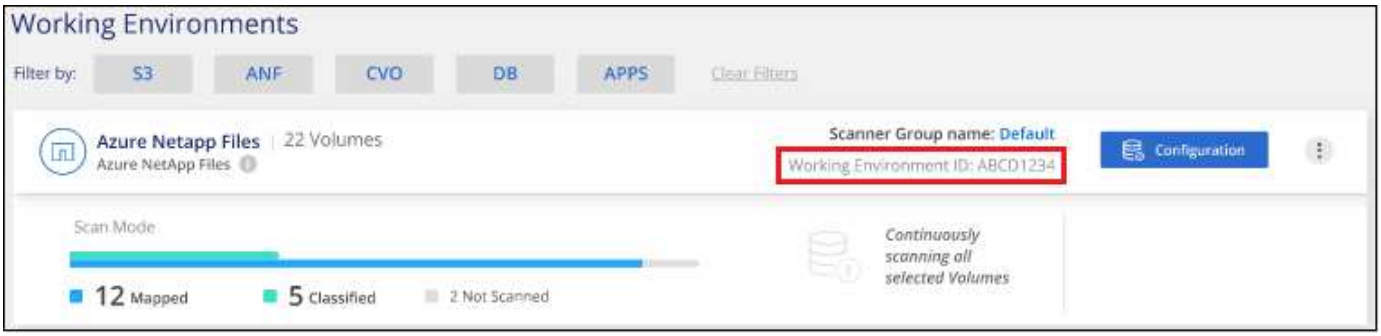
Risultato

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

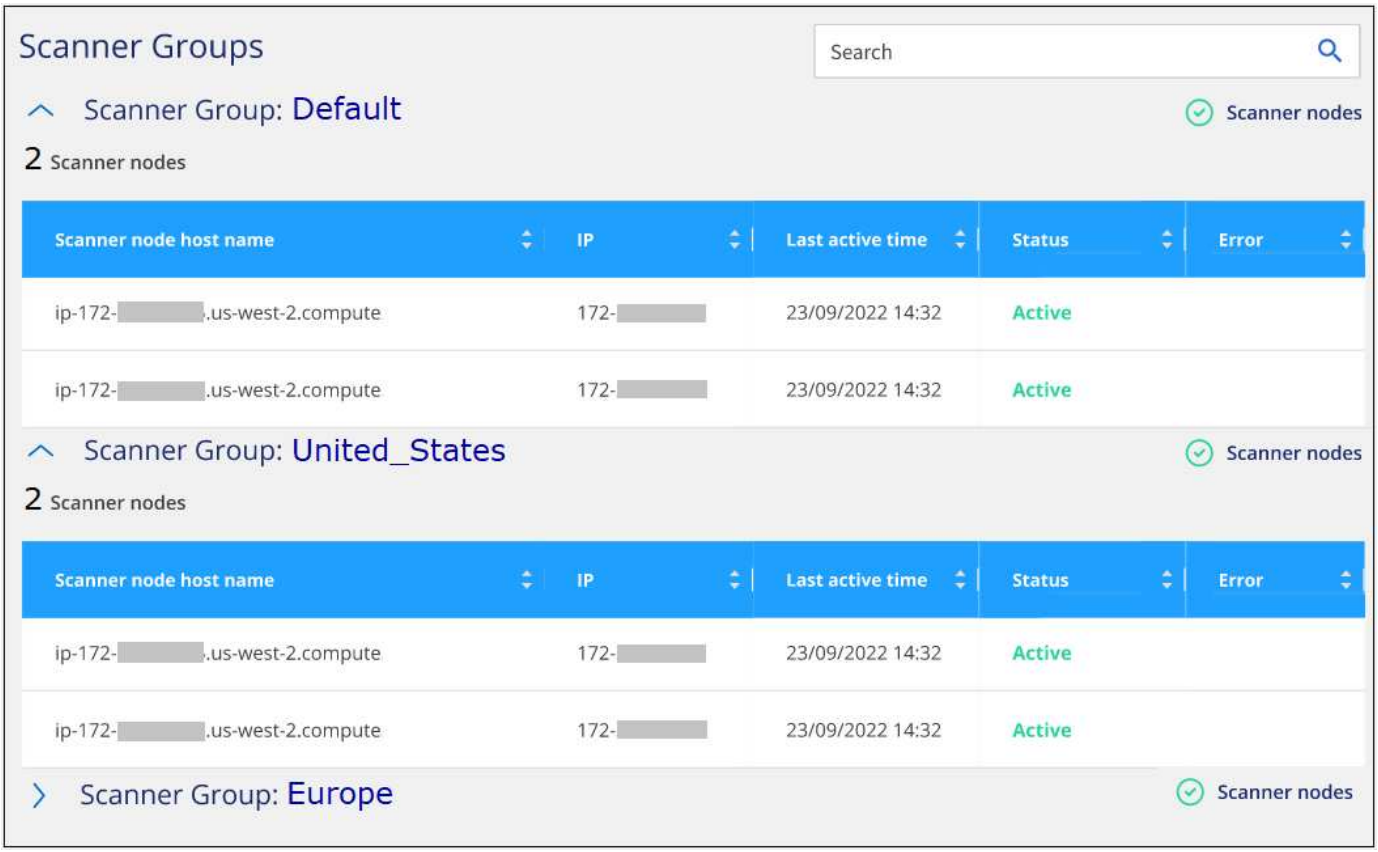
Cosa c'è di nuovo

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.

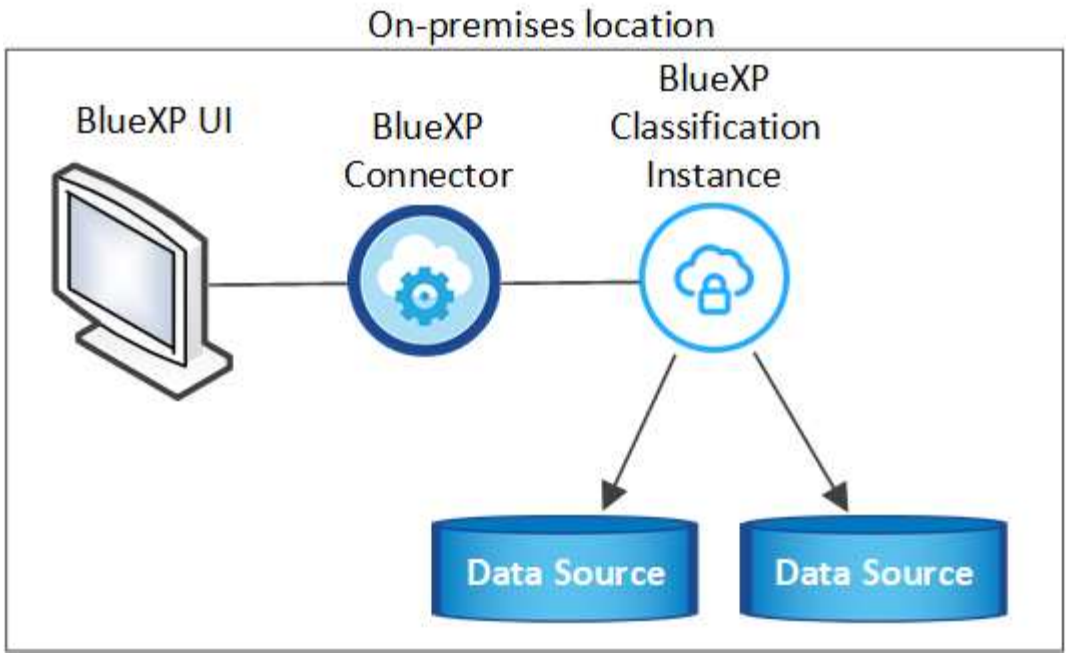
Tipo di connessione	Porte	Descrizione
Connettore <> classificazione BlueXP	8080 (TCP), 6000 (TCP), 443 (TCP) E 80	Il gruppo di sicurezza per il connettore deve consentire il traffico in entrata e in uscita sulle porte 6000 e 443 da e verso l'istanza di classificazione BlueXP. • È necessaria la porta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

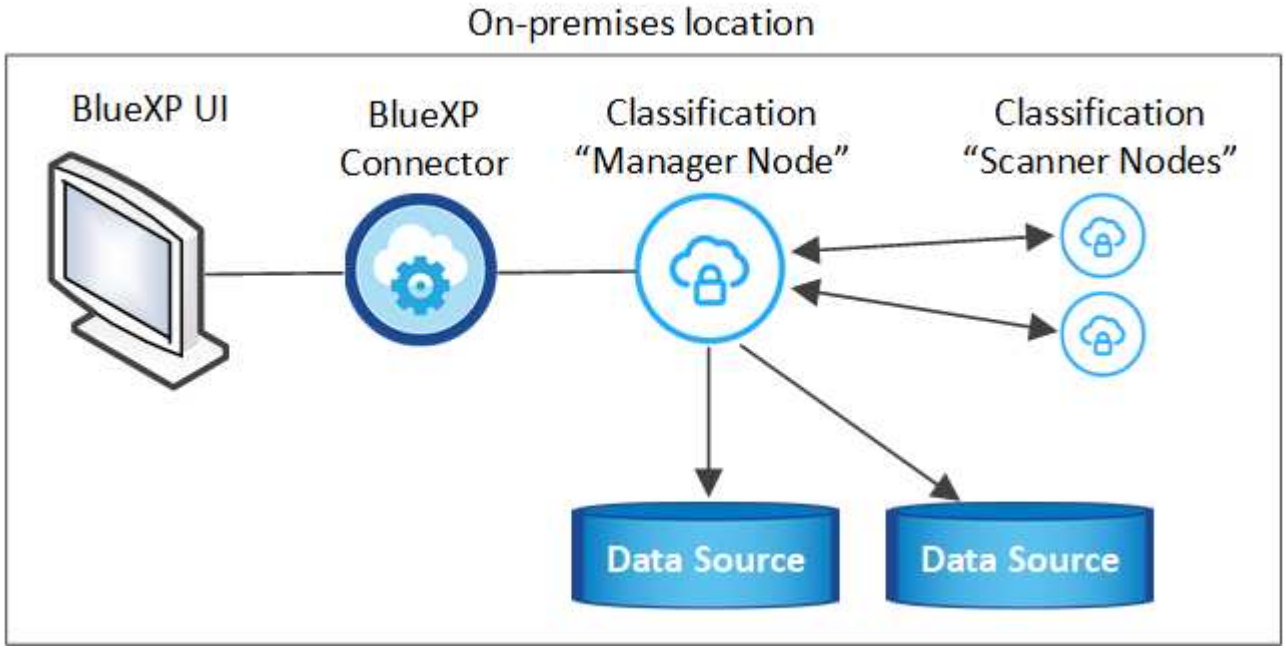
Se si utilizzano più host di classificazione BlueXP per fornire ulteriore potenza di elaborazione per eseguire la scansione delle origini dati, è necessario attivare porte/protocolli aggiuntivi. "Vedere i requisiti aggiuntivi per le porte".

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:

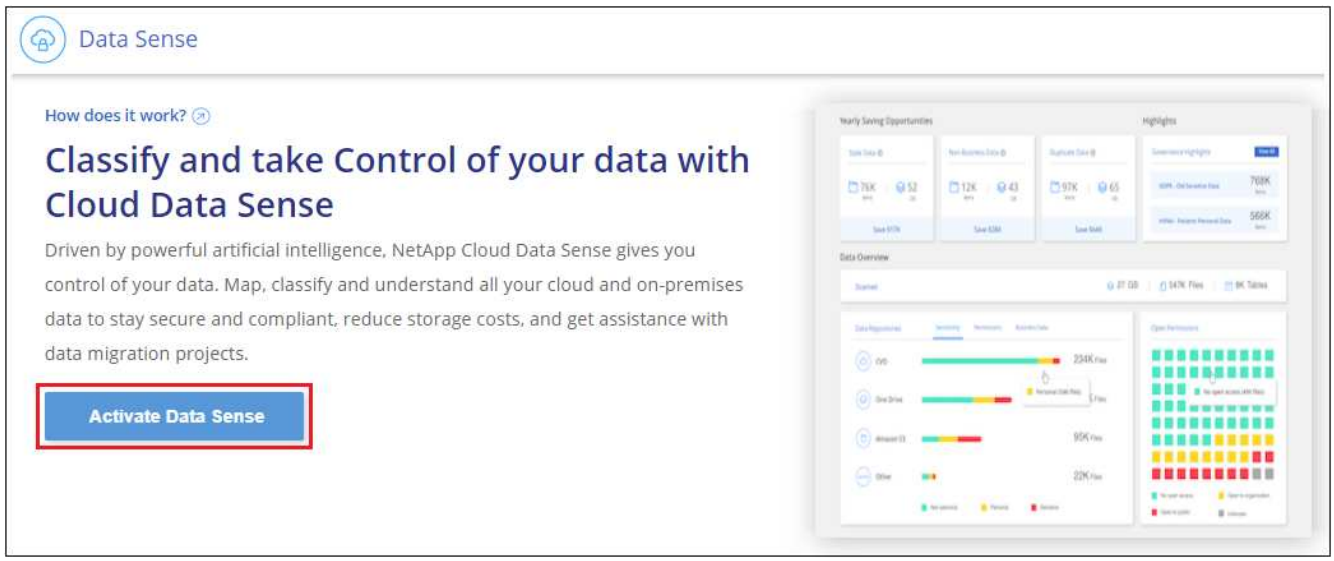
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

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

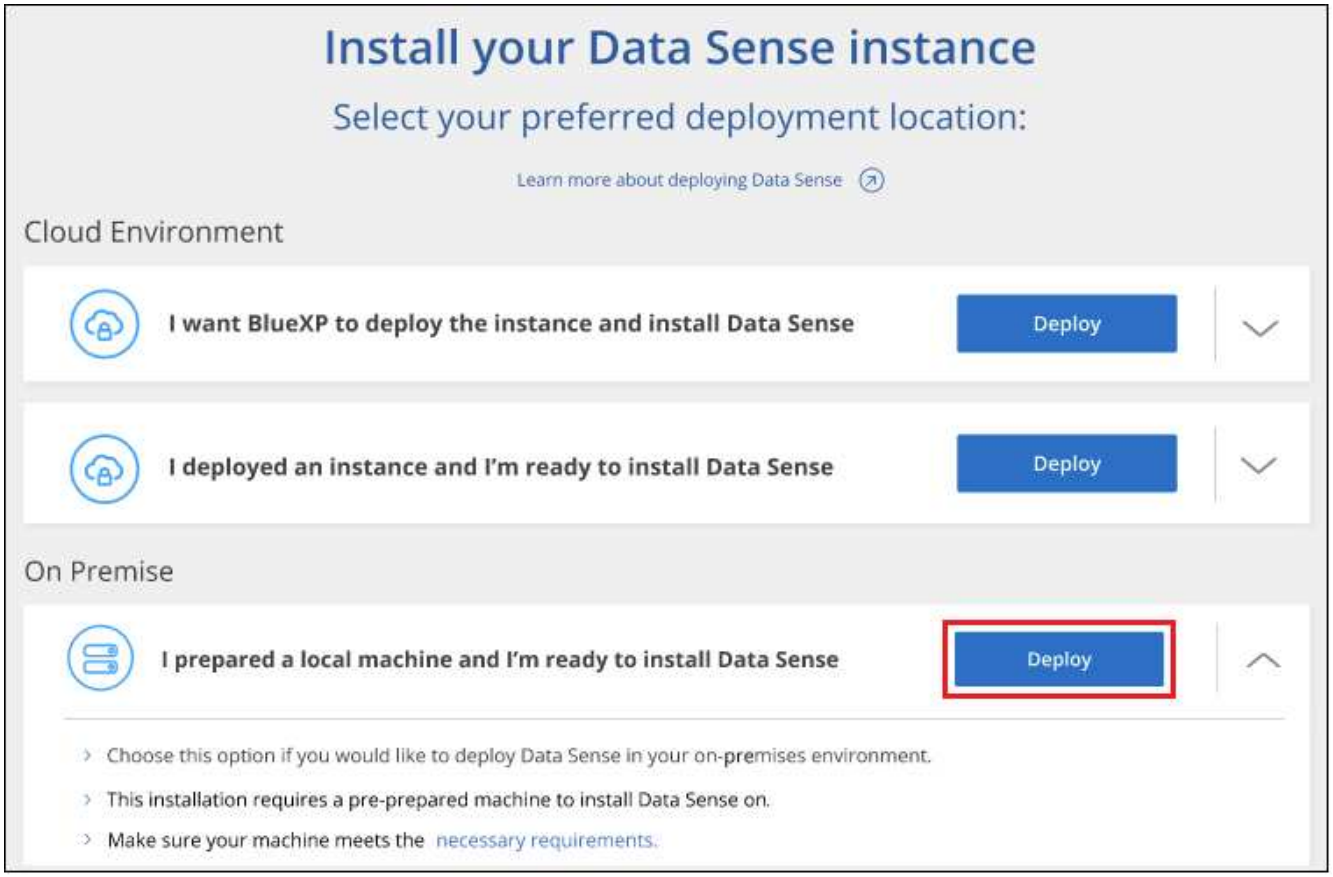
4. Decomprimere il file di installazione sul computer host, ad esempio:

```
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".

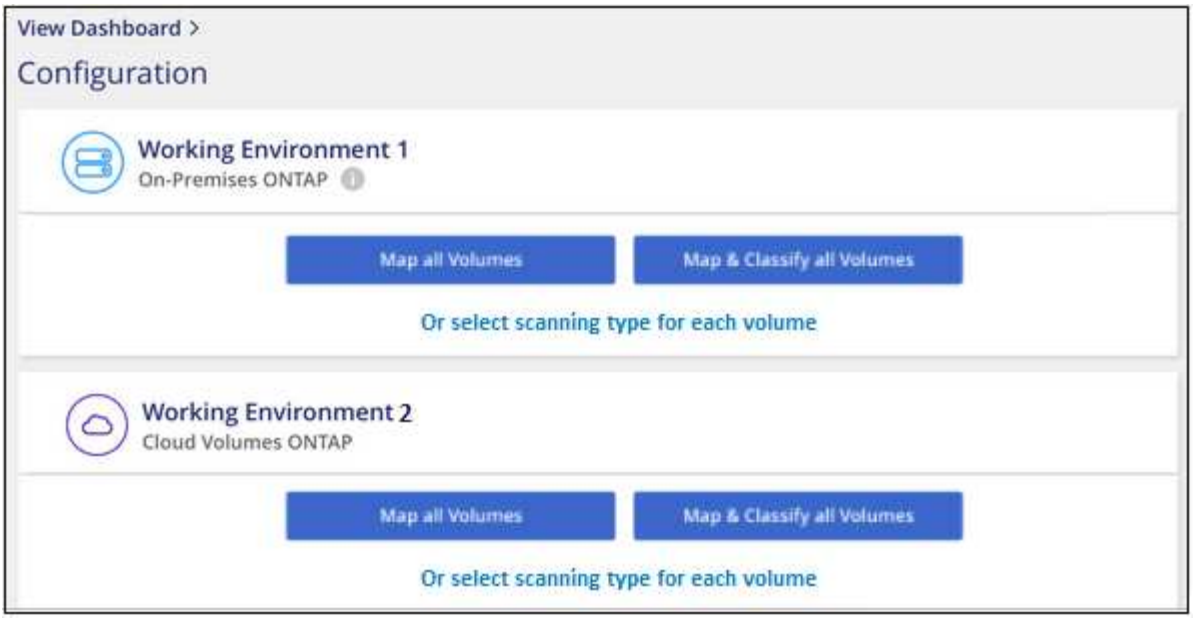
Se si esegue la scansione di sistemi ONTAP on-premise che sono stati installati in un sito buio e che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector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

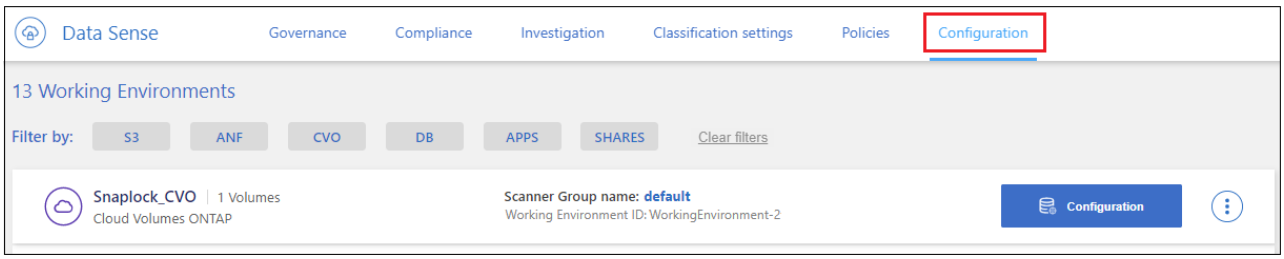
Fasi

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).

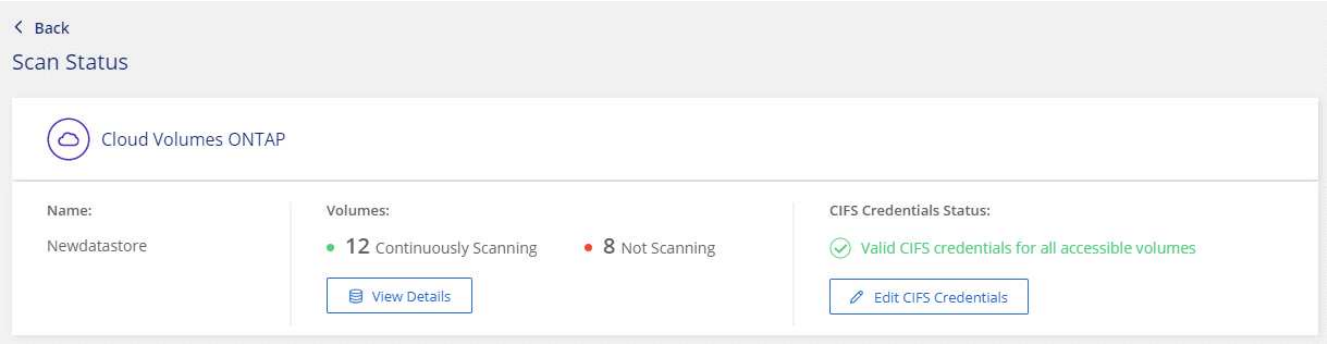


   b. Per ciascun ambiente di lavoro, fare clic su **Edit CIFS Credentials** (Modifica credenziali CIFS) e immettere il nome utente e la password necessari per la classificazione BlueXP per accedere ai volumi CIFS nel sistema.

      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.

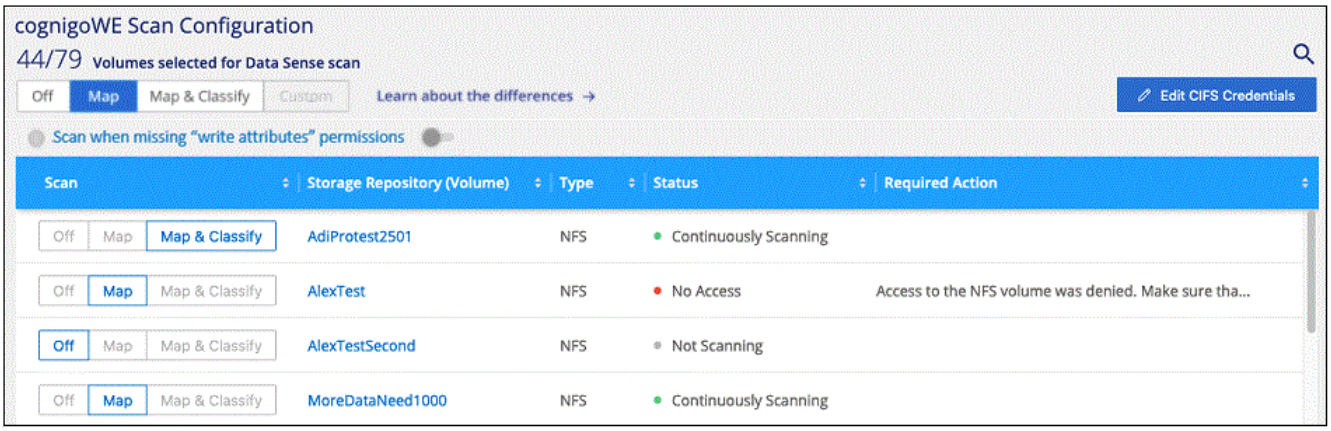
      Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory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

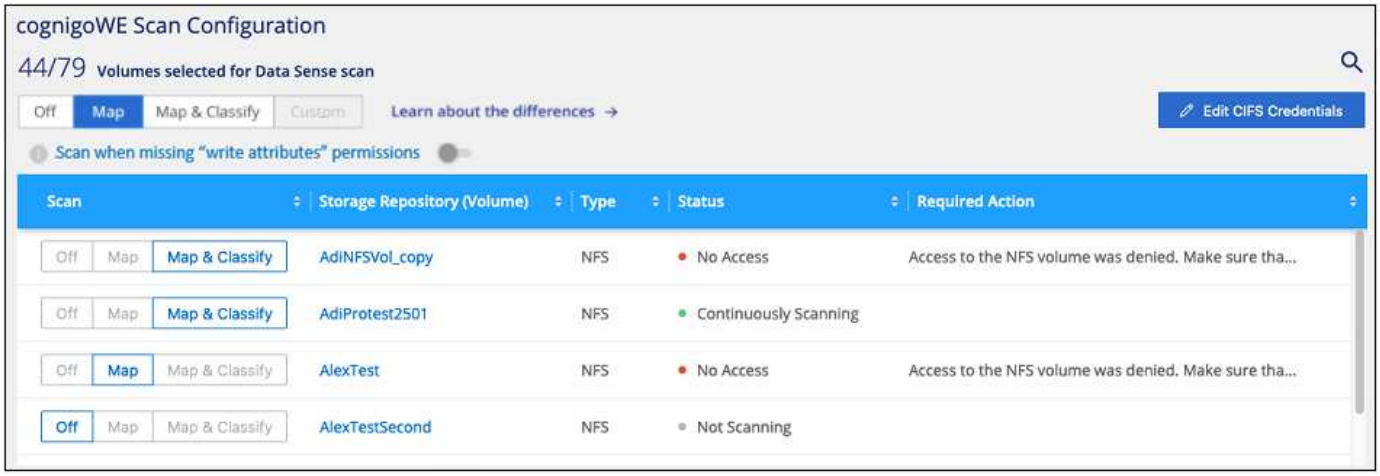
   Ad esempio, l'immagine seguente mostra quattro volumi, uno dei quali non è in grado di eseguire la scansione a causa di problemi di connettività di rete tra l'istanza di classificazione BlueXP e il volume.



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".



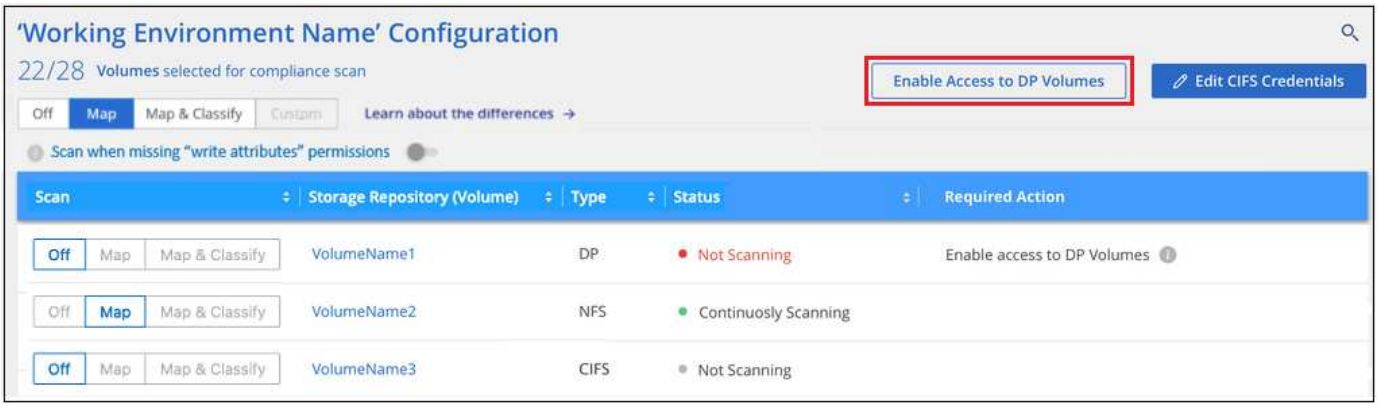
A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura su un volume	Nell'area del volume, fare clic su **Map** (Mappa)
Abilitare la scansione completa su un volume	Nell'area del volume, fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su un volume	Nell'area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

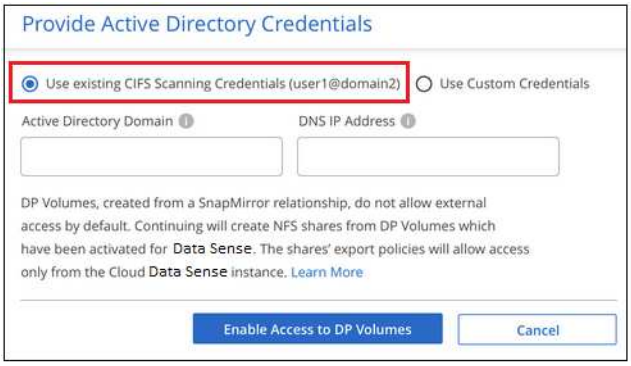
Inizialmente, l'elenco dei volumi identifica questi volumi come *Type* **DP** con *Status* **Not Scanning** e *Required Action* **Enable Access to DP Volumes**.

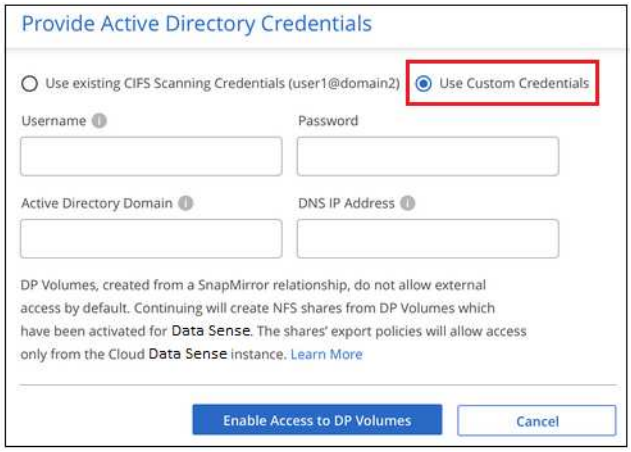


Fasi

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.

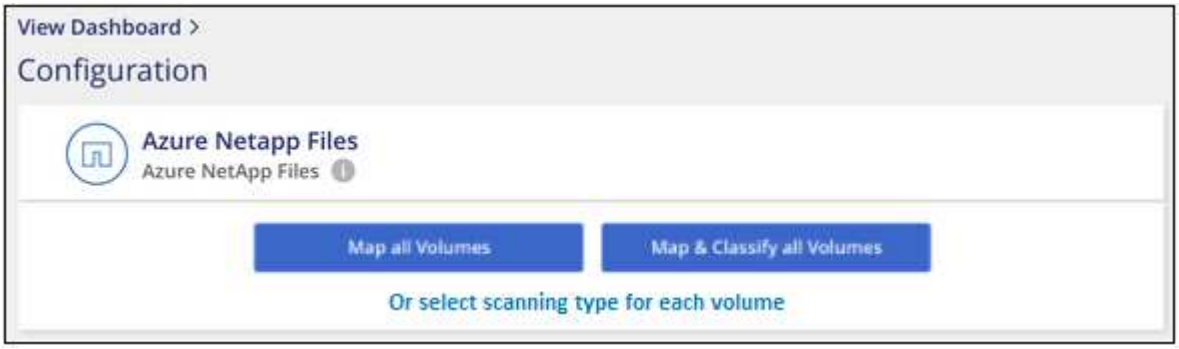
Nota: l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei volumi Azure NetApp Files.

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.

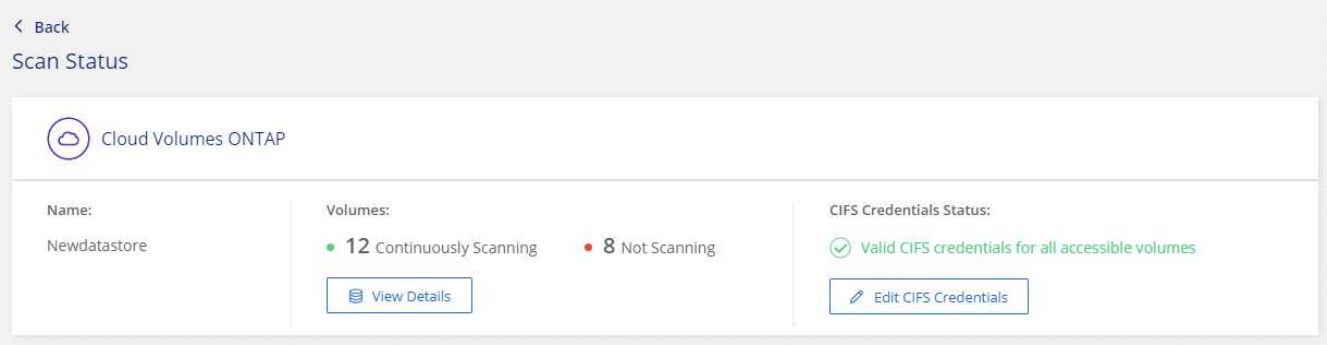
   a. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification** (Governance > classificazione), quindi selezionare la scheda **Configuration** (Configurazione).

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.

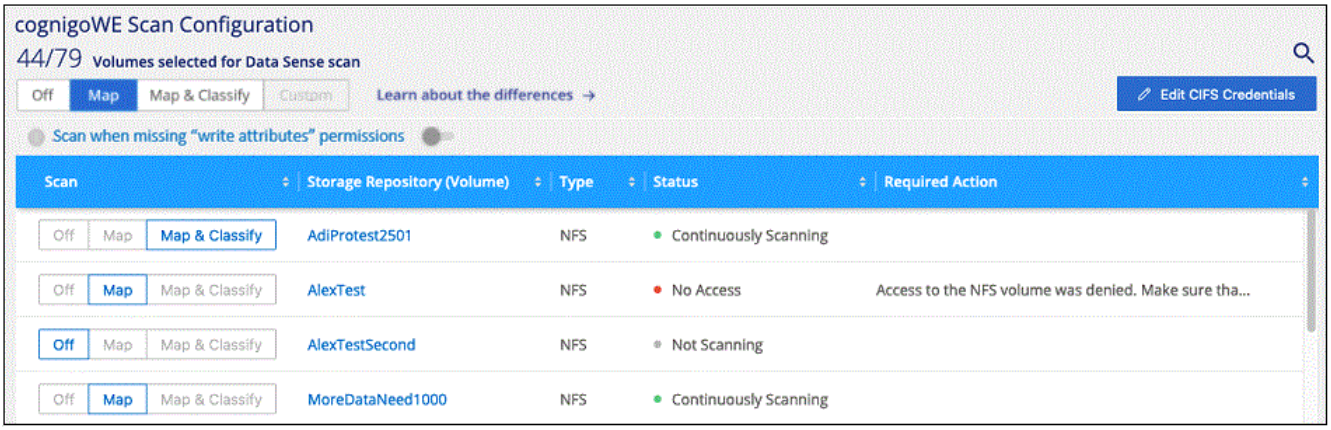
   Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory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

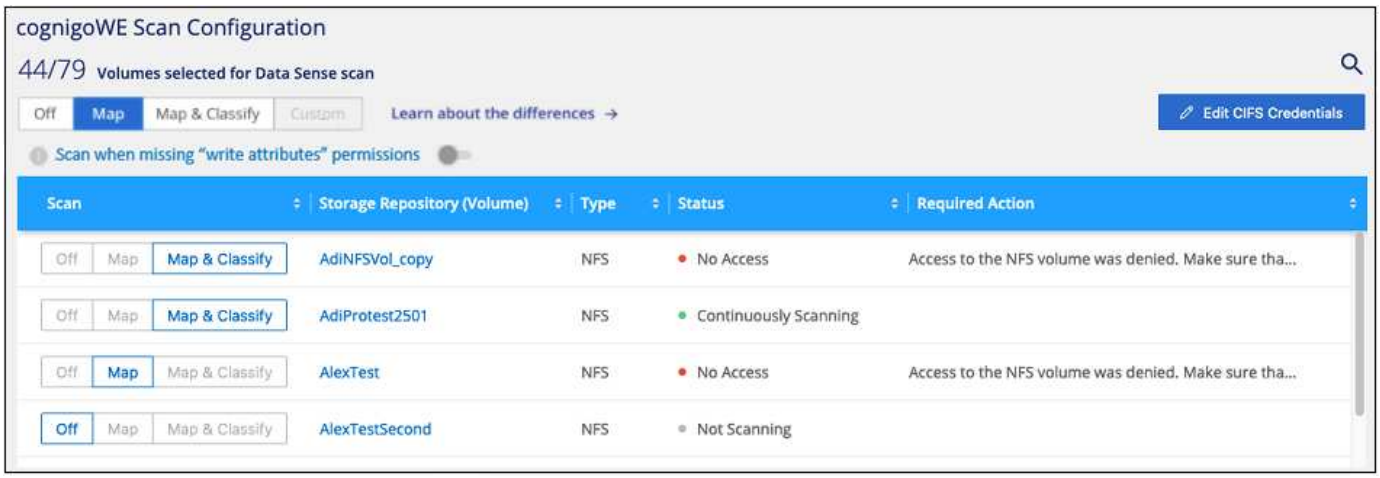
   Ad esempio, l'immagine seguente mostra quattro volumi, uno dei quali non è in grado di eseguire la scansione a causa di problemi di connettività di rete tra l'istanza di classificazione BlueXP e il volume.



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.

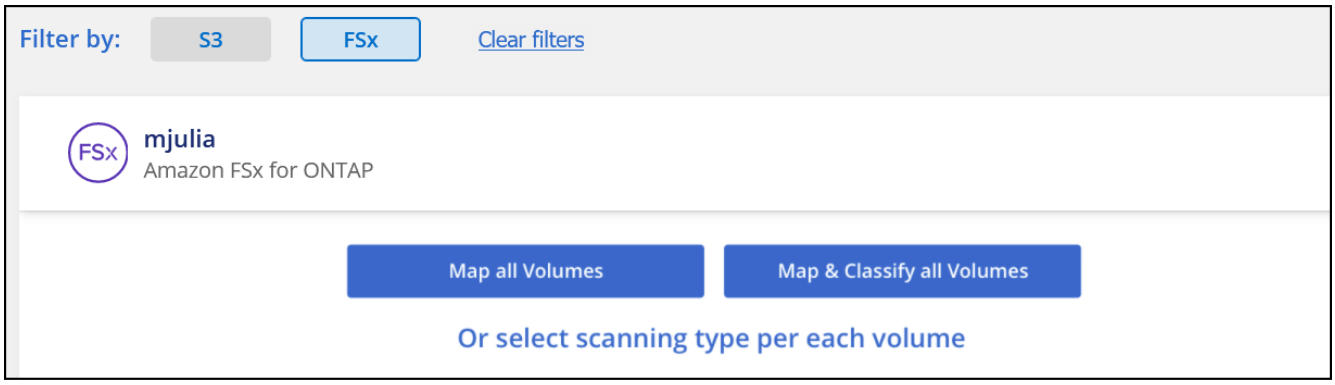
Nota: l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei volumi FSX.

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.

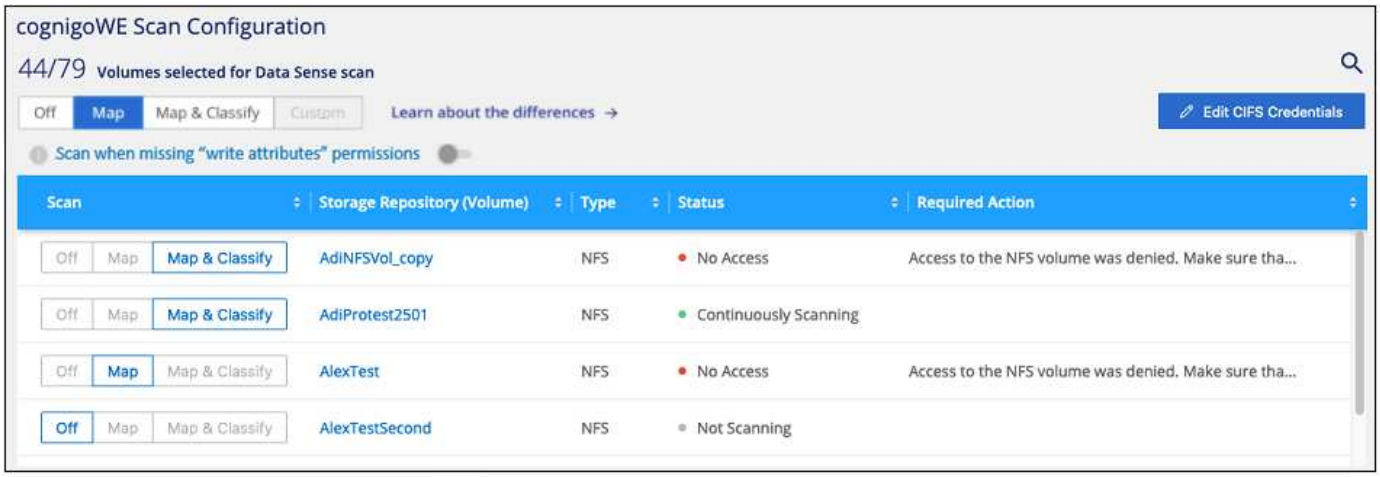
      Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory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

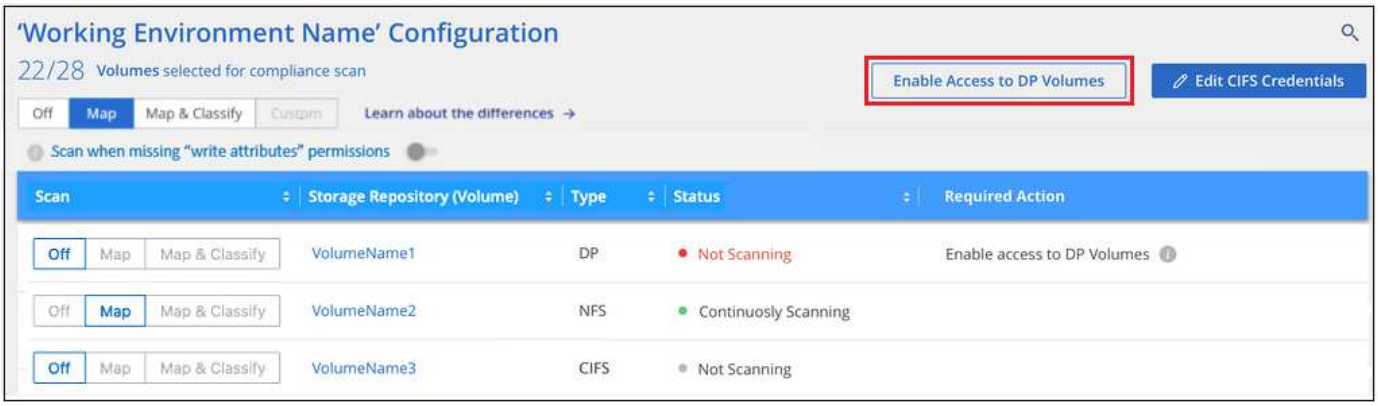
A:	Eseguire questa operazione:
Abilitare la scansione completa su un volume	Nell'area del volume, fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su un volume	Nell'area del volume, fare clic su **Off**
Abilitare le scansioni di sola mappatura su tutti i volumi	Nell'area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

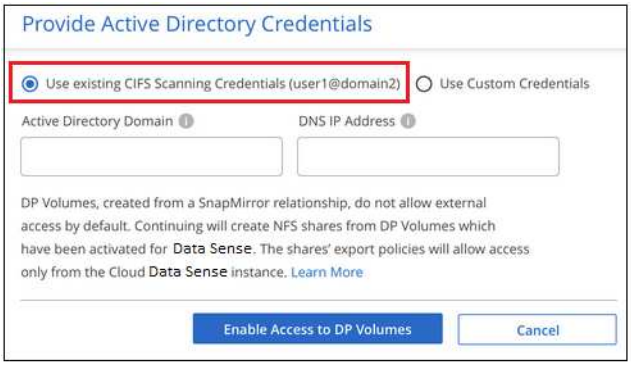


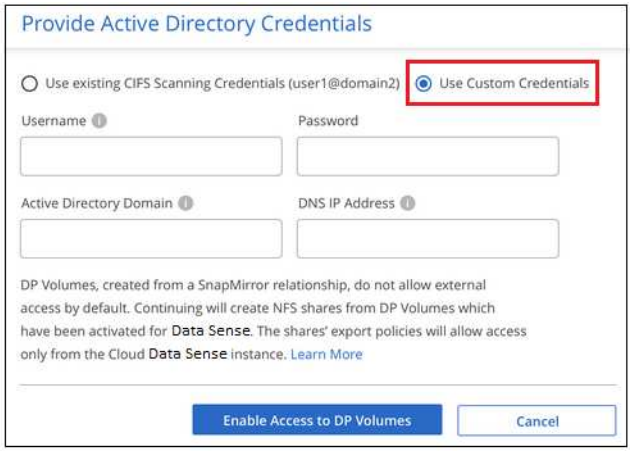
Fasi

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.

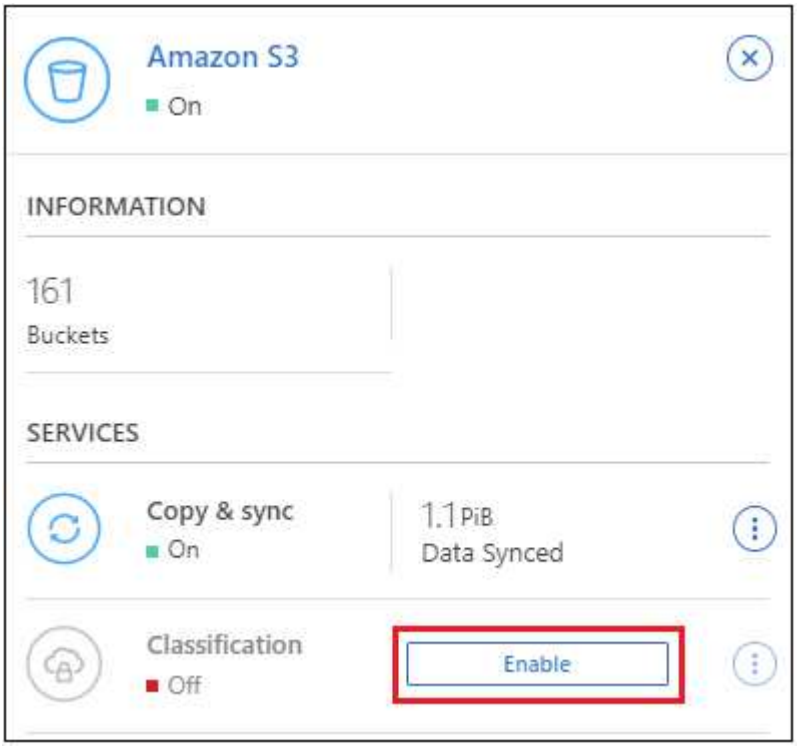
Attivazione della classificazione BlueXP nell'ambiente di lavoro S3

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

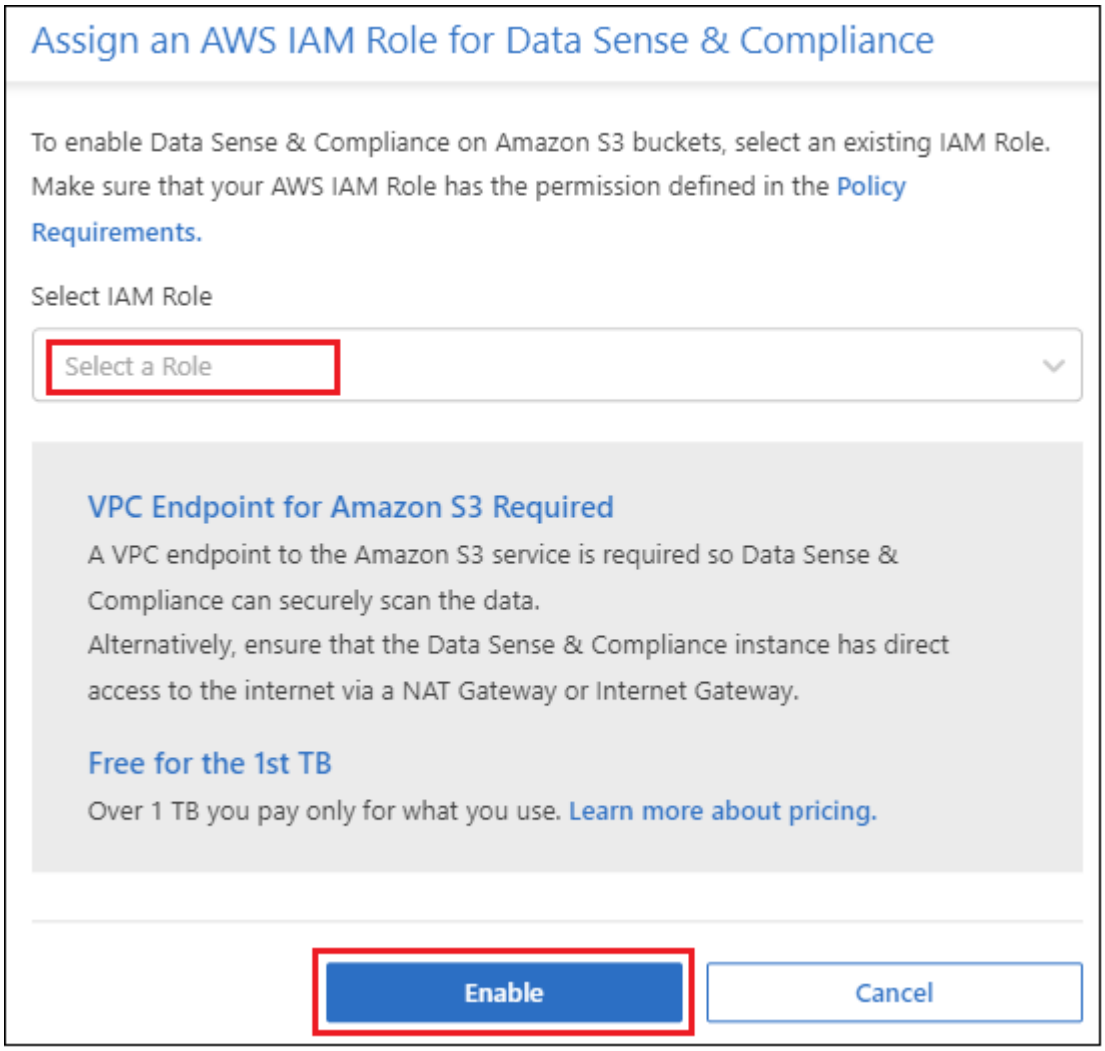
Fasi

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

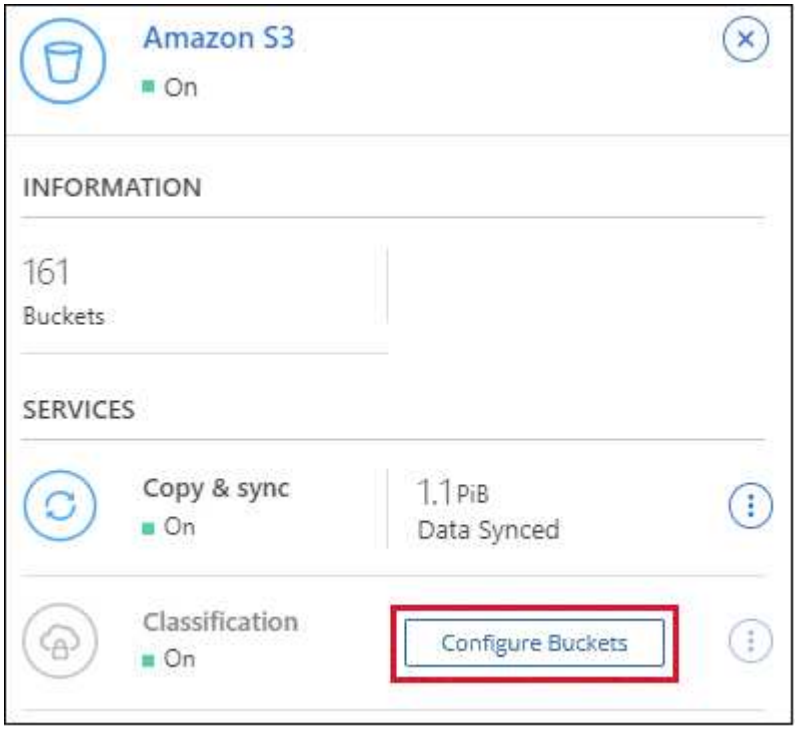
Dopo che BlueXP ha attivato la classificazione BlueXP su Amazon S3, il passaggio successivo consiste nella configurazione dei bucket che si desidera sottoporre a scansione.

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.

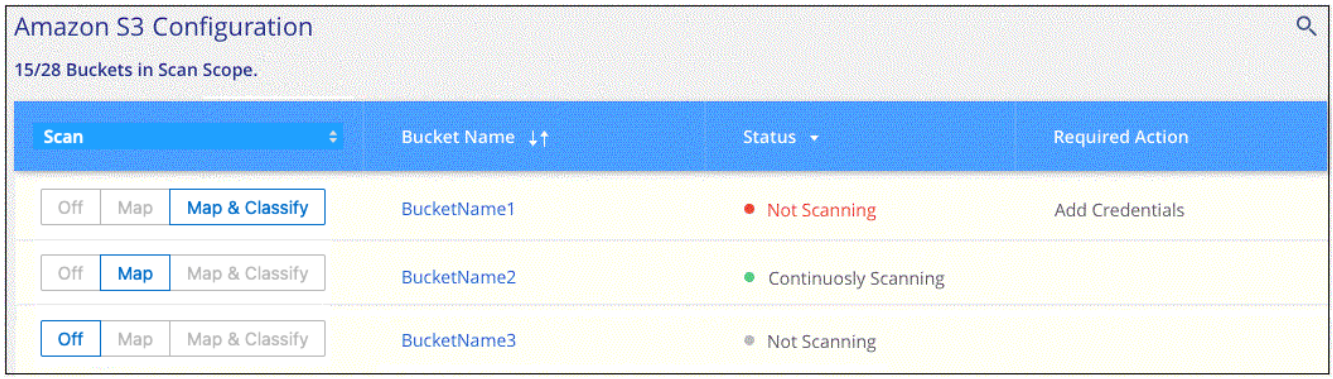
La classificazione BlueXP può anche Eseguire la scansione dei bucket S3 che si trovano in diversi account AWS.

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

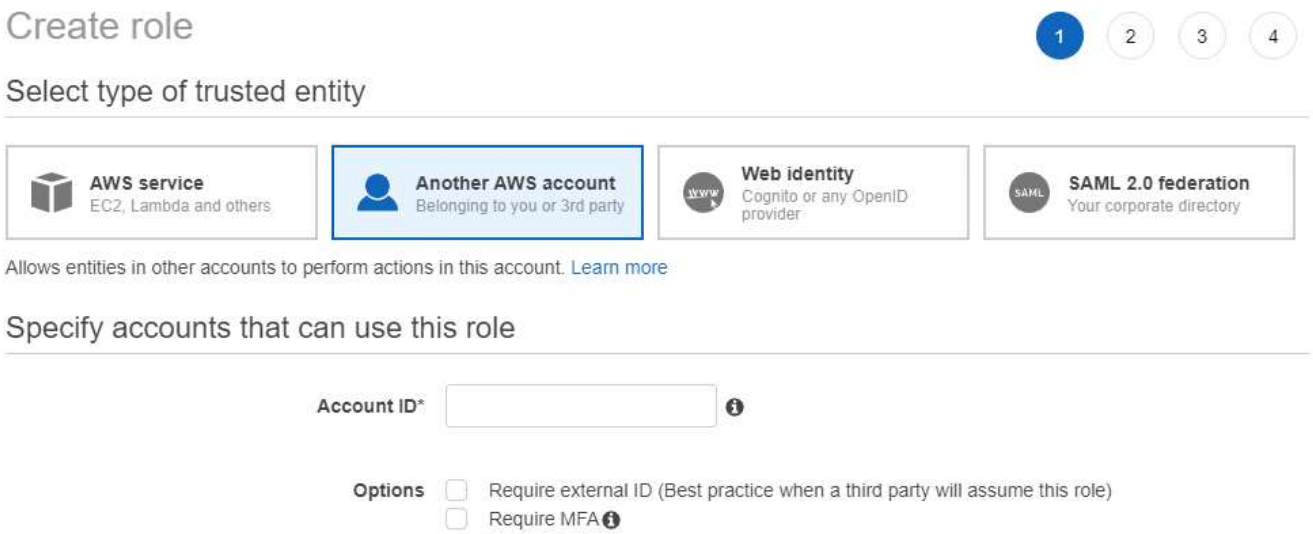
La classificazione BlueXP avvia la scansione dei bucket S3 abilitati. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

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.

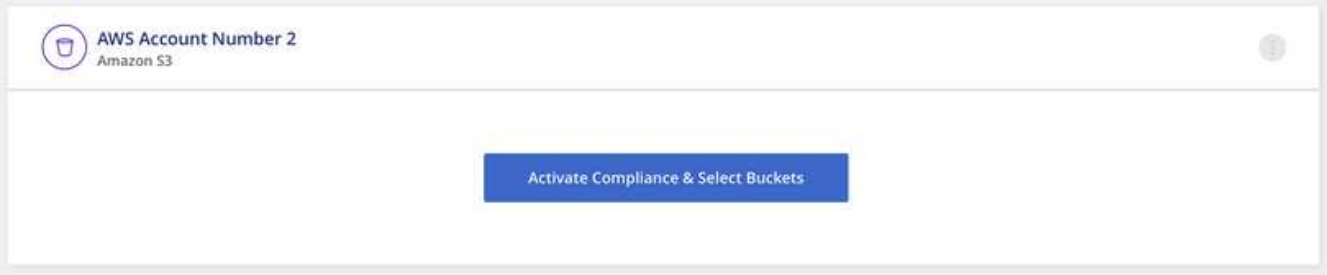
b. Fare clic su **Allega policy**, quindi su **Crea policy**.

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".

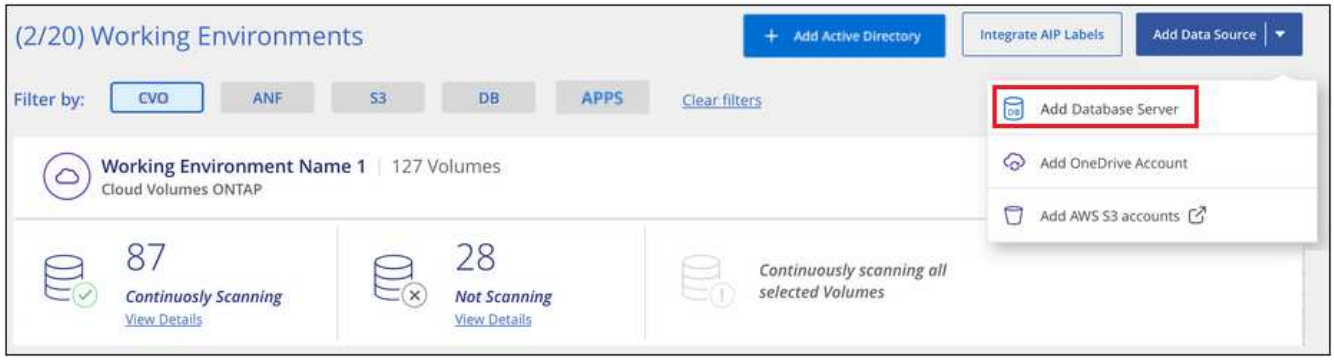
Se si eseguono scansioni di schemi di database installati in un sito buio che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella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

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

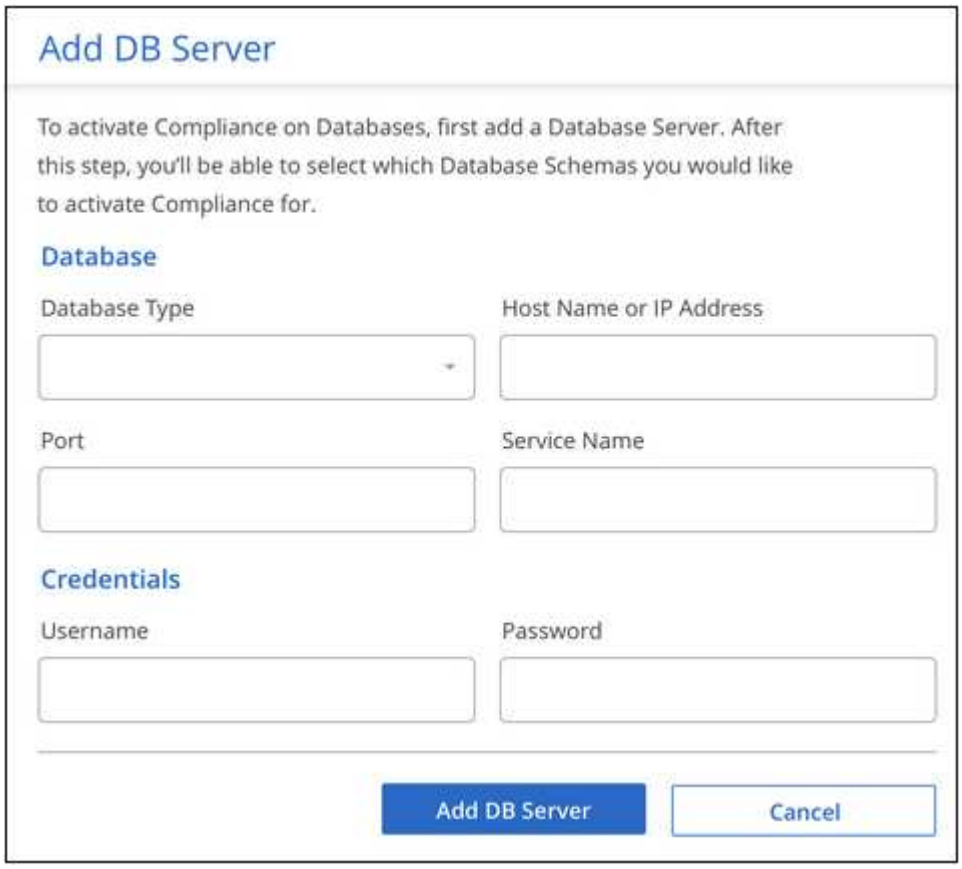
Aggiungere il server database

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.

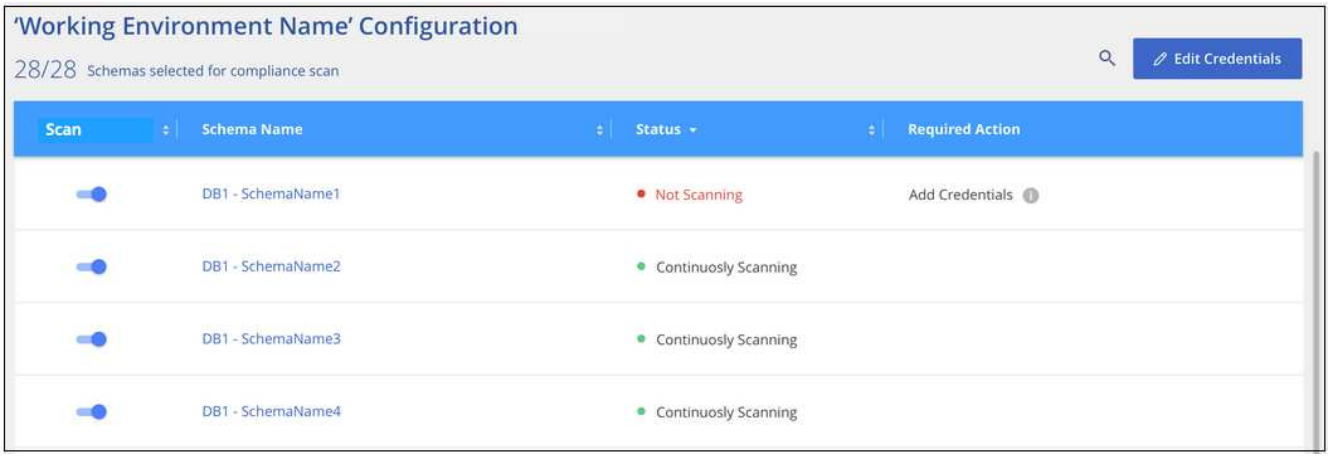
Abilitare e disabilitare le scansioni di conformità sugli schemi di database

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".

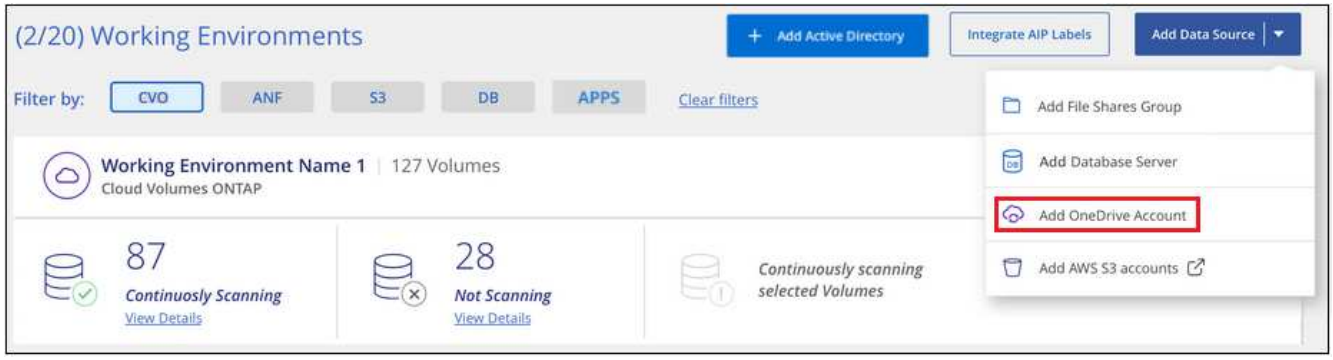
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

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.

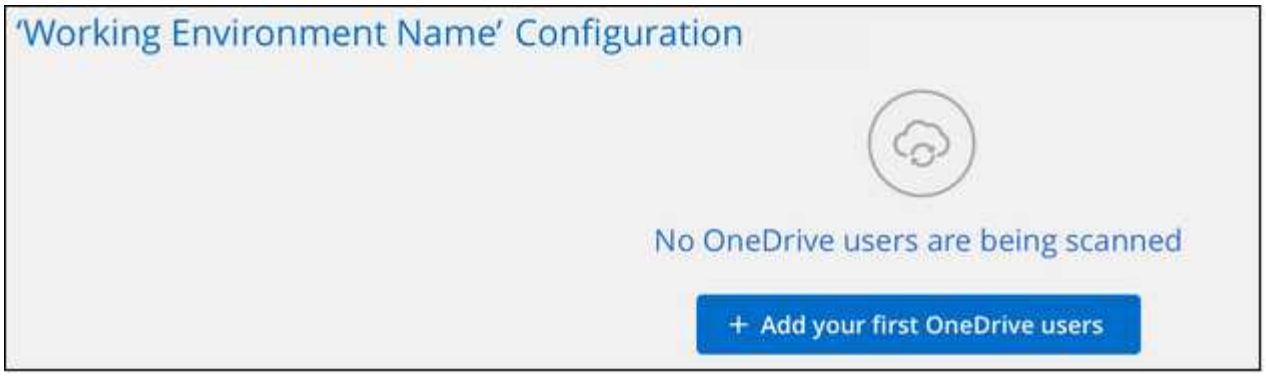
Aggiunta di utenti OneDrive alle scansioni di conformità

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.

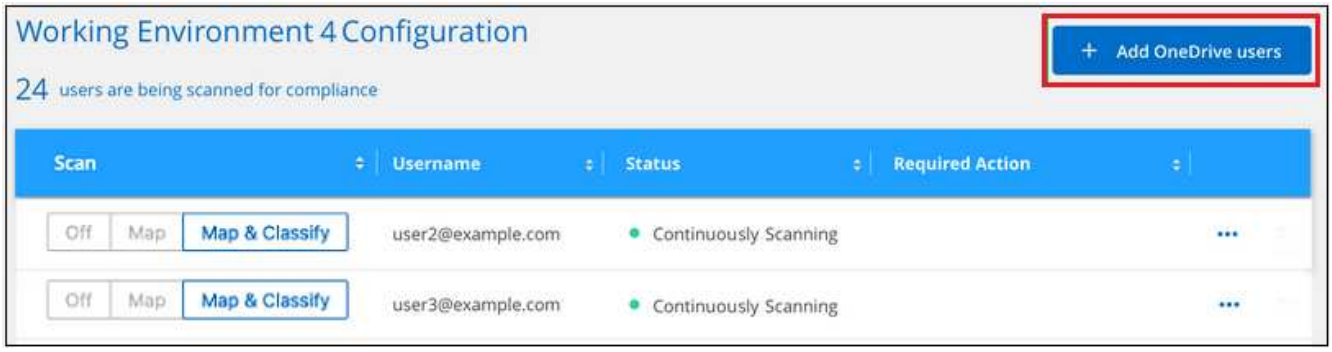
Fasi

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

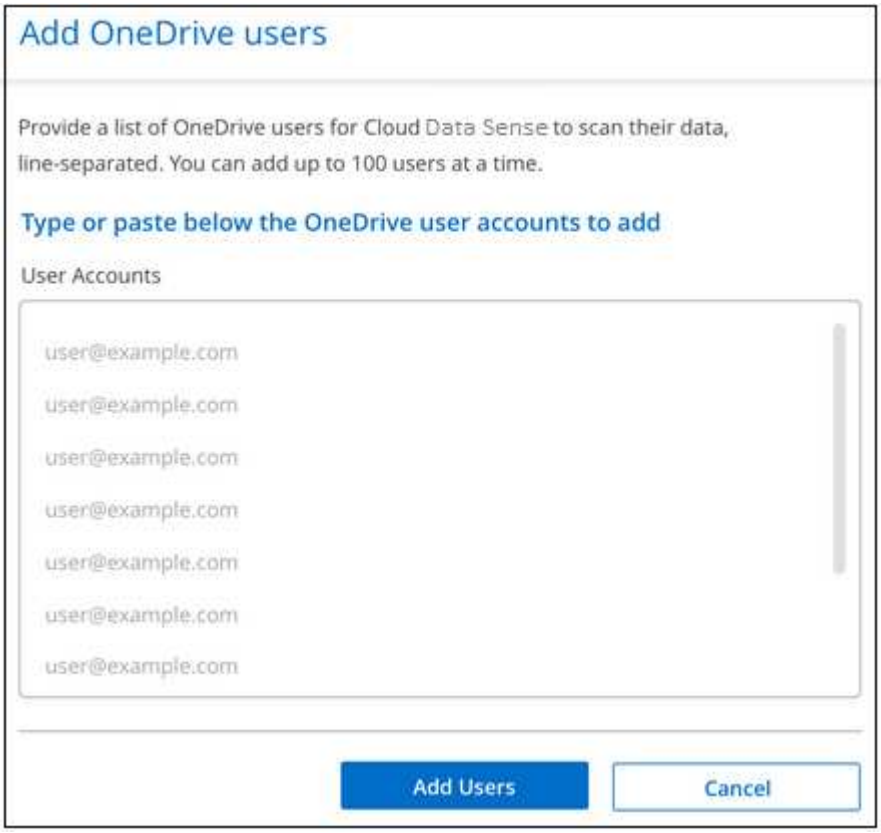
2. Se è la prima volta che si aggiungono utenti per questo account OneDrive, fare clic su **Aggiungi i primi utenti OneDrive**.



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.

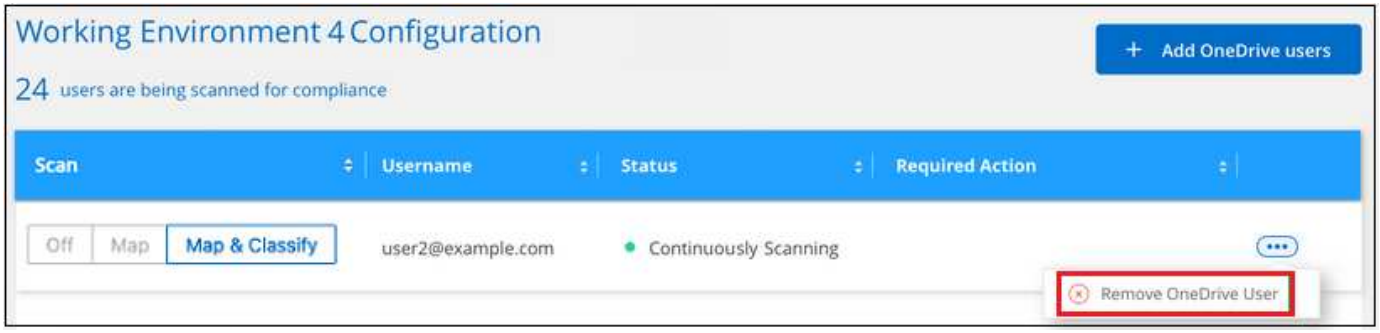
A:	Eseguire questa operazione:
Attiva scansioni solo mappatura sui file utente	Fare clic su **Map** (Mappa)
Attiva scansioni complete sui file utente	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione dei file utente	Fare clic su **Off**

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".

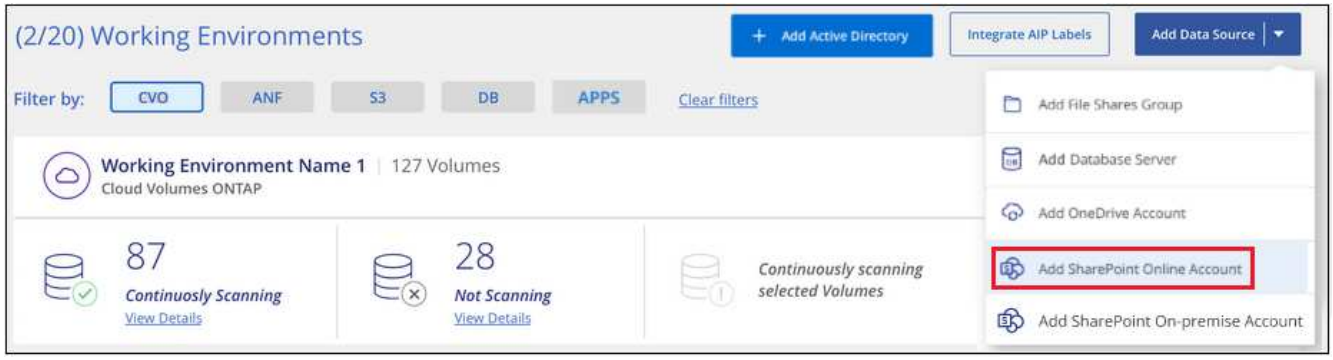
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

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.

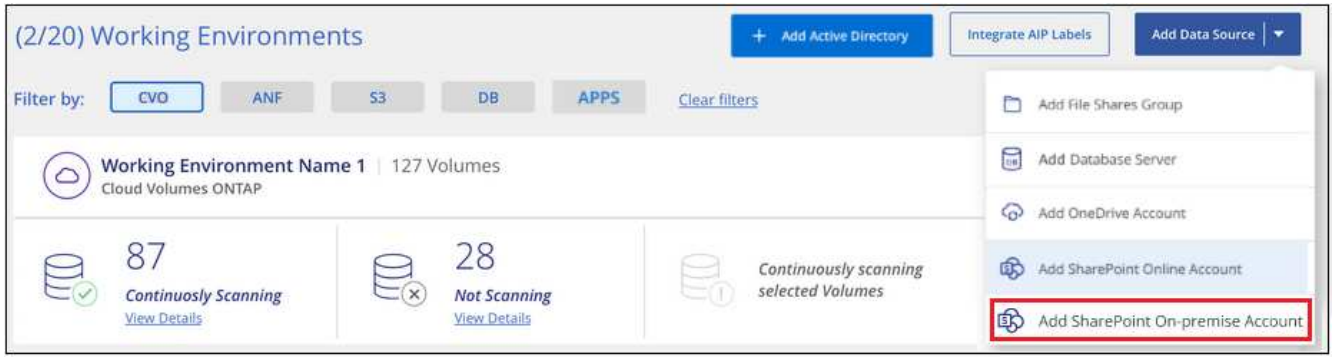
L'account SharePoint Online viene aggiunto all'elenco degli ambienti di lavoro.

Aggiunta di un account SharePoint on-premise

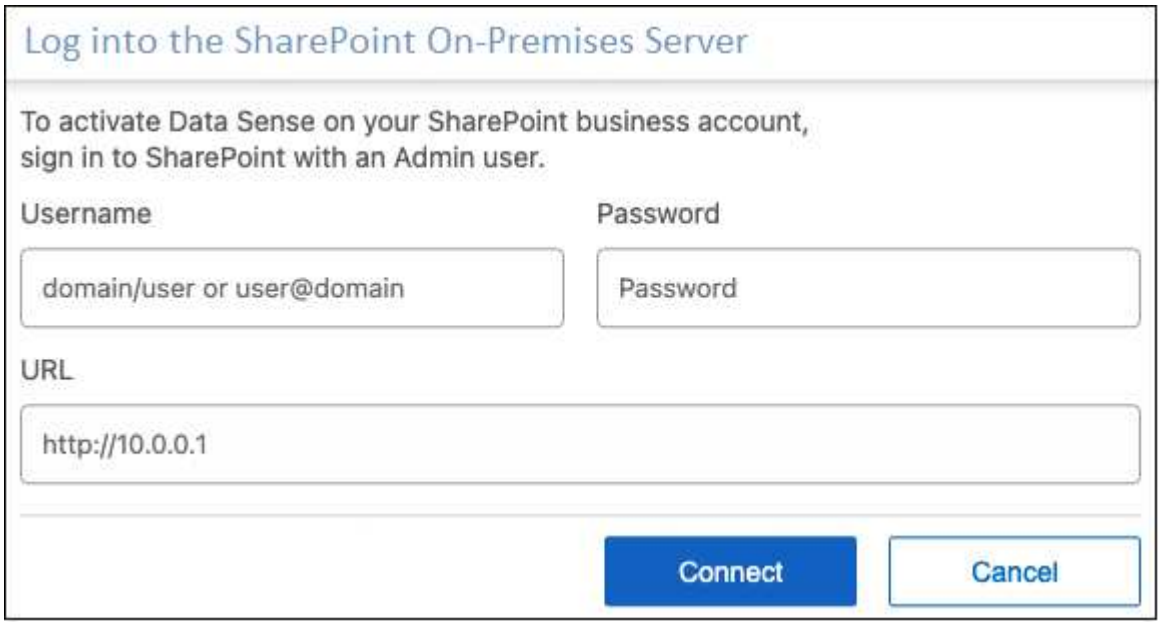
Aggiungere l'account SharePoint on-premise in cui risiedono i file utente.

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.

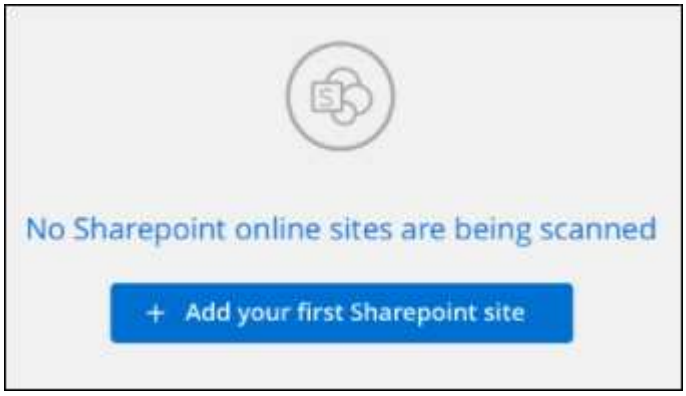
Aggiunta di siti SharePoint alle scansioni di conformità

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

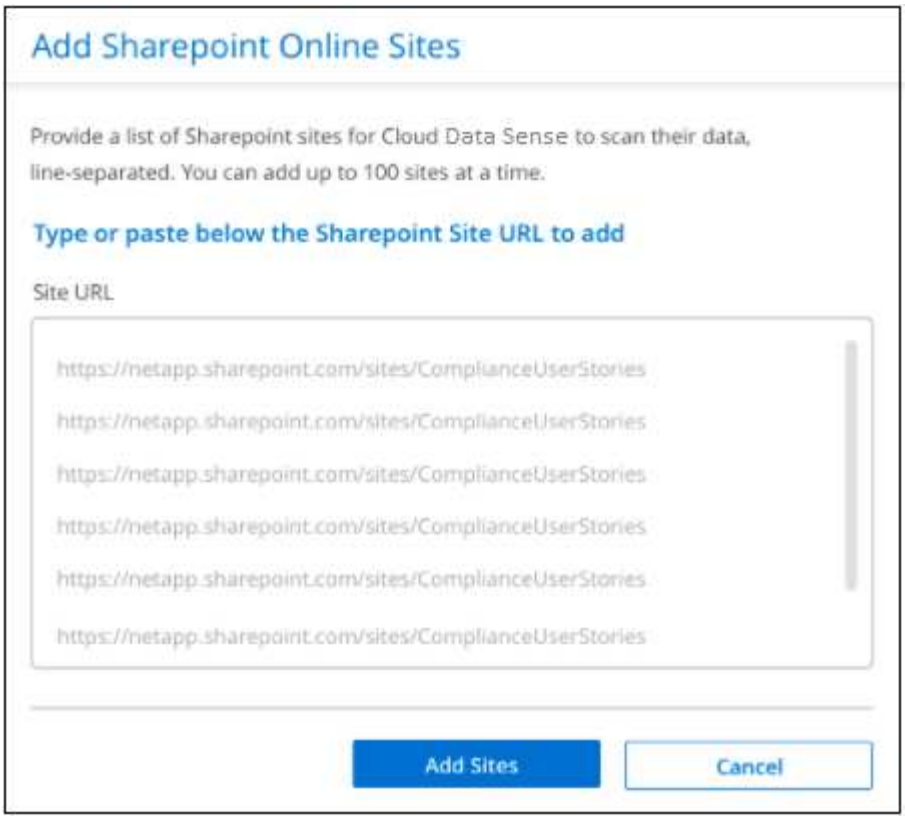
1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** dell'account SharePoint.

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.

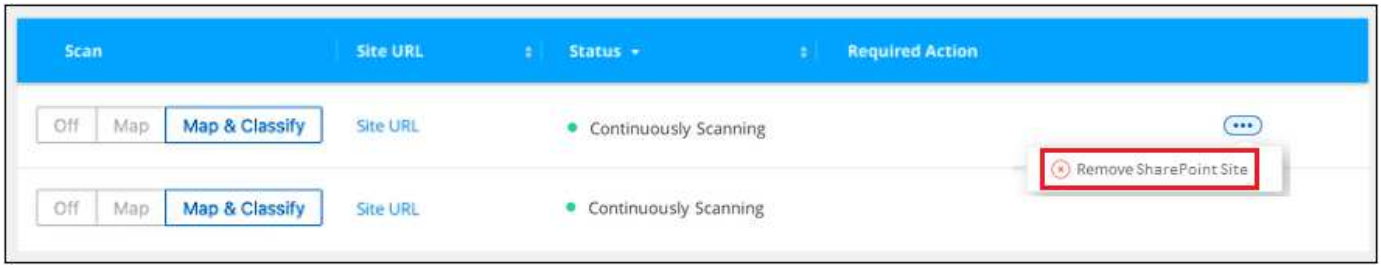
A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura sui file	Fare clic su **Map** (Mappa)
Attivare scansioni complete sui file	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione dei file	Fare clic su **Off**

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".

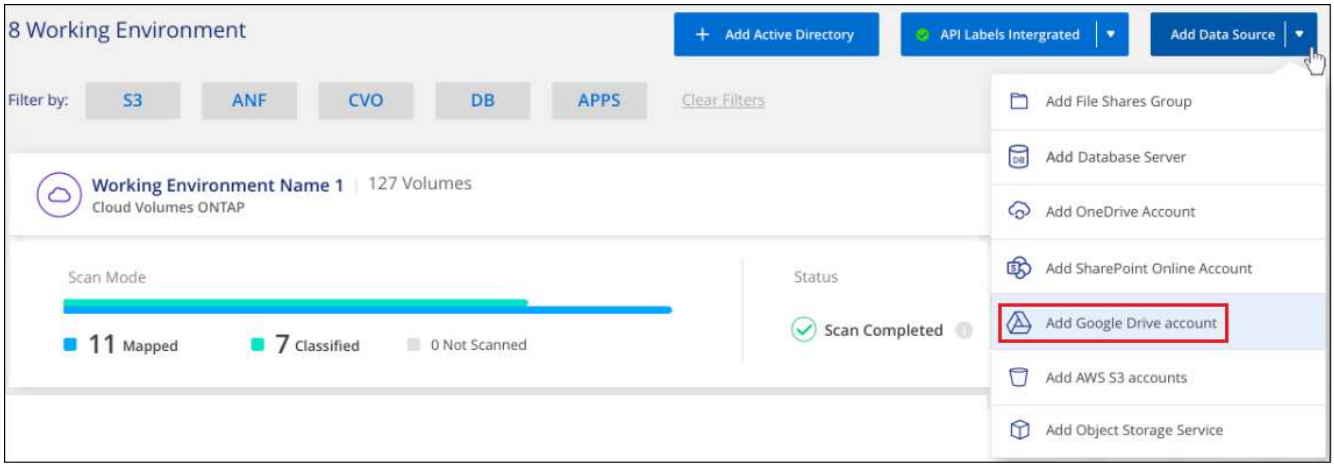
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

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.

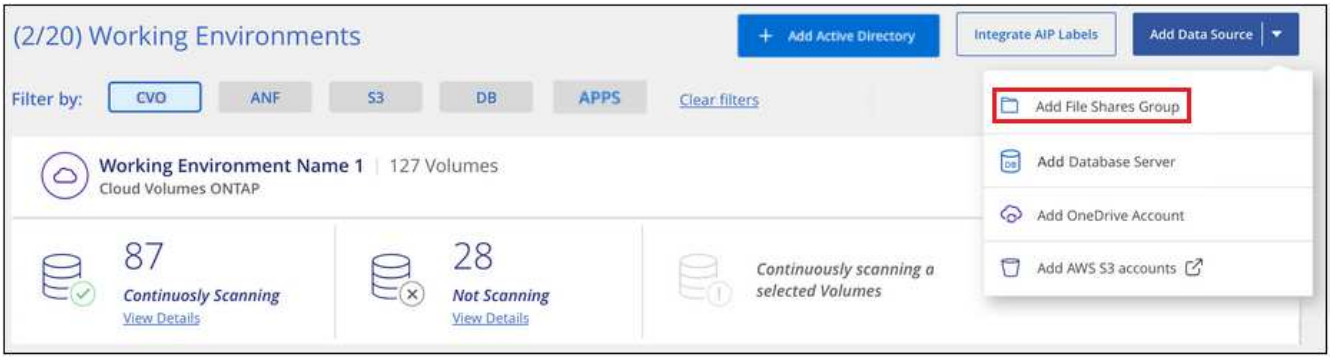
Creazione del gruppo per le condivisioni file

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>`.

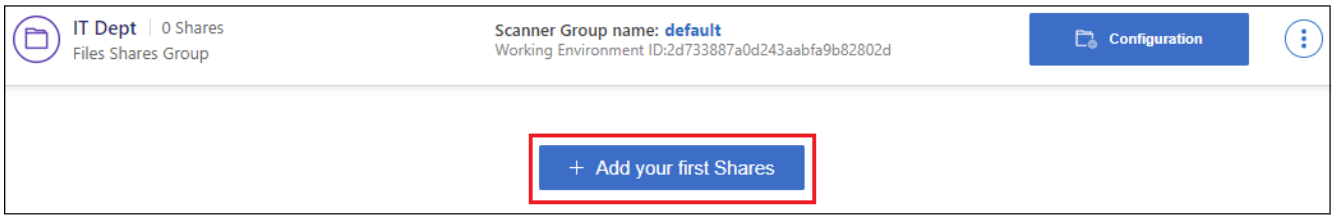
È possibile aggiungere singole condivisioni di file oppure fornire un elenco separato da righe delle condivisioni di file che si desidera sottoporre a scansione. È possibile aggiungere fino a 100 condivisioni alla volta.

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.

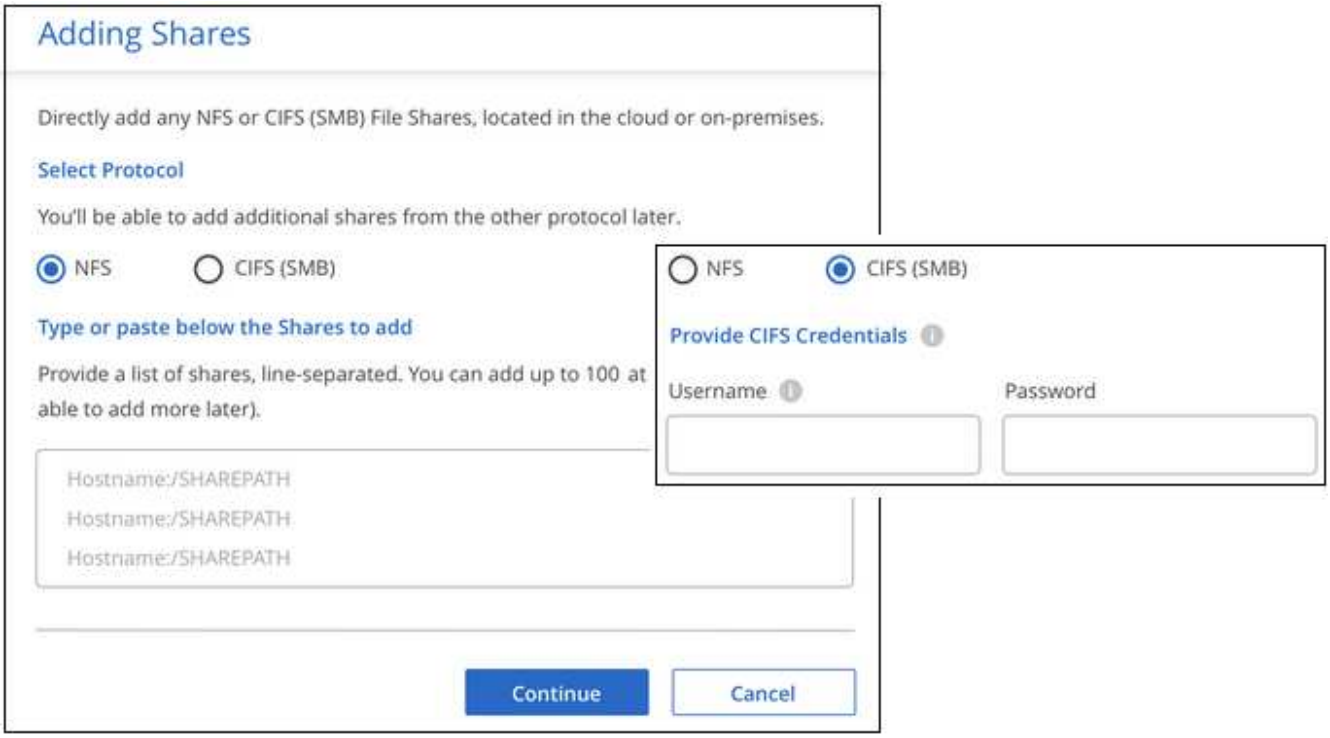
2. Se è la prima volta che si aggiungono condivisioni file per questo gruppo di condivisioni file, fare clic su **Aggiungi le prime condivisioni**.



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**

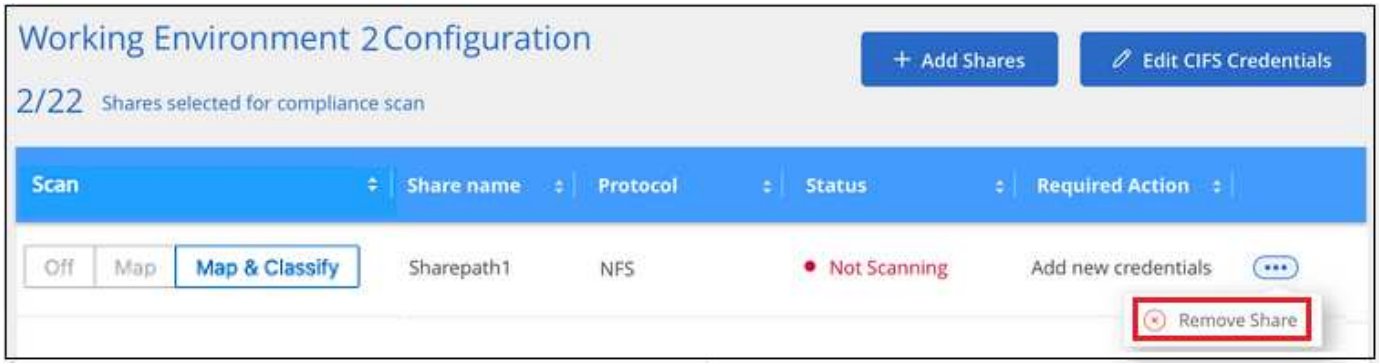
Per impostazione predefinita, lo switch nella parte superiore della pagina per le autorizzazioni **Scan when missing "write attributa" (Esegui scansione quando mancano gli attributi di scrittura)** è disattivato. Ciò significa che se la classificazione di BlueXP non dispone di permessi di scrittura in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

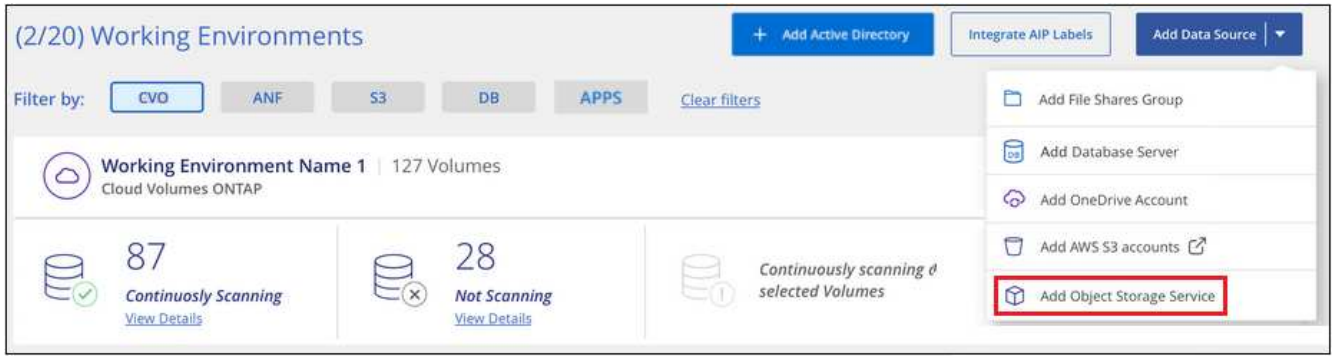
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Aggiunta del servizio di storage a oggetti alla classificazione BlueXP

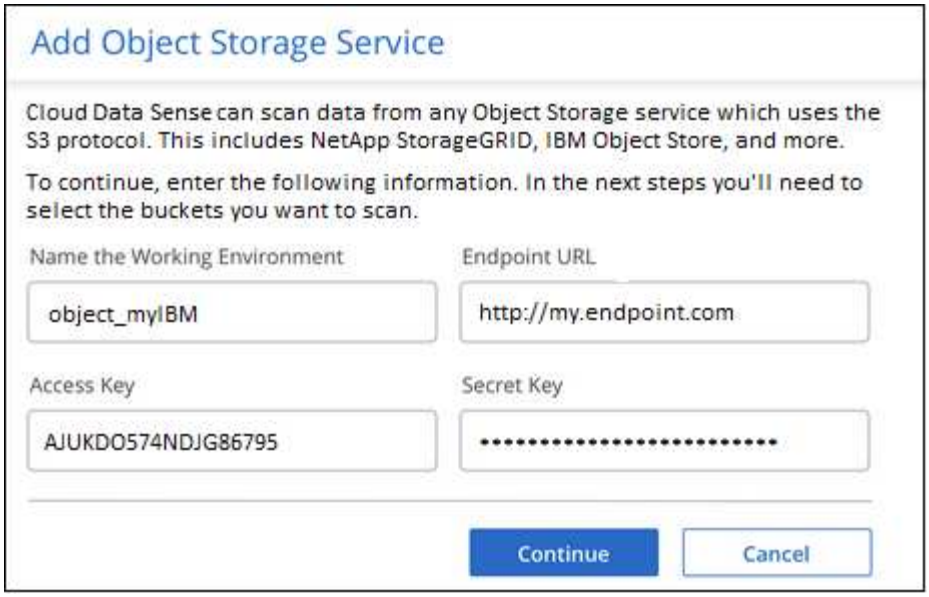
Aggiungere il servizio di storage a oggetti.

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

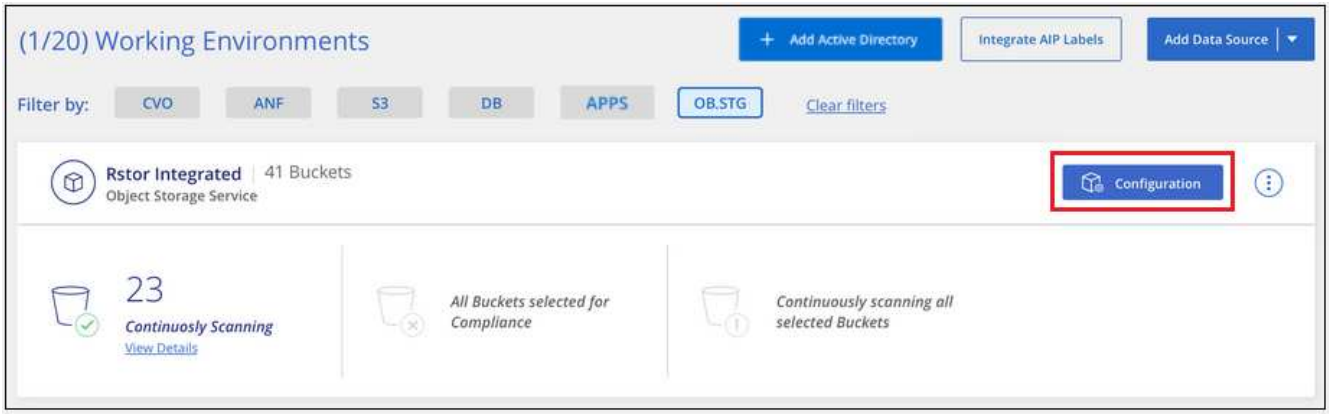
Il nuovo servizio di storage a oggetti viene aggiunto all'elenco degli ambienti di lavoro.

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

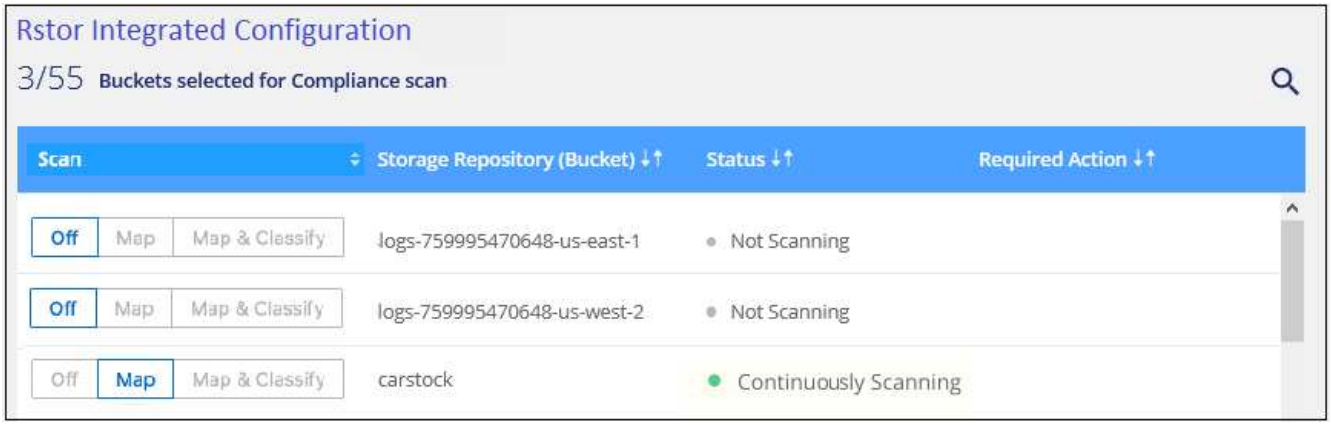
Dopo aver attivato la classificazione BlueXP sul servizio di storage a oggetti, il passaggio successivo consiste nel configurare i bucket che si desidera sottoporre a scansione. La classificazione BlueXP rileva tali bucket e li visualizza nell'ambiente di lavoro creato.

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

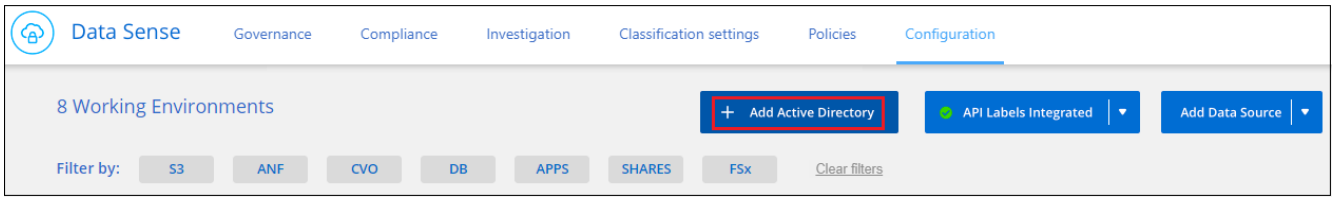
    oppure

  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

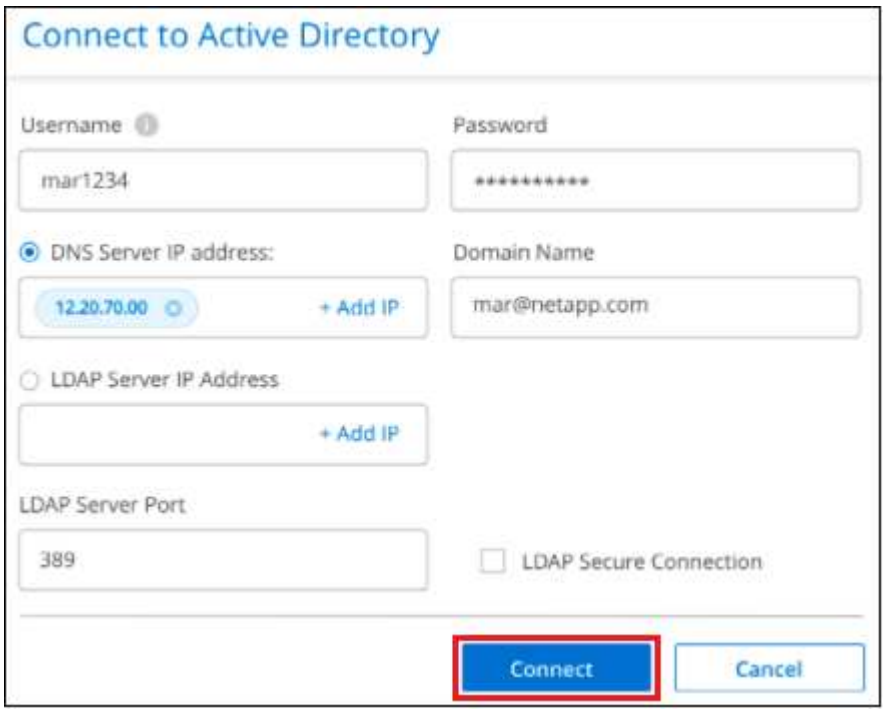
Fasi

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

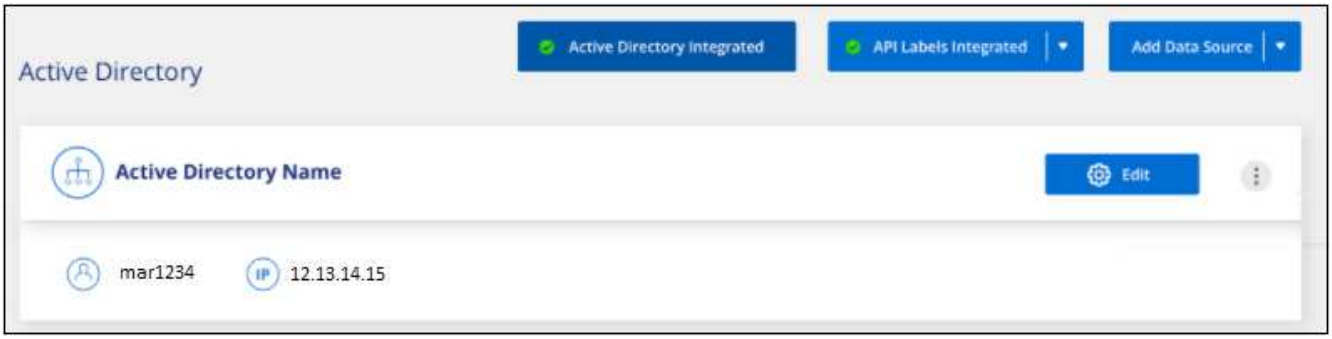


2. Nella finestra di dialogo connessione ad Active Directory, immettere i dettagli di Active Directory e fare clic su **Connetti**.

   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:

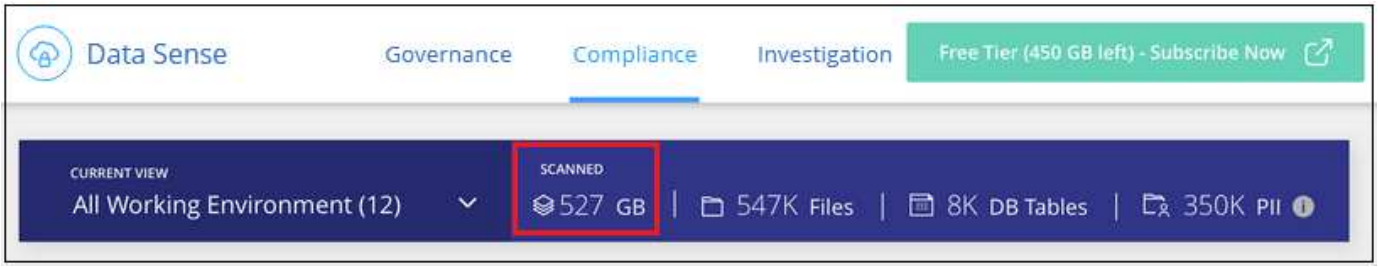
- Se hai già sottoscritto l'abbonamento BlueXP pay-as-you-go (PAYGO) nel mercato del tuo cloud provider, sarai automaticamente iscritto anche alla classificazione BlueXP. Non dovrai più iscriverti.
- La classificazione BlueXP (Data Sense) Bring-Your-Own-License (BYOL) è una licenza *floating* che è possibile 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

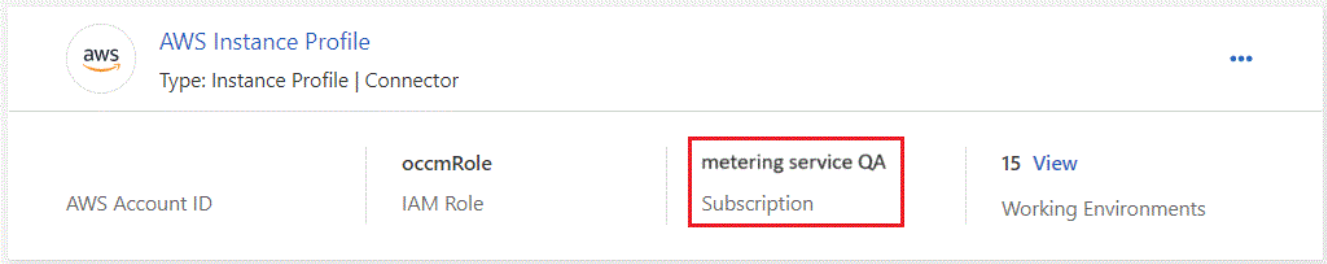
Questi passaggi devono essere completati da un utente che ha il ruolo di *account Admin*.

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

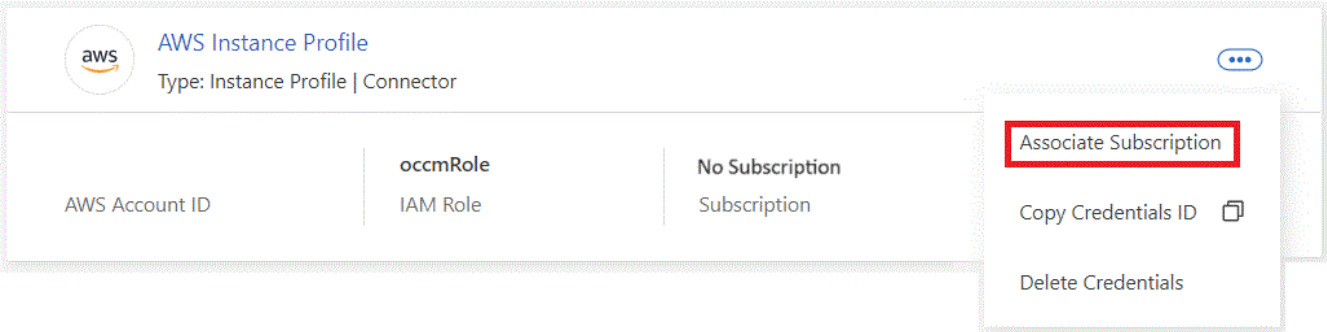
2. Fare clic su **credenziali** e individuare le credenziali per il profilo dell'istanza AWS, l'identità del servizio gestito Azure o Google Project.

   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

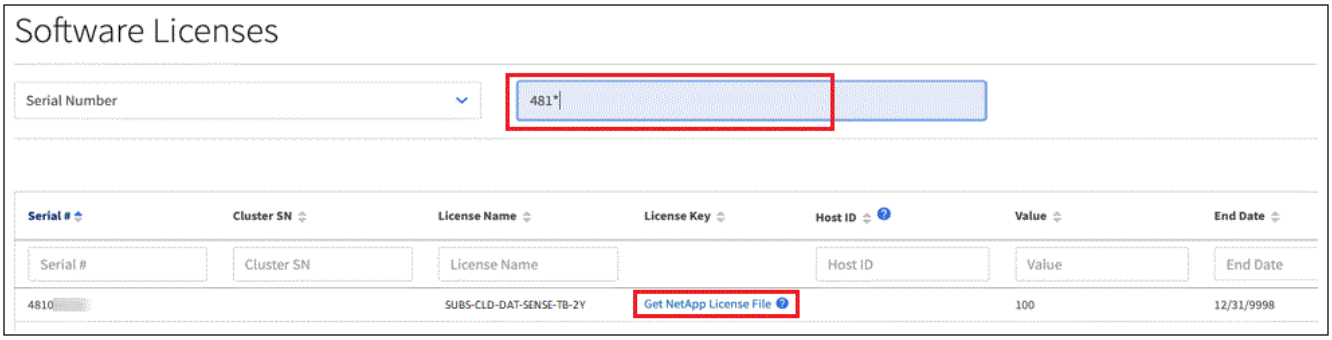
  Individua questo numero nell'ordine di vendita o contatta l'account team per ottenere queste informazioni.

- ID account BlueXP

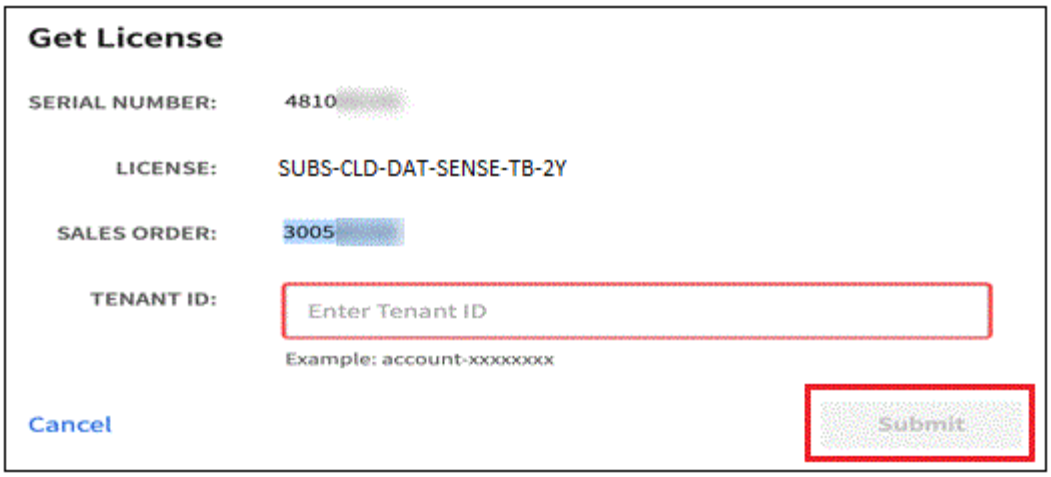
  Puoi trovare il tuo ID account BlueXP selezionando l'elenco a discesa **account** nella parte superiore di BlueXP, quindi facendo clic su **Gestisci account** accanto all'account. L'ID account si trova nella scheda Panoramica. Per i siti in modalità privata senza accesso a Internet, utilizzare **account-DARKSITE1**.

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

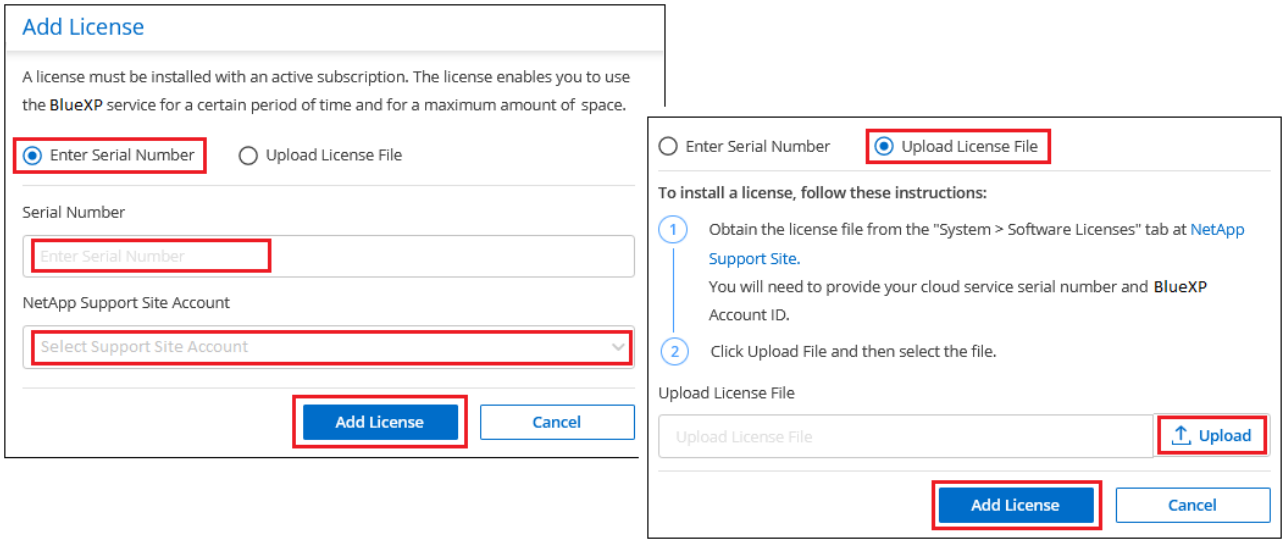
Dopo aver acquistato una licenza di classificazione BlueXP (Data Sense) per l'account BlueXP, è necessario aggiungere la licenza a BlueXP per utilizzare il servizio di classificazione BlueXP.

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.



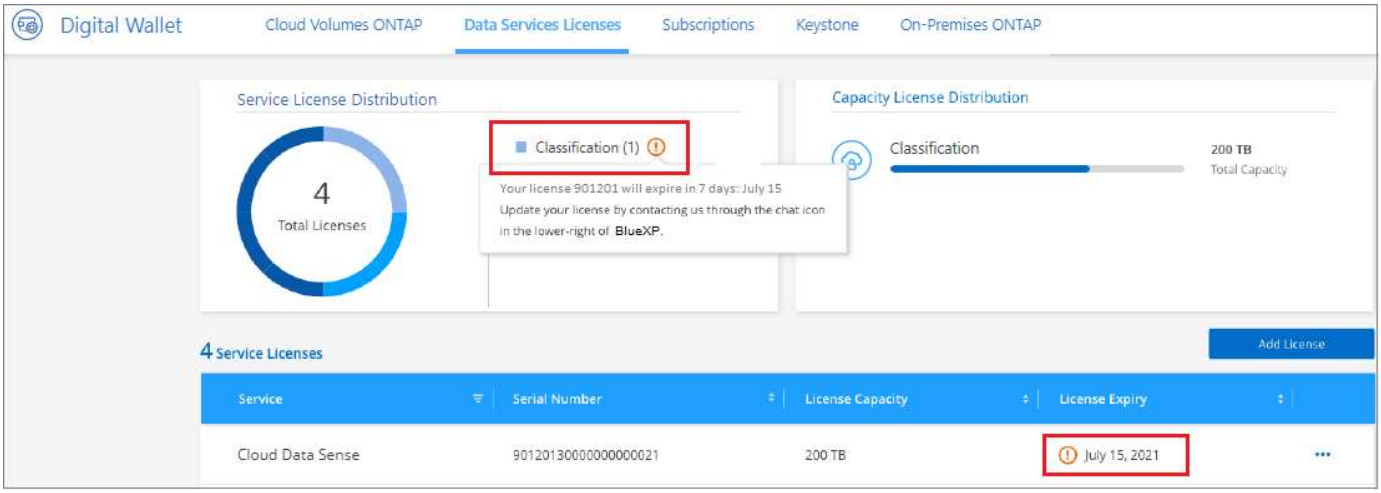
Risultato

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.

Utilizzare la classificazione BlueXP

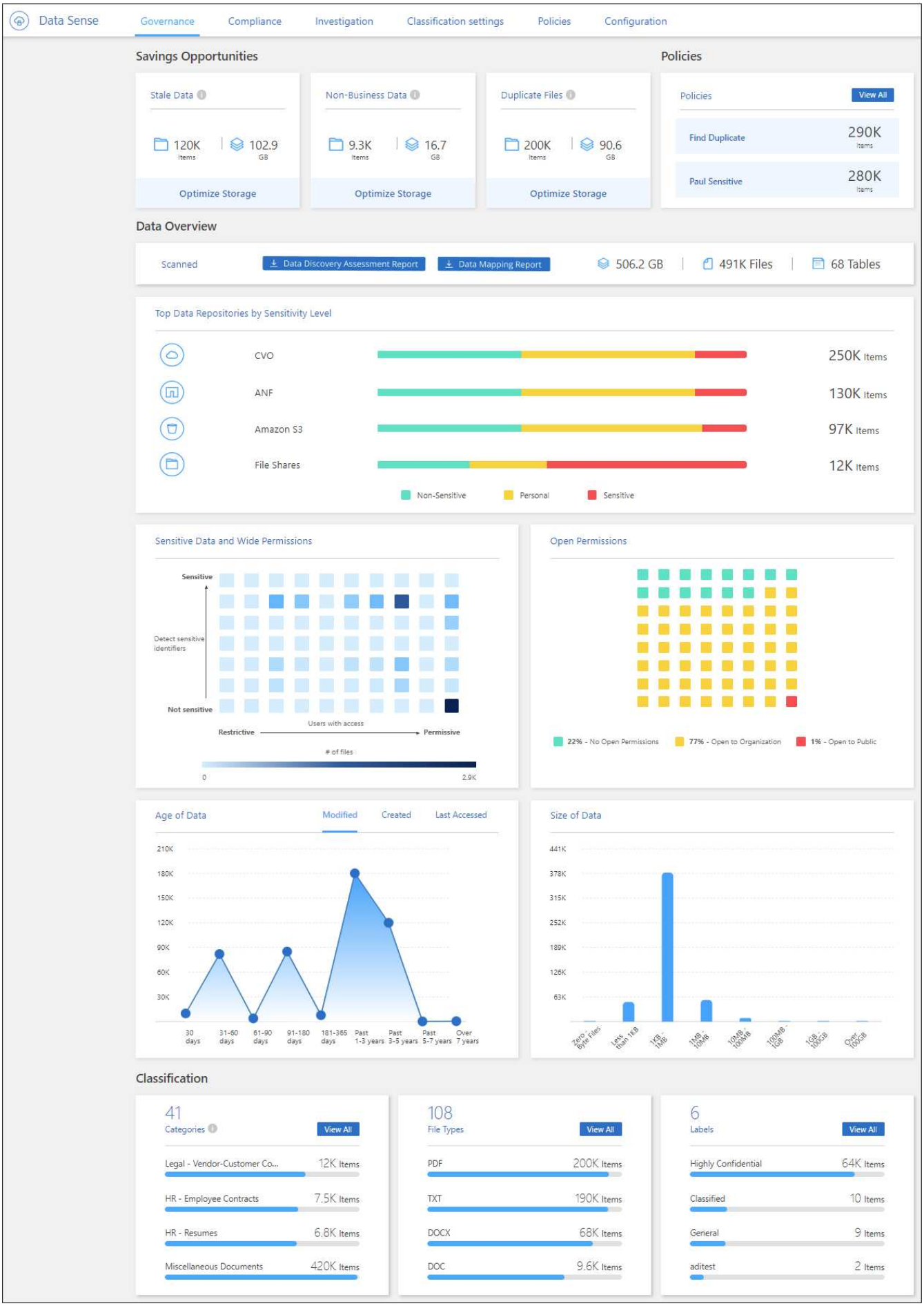
Visualizzare i dettagli di governance sui dati archiviati nell’organizzazione

Ottieni il controllo dei costi relativi ai dati sulle risorse di storage della tua organizzazione. La classificazione BlueXP identifica la quantità di dati obsoleti, dati non aziendali, file duplicati e file molto grandi nei sistemi, in modo da poter decidere se rimuovere o tierare alcuni file in uno storage a oggetti meno costoso.

Inoltre, se si prevede di migrare i dati da posizioni on-premise al cloud, è possibile visualizzare le dimensioni dei dati e se alcuni di essi contengono informazioni sensibili prima di spostarli.

Dashboard di governance

La dashboard di governance fornisce informazioni che consentono di aumentare l’efficienza e controllare i costi relativi ai dati memorizzati nelle risorse di storage.


Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
120K Items
102.9 GB
Optimize Storage
Non-Business Data
9.3K Items
16.7 GB
Optimize Storage
Duplicate Files
200K Items
90.6 GB
Optimize Storage
Policies
Policies
View All
Find Duplicate 290K Items
Paul Sensitive 280K Items
Data Overview
Scanned
Data Discovery Assessment Report
Data Mapping Report
506.2 GB
491K Files
68 Tables
Top Data Repositories by Sensitivity Level
CVO 250K Items
ANF 130K Items
Amazon S3 97K Items
File Shares 12K Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detect sensitive identifiers
Not sensitive
Users with access
Restrictive
Permissive
# of files
0
2.9K
Open Permissions
22% - No Open Permissions
77% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
210K
180K
150K
120K
90K
60K
30K
30 days
31-60 days
61-90 days
91-180 days
181-365 days
Past 1-3 years
Past 3-5 years
Past 5-7 years
Over 7 years
Size of Data
441K
378K
315K
252K
189K
126K
63K
Zero Byte Files
Less than 1KB
1KB - 1MB
1MB - 10MB
10MB - 100MB
100MB - 1GB
1GB - 10GB
Over 10GB
Classification
41
Categories
View All
Legal - Vendor-Customer Co... 12K Items
HR - Employee Contracts 7.5K Items
HR - Resumes 6.8K Items
Miscellaneous Documents 420K Items
108
File Types
View All
PDF 200K Items
TXT 190K Items
DOCX 68K Items
DOC 9.6K Items
6
Labels
View All
Highly Confidential 64K Items
Classified 10 Items
General 9 Items
aditest 2 Items

Risparmiare opportunità

È possibile esaminare gli elementi nell'area *Saving Opportunities* per verificare se sono presenti dati da eliminare o da assegnare allo storage a oggetti meno costoso. Fare clic su ciascun elemento per visualizzare i risultati filtrati nella pagina di analisi.

- **Dati obsoleti** - dati modificati più di 3 anni fa.
- **Dati non aziendali** - dati considerati non correlati al business, in base alla categoria o al tipo di file. Ciò include:
  - Dati dell'applicazione
  - Audio
  - Eseguibili
  - Immagini
  - Registri
  - Video
  - Varie (categoria generale "Altro")
- **File duplicati** - file duplicati in altre posizioni nelle origini dati che si stanno eseguendo la scansione. "Scopri quali tipi di file duplicati vengono visualizzati".

  NOTA

  Se una qualsiasi delle origini dati implementa il tiering dei dati, i dati vecchi che risiedono già nello storage a oggetti possono essere identificati nella categoria *dati obsoleti*.

Policy con il maggior numero di risultati

Nell'area *Policies*, i criteri con il maggior numero di risultati vengono visualizzati in cima all'elenco. Fare clic sul nome di una policy per visualizzare i risultati nella pagina delle analisi. Fare clic su **View All** (Visualizza tutto) per visualizzare l'elenco di tutte le policy disponibili.

Fare clic su "qui" Per ulteriori informazioni sulle policy.

Panoramica dei dati

La sezione *Data Overview* fornisce una rapida panoramica di tutti i dati sottoposti a scansione. Fare clic sul pulsante per scaricare un report di mappatura dei dati completo che include capacità di utilizzo, età dei dati, dimensione dei dati e tipi di file per tutti gli ambienti di lavoro e le origini dati. Vedere Report di mappatura dei dati per informazioni dettagliate su questo report.

Principali repository di dati elencati in base alla sensibilità dei dati

L'area *Top Data Repository per livello di sensibilità* elenca i primi quattro repository di dati (ambienti di lavoro e origini dati) che contengono gli elementi più sensibili. Il grafico a barre per ciascun ambiente di lavoro è suddiviso in:

- Dati non sensibili
- Dati personali
- Dati personali sensibili

È possibile passare il mouse su ciascuna sezione per visualizzare il numero totale di elementi in ciascuna

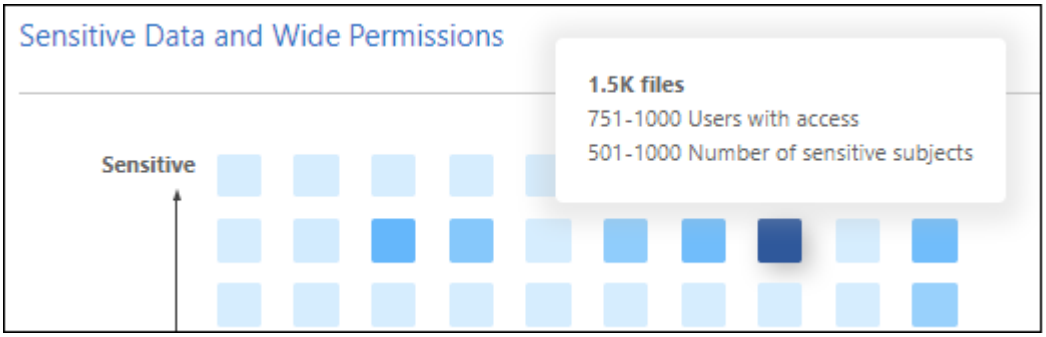
categoria.

Fare clic su ciascuna area per visualizzare i risultati filtrati nella pagina di analisi in modo da poter analizzare ulteriormente.

Dati elencati in base alla sensibilità e alle autorizzazioni estese

L'area *dati sensibili e permessi estesi* fornisce una mappa termica dei file che contengono dati sensibili (inclusi dati personali sensibili e sensibili) e che sono eccessivamente permissivi. In questo modo è possibile individuare i rischi associati ai dati sensibili.

La classificazione dei file dipende dal numero di utenti autorizzati ad accedere ai file sull'asse X (dal più basso al più alto) e dal numero di identificatori sensibili all'interno dei file sull'asse Y (dal più basso al più alto). I blocchi rappresentano il numero di file che corrispondono agli elementi degli assi X e Y. I blocchi di colore più chiaro sono buoni, con meno utenti in grado di accedere ai file e con meno identificatori sensibili per file. I blocchi più scuri sono gli elementi che potresti voler esaminare. Ad esempio, la schermata seguente mostra il testo del passaggio del mouse per il blocco blu scuro. Indica che sono disponibili 1,500 file a cui hanno accesso 751-100 utenti e 501-100 identificatori sensibili per file.



È possibile fare clic sul blocco desiderato per visualizzare i risultati filtrati dei file interessati nella pagina di analisi, in modo da poter analizzare ulteriormente.

Se non si è integrato un servizio di identità con la classificazione BlueXP, in questo pannello non viene visualizzato alcun dato. "Scopri come integrare il servizio Active Directory con la classificazione BlueXP".

> Questo pannello supporta i file in condivisioni CIFS, OneDrive e origini dati SharePoint. Attualmente non è disponibile alcun supporto per database, Google Drive, Amazon S3 e storage a oggetti generici.

Dati elencati in base ai tipi di autorizzazioni aperte

L'area *Open Permissions* mostra la percentuale per ciascun tipo di permessi esistenti per tutti i file sottoposti a scansione. Il grafico mostra i seguenti tipi di autorizzazioni:

- Nessuna autorizzazione aperta
- Aperto all'organizzazione
- Aperto al pubblico
- Accesso sconosciuto

È possibile passare il mouse su ciascuna sezione per visualizzare il numero totale di file in ciascuna categoria. Fare clic su ciascuna area per visualizzare i risultati filtrati nella pagina di analisi in modo da poter analizzare ulteriormente.

Età dei dati e dimensioni dei grafici dei dati

È possibile esaminare gli elementi nei grafici *Age* e *Size* per verificare se sono presenti dati da eliminare o da assegnare allo storage a oggetti meno costoso.

È possibile passare il mouse su un punto dei grafici per visualizzare i dettagli relativi all'età o alle dimensioni dei dati in tale categoria. Fare clic per visualizzare tutti i file filtrati in base all'età o all'intervallo di dimensioni.

- **Age of Data graph** - classifica i dati in base all'ora in cui sono stati creati, all'ultima volta in cui sono stati utilizzati o all'ultima volta in cui sono stati modificati.
- **Dimensione del grafico dei dati** - classifica i dati in base alle dimensioni.

  NOTA

  Se una qualsiasi delle origini dati implementa il tiering dei dati, i dati vecchi che risiedono già nello storage a oggetti possono essere identificati nel grafico *Age of Data*.

Classificazioni dei dati più identificate

L'area *Classification* fornisce un elenco dei più identificati "Categorie", "Tipi di file", e. "Etichette AIP" nei dati sottoposti a scansione.

Categorie

Le categorie possono aiutarti a capire cosa accade con i tuoi dati mostrando i tipi di informazioni di cui disponi. Ad esempio, una categoria come "curriculum" o "contratti dipendenti" può includere dati sensibili. Quando si analizzano i risultati, è possibile che i contratti dei dipendenti siano memorizzati in una posizione non sicura. A questo punto, è possibile correggere il problema.

Vedere "Visualizzazione dei file in base alle categorie" per ulteriori informazioni.

Tipi di file

La revisione dei tipi di file consente di controllare i dati sensibili, poiché alcuni tipi di file potrebbero non essere memorizzati correttamente.

Vedere "Visualizzazione dei tipi di file" per ulteriori informazioni.

Etichette AIP

Se si è abbonati ad Azure Information Protection (AIP), è possibile classificare e proteggere documenti e file applicando etichette ai contenuti. La revisione delle etichette AIP più utilizzate assegnate ai file consente di visualizzare le etichette più utilizzate nei file.

Vedere "Etichette AIP" per ulteriori informazioni.

Report di mappatura dei dati

Il Data Mapping Report fornisce una panoramica dei dati memorizzati nelle origini dati aziendali per assisterti nelle decisioni relative a migrazione, backup, sicurezza e processi di conformità. Il report elenca prima una panoramica che riepiloga tutti gli ambienti di lavoro e le origini dati, quindi fornisce un'analisi dettagliata per ciascun ambiente di lavoro.

Il report contiene le seguenti informazioni:

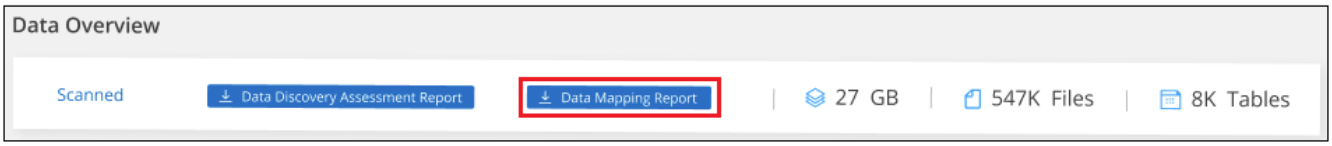
Categoria	Descrizione
Capacità di utilizzo	Per tutti gli ambienti di lavoro: Elenca il numero di file e la capacità utilizzata per ciascun ambiente di lavoro. Per ambienti di lavoro singoli: Elenca i file che utilizzano la capacità maggiore.
Età dei dati	Fornisce tre grafici e grafici per la data di creazione, l'ultima modifica o l'ultimo accesso ai file. Elenca il numero di file e la relativa capacità utilizzata, in base a determinati intervalli di date.
Dimensione dei dati	Elenca il numero di file presenti in determinati intervalli di dimensioni negli ambienti di lavoro.
Tipi di file	Elenca il numero totale di file e la capacità utilizzata per ciascun tipo di file memorizzato negli ambienti di lavoro.

Generare il rapporto di mappatura dati

Questo report viene generato dalla scheda Governance della classificazione BlueXP.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Governance**, quindi sul pulsante **Data Mapping Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in base alle esigenze.

Se il report è più grande di 1 MB, il file PDF viene conservato nell'istanza di classificazione di BlueXP e viene visualizzato un messaggio a comparsa relativo alla posizione esatta. Quando la classificazione BlueXP viene installata su una macchina Linux in sede o su una macchina Linux implementata nel cloud, è possibile accedere direttamente al file PDF. Quando la classificazione BlueXP viene implementata nel cloud, è necessario eseguire l'SSH nell'istanza di classificazione BlueXP per scaricare il file PDF. "Scopri come accedere ai dati sull'istanza di Classification".

Nota: È possibile personalizzare il nome della società visualizzato nella prima pagina del report dalla parte superiore della pagina di classificazione di BlueXP facendo clic su ⋮ Quindi fare clic su **Cambia nome azienda**. La volta successiva che si genera il report, questo includerà il nuovo nome.

Report sulla valutazione del rilevamento dei dati

Il Data Discovery Assessment Report fornisce un'analisi di alto livello dell'ambiente sottoposto a scansione per evidenziare i risultati del sistema e mostrare le aree di interesse e le potenziali fasi di correzione. I risultati si basano sia sulla mappatura che sulla classificazione dei dati. L'obiettivo di questo report è quello di sensibilizzare l'utente su tre aspetti significativi del set di dati:

Funzione	Descrizione
Problemi di governance dei dati	Un'immagine dettagliata di tutti i dati in tuo possesso e delle aree in cui puoi ridurre la quantità di dati per risparmiare sui costi.
Esposizioni alla sicurezza dei dati	Aree in cui i dati sono accessibili ad attacchi interni o esterni a causa di ampie autorizzazioni di accesso.
Lacune nella compliance dei dati	Dove si trovano le informazioni personali o sensibili per motivi di sicurezza e DSAR (richieste di accesso dei soggetti).

Dopo la valutazione, questo report identifica le aree in cui è possibile:

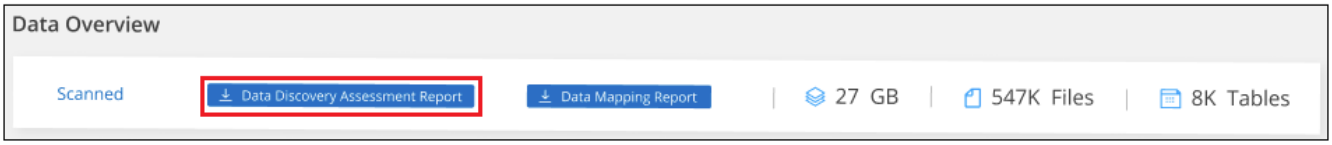
- Riduci i costi di storage modificando la policy di conservazione o spostando o eliminando determinati dati (dati obsoleti, duplicati o non aziendali)
- Proteggi i tuoi dati che dispongono di ampie autorizzazioni rivedendo le policy di gestione dei gruppi globali
- Proteggi i tuoi dati personali o sensibili trasferendo le informazioni personali in archivi di dati più sicuri

Generare il report di valutazione per il rilevamento dei dati

Questo report viene generato dalla scheda Governance della classificazione BlueXP.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Governance**, quindi sul pulsante **Data Discovery Assessment Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in base alle esigenze.

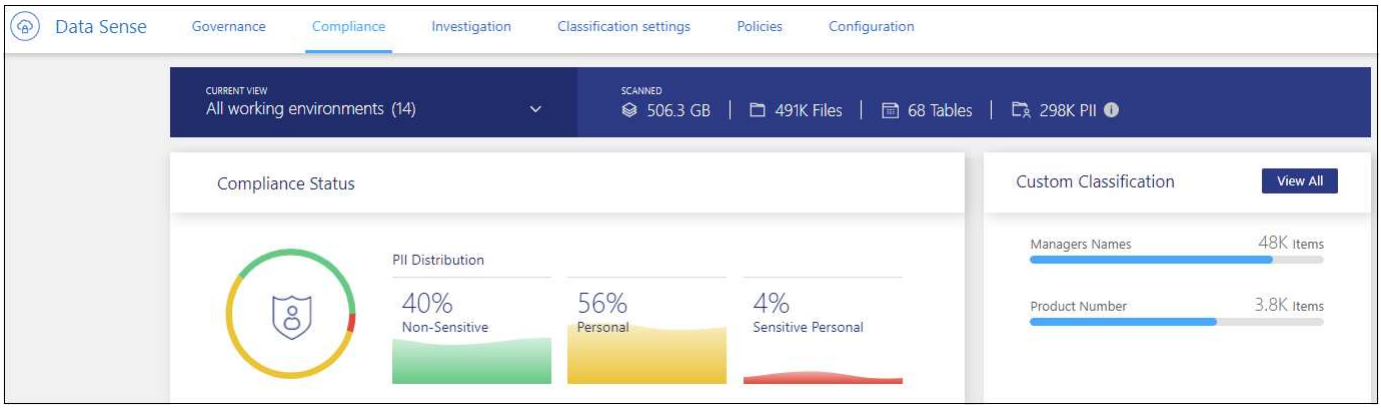
Nota: È possibile personalizzare il nome della società visualizzato nella prima pagina del report dalla parte superiore della pagina di classificazione di BlueXP facendo clic su ⋮ Quindi fare clic su **Cambia nome azienda**. La volta successiva che si genera il report, questo includerà il nuovo nome.

Consente di visualizzare i dettagli di conformità relativi ai dati archiviati nell'organizzazione

Ottieni il controllo dei tuoi dati privati visualizzando i dettagli relativi ai dati personali e ai dati personali sensibili della tua organizzazione. È inoltre possibile ottenere visibilità esaminando le categorie e i tipi di file che BlueXP classifica trovato nei dati.

> Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.

Per impostazione predefinita, la dashboard di classificazione BlueXP visualizza i dati di conformità per tutti gli ambienti di lavoro e i database.



Se si desidera visualizzare i dati solo per alcuni ambienti di lavoro, selezionare gli ambienti di lavoro.

È inoltre possibile filtrare i risultati dalla pagina Data Investigation (analisi dati) e scaricare un report dei risultati come file CSV. Vedere "Filtraggio dei dati nella pagina Data Investigation" per ulteriori informazioni.

Consente di visualizzare i file che contengono dati personali

La classificazione BlueXP identifica automaticamente parole, stringhe e modelli specifici (Regex) all'interno dei dati. Ad esempio, informazioni di identificazione personale (PII), numeri di carta di credito, numeri di previdenza sociale, numeri di conto bancario, password, e molto altro ancora. "Consulta l'elenco completo". La classificazione BlueXP identifica questo tipo di informazioni nei singoli file, nei file all'interno delle directory (condivisioni e cartelle) e nelle tabelle dei database.

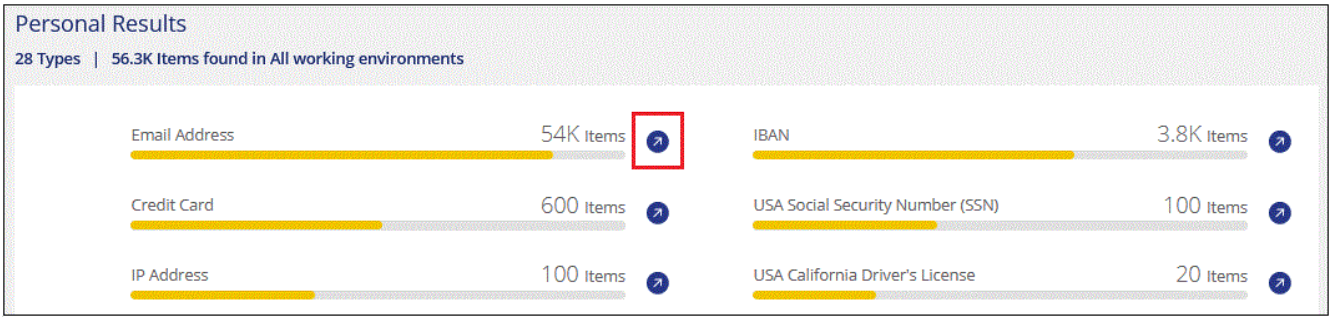
Inoltre, se è stato aggiunto un server di database da sottoporre a scansione, la funzione *Data Fusion* consente di eseguire la scansione dei file per identificare se gli identificatori univoci dei database sono presenti in tali file o in altri database. Vedere "Aggiunta di identificatori di dati personali mediante Data Fusion" per ulteriori informazioni.

Per alcuni tipi di dati personali, la classificazione BlueXP utilizza *Proximity Validation* per validarne i risultati. La convalida avviene cercando una o più parole chiave predefinite in prossimità dei dati personali trovati. Ad esempio, la classificazione BlueXP identifica un Numero di previdenza sociale (SSN) come SSN se viene visualizzato un termine di prossimità, ad esempio *SSN* o *social Security*. "La tabella dei dati personali" Mostra quando la classificazione BlueXP utilizza la convalida di prossimità.

Fasi

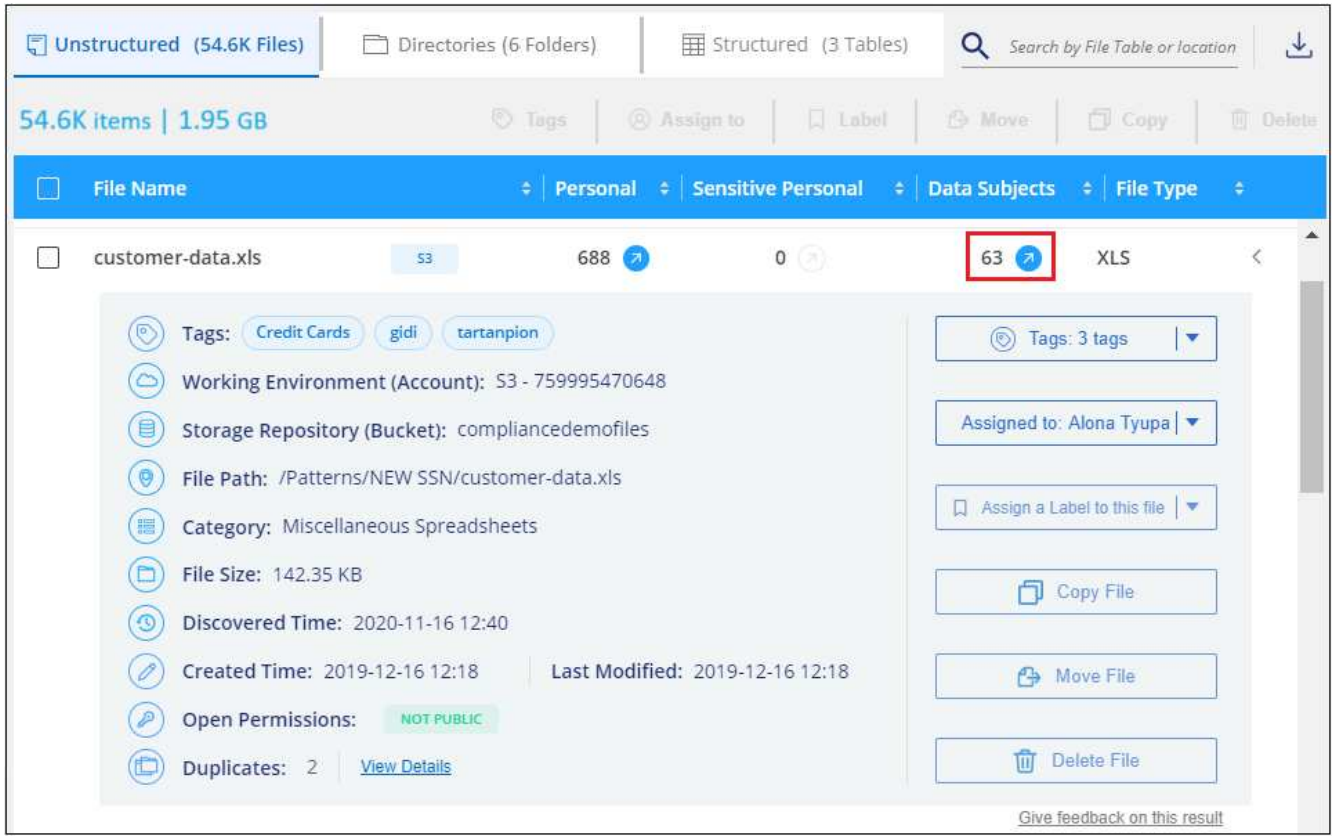
1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**, quindi fare clic sulla scheda **Compliance**.
2. Per esaminare i dettagli di tutti i dati personali, fare clic sull'icona accanto alla percentuale dei dati personali.

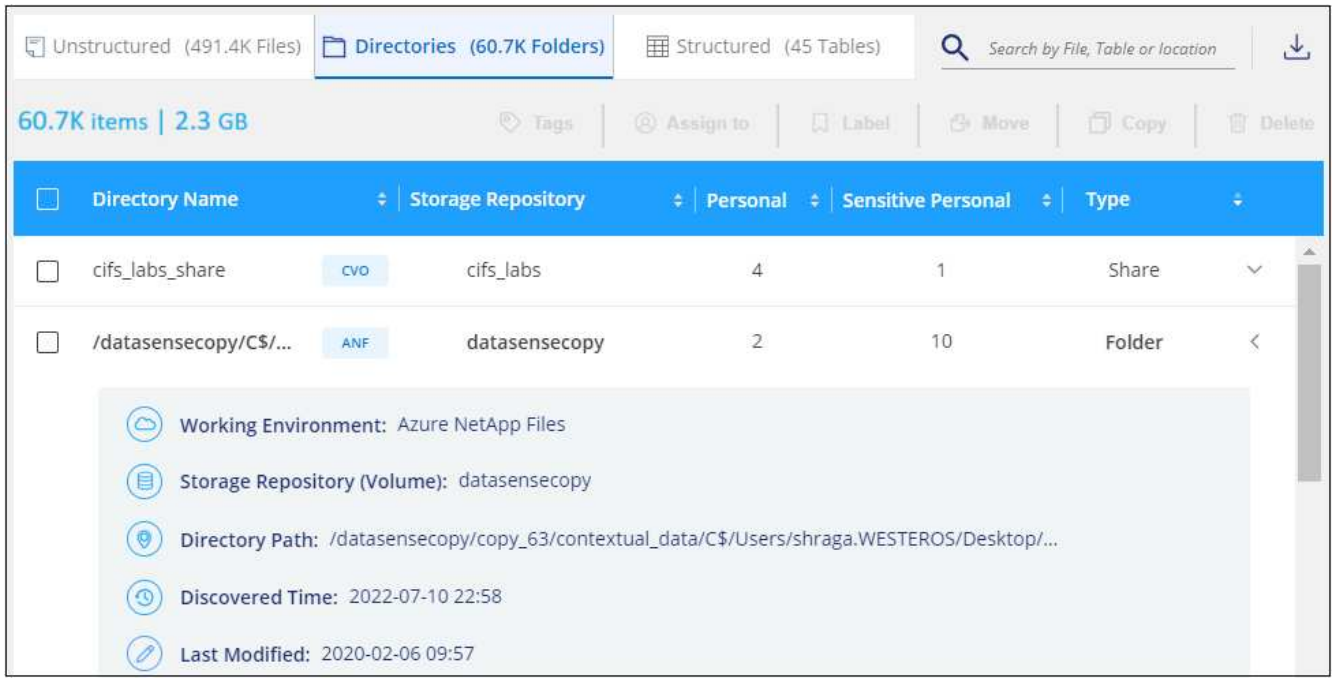
3. Per esaminare i dettagli di un tipo specifico di dati personali, fare clic su **Visualizza tutto**, quindi fare clic sull'icona **esamina risultati** per un tipo specifico di dati personali, ad esempio indirizzi e-mail.



4. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

   Le 2 schermate riportate di seguito mostrano i dati personali presenti nei singoli file e contenuti nei file all'interno delle directory (condivisioni e cartelle). È inoltre possibile selezionare la scheda **Structured** per visualizzare i dati personali trovati nei database.





Consente di visualizzare i file che contengono dati personali sensibili

La classificazione BlueXP identifica automaticamente tipi speciali di informazioni personali sensibili, come definito dalle normative sulla privacy, ad esempio "articoli 9 e 10 del GDPR". Ad esempio, informazioni relative alla salute, all'origine etnica o all'orientamento sessuale di una persona. "Consulta l'elenco completo". La classificazione BlueXP identifica questo tipo di informazioni nei singoli file, nei file all'interno delle directory (condivisioni e cartelle) e nelle tabelle dei database.

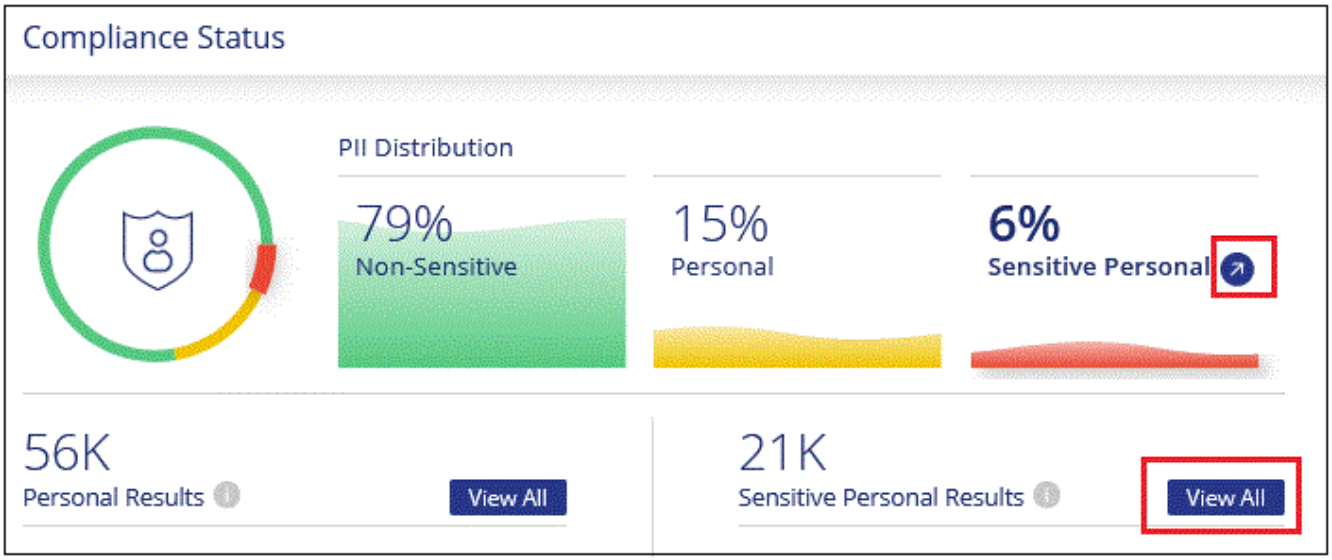
La classificazione BlueXP utilizza l'intelligenza artificiale (ai), l'elaborazione del linguaggio naturale (NLP), l'apprendimento automatico (ML) e il calcolo cognitivo (CC) per comprendere il significato del contenuto che scansiona al fine di estrarre le entità e classificarlo di conseguenza.

Ad esempio, una categoria di dati GDPR sensibili è l'origine etnica. Grazie alle sue capacità NLP, la classificazione BlueXP è in grado di distinguere la differenza tra una frase che recita "George is Mexican" (che indica i dati sensibili come specificato nell'articolo 9 del GDPR) e "George is Eating Mexican Food" (George sta mangiando cibo messicano).

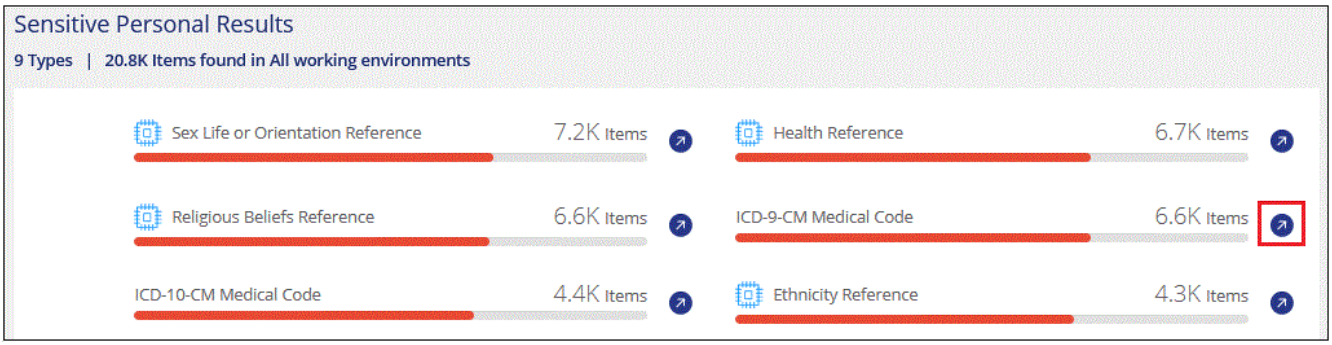
> Quando si esegue la scansione di dati personali sensibili, è supportata solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**, quindi fare clic sulla scheda **Compliance**.
2. Per esaminare i dettagli di tutti i dati personali sensibili, fare clic sull'icona accanto alla percentuale dei dati personali sensibili.



3. Per esaminare i dettagli di un tipo specifico di dati personali sensibili, fare clic su **Visualizza tutto**, quindi fare clic sull'icona **esamina risultati** per un tipo specifico di dati personali sensibili.



4. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

Visualizzare i file per categorie

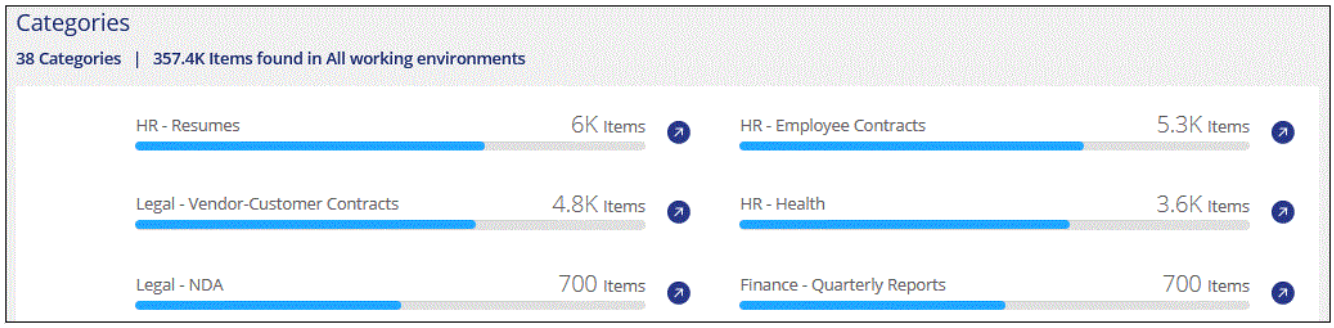
La classificazione BlueXP prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. "Vedere l'elenco delle categorie".

Le categorie possono aiutarti a capire cosa accade con i tuoi dati mostrando i tipi di informazioni di cui disponi. Ad esempio, una categoria come i curriculum o i contratti dei dipendenti può includere dati sensibili. Quando si analizzano i risultati, è possibile che i contratti dei dipendenti siano memorizzati in una posizione non sicura. A questo punto, è possibile correggere il problema.

> Le categorie sono supportate in inglese, tedesco e spagnolo. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**, quindi fare clic sulla scheda **Compliance**.
2. Fare clic sull'icona **esamina risultati** di una delle 4 categorie principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto** e quindi sull'icona corrispondente a una delle categorie.



3. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

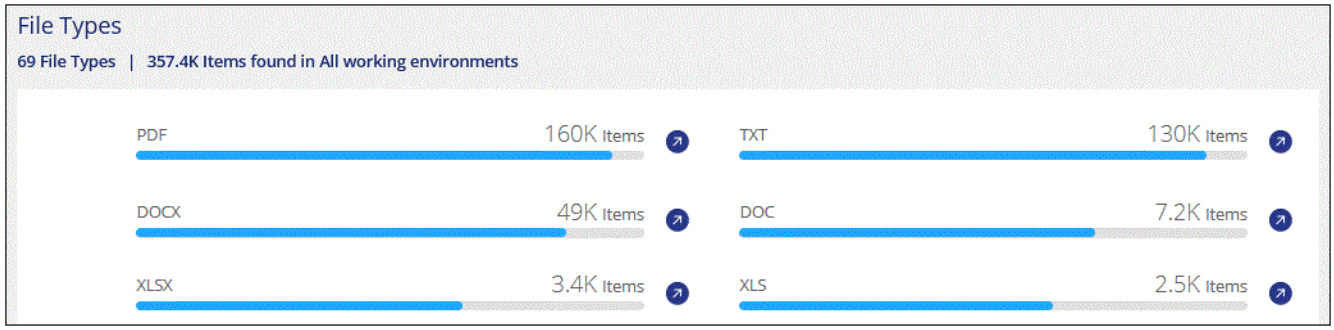
Visualizzare i file in base ai tipi di file

La classificazione BlueXP prende i dati sottoposti a scansione e li suddivide in base al tipo di file. La revisione dei tipi di file consente di controllare i dati sensibili, poiché alcuni tipi di file potrebbero non essere memorizzati correttamente. "Vedere l'elenco dei tipi di file".

Ad esempio, è possibile memorizzare file CAD che includono informazioni molto sensibili sull'organizzazione. Se non sono protetti, è possibile assumere il controllo dei dati sensibili limitando le autorizzazioni o spostando i file in un'altra posizione.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**, quindi fare clic sulla scheda **Compliance**.
2. Fare clic sull'icona **esamina risultati** per uno dei 4 tipi di file principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto**, quindi fare clic sull'icona corrispondente a uno qualsiasi dei tipi di file.



3. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

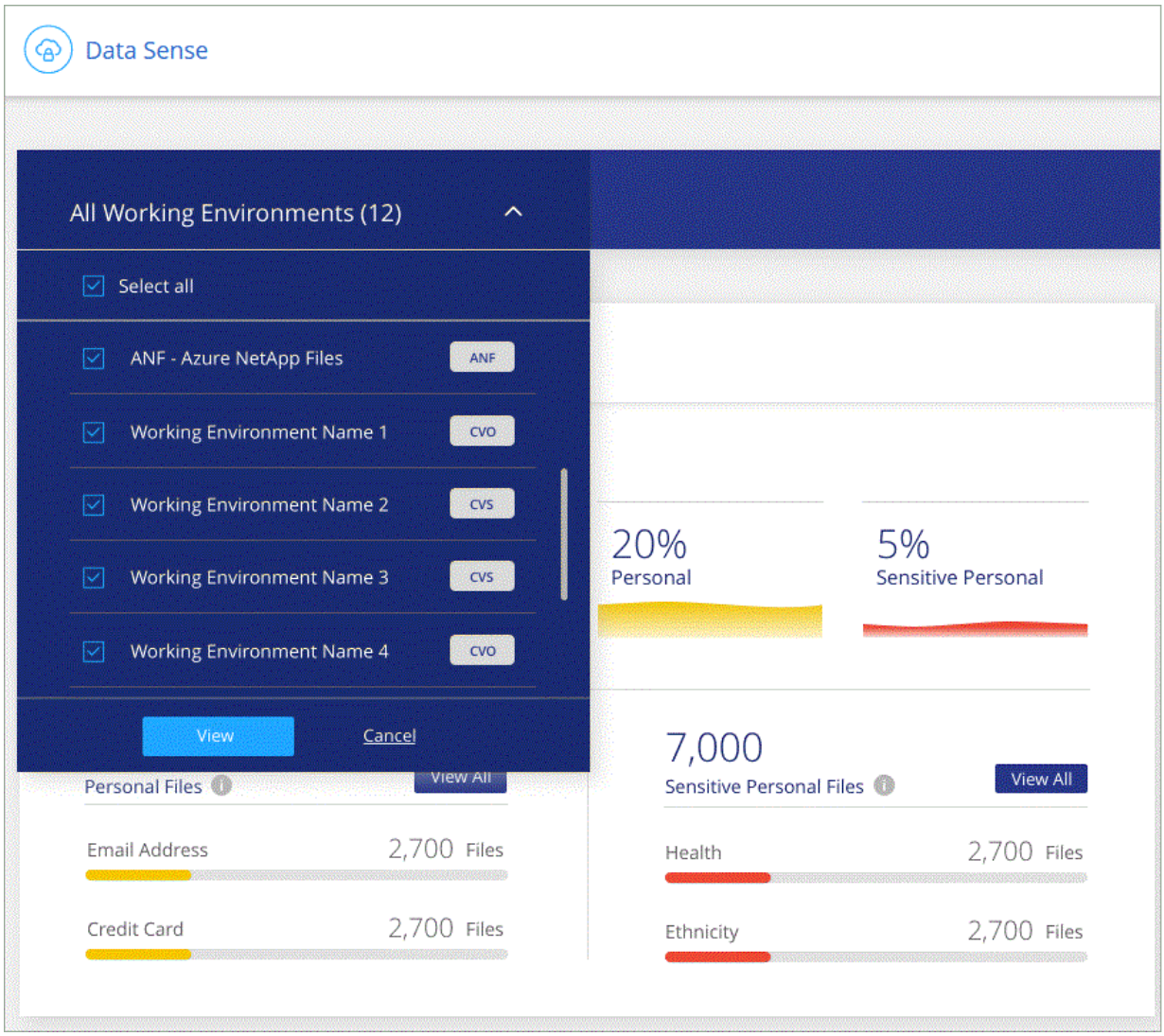
Visualizza i dati del dashboard per ambienti di lavoro specifici

È possibile filtrare il contenuto della dashboard di classificazione BlueXP per visualizzare i dati di conformità per tutti gli ambienti di lavoro e i database o solo per ambienti di lavoro specifici.

Quando si filtra la dashboard, la classificazione BlueXP regola i dati di conformità e invia report solo agli ambienti di lavoro selezionati.

Fasi

1. Fare clic sul menu a discesa del filtro, selezionare gli ambienti di lavoro per i quali si desidera visualizzare i dati e fare clic su **View** (Visualizza).



Categorie di dati privati

Esistono molti tipi di dati privati che la classificazione BlueXP può identificare nei volumi, nei bucket Amazon S3, nei database, nelle cartelle OneDrive, negli account SharePoint, E Google Drive. Vedere le categorie riportate di seguito.

> Se hai bisogno della classificazione BlueXP per identificare altri tipi di dati privati, come ad esempio numeri di identificazione nazionali aggiuntivi o identificatori sanitari, invia un'email a ng-contact-data-sense@netapp.com con la tua richiesta.

Tipi di dati personali

I dati personali contenuti nei file possono essere dati personali di carattere generale o identificativi nazionali. La terza colonna nella tabella seguente indica se la classificazione BlueXP utilizza "convalida della prossimità" per convalidare i risultati per l'identificatore.

Le lingue in cui questi elementi possono essere riconosciuti sono identificate nella tabella.

Nota: È possibile aggiungere all'elenco dei dati personali presenti nei file. Se si esegue la scansione di un

server di database, la funzione *Data Fusion* consente di scegliere gli identificatori aggiuntivi che la classificazione BlueXP dovrà cercare nelle scansioni selezionando le colonne in una tabella di database. È inoltre possibile aggiungere parole chiave personalizzate da un file di testo o modelli personalizzati utilizzando un'espressione regolare. Vedere "Aggiunta di identificatori di dati personali alle scansioni di classificazione BlueXP" per ulteriori informazioni.

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese
Generale	Numero della carta di credito	No	✓	✓	✓		✓
	Soggetti dei dati	No	✓	✓	✓		
	Indirizzo e-mail	No	✓	✓	✓		✓
	Numero IBAN (International Bank account Number)	No	✓	✓	✓		✓
	Indirizzo IP	No	✓	✓	✓		✓
	Password	Sì	✓	✓	✓		✓

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese
Identificatori nazionali							

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese
	ID svedese	Sì	✓	✓	✓		
	Texas driver's License	Sì	✓	✓	✓		
	REGNO UNITO ID (NINO)	Sì	✓	✓	✓		
	USA California driver's License	Sì	✓	✓	✓		
	USA, Indiana driver's License	Sì	✓	✓	✓		
	USA New York driver's License	Sì	✓	✓	✓		
	Numero di previdenza sociale (SSN) USA	Sì	✓	✓	✓		

Tipi di dati personali sensibili

I dati personali sensibili che la classificazione BlueXP può trovare nei file includono il seguente elenco.

Al momento, gli elementi di questa categoria possono essere riconosciuti solo in inglese.

Riferimento alle procedure penali
Dati relativi alle condanne e ai reati penali di una persona fisica.

Riferimento di etnia
Dati relativi alla razza o all'origine etnica di una persona fisica.

Riferimento di salute
Dati relativi alla salute di una persona fisica.

Codici medici ICD-9-CM
Codici utilizzati nel settore medico e sanitario.

Codici medici ICD-10-CM
Codici utilizzati nel settore medico e sanitario.

Riferimento alle credenze filosofiche
Dati relativi alle convinzioni filosofiche di una persona naturale.

Opinioni politiche riferimento
Dati relativi alle opinioni politiche di una persona fisica.

Riferimenti alle credenze religiose
Dati relativi alle convinzioni religiose di una persona fisica.

Sex Life o orientamento di riferimento
Dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Tipi di categorie

La classificazione BlueXP classifica i tuoi dati nel modo seguente.

La maggior parte di queste categorie può essere riconosciuta in inglese, tedesco e spagnolo.

Categoria	Tipo	Inglese	Tedesco	Spagnolo
Finanza	Bilanci	✓	✓	✓
	Ordini di acquisto	✓	✓	✓
	Fatture	✓	✓	✓
	Report trimestrali	✓	✓	✓
FC	Controlli in background	✓		✓
	Piani di compensazione	✓	✓	✓
	Contratti con i dipendenti	✓		✓
	Recensioni dei dipendenti	✓		✓
	Salute	✓		✓
	Riprende	✓	✓	✓
Legale	NDA	✓	✓	✓
	Contratti fornitore-cliente	✓	✓	✓
Marketing	Campagne	✓	✓	✓
	Conferenze	✓	✓	✓
Operazioni	Report di audit	✓	✓	✓
Vendite	Ordini di vendita	✓	✓	
Servizi	RFI	✓		✓
	RFP	✓		✓
	SOW	✓	✓	✓
	Formazione	✓	✓	✓
Supporto	Reclami e biglietti	✓	✓	✓

I seguenti metadati sono anche classificati e identificati nelle stesse lingue supportate:

- Dati dell’applicazione
- Archiviare i file
- Audio
- Dati delle applicazioni di business
- File CAD
- Codice
- Corrotto
- Database e file di indice
- Classificazione BlueXP Breadcrumbs
- File di progettazione
- Email Application Data (dati applicazione email)

- Crittografato (file con un elevato punteggio di entropia)
- Eseguibili
- Dati delle applicazioni finanziarie
- Health Application Data
- Immagini
- Registri
- Documenti vari
- Presentazioni varie
- Fogli di calcolo vari
- Varie "Sconosciuto"
- File protetti da password
- Dati strutturati
- Video
- File a byte zero

Tipi di file

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.

Tuttavia, 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
```

Accuratezza delle informazioni rilevate

NetApp non può garantire la precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla classificazione BlueXP. È sempre necessario convalidare le informazioni esaminando i dati.

In base ai nostri test, la tabella seguente mostra l'accuratezza delle informazioni rilevate dalla classificazione BlueXP. Lo suddivideremo per *precisione* e *richiamo*:

Precisione

La probabilità che la classificazione BlueXP trovi sia stata identificata correttamente. Ad esempio, un tasso di precisione del 90% per i dati personali significa che 9 file su 10 identificati come contenenti informazioni personali contengono effettivamente informazioni personali. 1 file su 10 sarebbe un falso positivo.

Ricorda

Probabilità che la classificazione BlueXP trovi ciò che dovrebbe. Ad esempio, un tasso di richiamo del 70% per i dati personali significa che la classificazione BlueXP può identificare 7 file su 10 che contengono effettivamente informazioni personali nella tua organizzazione. La classificazione di BlueXP non consentirebbe il 30% dei dati e non verrà visualizzata nella dashboard.

Stiamo costantemente migliorando la precisione dei nostri risultati. Tali miglioramenti saranno automaticamente disponibili nelle future release di classificazione BlueXP.

Tipo	Precisione	Ricorda
Dati personali - Generale	90%-95%	60%-80%
Dati personali - identificatori del Paese	30%-60%	40%-60%
Dati personali sensibili	80%-95%	20%-30%
Categorie	90%-97%	60%-80%

Esaminare i dati memorizzati nella propria organizzazione

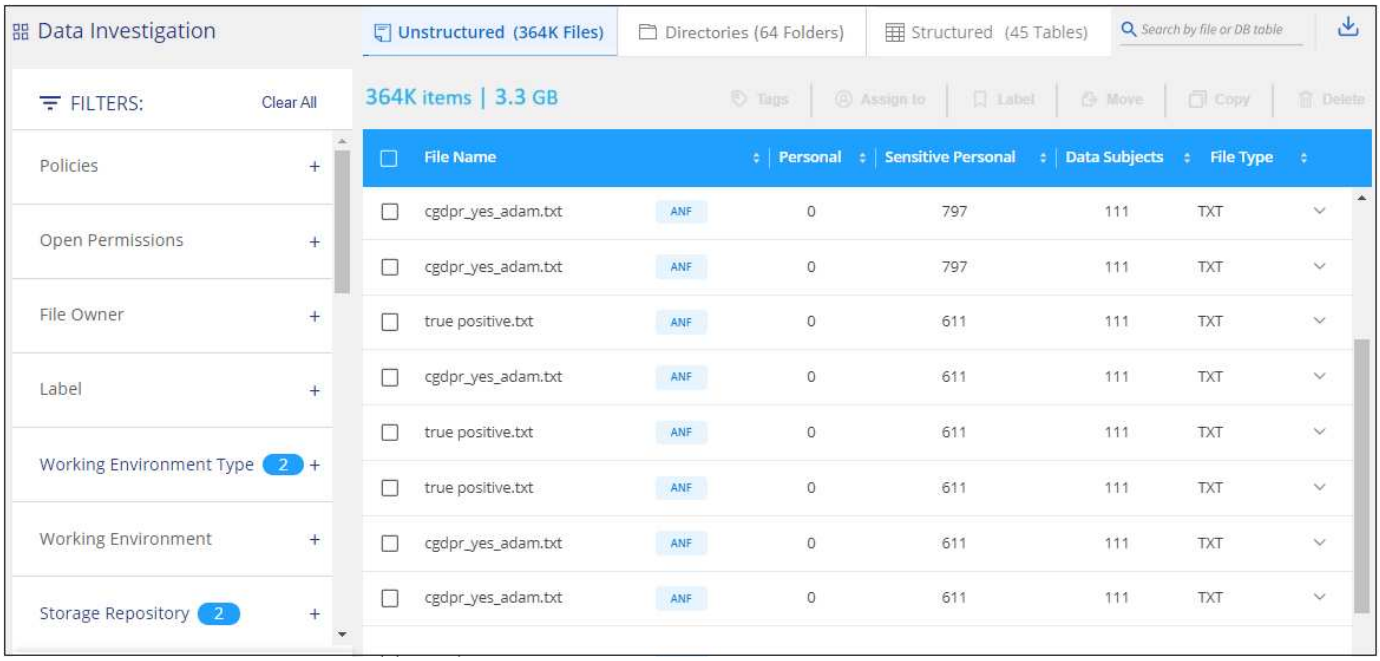
È possibile analizzare i dati dell'organizzazione visualizzando i dettagli nella pagina Data Investigation. È possibile accedere a questa pagina da molte aree dell'interfaccia utente di classificazione di BlueXP, tra cui le dashboard di governance e conformità.

> Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.

Filtrare i dati nella pagina analisi dati

È possibile filtrare il contenuto della pagina di analisi per visualizzare solo i risultati desiderati. Si tratta di una funzione molto potente, in quanto dopo aver perfezionato i dati, è possibile utilizzare la barra dei pulsanti nella parte superiore della pagina per eseguire una serie di azioni, tra cui la copia di file, lo spostamento di file, l'aggiunta di un tag o di un'etichetta AIP ai file e molto altro.

Se si desidera scaricare il contenuto della pagina come report dopo averlo perfezionato, fare clic su pulsante. Fare clic qui per ulteriori informazioni sul report Data Investigation.



- Le schede di livello superiore consentono di visualizzare i dati di file (dati non strutturati), directory (cartelle e condivisioni di file) o database (dati strutturati).
- I controlli nella parte superiore di ciascuna colonna consentono di ordinare i risultati in ordine numerico o

alfabetico.

- I filtri del riquadro sinistro consentono di perfezionare i risultati selezionando gli attributi descritti nelle sezioni successive.

Filtra i dati in base alla sensibilità e al contenuto

Utilizzare i seguenti filtri per visualizzare la quantità di informazioni sensibili contenute nei dati.

Filtro	Dettagli
Categoria	Selezionare "tipi di categorie".
Livello di sensibilità	Selezionare il livello di sensibilità: Personal (personale), Sensitive Personal (personale sensibile) o non Sensitive (non sensibile).
Numero di identificatori	Selezionare l'intervallo di identificatori sensibili rilevati per file. Include dati personali e dati personali sensibili. Durante il filtraggio nelle directory, la classificazione BlueXP totalizza le corrispondenze di tutti i file in ogni cartella (e sottocartelle). NOTA: La versione di dicembre 2023 (versione 1.26.6) ha temporaneamente rimosso l'opzione per calcolare il numero di dati personali identificabili (PII) per Directory.
Dati personali	Selezionare "tipi di dati personali".
Dati personali sensibili	Selezionare "tipi di dati personali sensibili".
Soggetto interessato	Inserire il nome completo o l'identificativo noto di un soggetto. "Scopri di più sugli argomenti dei dati qui".

Filtrare i dati in base al proprietario dell'utente e alle autorizzazioni dell'utente

Utilizzare i seguenti filtri per visualizzare i proprietari dei file e le autorizzazioni di accesso ai dati.

Filtro	Dettagli
Aprire permessi	Selezionare il tipo di permessi all'interno dei dati e all'interno di cartelle/condivisioni.
Autorizzazioni utente/gruppo	Selezionare uno o più nomi utente e/o nomi di gruppo oppure immettere un nome parziale.
Proprietario del file	Immettere il nome del proprietario del file.
Numero di utenti con accesso	Selezionare uno o più intervalli di categorie per visualizzare i file e le cartelle aperti a un determinato numero di utenti.

Filtrare i dati in base all'ora

Utilizzare i seguenti filtri per visualizzare i dati in base ai criteri temporali.

Filtro	Dettagli
Ora di creazione	Selezionare un intervallo di tempo in cui è stato creato il file. È inoltre possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca.

Filtro	Dettagli
Tempo scoperto	Selezionare un intervallo di tempo in cui la classificazione BlueXP ha rilevato il file. È inoltre possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca.
Ultima modifica	Selezionare un intervallo di tempo in cui il file è stato modificato per l'ultima volta. È inoltre possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca.
Ultimo accesso	Selezionare un intervallo di tempo in cui è stato eseguito l'ultimo accesso al file o alla directory (solo CIFS o NFS). È inoltre possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca. Per i tipi di file sottoposti a scansione dalla classificazione BlueXP, questa è l'ultima volta che la classificazione BlueXP ha sottoposto a scansione il file. Si noti che la classificazione BlueXP non estrae l'ultimo tempo di accesso dalle seguenti origini dati: SharePoint Online, SharePoint on-premise (SharePoint Server), OneDrive, Google Drive e Amazon S3.

Filtra i dati in base ai metadati

Utilizzare i seguenti filtri per visualizzare i dati in base alla posizione, alle dimensioni e alla directory o al tipo di file.

Filtro	Dettagli
Percorso del file	Immettere fino a 20 percorsi parziali o completi che si desidera includere o escludere dalla query. Se si immettono entrambi i percorsi di inclusione ed esclusione, la classificazione BlueXP individua prima tutti i file nei percorsi inclusi, quindi rimuove i file dai percorsi esclusi e visualizza i risultati. Si noti che l'utilizzo di "*" in questo filtro non ha alcun effetto e che non è possibile escludere cartelle specifiche dalla scansione: Verranno acquisite tutte le directory e i file presenti in una condivisione configurata.
Tipo di directory	Selezionare il tipo di directory; "Share" (Condividi) o "Folder" (cartella).
Tipo di file	Selezionare "tipi di file".
Dimensione del file	Selezionare l'intervallo di dimensioni del file.
Hash del file	Inserire l'hash del file per trovare un file specifico, anche se il nome è diverso.

Filtrare i dati in base al tipo di storage

Utilizzare i seguenti filtri per visualizzare i dati in base al tipo di storage.

Filtro	Dettagli
Tipo di ambiente di lavoro	Selezionare il tipo di ambiente di lavoro. OneDrive, SharePoint e Google Drive sono classificati in "App".
Nome dell'ambiente di lavoro	Selezionare ambienti di lavoro specifici.

Filtro	Dettagli
Repository di storage	Selezionare il repository di storage, ad esempio un volume o uno schema.

Filtra i dati in base a tag, etichette, utenti assegnati e policy

Utilizzare i seguenti filtri per visualizzare i dati in base alle etichette o ai tag AIP.

Filtro	Dettagli
Policy	Selezionare una o più policy. Vai "qui" per visualizzare l'elenco dei criteri esistenti e creare criteri personalizzati.
Etichetta	Selezionare "Etichette AIP" assegnati ai file.
Tag	Selezionare "il tag o i tag" assegnati ai file.
Assegnato a.	Selezionare il nome della persona a cui è assegnato il file.

Filtrare i dati in base allo stato dell'analisi

Utilizzare il seguente filtro per visualizzare i dati in base allo stato di scansione della classificazione BlueXP.

Filtro	Dettagli
Stato dell'analisi	Selezionare un'opzione per visualizzare l'elenco dei file in attesa di prima scansione, completati in scansione, in attesa di scansione o che non sono stati sottoposti a scansione.
Evento di analisi della scansione	Selezionare se si desidera visualizzare i file che non sono stati classificati perché la classificazione BlueXP non ha potuto ripristinare l'ultimo tempo di accesso o i file che sono stati classificati anche se la classificazione BlueXP non ha potuto ripristinare l'ultimo tempo di accesso.

"Vedere i dettagli sull'indicatore data/ora dell'ultimo accesso" Per ulteriori informazioni sugli elementi visualizzati nella pagina di analisi durante il filtraggio utilizzando l'evento di analisi scansione.

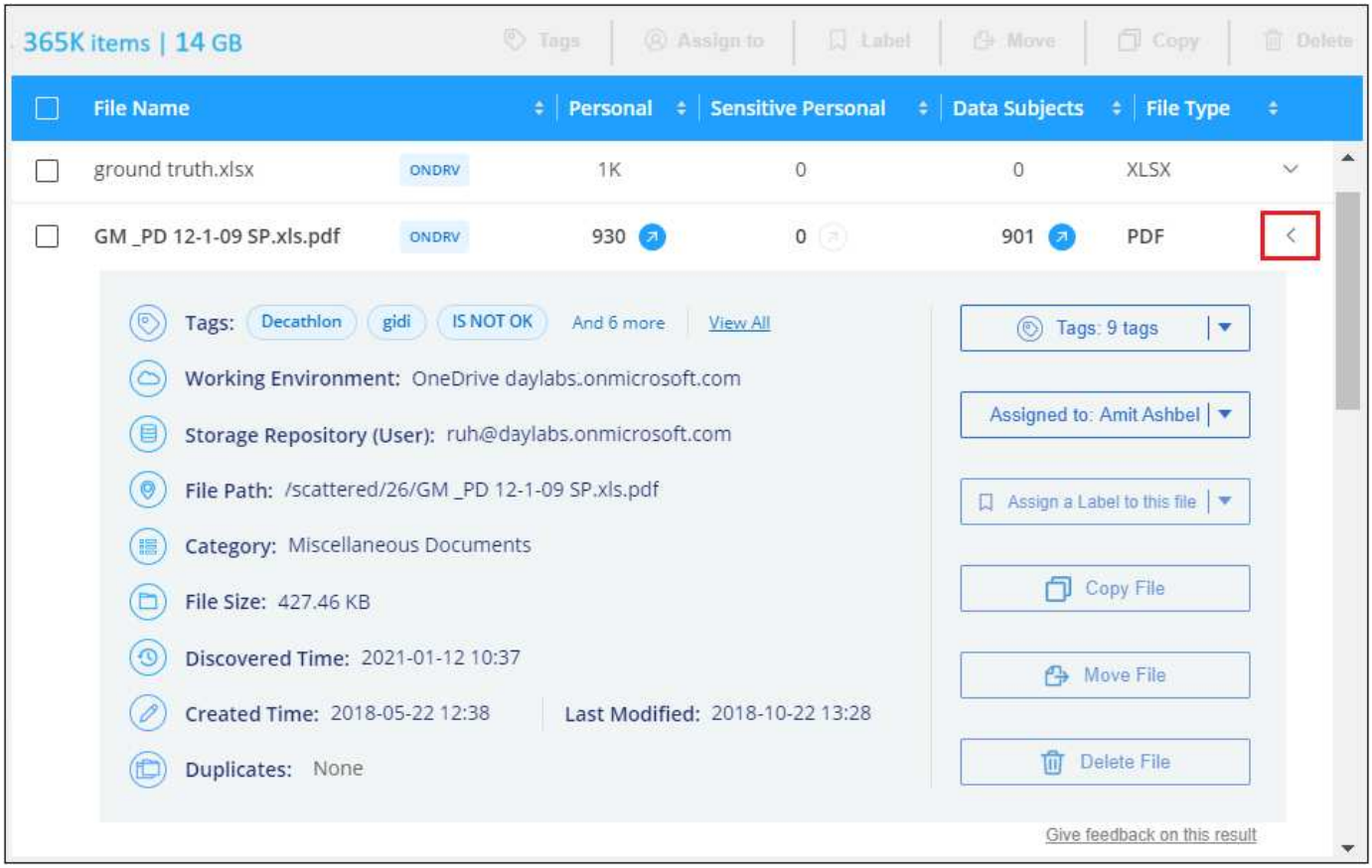
Filtra i dati in base ai duplicati

Utilizzare il seguente filtro per visualizzare i file duplicati nello storage.

Filtro	Dettagli
Duplicati	Selezionare se il file viene duplicato nei repository.

Visualizzare i metadati dei file

Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per visualizzare i metadati del file in un singolo file.



Oltre a mostrare l'ambiente di lavoro e il volume in cui si trova il file, i metadati mostrano molte più informazioni, tra cui le autorizzazioni del file, il proprietario del file, l'eventuale presenza di duplicati del file e l'etichetta AIP assegnata (se disponibile) "AIP integrato nella classificazione BlueXP"). Queste informazioni sono utili se stai pensando di "Creare policy" perché è possibile visualizzare tutte le informazioni che è possibile utilizzare per filtrare i dati.

Tenere presente che non tutte le informazioni sono disponibili per tutte le origini dati, ma solo quelle appropriate per tale origine. Ad esempio, il nome del volume, le autorizzazioni e le etichette AIP non sono rilevanti per i file di database.

Quando si visualizzano i dettagli di un singolo file, è possibile eseguire alcune operazioni sul file:

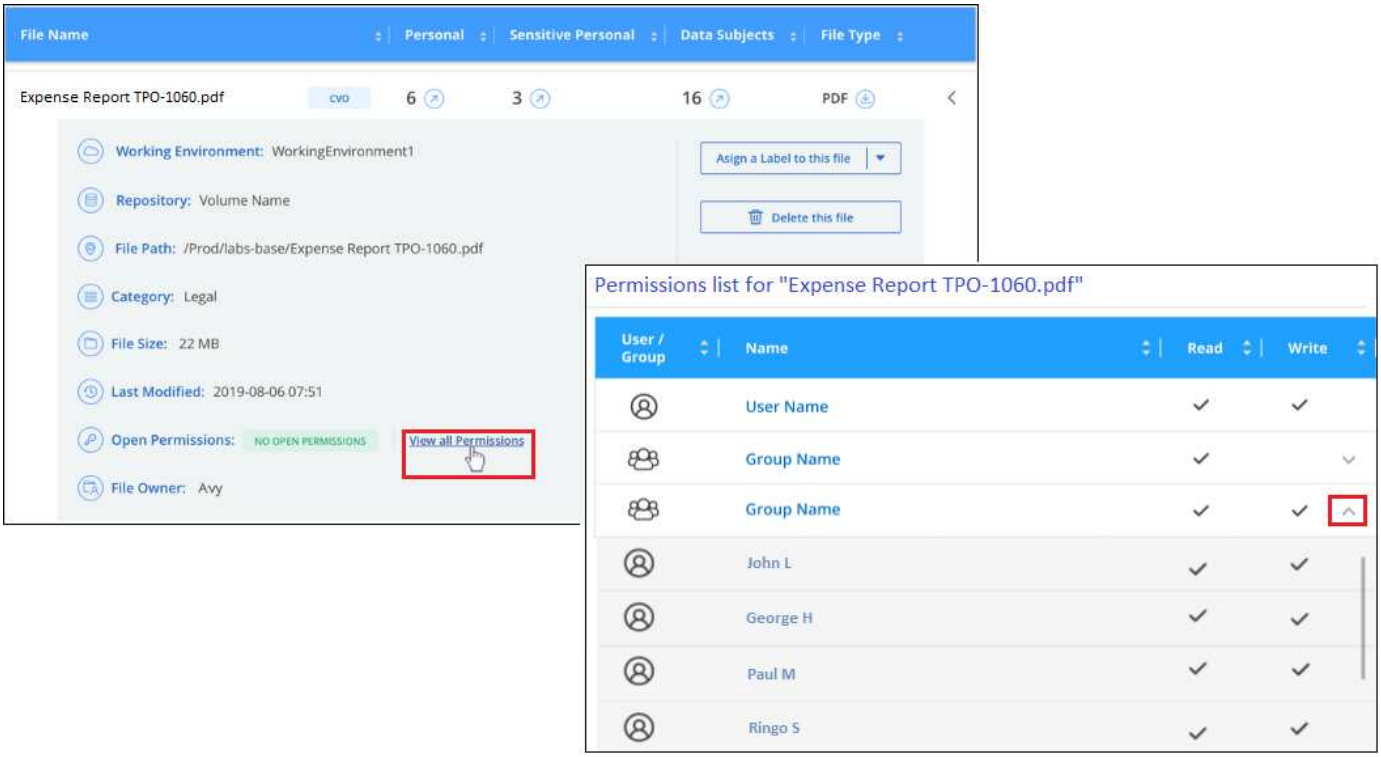
- È possibile spostare o copiare il file in qualsiasi condivisione NFS. Vedere "Spostamento dei file di origine in una condivisione NFS" e. "Copia dei file di origine in una condivisione NFS" per ulteriori informazioni.
- È possibile eliminare il file. Vedere "Eliminazione dei file di origine" per ulteriori informazioni.
- È possibile assegnare un determinato Stato al file. Vedere "Applicazione di tag" per ulteriori informazioni.
- È possibile assegnare il file a un utente BlueXP per essere responsabile di eventuali azioni di follow-up che devono essere eseguite sul file. Vedere "Assegnazione di utenti a un file" per ulteriori informazioni.
- Se sono state integrate etichette AIP con classificazione BlueXP, è possibile assegnare un'etichetta a questo file o modificarla se già esistente. Vedere "Assegnazione manuale delle etichette AIP" per ulteriori informazioni.

Visualizzare le autorizzazioni per file e directory

Per visualizzare un elenco di tutti gli utenti o gruppi che hanno accesso a un file o a una directory e i tipi di autorizzazioni di cui dispongono, fare clic su **Visualizza tutte le autorizzazioni**. Questo pulsante è disponibile

solo per i dati in condivisioni CIFS, SharePoint Online, SharePoint on-premise e OneDrive.

Si noti che se vengono visualizzati i SID (Security Identifier) invece dei nomi di utenti e gruppi, è necessario integrare Active Directory nella classificazione BlueXP. "Scopri come farlo".



Fare clic su ⌄ per consentire a qualsiasi gruppo di visualizzare l'elenco degli utenti che fanno parte del gruppo.

Inoltre, È possibile fare clic sul nome di un utente o di un gruppo e viene visualizzata la pagina di analisi con il nome dell'utente o del gruppo inserito nel filtro "User / Group Permissions" (autorizzazioni utente / gruppo), in modo da visualizzare tutti i file e le directory a cui l'utente o il gruppo ha accesso.

Verificare la presenza di file duplicati nei sistemi di storage

È possibile visualizzare se i file duplicati vengono memorizzati nei sistemi storage. Ciò è utile se si desidera identificare le aree in cui è possibile risparmiare spazio di storage. Può anche essere utile assicurarsi che alcuni file con autorizzazioni specifiche o informazioni sensibili non vengano duplicati inutilmente nei sistemi di storage.

Tutti i file (esclusi i database) di dimensioni pari o superiori a 1 MB e contenenti informazioni personali o riservate vengono confrontati per verificare se sono presenti duplicati. È possibile utilizzare i filtri della pagina di analisi "dimensione file" insieme a "duplicati" per vedere quali file di un determinato intervallo di dimensioni sono duplicati nell'ambiente in uso.

La classificazione BlueXP utilizza la tecnologia di hashing per determinare i file duplicati. Se un file ha lo stesso codice hash di un altro file, possiamo essere sicuri al 100% che i file siano duplicati esatti - anche se i nomi dei file sono diversi.

È possibile scaricare l'elenco dei file duplicati e inviarlo all'amministratore dello storage in modo che possa decidere quali file, se presenti, possono essere cancellati. Oppure è possibile "eliminare il file" se si è sicuri che non è necessaria una versione specifica del file.

Visualizzare tutti i file duplicati

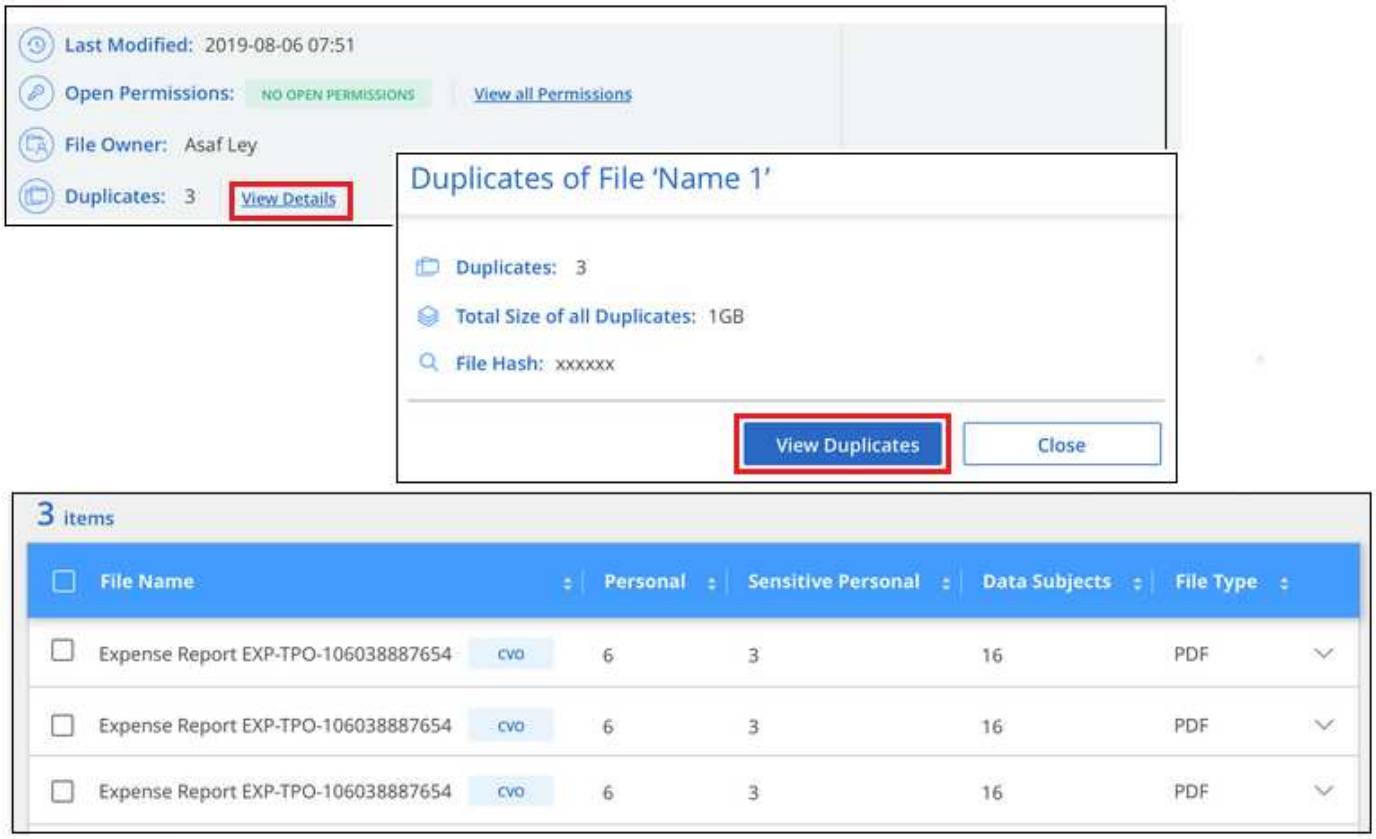
Se si desidera un elenco di tutti i file duplicati negli ambienti di lavoro e nelle origini dati in scansione, è possibile utilizzare il filtro **duplicati > ha duplicati** nella pagina analisi dati.

Tutti i file duplicati vengono visualizzati nella pagina risultati.

Visualizzare se un file specifico è duplicato

Se si desidera vedere se un singolo file ha duplicati, fare clic su nel riquadro risultati analisi dati ⌄ per visualizzare i metadati del file in un singolo file. Se sono presenti duplicati di un determinato file, queste informazioni vengono visualizzate accanto al campo *duplicati*.

Per visualizzare l'elenco dei file duplicati e la loro posizione, fare clic su **View Details** (Visualizza dettagli). Nella pagina successiva, fare clic su **View Duplicates** (Visualizza duplicati) per visualizzare i file nella pagina di analisi.



È possibile utilizzare il valore "hash del file" fornito in questa pagina e immetterlo direttamente nella pagina di analisi per cercare un file duplicato specifico in qualsiasi momento, oppure utilizzarlo in un criterio.

Report sull'analisi dei dati

Il Data Investigation Report (Report analisi dati) è un download del contenuto filtrato della pagina Data Investigation (analisi dati).

Il rapporto è disponibile in due formati diversi:

- Come file .CSV che è possibile salvare sul computer locale.

  Questo rapporto può includere un massimo di 10.000 righe di dati.

- Come file .JSON esportato in una condivisione NFS.

  Se sono presenti più di 250.000 righe di dati, vengono creati file .JSON aggiuntivi.

  Quando si esporta in una condivisione file, assicurarsi che la classificazione BlueXP disponga delle autorizzazioni corrette per l'accesso all'esportazione.

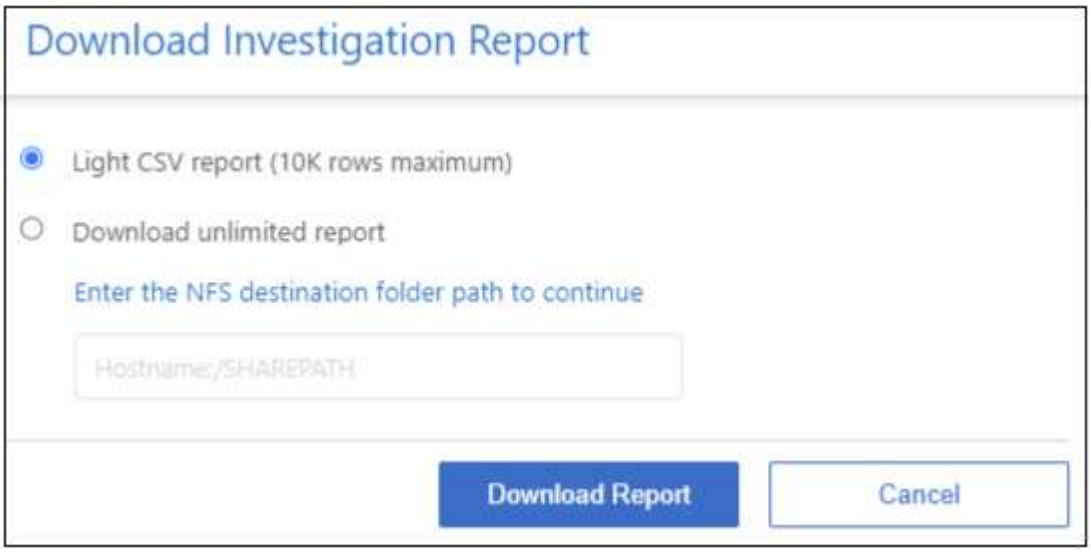
Se la classificazione BlueXP sta scansionando file (dati non strutturati), directory (cartelle e condivisioni di file) e database (dati strutturati), possono essere scaricati fino a tre file di report.

Generare il rapporto analisi dati

Fasi

1. Dalla pagina Data Investigation (analisi dati), fare clic su nella parte superiore destra della pagina.
2. Selezionare se si desidera scaricare un report .CSV o .JSON dei dati e fare clic su **Download Report**.

   Quando si seleziona un report .JSON, inserire il nome della condivisione NFS in cui verrà scaricato il report nel formato `<host_name>:/<share_path>`.



Risultato

Viene visualizzata una finestra di dialogo che indica che i report sono in fase di download.

È possibile visualizzare lo stato di avanzamento della generazione di report JSON in "Riquadro Actions Status (Stato azioni)".

Contenuto di ciascun report di analisi dei dati

Il **Report dati file non strutturati** include le seguenti informazioni sui file:

- Nome del file
- Tipo di ubicazione

- Nome dell’ambiente di lavoro
- Repository di storage (ad esempio, un volume, un bucket, condivisioni)
- Tipo di repository
- Percorso del file
- Tipo di file
- Dimensioni file (in MB)
- Ora di creazione
- Ultima modifica
- Ultimo accesso
- Proprietario del file
- Categoria
- Informazioni personali
- Informazioni personali sensibili
- Autorizzazioni aperte
- Errore analisi scansione
- Data di rilevamento dell’eliminazione

  Una data di rilevamento dell’eliminazione identifica la data in cui il file è stato cancellato o spostato. In questo modo è possibile identificare quando sono stati spostati file sensibili. I file cancellati non fanno parte del numero di file visualizzato nella dashboard o nella pagina di analisi. I file vengono visualizzati solo nei report CSV.

Il **Report dati directory non strutturate** include le seguenti informazioni relative alle cartelle e alle condivisioni di file:

- Tipo di ambiente di lavoro
- Nome dell’ambiente di lavoro
- Nome directory
- Repository di storage (ad esempio, una cartella o condivisioni di file)
- Proprietario directory
- Ora di creazione
- Tempo scoperto
- Ultima modifica
- Ultimo accesso
- Autorizzazioni aperte
- Tipo di directory

Il **Structured Data Report** include le seguenti informazioni sulle tabelle di database:

- DB Nome tabella
- Tipo di ubicazione

- Nome dell'ambiente di lavoro
- Repository di storage (ad esempio, uno schema)
- Numero di colonne
- Numero di righe
- Informazioni personali
- Informazioni personali sensibili

Organizzare i dati privati

La classificazione BlueXP offre diversi modi per gestire e organizzare i dati privati. In questo modo è più semplice visualizzare i dati più importanti per te.

- Se si è abbonati a. "Azure Information Protection (AIP)" Per classificare e proteggere i file, è possibile utilizzare la classificazione BlueXP per gestire le etichette AIP.

> La release di dicembre 2023 (v1.26.6) ha temporaneamente rimosso l'opzione di integrare i dati utilizzando le etichette AIP (Azure Information Protection).

- È possibile aggiungere tag ai file che si desidera contrassegnare per l'organizzazione o per alcuni tipi di follow-up.
- È possibile assegnare un utente BlueXP a un file specifico o a più file, in modo che la persona possa essere responsabile della gestione del file.
- Utilizzando la funzionalità "Policy" è possibile creare query di ricerca personalizzate in modo da visualizzare facilmente i risultati facendo clic su un pulsante.
- È possibile inviare avvisi e-mail agli utenti di BlueXP o a qualsiasi altro indirizzo e-mail, quando alcuni criteri critici restituiscono risultati.

> Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.

È necessario utilizzare tag o etichette?

Di seguito è riportato un confronto tra il tag di classificazione BlueXP e l'etichettatura Azure Information Protection.

Tag	Etichette
I tag di file sono parte integrante della classificazione BlueXP.	Richiede l'iscrizione a Azure Information Protection (AIP).
Il tag viene conservato solo nel database di classificazione BlueXP e non viene scritto nel file. Il file non viene modificato, né il file a cui si accede o modificato.	L'etichetta fa parte del file e quando l'etichetta cambia, il file cambia. Questa modifica modifica modifica modifica anche i tempi di accesso e modifica del file.
È possibile avere più tag su un singolo file.	È possibile avere un'etichetta su un singolo file.

Tag	Etichette
Il tag può essere utilizzato per l'azione di classificazione interna di BlueXP, come copia, spostamento, eliminazione, esecuzione di un criterio, ecc.	Altri sistemi in grado di leggere il file possono vedere l'etichetta, che può essere utilizzata per un'ulteriore automazione.
Viene utilizzata solo una singola chiamata API per verificare se un file ha un tag.	

Categorizzare i dati utilizzando le etichette AIP

È possibile gestire le etichette AIP nei file che la classificazione BlueXP sta analizzando, se si è abbonati "Azure Information Protection (AIP)". AIP consente di classificare e proteggere documenti e file applicando etichette ai contenuti. La classificazione BlueXP consente di visualizzare le etichette già assegnate ai file, aggiungere etichette ai file e modificare le etichette quando esiste già un'etichetta.

La classificazione BlueXP supporta le etichette AIP nei seguenti tipi di file: .DOC, .DOCX, .PDF, .PPTX, .XLS, XLSX.

- Al momento non è possibile modificare le etichette in file di dimensioni superiori a 30 MB. Per gli account OneDrive, SharePoint e Google Drive, la dimensione massima del file è di 4 MB.
- Se un file ha un'etichetta che non esiste più in AIP, la classificazione BlueXP lo considera come un file senza un'etichetta.
- Se la classificazione BlueXP è stata implementata in un'area governativa o in una posizione on-premise che non dispone di accesso a Internet (nota anche come sito oscuro), la funzionalità dell'etichetta AIP non è disponibile.

Integrare le etichette AIP nell'area di lavoro

Prima di poter gestire le etichette AIP, è necessario integrare la funzionalità dell'etichetta AIP nella classificazione BlueXP accedendo all'account Azure esistente. Una volta attivata, è possibile gestire le etichette AIP all'interno dei file per tutti "origini dati" Nello spazio di lavoro BlueXP.

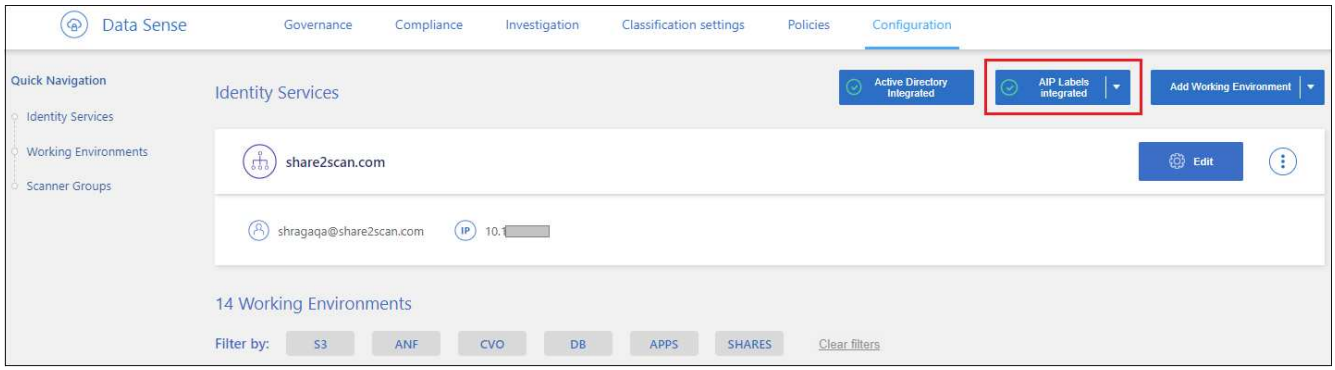
Requisiti

- È necessario disporre di un account e di una licenza di Azure Information Protection.
- È necessario disporre delle credenziali di accesso per l'account Azure.
- Se intendi modificare le etichette nei file che risiedono nei bucket Amazon S3, assicurati che l'autorizzazione sia `s3:PutObject` È incluso nel ruolo IAM. Vedere "Impostazione del ruolo IAM".

Fasi

1. Dalla pagina di configurazione della classificazione BlueXP, fare clic su **integra etichette AIP**.

2. Nella finestra di dialogo integra etichette AIP, fare clic su **Accedi ad Azure**.
3. Nella pagina Microsoft visualizzata, selezionare l'account e immettere le credenziali richieste.
4. Tornare alla scheda classificazione BlueXP e viene visualizzato il messaggio "*AIP Labels Were successfully Integrated with the account <account_name>*" (le etichette AIP sono state integrate correttamente con l'account BlueXP_).
5. Fare clic su **Close** (Chiudi) per visualizzare il testo *AIP Labels Integrated* (etichette AIP integrate) nella parte superiore della pagina.



Risultato

È possibile visualizzare e assegnare le etichette AIP dal riquadro dei risultati della pagina di analisi. È inoltre possibile assegnare etichette AIP ai file utilizzando i criteri.

Visualizzare le etichette AIP nei file

È possibile visualizzare l'etichetta AIP corrente assegnata a un file.

Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per espandere i dettagli dei metadati del file.

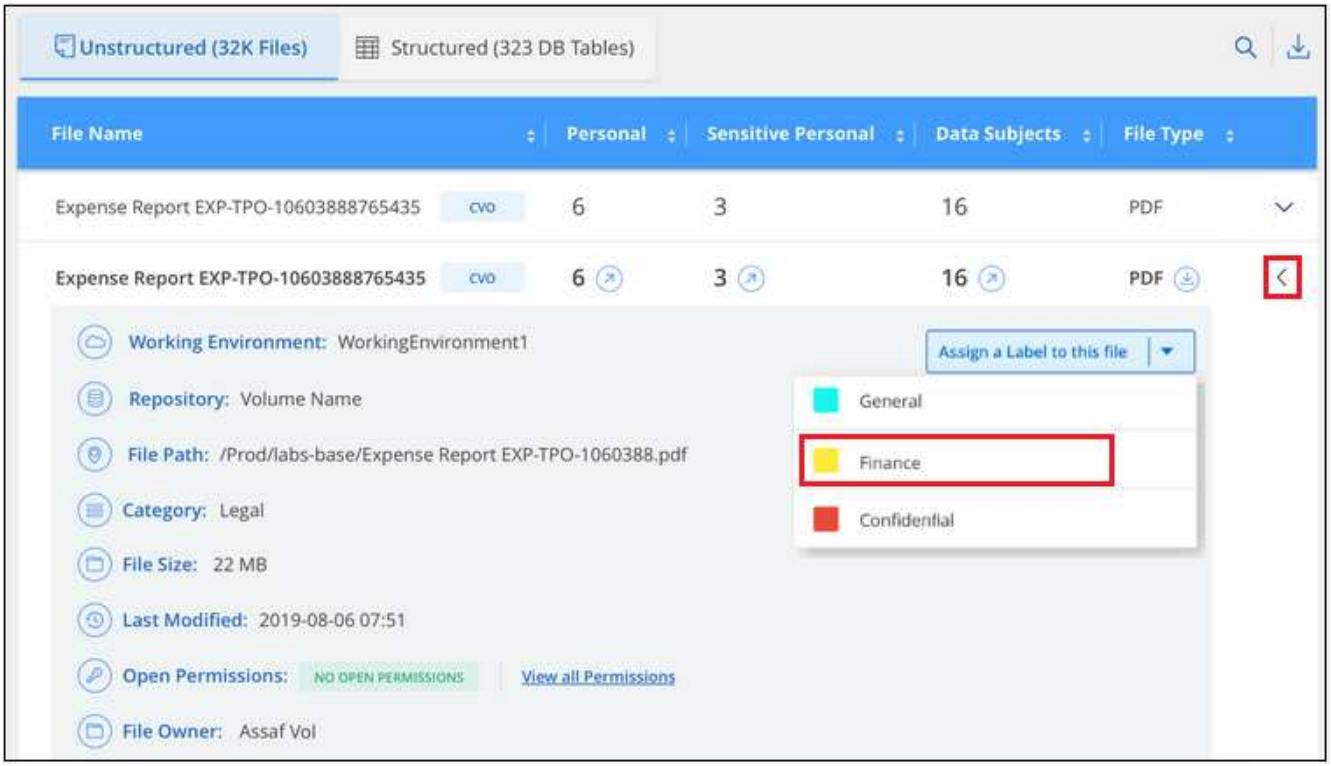
Assegnare manualmente le etichette AIP

È possibile aggiungere, modificare e rimuovere le etichette AIP dai file utilizzando la classificazione BlueXP.

Per assegnare un'etichetta AIP a un singolo file, procedere come segue.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per espandere i dettagli dei metadati del file.



2. Fare clic su **Assegna un'etichetta a questo file**, quindi selezionare l'etichetta.

   L'etichetta viene visualizzata nei metadati del file.

Per assegnare un'etichetta AIP a più file, procedere come segue. Nota: È possibile assegnare un'etichetta AIP a un massimo di 20 file alla volta (una pagina nell'interfaccia utente).

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da etichettare.

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (☑ Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (☑ File Name).

2. Dalla barra dei pulsanti, fare clic su **etichetta** e selezionare l'etichetta AIP:

L'etichetta AIP viene aggiunta ai metadati di tutti i file selezionati.

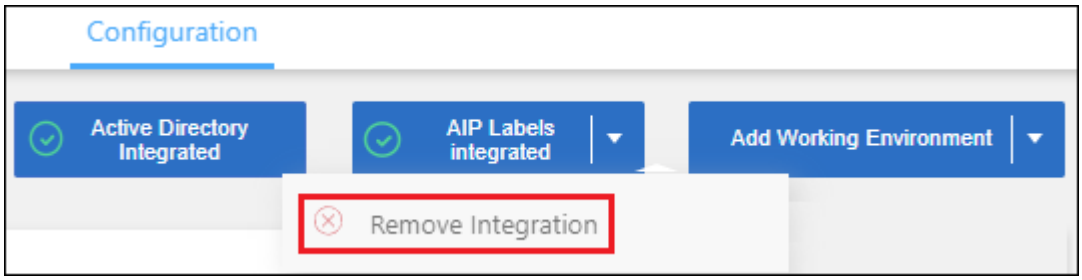
Rimuovere l'integrazione AIP

Se non si desidera più gestire le etichette AIP nei file, è possibile rimuovere l'account AIP dall'interfaccia di classificazione BlueXP.

Si noti che non vengono apportate modifiche alle etichette aggiunte utilizzando la classificazione BlueXP. Le etichette presenti nei file rimarranno quelle attualmente esistenti.

Fasi

1. Dalla pagina *Configuration*, fare clic su **AIP Labels Integrated > Remove Integration** (etichette AIP integrate > Rimuovi integrazione).



2. Fare clic su **Remove Integration** (Rimuovi integrazione) nella finestra di dialogo di conferma.

Applicare i tag per gestire i file digitalizzati

È possibile aggiungere un tag ai file che si desidera contrassegnare per alcuni tipi di follow-up. Ad esempio, è possibile che siano stati trovati alcuni file duplicati e si desidera eliminarne uno, ma è necessario controllare quale file eliminare. È possibile aggiungere un tag "Check to delete" al file in modo da sapere che questo file richiede una ricerca e un qualche tipo di azione futura.

La classificazione BlueXP consente di visualizzare i tag assegnati ai file, aggiungere o rimuovere tag dai file e modificare il nome o eliminare un tag esistente.

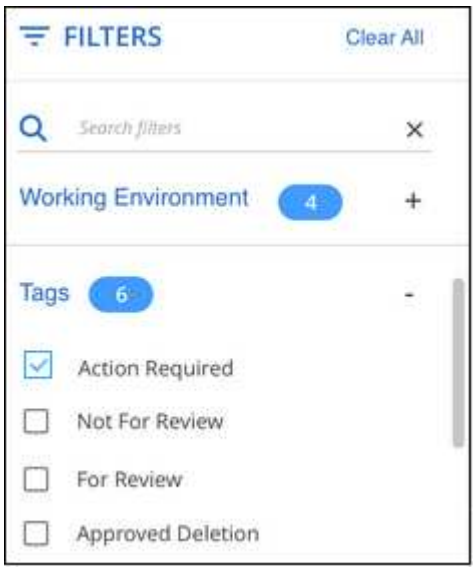
Tenere presente che il tag non viene aggiunto al file allo stesso modo in cui le etichette AIP fanno parte dei metadati del file. Il tag è appena visto dagli utenti di BlueXP che utilizzano la classificazione BlueXP in modo da poter vedere se un file deve essere cancellato o controllato per un certo tipo di follow-up.

I tag assegnati ai file nella classificazione BlueXP non sono correlati ai tag che è possibile aggiungere alle risorse, come volumi o istanze di macchine virtuali. I tag di classificazione BlueXP vengono applicati a livello di file.

Consente di visualizzare i file a cui sono stati applicati determinati tag

È possibile visualizzare tutti i file con tag specifici assegnati.

1. Fare clic sulla scheda **Investigation** dalla classificazione BlueXP.
2. Nella pagina Data Investigation (analisi dati), fare clic su **Tags** nel riquadro Filters (filtri), quindi selezionare i tag richiesti.



Il riquadro dei risultati dell'analisi visualizza tutti i file a cui sono stati assegnati i tag.

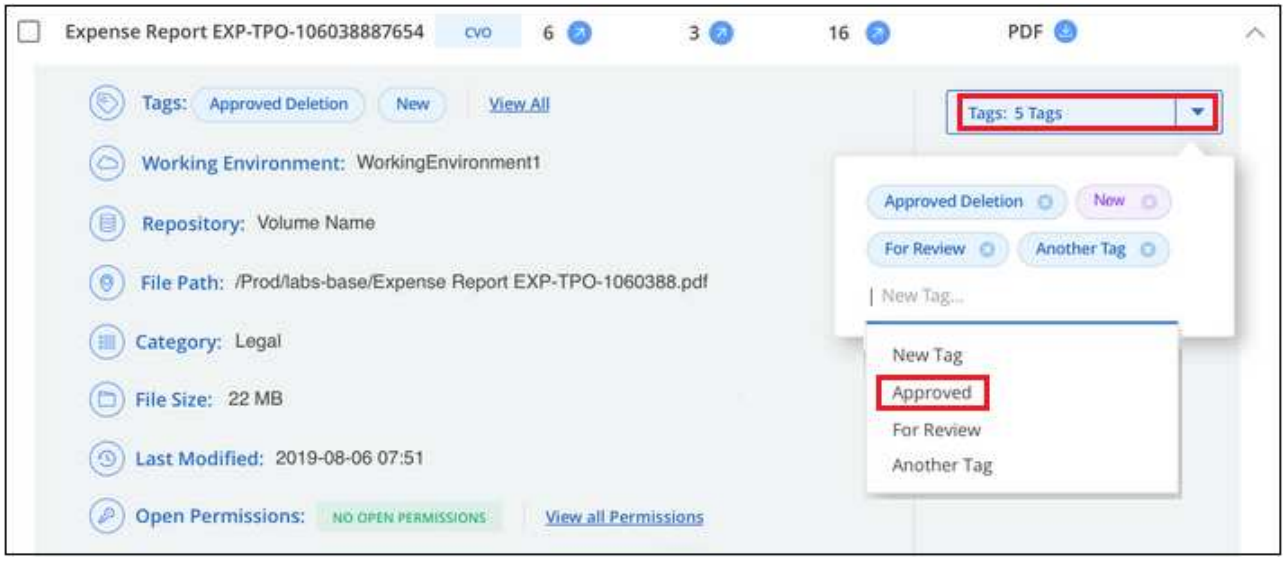
Assegnare tag ai file

È possibile aggiungere tag a un singolo file o a un gruppo di file.

Per aggiungere un tag a un singolo file:

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per espandere i dettagli dei metadati del file.
2. Fare clic sul campo **Tag** per visualizzare i tag attualmente assegnati.
3. Aggiungere il tag o i tag:
   - Per assegnare un tag esistente, fare clic nel campo **New Tag…** e iniziare a digitare il nome del tag. Quando viene visualizzato il tag desiderato, selezionarlo e premere **Invio**.
   - Per creare un nuovo tag e assegnarlo al file, fare clic nel campo **New Tag…**, inserire il nome del nuovo tag e premere **Invio**.



Il tag viene visualizzato nei metadati del file.

Per aggiungere un tag a più file:

Fasi

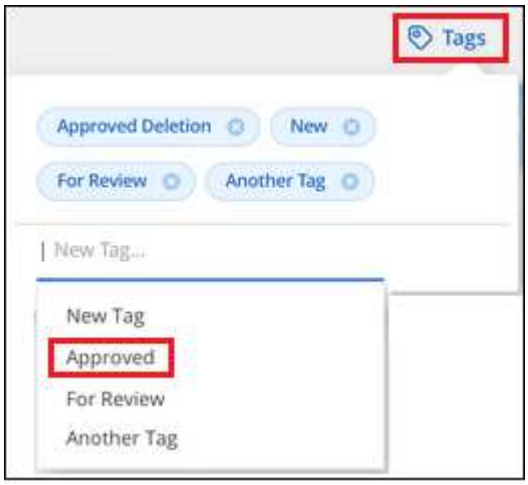
1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da contrassegnare.

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
   - Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All **20** Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.

     È possibile applicare tag a un massimo di 100.000 file alla volta.

2. Dalla barra dei pulsanti, fare clic su **Tag** per visualizzare i tag attualmente assegnati.
3. Aggiungere il tag o i tag:
   - Per assegnare un tag esistente, fare clic nel campo **New Tag…** e iniziare a digitare il nome del tag. Quando viene visualizzato il tag desiderato, selezionarlo e premere **Invio**.

- Per creare un nuovo tag e assegnarlo al file, fare clic nel campo **New Tag…**, inserire il nome del nuovo tag e premere **Invio**.



4. Approva l'aggiunta dei tag nella finestra di dialogo di conferma e i tag vengono aggiunti ai metadati per tutti i file selezionati.

Eliminare i tag dai file

Puoi eliminare un tag se non ne hai più bisogno.

Fare clic sulla * x* per un tag esistente.

Se sono stati selezionati più file, il tag viene rimosso da tutti i file.

Assegnare agli utenti la gestione di determinati file

È possibile assegnare un utente BlueXP a un file specifico o a più file, in modo che la persona possa essere responsabile di eventuali azioni di follow-up che devono essere eseguite sul file. Questa funzionalità viene spesso utilizzata con la funzione per aggiungere tag di stato personalizzati a un file.

Ad esempio, è possibile che il file contenga alcuni dati personali che consentono a troppi utenti di accedere in lettura e scrittura (autorizzazioni aperte). È quindi possibile assegnare il tag di stato "Change permissions" e assegnare questo file all'utente "Joan Smith" in modo che possa decidere come risolvere il problema. Una volta risolto il problema, è possibile modificare il tag Status (Stato) in "Completed" (completato).

Si noti che il nome utente non viene aggiunto al file come parte dei metadati del file, ma viene visualizzato solo dagli utenti BlueXP quando si utilizza la classificazione BlueXP.

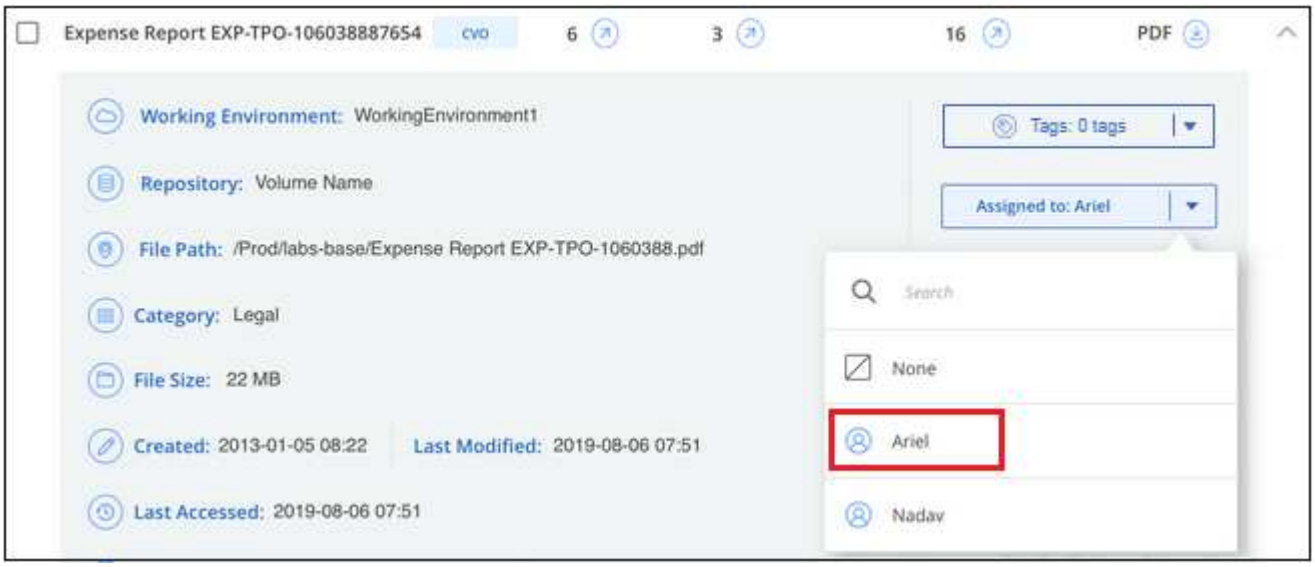
Un nuovo filtro nella pagina di analisi consente di visualizzare facilmente tutti i file con la stessa persona nel campo "assegnato a".

Per assegnare un utente a un singolo file, procedere come segue.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per espandere i dettagli dei metadati del file.

2. Fare clic sul campo **assegnato a** e selezionare il nome utente.



Il nome utente viene visualizzato nei metadati del file.

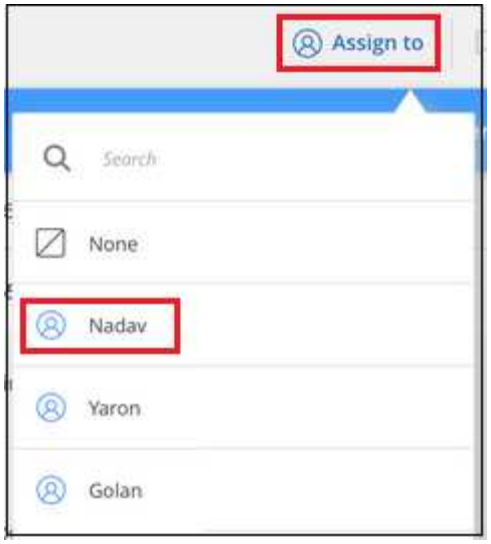
Per assegnare un utente a più file, procedere come segue. Nota: È possibile assegnare un utente a un massimo di 20 file alla volta (una pagina nell'interfaccia utente).

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file che si desidera assegnare a un utente.

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).

2. Dalla barra dei pulsanti, fare clic su **Assegna a** e selezionare il nome utente:



L'utente viene aggiunto ai metadati per tutti i file selezionati.

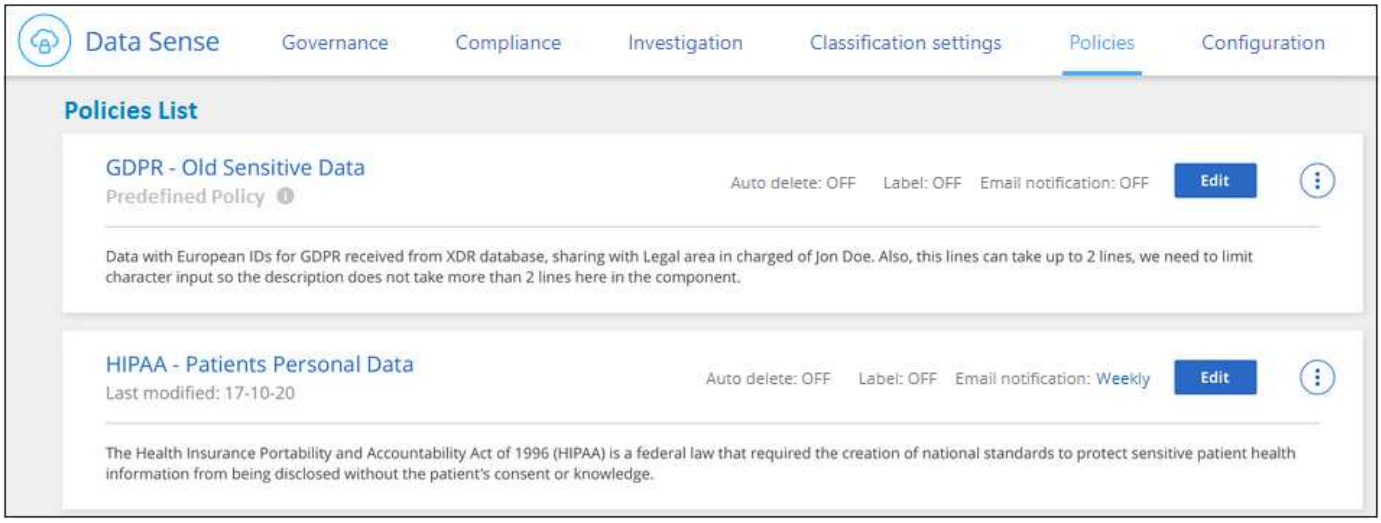
Assegnare policy ai dati

Le policy sono come un elenco preferito di filtri personalizzati che forniscono i risultati della ricerca nella pagina di analisi per le query di conformità più frequenti. La classificazione BlueXP offre una serie di policy predefinite basate sulle richieste più comuni dei clienti. È possibile creare policy personalizzate che forniscano risultati per ricerche specifiche della propria organizzazione.

Le policy offrono le seguenti funzionalità:

- Policy predefinite NetApp in base alle richieste degli utenti
- Possibilità di creare policy personalizzate
- Aprire la pagina delle analisi con i risultati delle policy in un click
- Invia avvisi e-mail agli utenti BlueXP o a qualsiasi altro indirizzo e-mail, quando alcune policy critiche restituiscono risultati, in modo da poter ricevere notifiche per proteggere i tuoi dati
- Assegnare automaticamente le etichette AIP (Azure Information Protection) a tutti i file che corrispondono ai criteri definiti in una policy
- Elimina automaticamente i file (una volta al giorno) quando alcune policy restituiscono risultati, in modo da proteggere automaticamente i dati

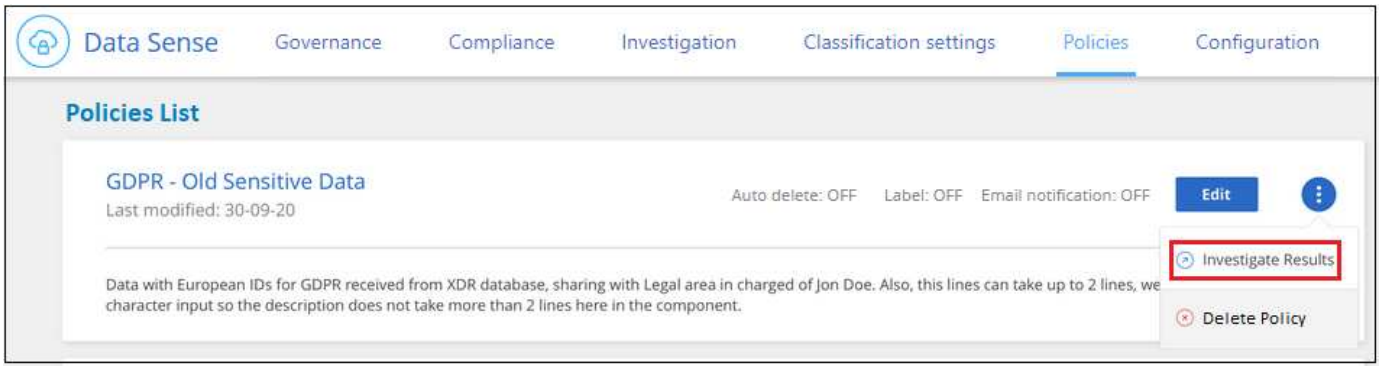
La scheda **Policies** nella dashboard di conformità elenca tutti i criteri predefiniti e personalizzati disponibili in questa istanza della classificazione BlueXP.



Inoltre, i criteri vengono visualizzati nell'elenco dei filtri della pagina di analisi.

Visualizzare i risultati dei criteri nella pagina di analisi

Per visualizzare i risultati di un criterio nella pagina analisi, fare clic su ⋮ Per una policy specifica, quindi selezionare **esamina risultati**.



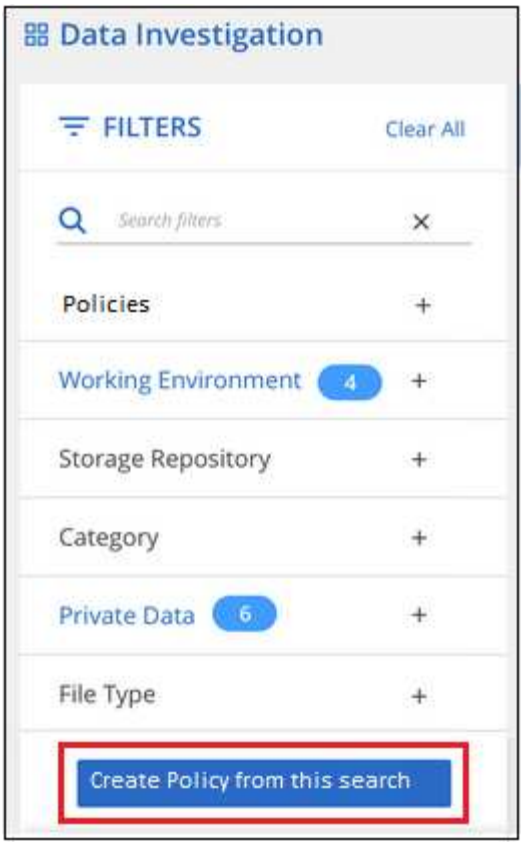
Creare criteri personalizzati

È possibile creare policy personalizzate che forniscano risultati per le ricerche specifiche della propria organizzazione. I risultati vengono restituiti per tutti i file e le directory (condivisioni e cartelle) che corrispondono ai criteri di ricerca.

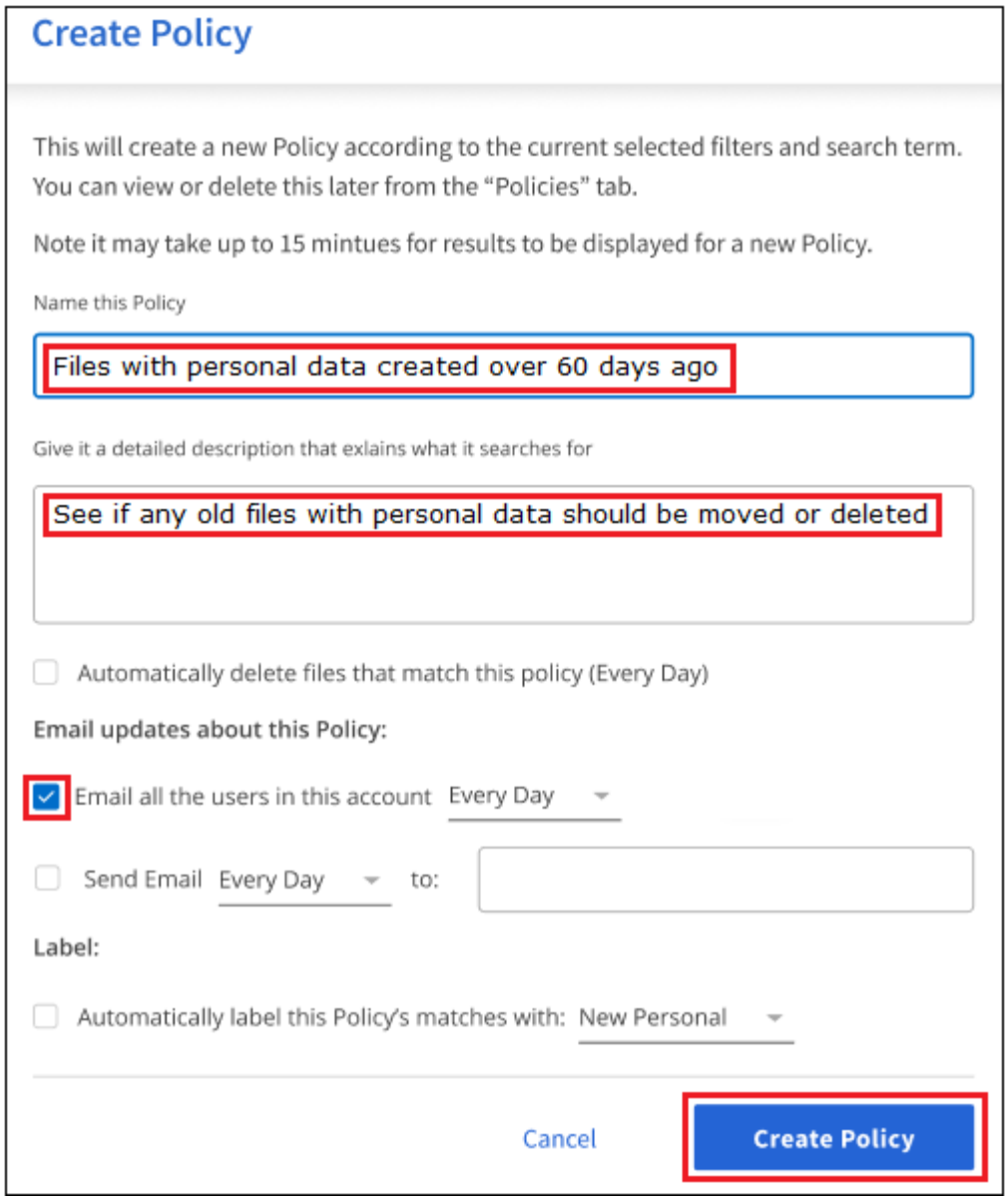
Tenere presente che le azioni per l'eliminazione dei dati e l'assegnazione delle etichette AIP in base ai risultati dei criteri sono valide solo per i file. Le directory che corrispondono ai criteri di ricerca non possono essere eliminate automaticamente o assegnate etichette AIP.

Fasi

1. Dalla pagina Data Investigation (analisi dati), definire la ricerca selezionando tutti i filtri che si desidera utilizzare. Vedere "Filtraggio dei dati nella pagina Data Investigation" per ulteriori informazioni.
2. Una volta che tutte le caratteristiche del filtro sono esattamente come desiderate, fare clic su **Create Policy from this search** (Crea policy da questa ricerca).



3. Assegnare un nome al criterio e selezionare altre azioni che possono essere eseguite dal criterio:
   a. Immettere un nome e una descrizione univoci.
   b. Se si desidera, selezionare la casella per eliminare automaticamente i file che corrispondono ai parametri del criterio. Scopri di più eliminazione dei file di origine mediante un criterio.
   c. Se si desidera inviare e-mail di notifica agli utenti BlueXP nell'account, selezionare la casella di controllo e scegliere l'intervallo di invio dell'e-mail. Scopri di più invio di avvisi e-mail in base ai risultati della policy.
   d. Se si desidera, selezionare la casella se si desidera che le e-mail di notifica vengano inviate ad altri utenti, immettere fino a 20 indirizzi e-mail e scegliere l'intervallo di invio dell'e-mail.
   e. Se si desidera, selezionare la casella per assegnare automaticamente le etichette AIP ai file che corrispondono ai parametri del criterio, quindi selezionare l'etichetta. (Solo se sono già state integrate le etichette AIP. Scopri di più "Etichette AIP".)
   f. Fare clic su **Crea policy**.



Risultato

Il nuovo criterio viene visualizzato nella scheda Criteri.

Invia avvisi e-mail quando vengono trovati dati non conformi

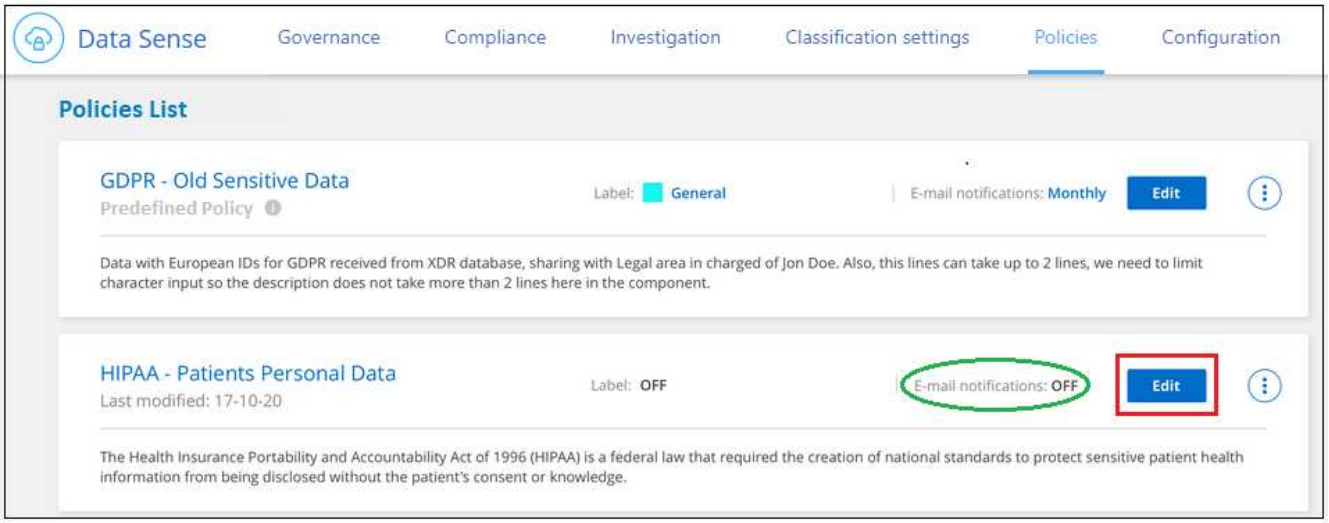
La classificazione BlueXP può inviare avvisi e-mail agli utenti BlueXP del tuo account quando alcune policy critiche restituiscono risultati, in modo da poter ricevere notifiche per proteggere i tuoi dati. È possibile scegliere di inviare le notifiche via email su base giornaliera, settimanale o mensile. Puoi anche scegliere di inviare avvisi e-mail a qualsiasi altro indirizzo e-mail (fino a 20 indirizzi e-mail) non presente nell'account BlueXP.

È possibile configurare questa impostazione quando si crea il criterio o quando si modifica un criterio.

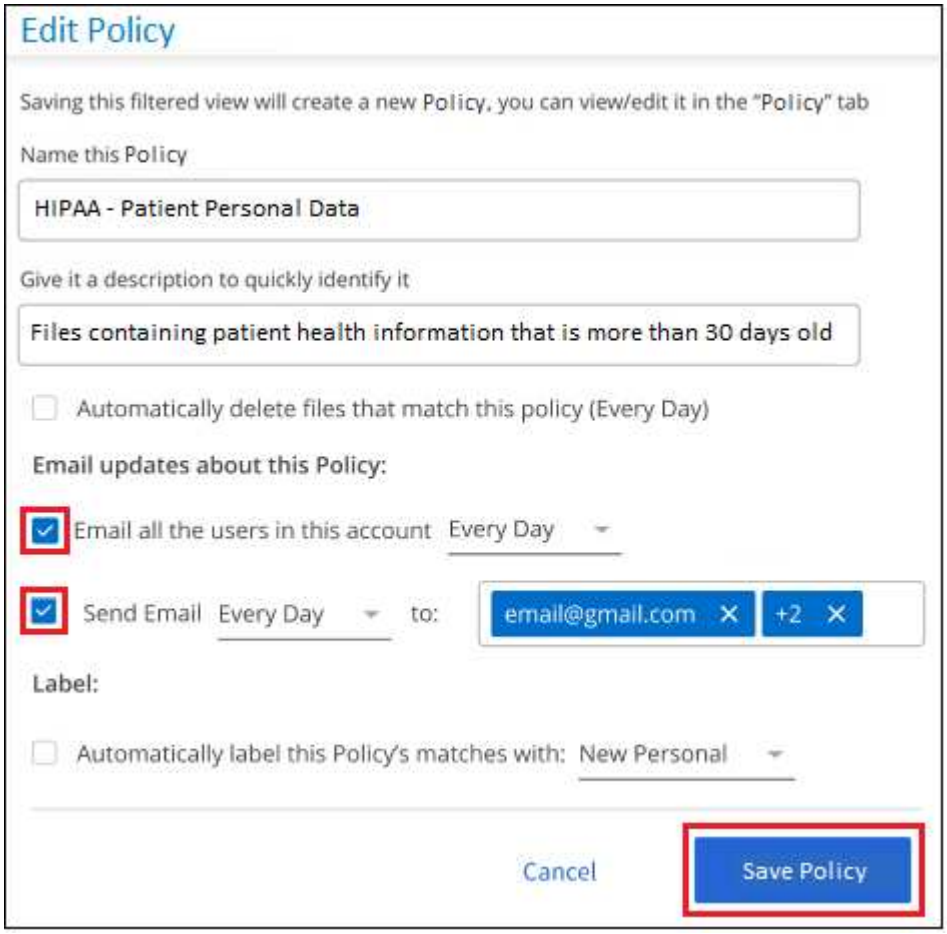
Per aggiungere aggiornamenti e-mail a una policy esistente, procedere come segue.

Fasi

1. Nella pagina elenco criteri, fare clic su **Modifica** per il criterio in cui si desidera aggiungere (o modificare) le impostazioni di posta elettronica.



2. Nella pagina Edit Policy (Modifica policy):
   a. Selezionare la casella "Email all the users in this account" (Invia tutti gli utenti di questo account) se si desidera inviare e-mail di notifica agli utenti dell'account BlueXP e scegliere l'intervallo di invio dell'e-mail (ad esempio, **Every Day**).
   b. Selezionare la casella "Send Email" (Invia e-mail) se si desidera inviare e-mail di notifica ad altri utenti, scegliere l'intervallo di invio e inserire fino a 20 indirizzi e-mail.



3. Fare clic su **Save Policy** (Salva policy) per visualizzare l'intervallo di invio del messaggio nella descrizione del criterio.

Risultato

La prima e-mail viene inviata ora se ci sono risultati dalla policy, ma solo se alcuni file soddisfano i criteri della policy. Non vengono inviate informazioni personali nelle e-mail di notifica. Il messaggio di posta elettronica indica la presenza di file che corrispondono ai criteri del criterio e fornisce un collegamento ai risultati del criterio.

Eliminare automaticamente i file di origine utilizzando i criteri

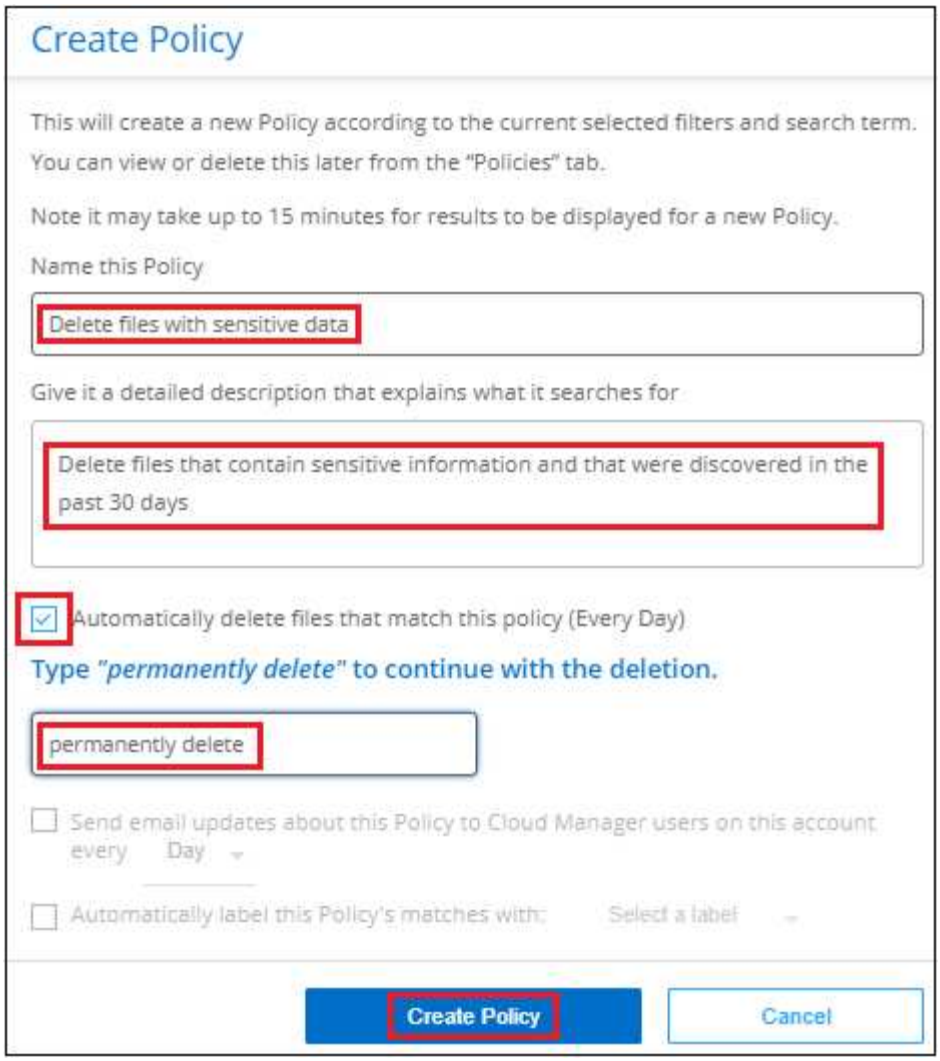
È possibile creare un criterio personalizzato per eliminare i file corrispondenti al criterio. Ad esempio, è possibile eliminare i file che contengono informazioni riservate e che sono stati rilevati dalla classificazione BlueXP negli ultimi 30 giorni.

Solo gli account Admins possono creare una policy per eliminare automaticamente i file.

> Tutti i file che corrispondono alla policy verranno eliminati definitivamente una volta al giorno.

Fasi

1. Dalla pagina Data Investigation (analisi dati), definire la ricerca selezionando tutti i filtri che si desidera utilizzare. Vedere "Filtraggio dei dati nella pagina Data Investigation" per ulteriori informazioni.
2. Una volta che tutte le caratteristiche del filtro sono esattamente come desiderate, fare clic su **Create Policy from this search** (Crea policy da questa ricerca).
3. Assegnare un nome al criterio e selezionare altre azioni che possono essere eseguite dal criterio:
   a. Immettere un nome e una descrizione univoci.
   b. Selezionare la casella "Elimina automaticamente i file corrispondenti a questa policy" e digitare **Elimina definitivamente** per confermare che si desidera che i file vengano eliminati in modo permanente da questa policy.
   c. Fare clic su **Crea policy**.



Risultato

Il nuovo criterio viene visualizzato nella scheda Criteri. I file che corrispondono al criterio vengono cancellati una volta al giorno quando il criterio viene eseguito.

È possibile visualizzare l'elenco dei file che sono stati eliminati in "Riquadro Actions Status (Stato azioni)".

Assegnare automaticamente le etichette AIP con i criteri

È possibile assegnare un'etichetta AIP a tutti i file che soddisfano i criteri del criterio. È possibile specificare l'etichetta AIP durante la creazione del criterio oppure aggiungerla quando si modifica un criterio.

Le etichette vengono aggiunte o aggiornate continuamente nei file mentre la classificazione BlueXP esegue la scansione dei file.

A seconda che un'etichetta sia già applicata a un file e del livello di classificazione dell'etichetta, quando si modifica un'etichetta vengono eseguite le seguenti azioni:

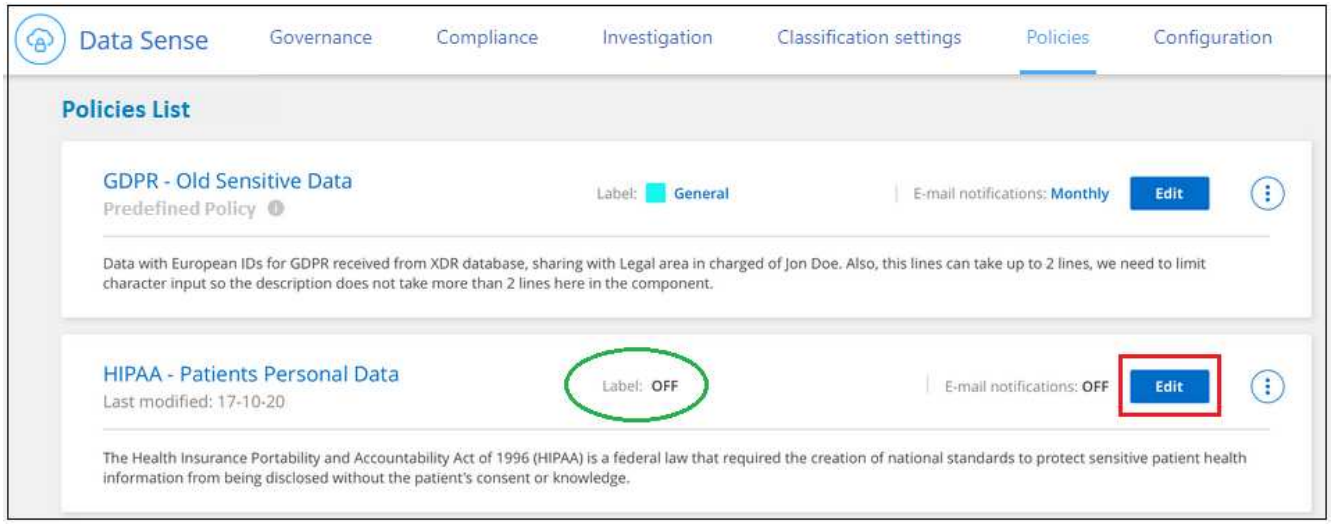
Se il file…	Quindi…
Non ha alcuna etichetta	L'etichetta viene aggiunta

Se il file…	Quindi…
Dispone di un'etichetta con un livello di classificazione inferiore	Viene aggiunta l'etichetta di livello superiore
Dispone di un'etichetta con un livello di classificazione superiore	Viene conservata l'etichetta di livello superiore
Viene assegnata un'etichetta sia manualmente che tramite un criterio	Viene aggiunta l'etichetta di livello superiore
Viene assegnata a due diverse etichette da due policy	Viene aggiunta l'etichetta di livello superiore

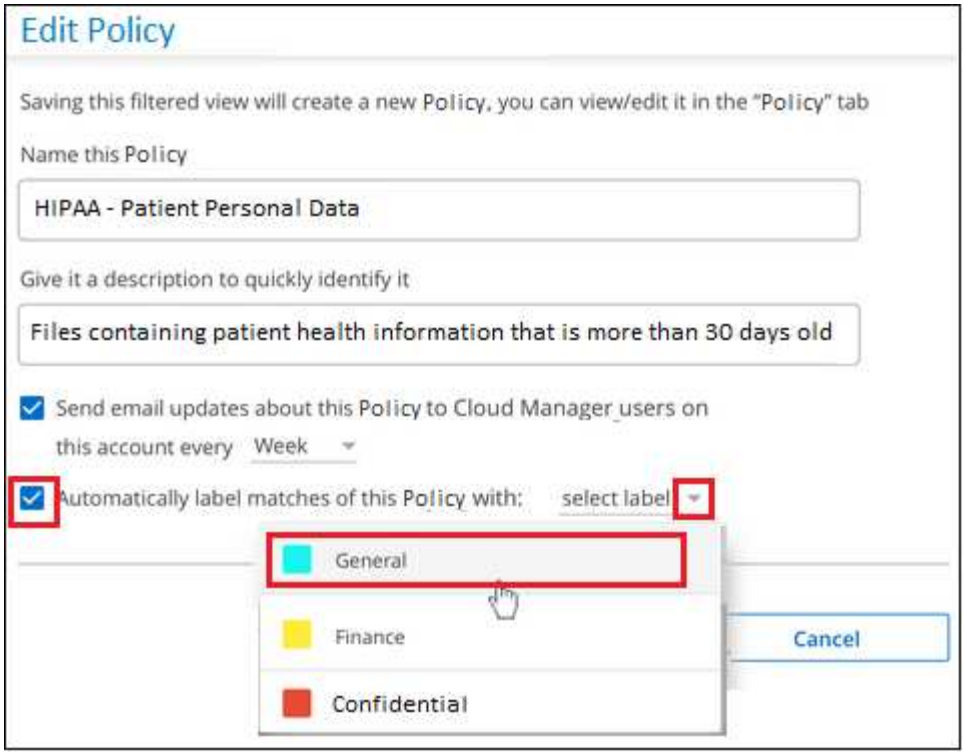
Per aggiungere un'etichetta AIP a una policy esistente, procedere come segue.

Fasi

1. Nella pagina elenco criteri, fare clic su **Modifica** per la policy in cui si desidera aggiungere (o modificare) l'etichetta AIP.



2. Nella pagina Edit Policy (Modifica policy), selezionare la casella per abilitare le etichette automatiche per i file che corrispondono ai parametri del Policy, quindi selezionare l'etichetta (ad esempio, **General**).



3. Fare clic su **Save Policy** (Salva policy) per visualizzare l'etichetta nella descrizione della policy.

> Se un criterio è stato configurato con un'etichetta, ma l'etichetta è stata rimossa da AIP, il nome dell'etichetta viene disattivato e l'etichetta non viene più assegnata.

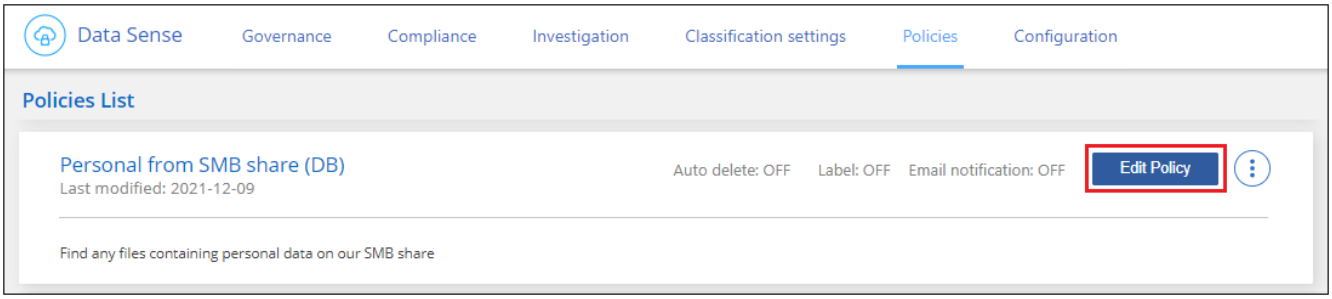
Modifica criteri

È possibile modificare qualsiasi criterio per un criterio esistente creato in precedenza. Questo può essere particolarmente utile se si desidera modificare la query (gli elementi definiti utilizzando filtri) per aggiungere o rimuovere determinati parametri.

Tenere presente che per le policy predefinite è possibile modificare solo se le notifiche e-mail vengono inviate e se vengono aggiunte etichette AIP. Non è possibile modificare altri valori.

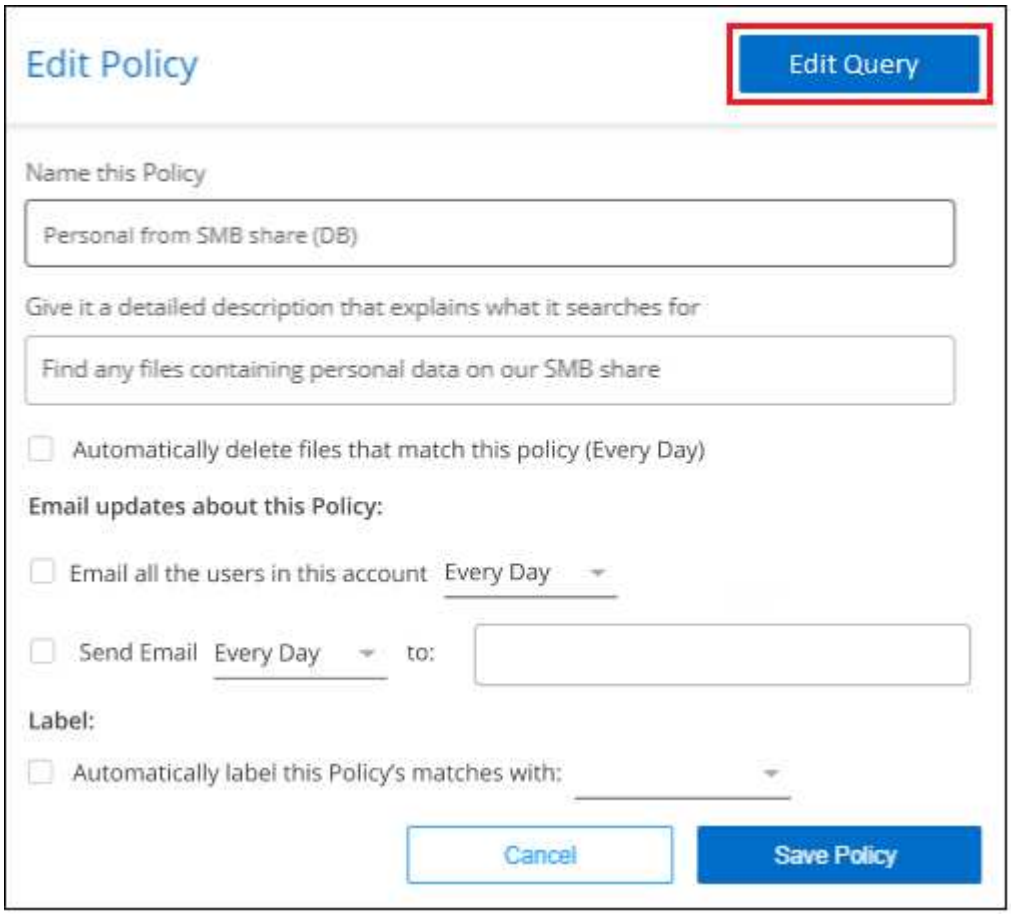
Fasi

1. Nella pagina elenco criteri, fare clic su **Modifica** per il criterio che si desidera modificare.

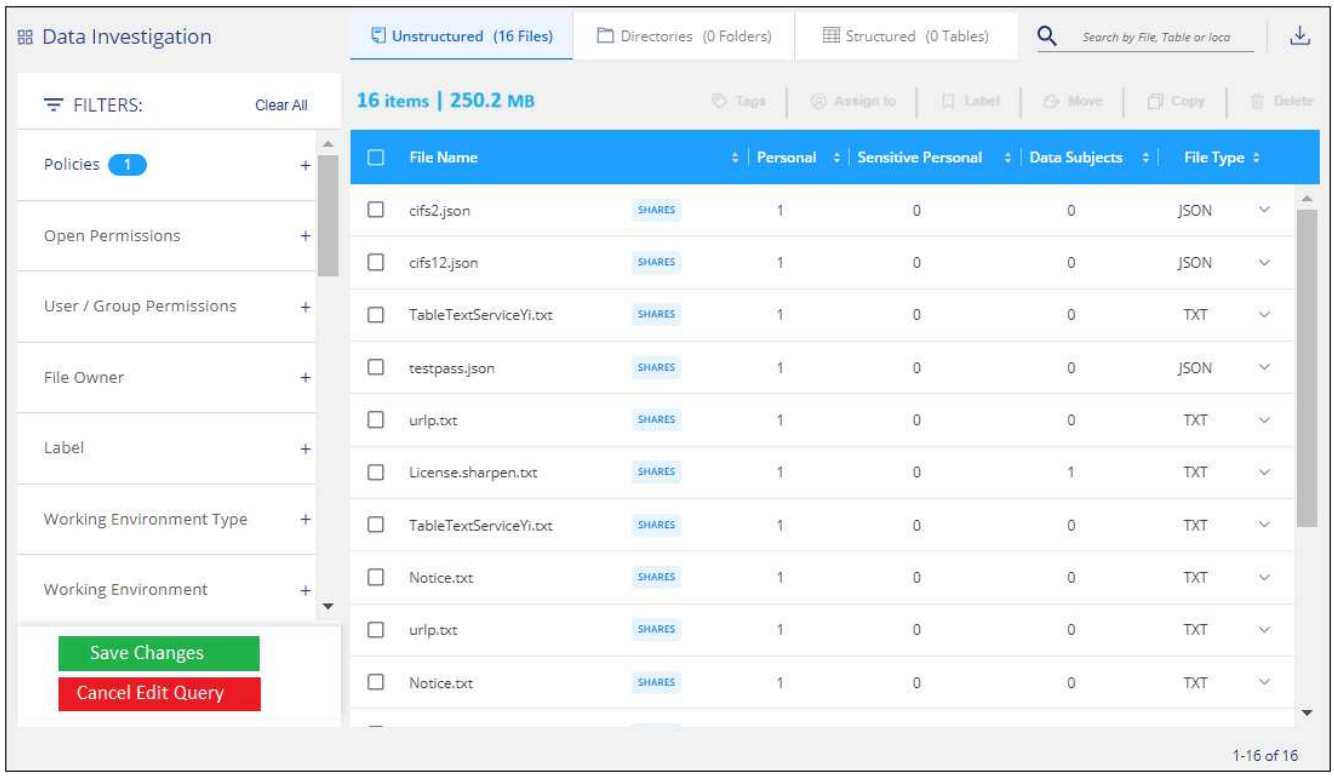


2. Se si desidera modificare gli elementi di questa pagina (nome, descrizione, invio di notifiche e-mail e aggiunta di etichette AIP), apportare la modifica e fare clic su **Save Policy** (Salva policy).

   Se si desidera modificare i filtri per la query salvata, fare clic su **Edit Query** (Modifica query).



3. Nella pagina di analisi che definisce la query, modificare la query aggiungendo, rimuovendo o personalizzando i filtri, quindi fare clic su **Save Changes** (Salva modifiche).



Risultato

La policy viene modificata immediatamente. Tutte le azioni definite per quel criterio per inviare un'email, aggiungere etichette AIP o eliminare file si verificheranno al successivo interno.

Delete Policy (Elimina policy)

È possibile eliminare qualsiasi policy personalizzata creata se non è più necessaria. Non è possibile eliminare alcuna policy predefinita.

Per eliminare un criterio, fare clic su Per una policy specifica, fare clic su **Delete Policy** (Elimina policy), quindi fare nuovamente clic su **Delete Policy** (Elimina policy) nella finestra di dialogo di conferma.

Elenco dei criteri predefiniti

La classificazione BlueXP fornisce le seguenti policy definite dal sistema:

Nome	Descrizione	Logica
S3 - dati privati esposti pubblicamente	Oggetti S3 contenenti informazioni personali o sensibili, con accesso pubblico aperto in lettura.	S3 Public E contiene informazioni personali o personali sensibili
PCI DSS - dati obsoleti in 30 giorni	File contenenti informazioni sulla carta di credito, modificati più di 30 giorni fa.	Contiene la carta di credito E l'ultima modifica in 30 giorni
HIPAA - dati obsoleti in 30 giorni	File contenenti informazioni sulla salute, modificati l'ultima volta 30 giorni fa.	Contiene i dati di salute (definiti come nel report HIPAA) E l'ultima modifica nell'arco di 30 giorni
Dati privati - obsoleti in 7 anni	File contenenti informazioni personali o sensibili, modificati da oltre 7 anni fa.	File contenenti informazioni personali o sensibili, modificati da oltre 7 anni fa
GDPR - cittadini europei	File contenenti più di 5 identificatori dei cittadini di un paese dell'UE o tabelle DB contenenti identificatori dei cittadini di un paese dell'UE.	File contenenti oltre 5 identificatori di un (uno) cittadino dell'UE o tabelle DB contenenti righe con oltre il 15% di colonne con identificatori UE di un paese. (Uno qualsiasi degli identificatori nazionali dei paesi europei. Non include Brasile, California, USA SSN, Israele, Sudafrica)
CCPA - residenti in California	File contenenti oltre 10 identificatori della licenza del driver California o tabelle DB con questo identificatore.	File contenenti oltre 10 identificatori della licenza di guida California O tabelle DB contenenti la licenza di guida California
Nomi dei soggetti dei dati - rischio elevato	File con oltre 50 nomi di soggetti dati.	File con oltre 50 nomi di soggetti dati
Indirizzi e-mail - rischio elevato	File con oltre 50 indirizzi e-mail o colonne DB con oltre il 50% delle righe contenenti indirizzi e-mail	File con oltre 50 indirizzi e-mail o colonne DB con oltre il 50% delle righe contenenti indirizzi e-mail
Dati personali - rischio elevato	File con oltre 20 ID dati personali o colonne DB con oltre il 50% delle righe contenenti identificativi dati personali.	File con oltre 20 colonne personali o DB con oltre il 50% delle righe contenenti dati personali

Nome	Descrizione	Logica
Dati personali sensibili - rischio elevato	File con oltre 20 identificatori di dati personali sensibili o colonne di database con oltre il 50% delle righe contenenti dati personali sensibili.	File con oltre 20 colonne personali sensibili o DB con oltre il 50% delle righe contenenti dati personali sensibili

Gestisci i tuoi dati privati

La classificazione BlueXP offre diversi modi per gestire i dati privati. Alcune funzionalità semplificano la preparazione alla migrazione dei dati, mentre altre funzionalità consentono di apportare modifiche ai dati.

- È possibile copiare i file in una condivisione NFS di destinazione se si desidera creare una copia di determinati dati e spostarli in una posizione NFS diversa.
- È possibile clonare un volume ONTAP in un nuovo volume, includendo solo i file selezionati dal volume di origine nel nuovo volume clonato. Ciò è utile per le situazioni in cui si esegue la migrazione dei dati e si desidera escludere alcuni file dal volume originale.
- È possibile copiare e sincronizzare i file da un repository di origine a una directory in una posizione di destinazione specifica. Questa funzione è utile per le situazioni in cui si esegue la migrazione dei dati da un sistema di origine a un altro mentre è ancora presente un'attività finale sui file di origine.
- Puoi spostare i file di origine che la classificazione BlueXP sta scansionando in qualsiasi condivisione NFS.
- È possibile eliminare i file che sembrano insicuri o troppo rischiosi da lasciare nel sistema di storage o che sono stati identificati come duplicati.

> - Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.
> - I dati degli account Google Drive al momento non possono utilizzare nessuna di queste funzionalità.

Copia dei file di origine

È possibile copiare qualsiasi file di origine sottoposto a scansione dalla classificazione BlueXP. Esistono tre tipi di operazioni di copia a seconda di ciò che si sta cercando di ottenere:

- **Copiare file** da volumi o origini dati uguali o diversi in una condivisione NFS di destinazione.

  Questo è utile se si desidera creare una copia di determinati dati e spostarli in una posizione NFS diversa.

- **Clonare un volume ONTAP** in un nuovo volume nello stesso aggregato, ma includere solo i file selezionati dal volume di origine nel nuovo volume clonato.

  Ciò è utile per le situazioni in cui si esegue la migrazione dei dati e si desidera escludere alcuni file dal volume originale. Questa azione utilizza "FlexClone di NetApp" funzionalità che consente di duplicare rapidamente il volume e rimuovere i file * non selezionati*.

- **Copiare e sincronizzare i file** da un singolo repository di origine (volume ONTAP, bucket S3, condivisione NFS, ecc.) a una directory in una destinazione specifica (destinazione).

Ciò è utile per le situazioni in cui si esegue la migrazione dei dati da un sistema di origine a un altro. Dopo la copia iniziale, il servizio sincronizza i dati modificati in base alla pianificazione impostata. Questa azione utilizza "Copia e sincronizzazione NetApp BlueXP" funzionalità per copiare e sincronizzare i dati da un'origine a una destinazione.

Copiare i file di origine in una condivisione NFS

Puoi copiare i file di origine che la classificazione BlueXP sta scansionando su qualsiasi condivisione NFS. La condivisione NFS non deve essere integrata con la classificazione BlueXP, devi solo conoscere il nome della condivisione NFS dove tutti i file selezionati verranno copiati nel formato `<host_name>:/<share_path>`.

Non è possibile copiare i file che risiedono nei database.

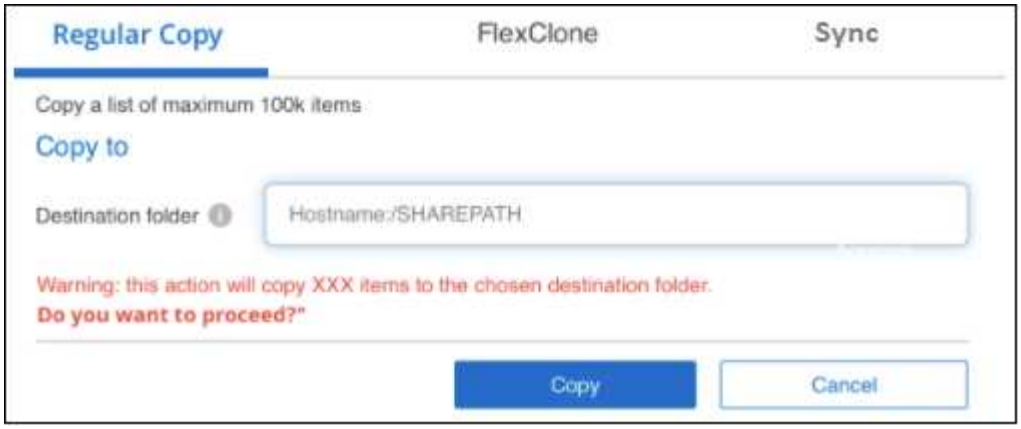
Requisiti

- Per copiare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).
- La copia dei file richiede che la condivisione NFS di destinazione consenta l'accesso dall'istanza di classificazione BlueXP.
- È possibile copiare da 1 a 100,000 file alla volta.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da copiare e fare clic su **Copy** (Copia).

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
   - Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All **20** Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.
2. Nella finestra di dialogo *Copy Files*, selezionare la scheda **Regular Copy**.



3. Immettere il nome della condivisione NFS in cui verranno copiati tutti i file selezionati nel formato `<host_name>:/<share_path>`E fare clic su **Copia**.

   Viene visualizzata una finestra di dialogo con lo stato dell'operazione di copia.

È possibile visualizzare l'avanzamento dell'operazione di copia in "Riquadro Actions Status (Stato azioni)".

Nota: È anche possibile copiare un singolo file quando si visualizzano i dettagli dei metadati di un file. Fare clic su **Copy file** (Copia file).

Clonazione dei dati del volume in un nuovo volume

È possibile clonare un volume ONTAP esistente sottoposto a scansione dalla classificazione BlueXP utilizzando la funzionalità NetApp *FlexClone*. Ciò consente di duplicare rapidamente il volume includendo solo i file selezionati. Ciò è utile se si stanno migrando i dati e si desidera escludere alcuni file dal volume originale o se si desidera creare una copia di un volume per il test.

Il nuovo volume viene creato nello stesso aggregato del volume di origine. Assicurarsi di disporre di spazio sufficiente per questo nuovo volume nell'aggregato prima di avviare questa attività. Se necessario, contattare l'amministratore dello storage.

Nota: i volumi FlexGroup non possono essere clonati perché non sono supportati da FlexClone.

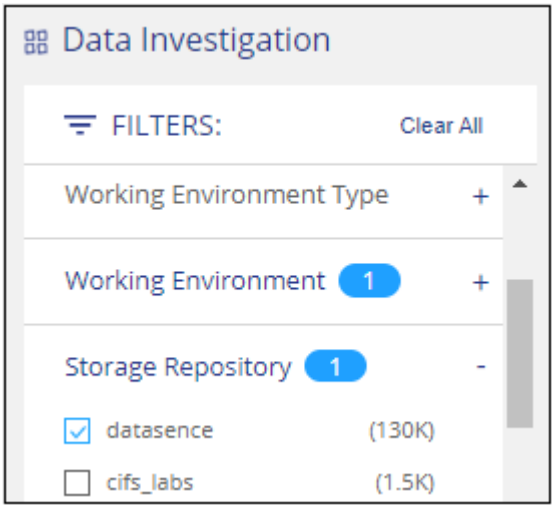
Requisiti

- Per copiare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).

- Selezionare un minimo di 20 file.
- Tutti i file selezionati devono provenire dallo stesso volume e il volume deve essere online.
- Il volume deve provenire da un sistema Cloud Volumes ONTAP o ONTAP on-premise. Al momento non sono supportate altre origini dati.
- La licenza FlexClone deve essere installata sul cluster. Questa licenza viene installata per impostazione predefinita sui sistemi Cloud Volumes ONTAP.

Fasi

1. Nel riquadro analisi dati, creare un filtro selezionando un singolo **ambiente di lavoro** e un singolo **repository di storage** per assicurarsi che tutti i file provengano dallo stesso volume ONTAP.



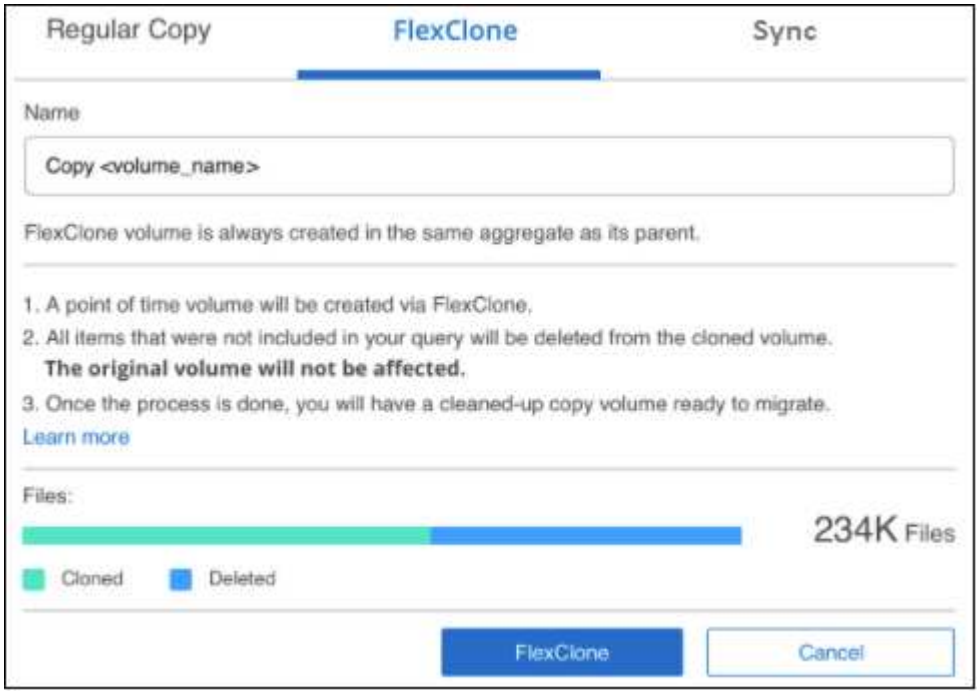
   Applicare eventuali altri filtri in modo da visualizzare solo i file che si desidera clonare nel nuovo volume.

2. Nel riquadro dei risultati dell'analisi, selezionare i file che si desidera clonare e fare clic su **Copy** (Copia).

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
   - Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All **20** Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.

3. Nella finestra di dialogo *Copy Files*, selezionare la scheda **FlexClone**. Questa pagina mostra il numero

totale di file che verranno clonati dal volume (i file selezionati) e il numero di file che non vengono inclusi/cancellati (i file non selezionati) dal volume clonato.



4. Inserire il nome del nuovo volume e fare clic su **FlexClone**.

   Viene visualizzata una finestra di dialogo con lo stato dell'operazione di clonazione.

Risultato

Il nuovo volume clonato viene creato nello stesso aggregato del volume di origine.

È possibile visualizzare lo stato di avanzamento dell'operazione di clonazione in "Riquadro Actions Status (Stato azioni)".

Se inizialmente è stato selezionato **Map All Volumes** (mappatura di tutti i volumi) o **Map & Classify All Volumes** (mappatura e classificazione di tutti i volumi) quando è stata attivata la classificazione BlueXP per l'ambiente di lavoro in cui risiede il volume di origine, la classificazione BlueXP eseguirà automaticamente la scansione del nuovo volume clonato. Se inizialmente non si è utilizzata una di queste selezioni, è necessario eseguire la scansione di questo nuovo volume "attivare manualmente la scansione sul volume".

Copiare e sincronizzare i file di origine in un sistema di destinazione

È possibile copiare i file di origine che la classificazione BlueXP sta scansionando da qualsiasi origine dati non strutturata supportata in una directory in una posizione di destinazione specifica ("Posizioni di destinazione supportate dalla copia e dalla sincronizzazione BlueXP"). Dopo la copia iniziale, tutti i dati modificati nei file vengono sincronizzati in base alla pianificazione configurata.

Ciò è utile per le situazioni in cui si esegue la migrazione dei dati da un sistema di origine a un altro. Questa azione utilizza "Copia e sincronizzazione NetApp BlueXP" funzionalità per copiare e sincronizzare i dati da un'origine a una destinazione.

Non puoi copiare e sincronizzare i file che risiedono in database, account OneDrive o account SharePoint.

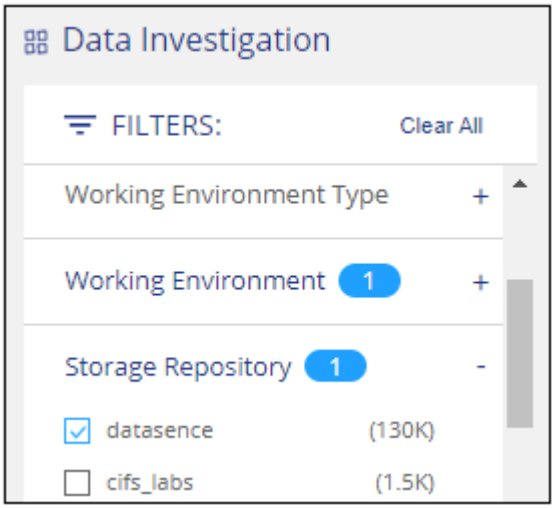
Requisiti

- Per copiare e sincronizzare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).
- Selezionare un minimo di 20 file.
- Tutti i file selezionati devono provenire dallo stesso repository di origine (volume ONTAP, bucket S3, condivisione NFS o CIFS, ecc.).
- È necessario attivare il servizio di copia e sincronizzazione BlueXP e configurare almeno un broker di dati da utilizzare per trasferire i file tra i sistemi di origine e di destinazione. Esaminare i requisiti di copia e sincronizzazione di BlueXP a partire da "Descrizione di avvio rapido".

  Si noti che il servizio di copia e sincronizzazione BlueXP prevede costi di servizio separati per le relazioni di sincronizzazione e comporta costi per le risorse se si implementa il broker di dati nel cloud.

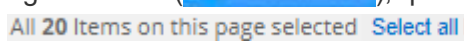
Fasi

1. Nel riquadro Data Investigation (analisi dati), creare un filtro selezionando un singolo **Working Environment** e un singolo **Storage Repository** per assicurarsi che tutti i file provengano dallo stesso repository.

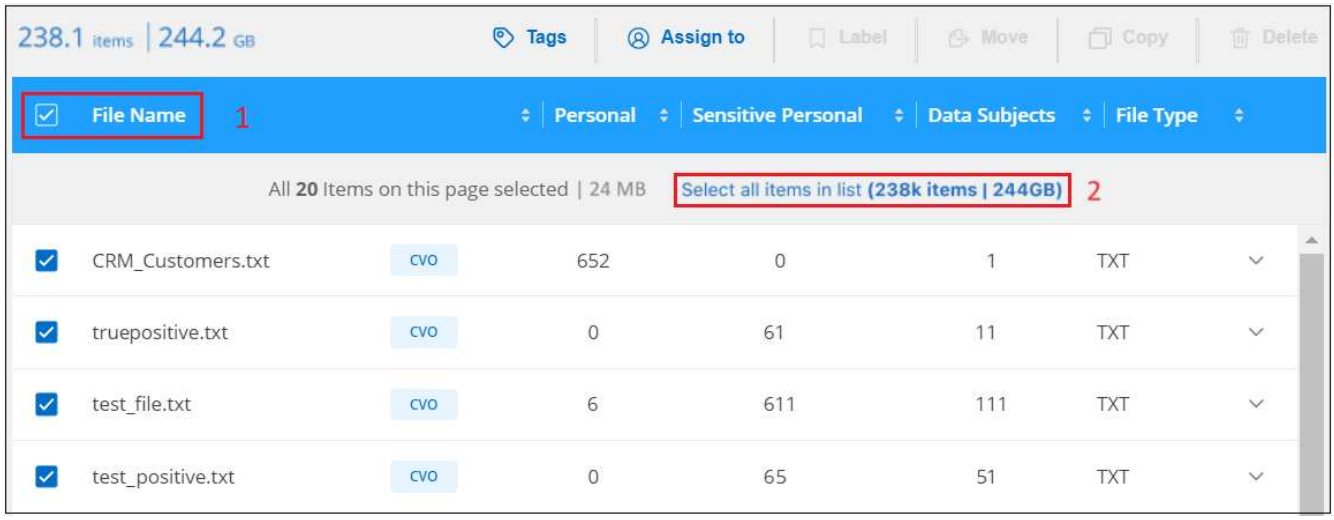


   Applicare eventuali altri filtri in modo da visualizzare solo i file che si desidera copiare e sincronizzare nel sistema di destinazione.

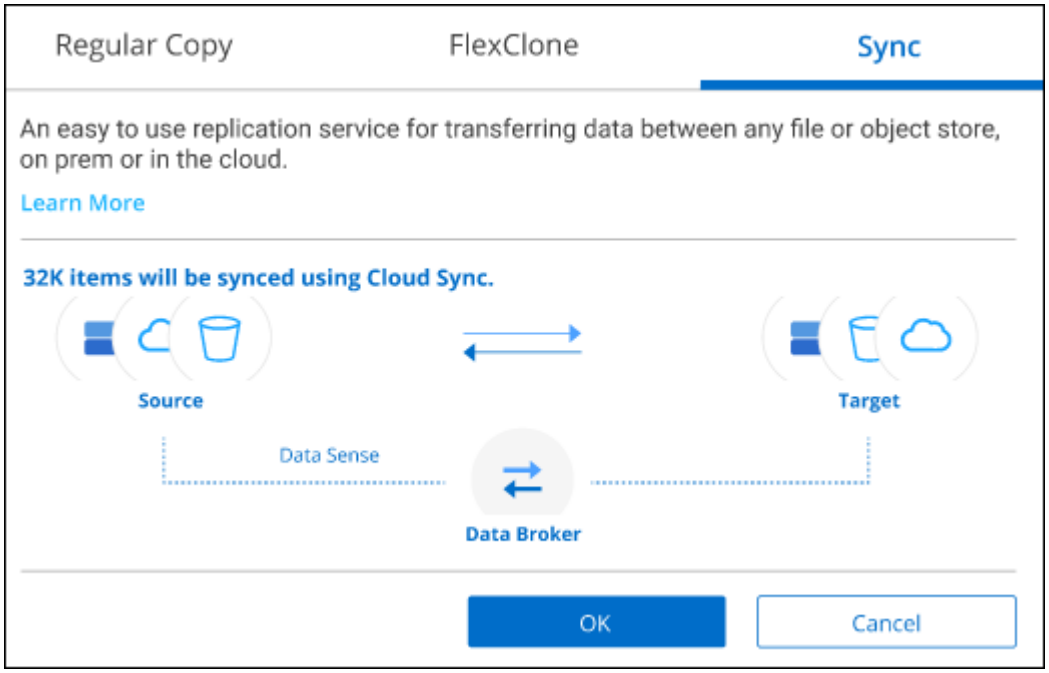
2. Nel riquadro dei risultati dell'analisi, selezionare tutti i file su tutte le pagine selezionando la casella nella riga del titolo (

), quindi nel messaggio a comparsa


Fare clic su **Select All ITEMS in list (xxx ITEMS)** (Seleziona tutti gli elementi nell'elenco (xxx elementi)**, quindi fare clic su *Copy** (Copia).



3. Nella finestra di dialogo *Copy Files*, selezionare la scheda **Sync**.



4. Se si è certi di voler sincronizzare i file selezionati in una posizione di destinazione, fare clic su **OK**.

   L'interfaccia utente di copia e sincronizzazione di BlueXP viene aperta in BlueXP.

   Viene richiesto di definire la relazione di sincronizzazione. Il sistema di origine viene prepopolato in base al repository e ai file già selezionati nella classificazione BlueXP.

5. È necessario selezionare il sistema di destinazione e selezionare (o creare) il Data Broker che si desidera utilizzare. Esaminare i requisiti di copia e sincronizzazione di BlueXP a partire da "Descrizione di avvio rapido".

Risultato

I file vengono copiati nel sistema di destinazione e sincronizzati in base alla pianificazione definita. Se si seleziona una sincronizzazione una tantum, i file vengono copiati e sincronizzati una sola volta. Se si sceglie una sincronizzazione periodica, i file vengono sincronizzati in base alla pianificazione. Si noti che se il sistema di origine aggiunge nuovi file che corrispondono alla query creata utilizzando i filtri, questi *nuovi* file verranno

copiati nella destinazione e sincronizzati in futuro.

Si noti che alcune delle normali operazioni di copia e sincronizzazione di BlueXP sono disabilitate quando vengono richiamate dalla classificazione BlueXP:

- Non è possibile utilizzare i pulsanti **Delete Files on Source** o **Delete Files on Target**.
- L'esecuzione di un report è disattivata.

Spostare i file di origine in una condivisione NFS

Puoi spostare i file di origine che la classificazione BlueXP sta scansionando in qualsiasi condivisione NFS. Non è necessario integrare la condivisione NFS con la classificazione BlueXP.

In alternativa, è possibile lasciare un file breadcrumb nella posizione del file spostato. Un file breadcrumb aiuta gli utenti a capire perché un file è stato spostato dalla posizione originale. Per ogni file spostato, il sistema crea un file breadcrumb nella posizione di origine denominata `<filename>-breadcrumb-<date>.txt`. È possibile aggiungere del testo nella finestra di dialogo che verrà aggiunta al file breadcrumb per indicare la posizione in cui è stato spostato il file e l'utente che lo ha spostato.

Si noti che la struttura della sottodirectory dal file di origine viene ricreata sulla condivisione di destinazione quando il file viene spostato, in modo da comprendere più facilmente da dove è stato spostato il file. Se esiste un file con lo stesso nome nella posizione di destinazione, il file non verrà spostato.

Non è possibile spostare i file che risiedono nei database.

Requisiti

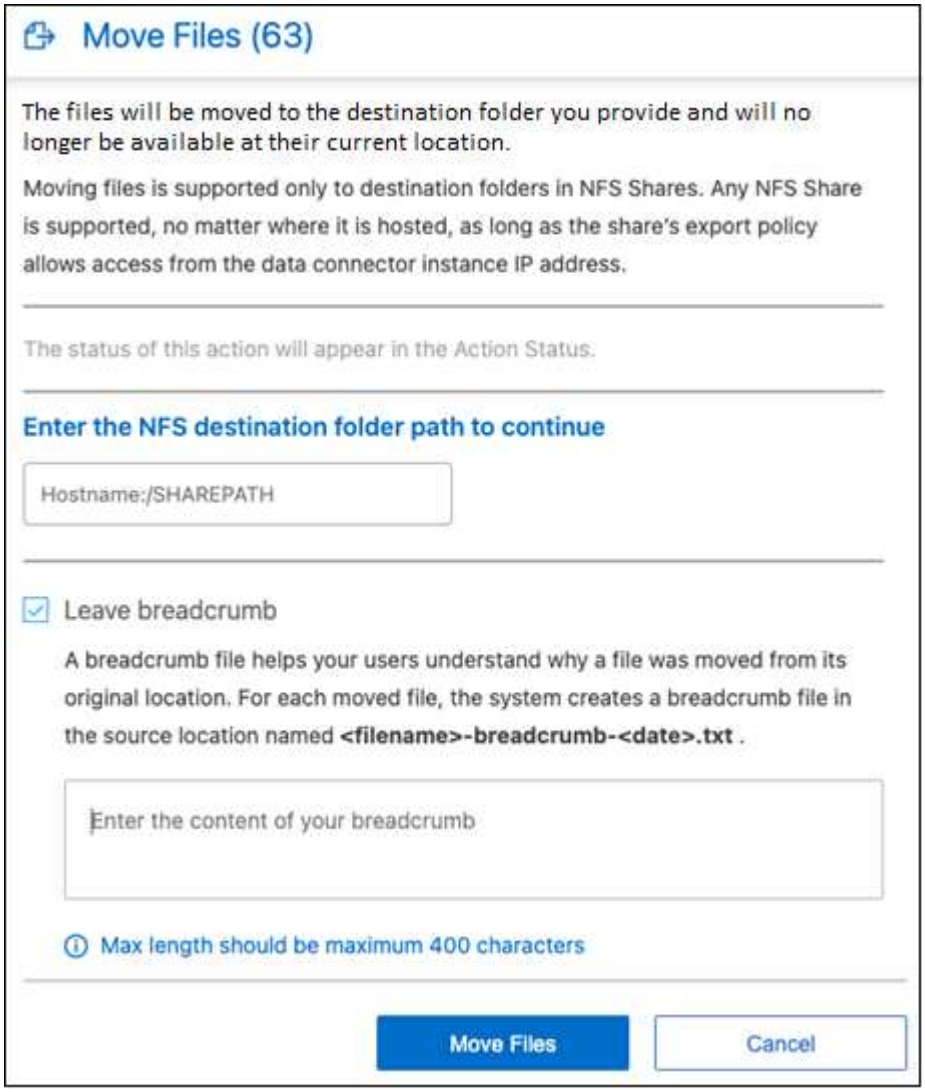
- Per spostare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).
- I file di origine possono trovarsi nelle seguenti origini dati: On-premise ONTAP, Cloud Volumes ONTAP, Azure NetApp Files, condivisioni file e SharePoint Online.
- È possibile spostare un massimo di 15 milioni di file alla volta.
- Vengono spostati solo i file di dimensioni pari o inferiori a 50 MB.
- La condivisione NFS di destinazione deve consentire l'accesso dall'indirizzo IP dell'istanza di classificazione BlueXP.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da spostare.

- Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
- Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
- Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All 20 Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.

2. Dalla barra dei pulsanti, fare clic su **Sposta**.



3. Nella finestra di dialogo *Move Files*, immettere il nome della condivisione NFS in cui verranno spostati tutti i file selezionati nel formato `<host_name>:/<share_path>`.
4. Se si desidera lasciare un file breadcrumb, selezionare la casella *Leave breadcrumb*. È possibile inserire del testo nella finestra di dialogo per indicare la posizione in cui è stato spostato il file, l'utente che lo ha spostato e qualsiasi altra informazione, come il motivo dello spostamento del file.
5. Fare clic su **Sposta file**.

Nota: È anche possibile spostare un singolo file quando si visualizzano i dettagli dei metadati di un file. Fare clic su **Sposta file**.

Eliminare i file di origine

È possibile rimuovere in modo permanente i file di origine che sembrano insicuri o troppo rischiosi da lasciare nel sistema di storage o che sono stati identificati come duplicati. Questa azione è permanente e non è possibile annullare o ripristinare.

È possibile eliminare i file manualmente dal riquadro analisi, oppure "Utilizzo automatico dei criteri".

> Non è possibile eliminare i file che risiedono nei database. Sono supportate tutte le altre origini dati.

L'eliminazione dei file richiede le seguenti autorizzazioni:

- Per i dati NFS - la policy di esportazione deve essere definita con permessi di scrittura.
- Per i dati CIFS - le credenziali CIFS devono disporre di permessi di scrittura.
- Per i dati S3 - il ruolo IAM deve includere la seguente autorizzazione: `s3:DeleteObject`.

Eliminare manualmente i file di origine

Requisiti

- Per eliminare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).
- È possibile eliminare un massimo di 100,000 file alla volta.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file che si desidera eliminare.

- Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
- Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
- Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All **20** Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.

2. Dalla barra dei pulsanti, fare clic su **Delete** (Elimina).
3. Poiché l'operazione di eliminazione è permanente, digitare "**permanentemente delete**" nella successiva finestra di dialogo *Delete file* e fare clic su **Delete file**.

È possibile visualizzare l'avanzamento dell'operazione di eliminazione in "Riquadro Actions Status (Stato azioni)".

Nota: È anche possibile eliminare un singolo file quando si visualizzano i dettagli dei metadati di un file. Fare clic su **Delete file** (Elimina file).

Visualizza i report sulla conformità

La classificazione BlueXP fornisce report che è possibile utilizzare per comprendere meglio lo stato del programma per la privacy dei dati della tua organizzazione.

Per impostazione predefinita, le dashboard di classificazione di BlueXP visualizzano i dati di conformità e governance per tutti gli ambienti di lavoro, i database e le origini dati. Se si desidera visualizzare report contenenti dati solo per alcuni ambienti di lavoro, selezionare gli ambienti di lavoro.

- I report descritti in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura possono generare solo il report di mappatura dei dati.
- NetApp non può garantire la precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla classificazione BlueXP. È sempre necessario convalidare le informazioni esaminando i dati.

Report sulla valutazione dei rischi per la privacy

Il report sulla valutazione dei rischi per la privacy fornisce una panoramica dello stato di rischio per la privacy della tua organizzazione, come richiesto dalle normative sulla privacy come GDPR e CCPA. Il report contiene le seguenti informazioni:

Stato di compliance

R punteggio di severità e la distribuzione dei dati, sia che si tratti di dati personali, non sensibili o sensibili.

Panoramica della valutazione

Analisi dei tipi di dati personali rilevati, nonché delle categorie di dati.

Argomenti trattati in questa valutazione

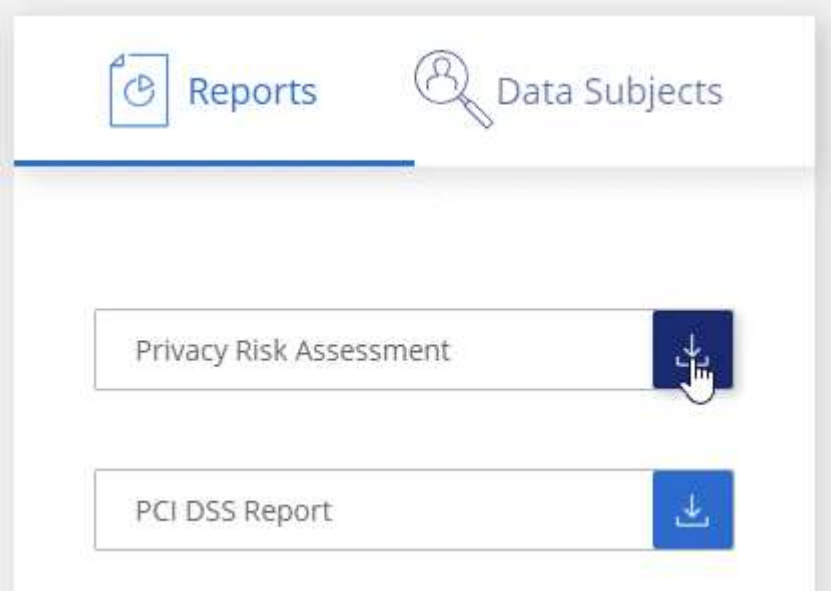
Il numero di persone, per località, per le quali sono stati trovati identificatori nazionali.

Generare Privacy Risk Assessment Report

Accedere alla scheda Compliance per generare il report.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Compliance**, quindi fare clic sull'icona di download accanto a **Privacy Risk Assessment** sotto **Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in

base alle esigenze.

Punteggio di severità

La classificazione BlueXP calcola il punteggio di severità per il Privacy Risk Assessment Report sulla base di tre variabili:

- La percentuale di dati personali su tutti i dati.
- La percentuale di dati personali sensibili rispetto a tutti i dati.
- La percentuale di file che includono soggetti dati, determinata da identificatori nazionali come ID nazionali, numeri di previdenza sociale e numeri di identificazione fiscale.

La logica utilizzata per determinare il punteggio è la seguente:

Punteggio di severità	Logica
0	Tutte e tre le variabili sono esattamente 0%
1	Una delle variabili è maggiore dello 0%
2	Una delle variabili è maggiore del 3%
3	Due delle variabili sono maggiori del 3%
4	Tre delle variabili sono maggiori del 3%
5	Una delle variabili è maggiore del 6%
6	Due delle variabili sono maggiori del 6%
7	Tre delle variabili sono maggiori del 6%
8	Una delle variabili è maggiore del 15%
9	Due delle variabili sono maggiori del 15%
10	Tre delle variabili sono maggiori del 15%

Report PCI DSS

Il report PCI DSS (Payment Card Industry Data Security Standard) consente di identificare la distribuzione delle informazioni sulle carte di credito nei file. Il report contiene le seguenti informazioni:

Panoramica

Quanti file contengono informazioni sulla carta di credito e in quali ambienti di lavoro.

Crittografia

La percentuale di file contenenti informazioni sulla carta di credito presenti in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Protezione ransomware

La percentuale di file contenenti informazioni sulla carta di credito che si trovano in ambienti di lavoro in cui la protezione ransomware è attivata o meno. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Conservazione

Il periodo di tempo in cui i file sono stati modificati per l'ultima volta. Ciò è utile perché non è necessario conservare le informazioni della carta di credito per un periodo di tempo superiore a quello necessario per elaborarle.

Distribuzione delle informazioni sulla carta di credito

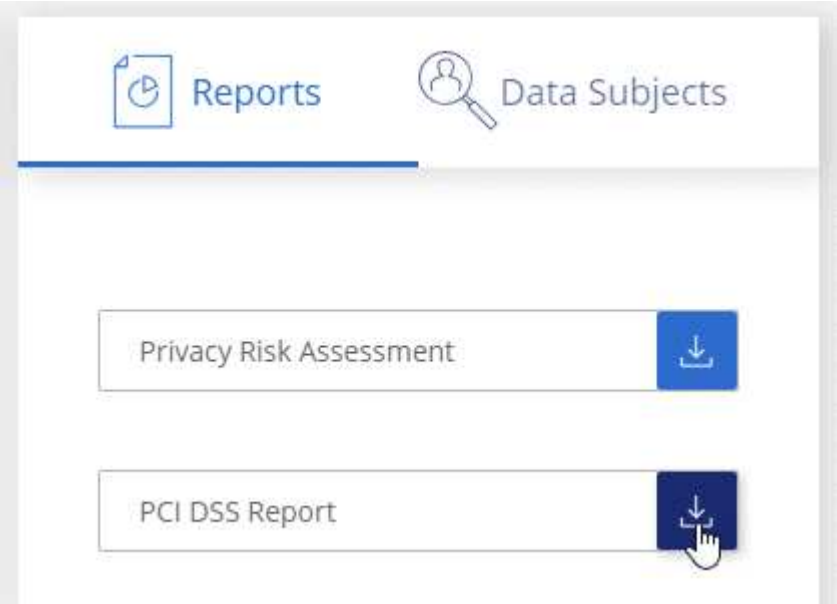
Gli ambienti di lavoro in cui sono state rilevate le informazioni sulla carta di credito e se sono attivate la crittografia e la protezione ransomware.

Generare il rapporto PCI DSS

Accedere alla scheda Compliance per generare il report.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Compliance**, quindi fare clic sull'icona di download accanto a **PCI DSS Report** sotto **Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in base alle esigenze.

Report HIPAA

Il report HIPAA (Health Insurance Portability and Accountability Act) consente di identificare i file contenenti informazioni sulla salute. È progettato per soddisfare i requisiti della tua organizzazione in materia di privacy dei dati HIPAA. Le informazioni che la classificazione BlueXP cerca includono:

- Schema di riferimento per lo stato di salute
- ICD-10-CM Codice medico
- Codice medico ICD-9-CM
- HR - Categoria di salute
- Categoria Health Application Data

Il report contiene le seguenti informazioni:

Panoramica

Quanti file contengono informazioni sullo stato di salute e in quali ambienti di lavoro.

Crittografia

La percentuale di file contenenti informazioni sullo stato di salute che si trovano in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Protezione ransomware

La percentuale di file contenenti informazioni sullo stato di salute che si trovano in ambienti di lavoro in cui la protezione ransomware è attivata o meno. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Conservazione

Il periodo di tempo in cui i file sono stati modificati per l'ultima volta. Ciò è utile perché non è necessario conservare le informazioni sulla salute per un periodo di tempo superiore a quello necessario per elaborarle.

Distribuzione delle informazioni sanitarie

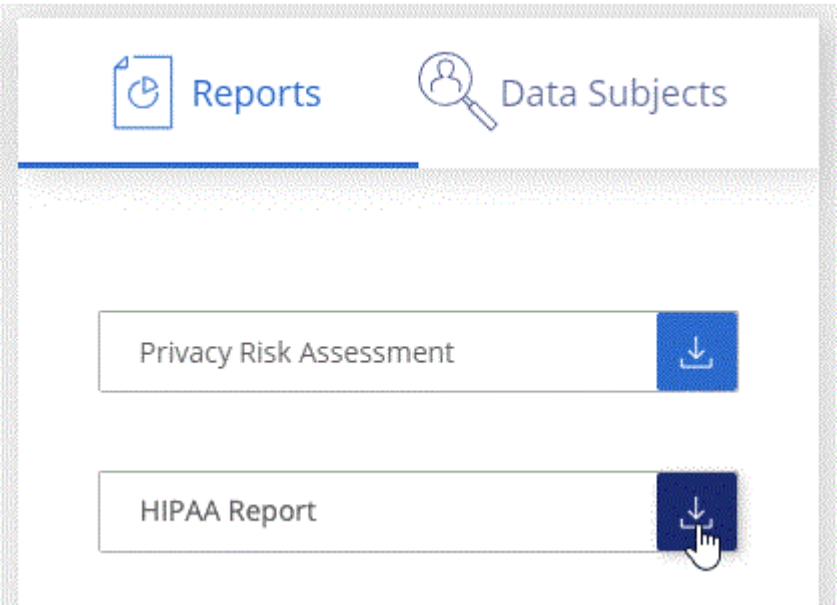
Gli ambienti di lavoro in cui sono state trovate le informazioni di salute e se sono attivate la crittografia e la protezione ransomware.

Generare il report HIPAA

Accedere alla scheda Compliance per generare il report.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Compliance**, quindi fare clic sull'icona di download accanto a **HIPAA Report** sotto **Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in base alle esigenze.

Che cos’è una richiesta di accesso ai dati?

Le normative sulla privacy, come il GDPR europeo, concedono ai soggetti interessati (come clienti o dipendenti) il diritto di accedere ai propri dati personali. Quando un soggetto interessato richiede queste informazioni, queste vengono denominate DSAR (data subject access request). Le organizzazioni devono rispondere a queste richieste "senza ritardi indebito" e al più tardi entro un mese dalla ricezione.

È possibile rispondere a una DSAR cercando il nome completo di un soggetto o l’identificatore noto (ad esempio un indirizzo e-mail) e scaricando un report. Il report è stato progettato per aiutare l’organizzazione a rispettare il GDPR o leggi simili sulla privacy dei dati.

In che modo la classificazione BlueXP può aiutarti a rispondere a una DSAR?

Quando si esegue una ricerca dell’oggetto dati, la classificazione BlueXP trova tutti i file, i bucket, OneDrive e gli account SharePoint che contengono il nome o l’identificatore di tale persona. La classificazione BlueXP verifica i dati pre-indicizzati più recenti per il nome o l’identificatore. Non avvia una nuova scansione.

Una volta completata la ricerca, è possibile scaricare l’elenco di file per un report Data Subject Access Request. Il report aggrega le informazioni dei dati e le inserisce in termini legali che è possibile inviare alla persona.

> La ricerca dei dati non è attualmente supportata nei database.

Cercare gli argomenti dei dati e scaricare i report

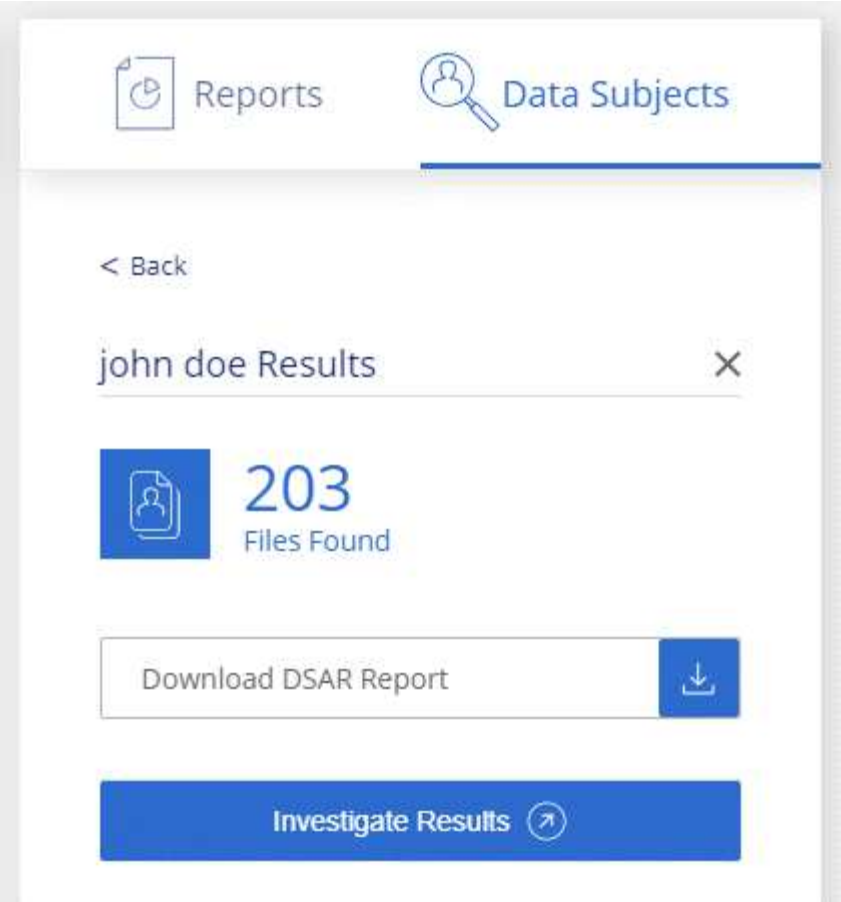
Cercare il nome completo o l’identificatore noto del soggetto interessato, quindi scaricare un report elenco file o un report DSAR. È possibile eseguire la ricerca in base a. "qualsiasi tipo di informazione personale".

> Sono supportati l’inglese, il tedesco, il giapponese e lo spagnolo durante la ricerca dei nomi degli argomenti dei dati. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Data subjects**.
3. Cercare il nome completo o l’identificativo noto dell’interessato.

   Ecco un esempio che mostra una ricerca per il nome *john Doe*:



4. Scegliere una delle opzioni disponibili:
   - **Download del report DSAR**: Una risposta formale alla richiesta di accesso che è possibile inviare al soggetto interessato. Questo report contiene informazioni generate automaticamente in base ai dati rilevati dalla classificazione BlueXP nell'oggetto dei dati ed è progettato per essere utilizzato come modello. Completare il modulo e esaminarlo internamente prima di inviarlo al soggetto interessato.
   - **Investigate Results**: Pagina che consente di analizzare i dati ricercando, ordinando, espandendo i dettagli di un file specifico e scaricando l'elenco dei file.

> Se sono presenti più di 10,000 risultati, nell'elenco dei file vengono visualizzati solo i primi 10,000 risultati.

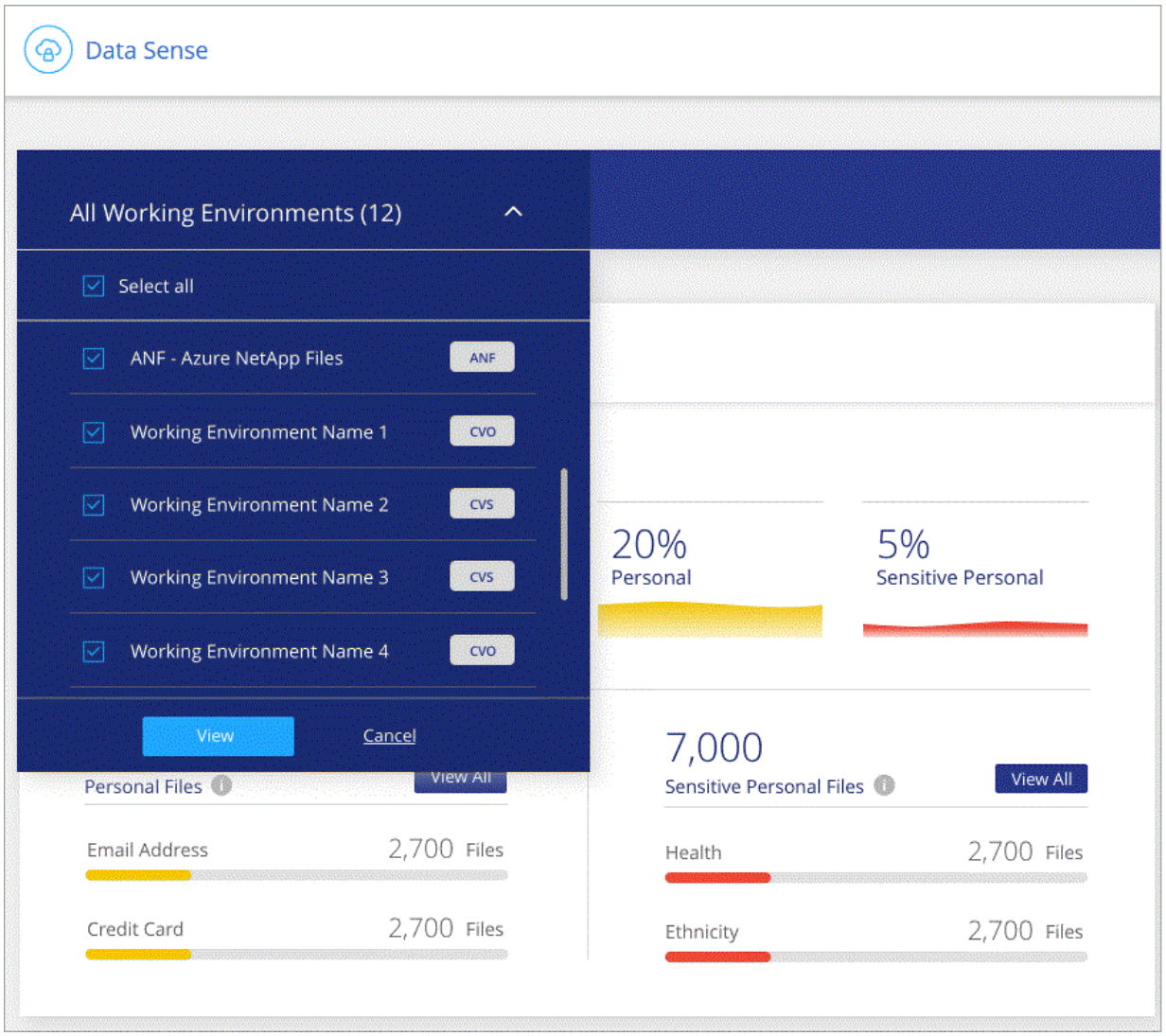
Selezionare gli ambienti di lavoro per i rapporti

È possibile filtrare i contenuti della dashboard di conformità della classificazione BlueXP per visualizzare i dati di conformità per tutti gli ambienti di lavoro e i database o solo per ambienti di lavoro specifici.

Quando si filtra la dashboard, la classificazione BlueXP regola i dati di conformità e invia report solo agli ambienti di lavoro selezionati.

Fasi

1. Fare clic sul menu a discesa del filtro, selezionare gli ambienti di lavoro per i quali si desidera visualizzare i dati e fare clic su **View** (Visualizza).


Data Sense
All Working Environments (12)
Select all
ANF - Azure NetApp Files
ANF
Working Environment Name 1
CVO
Working Environment Name 2
CVS
Working Environment Name 3
CVS
Working Environment Name 4
CVO
View
Cancel
20%
Personal
5%
Sensitive Personal
Personal Files
View All
Email Address
2,700 Files
Credit Card
2,700 Files
7,000
Sensitive Personal Files
View All
Health
2,700 Files
Ethnicity
2,700 Files

Gestire la classificazione BlueXP

Aggiungi identificatori di dati personali alle scansioni di classificazione BlueXP

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

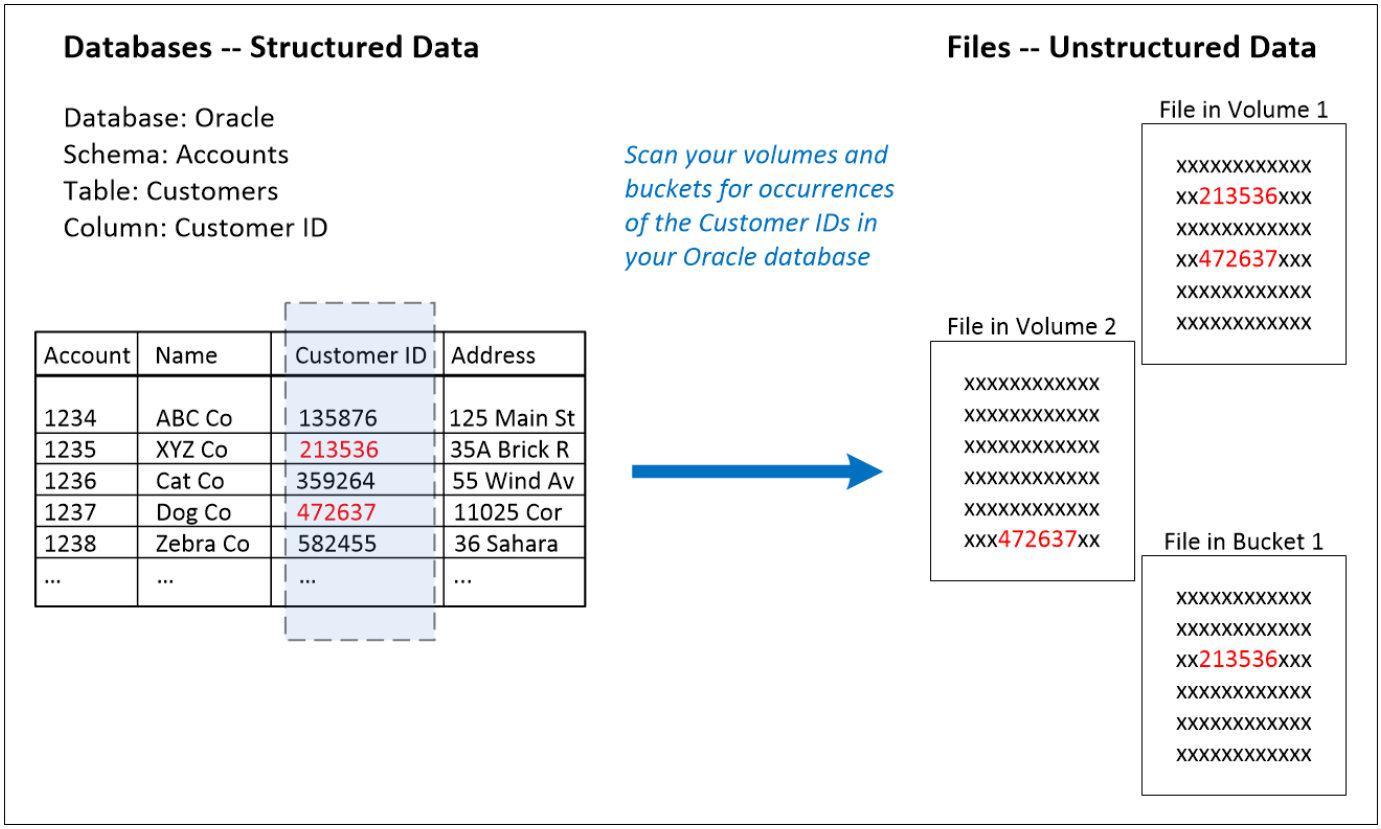
- È possibile aggiungere identificatori univoci in base a colonne specifiche nei database che si sta eseguendo la scansione.
- È possibile aggiungere parole chiave personalizzate da un file di testo — queste parole sono identificate all'interno dei dati.
- È possibile aggiungere un modello personale utilizzando un'espressione regolare (regex) — il regex viene aggiunto ai modelli predefiniti esistenti.
- È possibile aggiungere categorie personalizzate per identificare dove si trovano categorie specifiche di informazioni nei dati.

Tutti questi meccanismi per aggiungere criteri di scansione personalizzati sono supportati in tutte le lingue.

> Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.

Aggiungere identificatori di dati personali personalizzati dai database

Una funzionalità chiamata *Data Fusion* consente di eseguire la scansione dei dati delle organizzazioni per identificare se gli identificatori univoci dei database sono presenti in qualsiasi altra origine dati. È possibile scegliere gli identificatori aggiuntivi che la classificazione BlueXP ricerca nelle relative scansioni selezionando una o più colonne specifiche in una tabella di database. Ad esempio, il diagramma riportato di seguito mostra come i dati Fusion vengono utilizzati per eseguire la scansione di volumi, bucket e database per individuare le occorrenze di tutti gli ID cliente dal database Oracle.



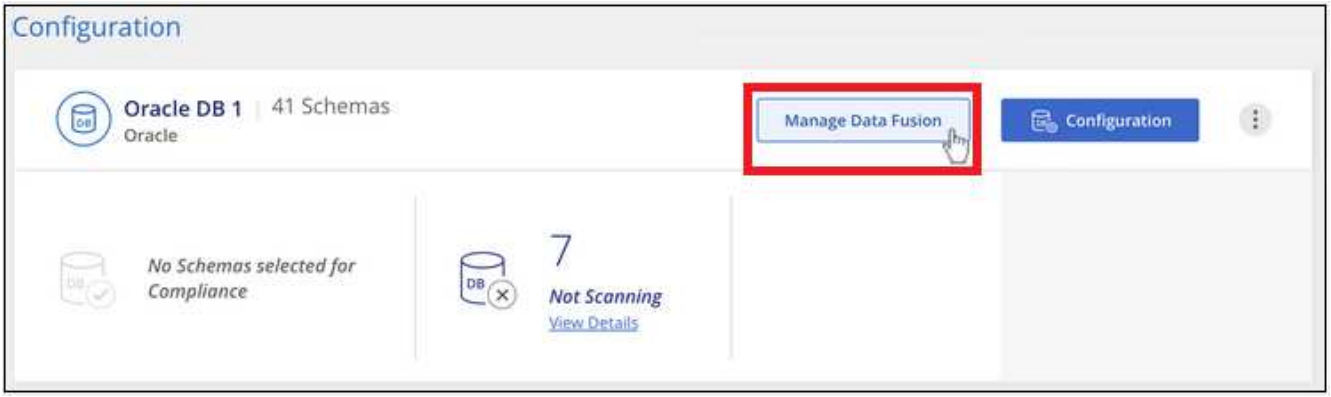
Come puoi vedere, sono stati trovati due ID cliente univoci in due volumi e in un bucket S3. Verranno identificate anche le corrispondenze presenti nelle tabelle del database.

Si noti che, dal momento che si esegue la scansione dei database, qualsiasi lingua in cui i dati vengono memorizzati verrà utilizzata per identificare i dati nelle future scansioni di classificazione di BlueXP.

Fasi

Devi avere "aggiunto almeno un server di database" Alla classificazione BlueXP prima di poter aggiungere origini Fusion dei dati.

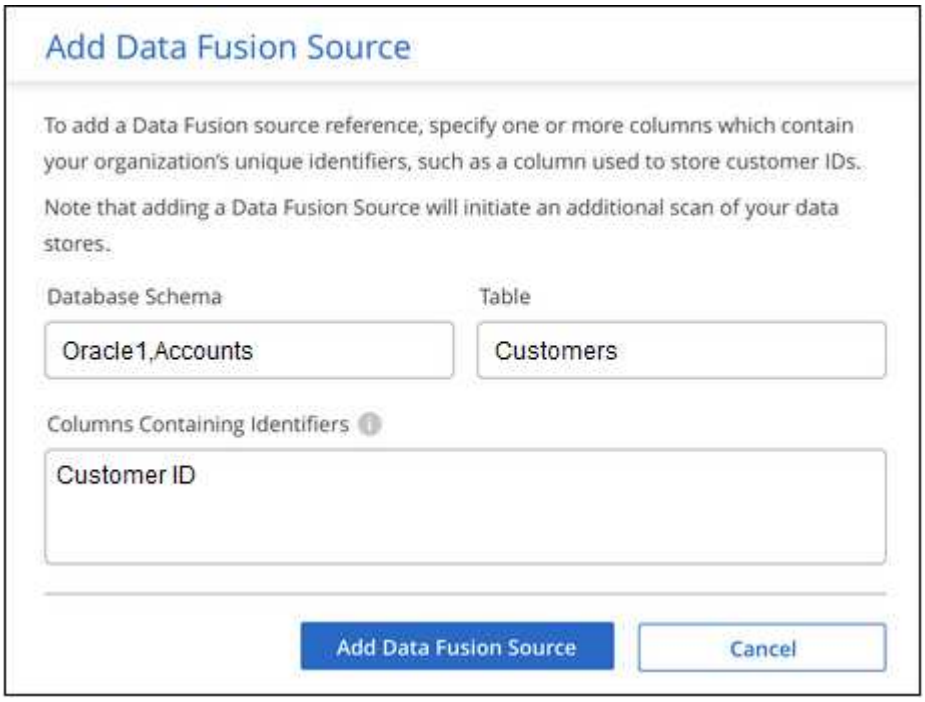
1. Nella pagina di configurazione, fare clic su **Manage Data Fusion** (Gestisci dati) nel database in cui risiedono i dati di origine.



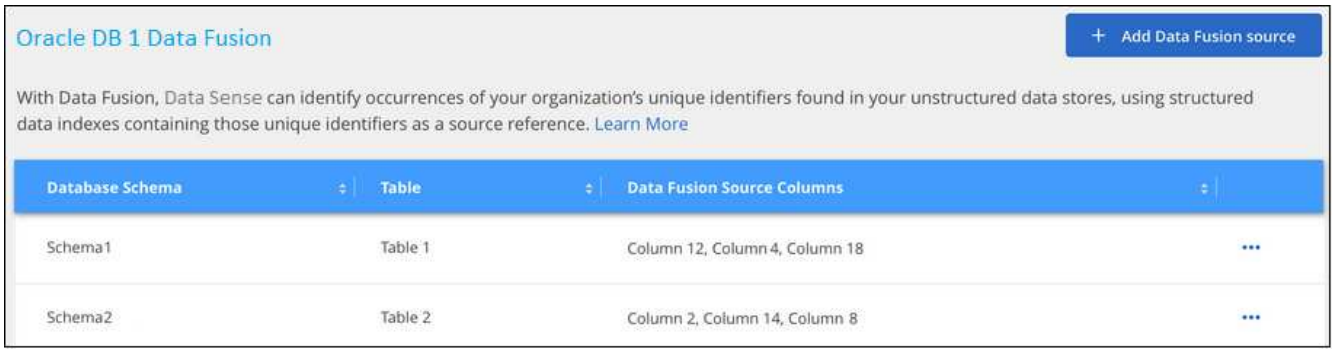
2. Fare clic su **Add Data Fusion source** (Aggiungi origine dati) nella pagina successiva.
3. Nella pagina *Aggiungi origine data Fusion*:

a. Selezionare lo schema del database dal menu a discesa.
b. Inserire il nome della tabella nello schema.
c. Inserire la colonna o le colonne che contengono gli identificatori univoci che si desidera utilizzare.

   Quando si aggiungono più colonne, inserire il nome di ciascuna colonna o il nome della vista tabella su una riga separata.

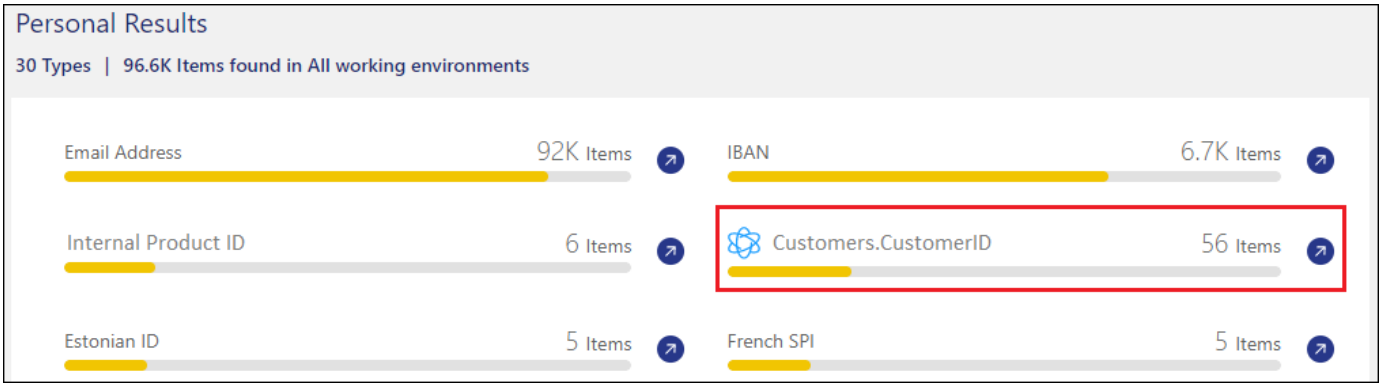


4. Fare clic su **Aggiungi origine Data Fusion**.



Risultati

Dopo la scansione successiva, i risultati includeranno queste nuove informazioni nella dashboard di conformità nella sezione "risultati personali" e nella pagina delle indagini nel filtro "dati personali". Il nome utilizzato per il classificatore viene visualizzato nell'elenco dei filtri, ad esempio `Customers.CustomerID`.



Eliminare un'origine Data Fusion

Se a un certo punto si decide di non eseguire la scansione dei file utilizzando una determinata origine Data Fusion, è possibile selezionare la riga di origine dalla pagina di inventario Data Fusion e fare clic su **Elimina origine Data Fusion**.

Aggiungere parole chiave personalizzate da un elenco di parole

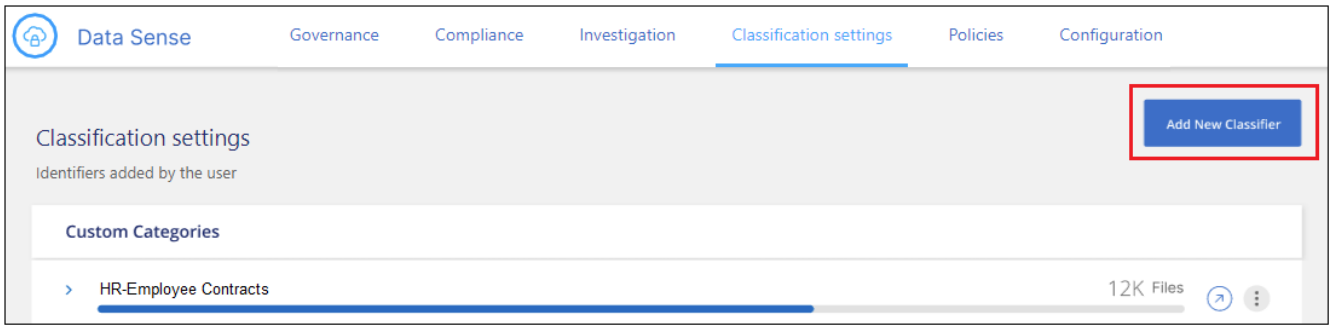
È possibile aggiungere parole chiave personalizzate alla classificazione BlueXP in modo che identifichi la posizione in cui tali informazioni sono contenute nei dati. È possibile aggiungere le parole chiave inserendo ciascuna parola che si desidera venga riconosciuta dalla classificazione BlueXP. Le parole chiave vengono aggiunte alle parole chiave predefinite già utilizzate dalla classificazione BlueXP e i risultati saranno visibili nella sezione modelli personali.

Ad esempio, è possibile visualizzare i nomi dei prodotti interni in tutti i file per assicurarsi che non siano accessibili in posizioni non sicure.

Dopo aver aggiornato le parole chiave personalizzate, la classificazione BlueXP riavvia la scansione di tutte le origini dati. Una volta completata la scansione, i nuovi risultati verranno visualizzati nella dashboard di conformità della classificazione BlueXP nella sezione "risultati personali" e nella pagina delle indagini nel filtro "dati personali".

Fasi

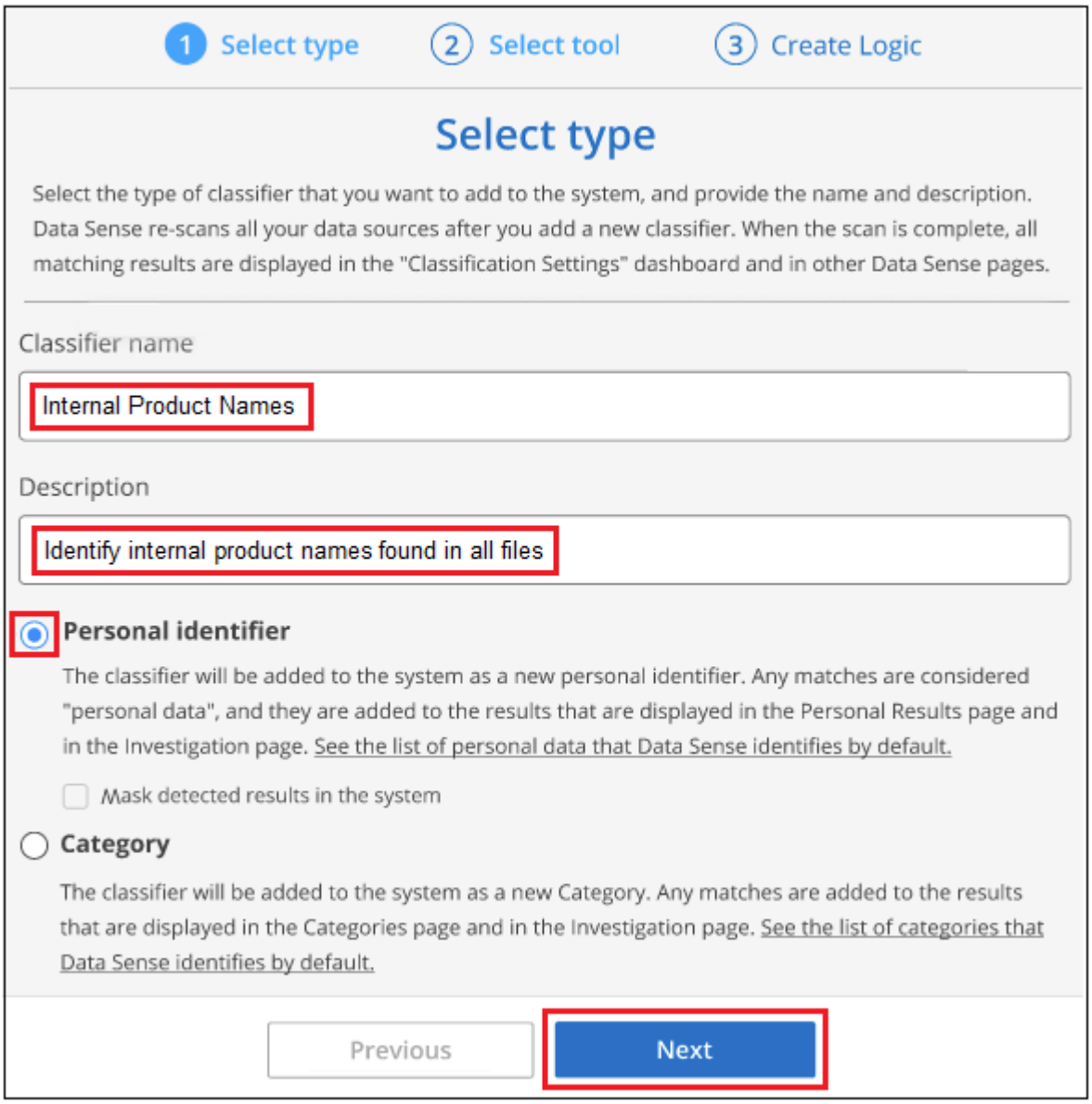
1. Dalla scheda *Impostazioni classificazione*, fare clic su **Aggiungi nuovo classificatore** per avviare la procedura guidata *Aggiungi classificatore personalizzato*.



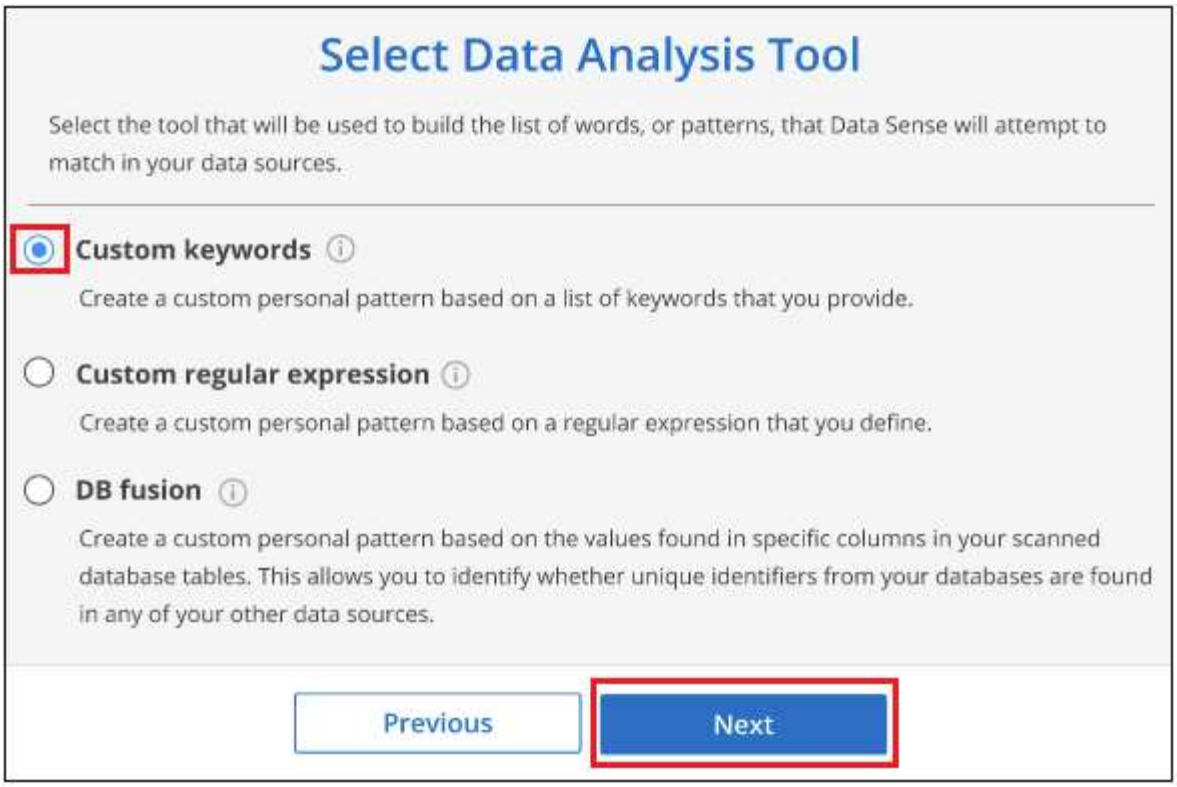
2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Personal identifier**, quindi fare clic su **Next**.

   Il nome immesso viene visualizzato nell'interfaccia utente di classificazione BlueXP come intestazione per i file sottoposti a scansione che corrispondono ai requisiti del classificatore e come nome del filtro nella pagina di analisi.

   Puoi anche selezionare la casella "Mask Detected Results in the system" (maschera risultati rilevati nel sistema) in modo che il risultato completo non venga visualizzato nell'interfaccia utente. Ad esempio, è possibile nascondere i numeri completi della carta di credito o dati personali simili (la maschera appare nell'interfaccia utente come segue: "Pass:[**] **** **** ****" 3434).

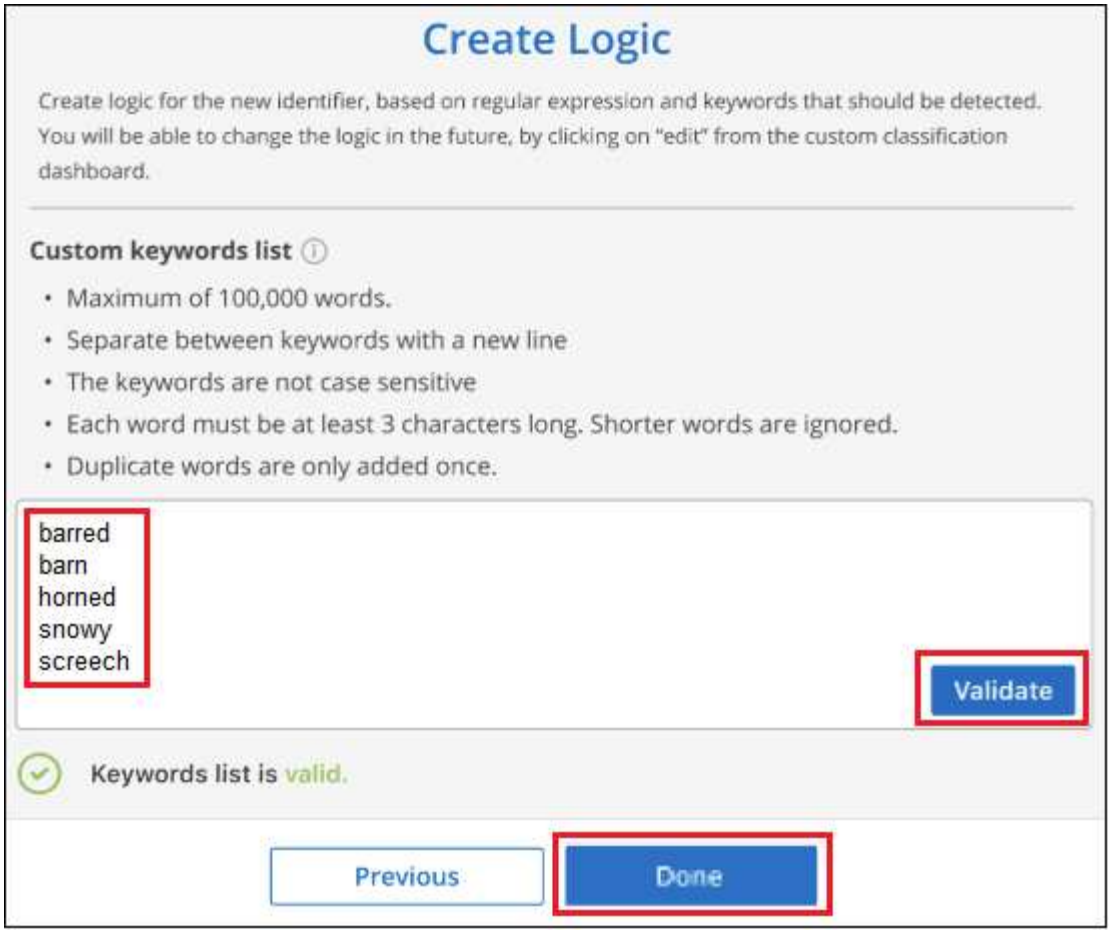


3. Nella pagina *Select Data Analysis Tool*, selezionare **Custom Keywords** come metodo da utilizzare per definire il classificatore, quindi fare clic su **Next**.



4. Nella pagina *Create Logic*, immettere le parole chiave che si desidera riconoscere, ciascuna parola su una riga separata, quindi fare clic su **Validate**.

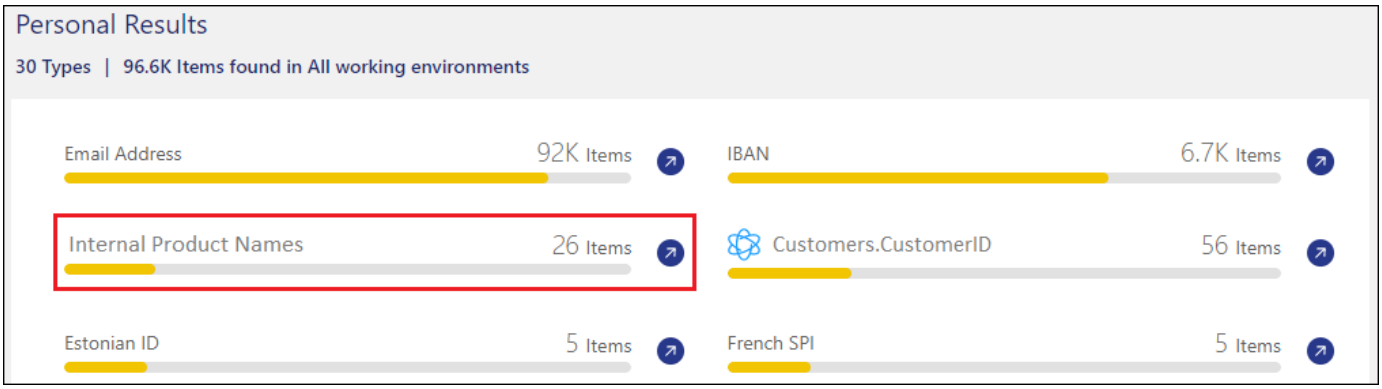
   La schermata seguente mostra i nomi dei prodotti interni (diversi tipi di gufi). La ricerca della classificazione BlueXP per questi elementi non fa distinzione tra maiuscole e minuscole.



5. Fare clic su **Done** e la classificazione BlueXP inizia a eseguire una nuova scansione dei dati.

Risultati

Una volta completata la scansione, i risultati includeranno queste nuove informazioni nella dashboard di conformità nella sezione "risultati personali" e nella pagina delle indagini nel filtro "dati personali".



Come potete vedere, il nome del classificatore viene utilizzato come nome nel pannello risultati personali. In questo modo è possibile attivare diversi gruppi di parole chiave e visualizzare i risultati per ciascun gruppo.

Aggiungere identificatori di dati personali personalizzati utilizzando un regex

È possibile aggiungere un modello personale per identificare informazioni specifiche nei dati utilizzando un'espressione regolare personalizzata (regex). Ciò consente di creare un nuovo regex personalizzato per identificare nuovi elementi di informazioni personali che non esistono ancora nel sistema. Il regex viene

aggiunto ai modelli predefiniti esistenti già utilizzati dalla classificazione BlueXP e i risultati saranno visibili nella sezione modelli personali.

Ad esempio, è possibile visualizzare la posizione in cui gli ID prodotto interni sono menzionati in tutti i file. Se l'ID prodotto ha una struttura chiara, ad esempio, si tratta di un numero a 12 cifre che inizia con 201, è possibile utilizzare la funzione regex personalizzata per cercarlo nei file. L'espressione regolare per questo esempio è **{9} b**.

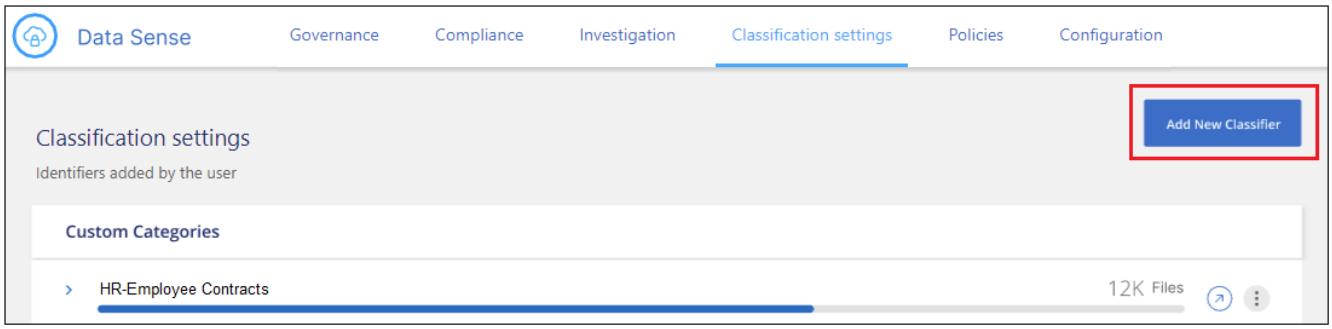
Dopo aver aggiunto il regex, la classificazione BlueXP riavvia la scansione di tutte le origini dati. Una volta completata la scansione, i nuovi risultati verranno visualizzati nella dashboard di conformità della classificazione BlueXP nella sezione "risultati personali" e nella pagina delle indagini nel filtro "dati personali".

Per assistenza nella creazione dell'espressione regolare, fare riferimento alla sezione "Espressioni regolari 101". Scegliere **Python** per il flavor per vedere i tipi di risultati che la classificazione BlueXP corrisponde all'espressione regolare. Il "Pagina del tester Python Regex" è utile anche visualizzando una rappresentazione grafica dei pattern.

> Attualmente non è consentito l'utilizzo di flag pattern quando si crea un regex - questo significa che non si dovrebbe utilizzare "/".

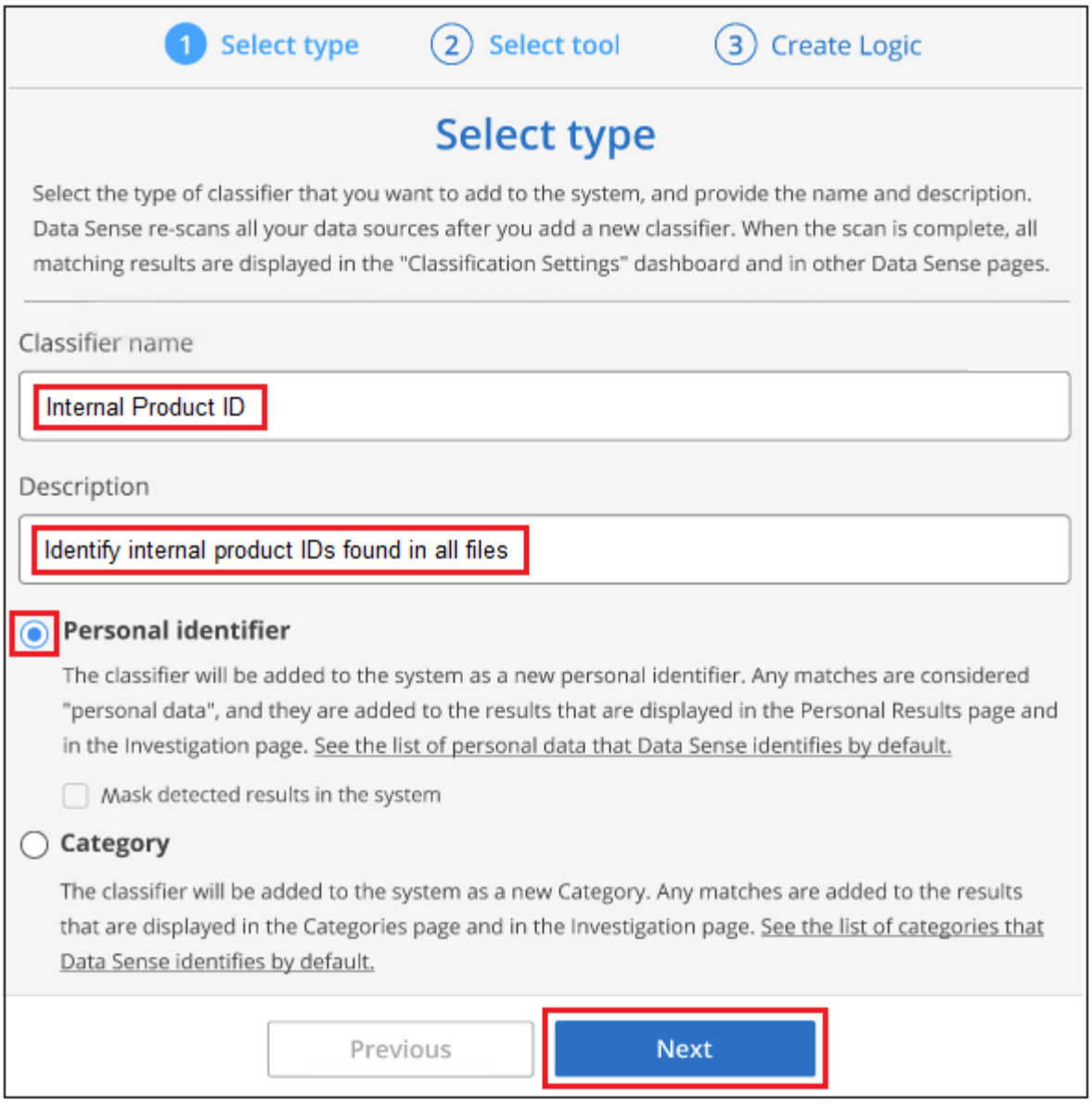
Fasi

1. Dalla scheda *Impostazioni classificazione*, fare clic su **Aggiungi nuovo classificatore** per avviare la procedura guidata *Aggiungi classificatore personalizzato*.

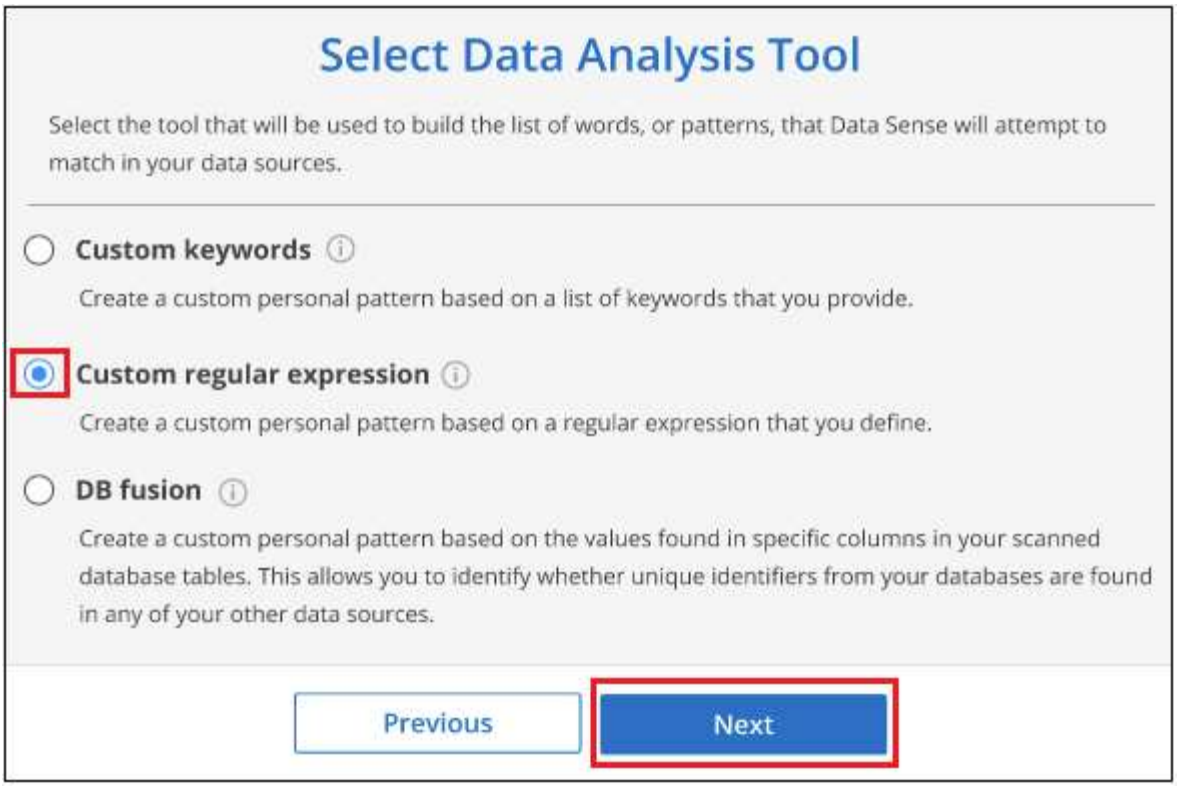


2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Personal identifier**, quindi fare clic su **Next**.

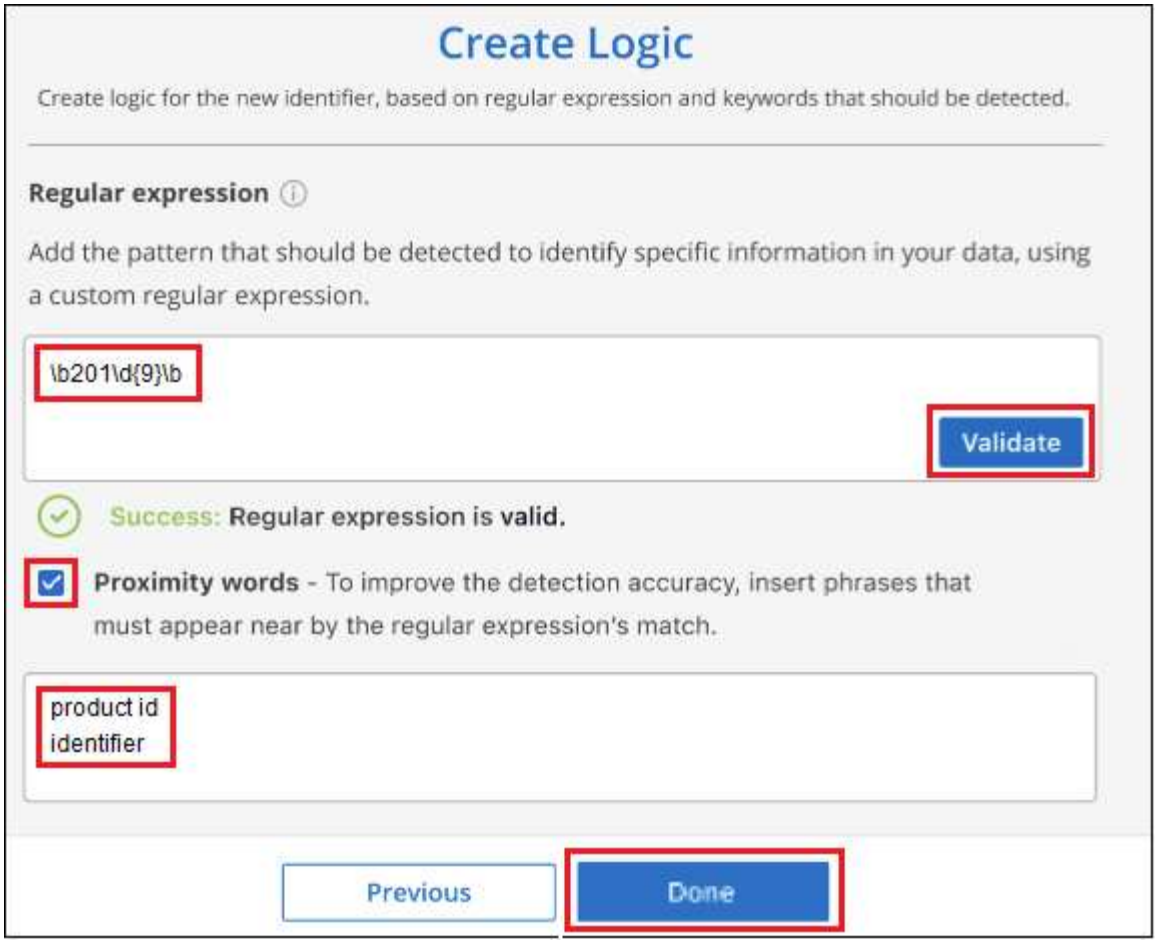
   Il nome immesso viene visualizzato nell'interfaccia utente di classificazione BlueXP come intestazione per i file sottoposti a scansione che corrispondono ai requisiti del classificatore e come nome del filtro nella pagina di analisi. Puoi anche selezionare la casella "Mask Detected Results in the system" (maschera risultati rilevati nel sistema) in modo che il risultato completo non venga visualizzato nell'interfaccia utente. Ad esempio, è possibile nascondere i numeri completi della carta di credito o dati personali simili.



3. Nella pagina *Select Data Analysis Tool*, selezionare **Custom Regular Expression** come metodo da utilizzare per definire il classificatore, quindi fare clic su **Next**.

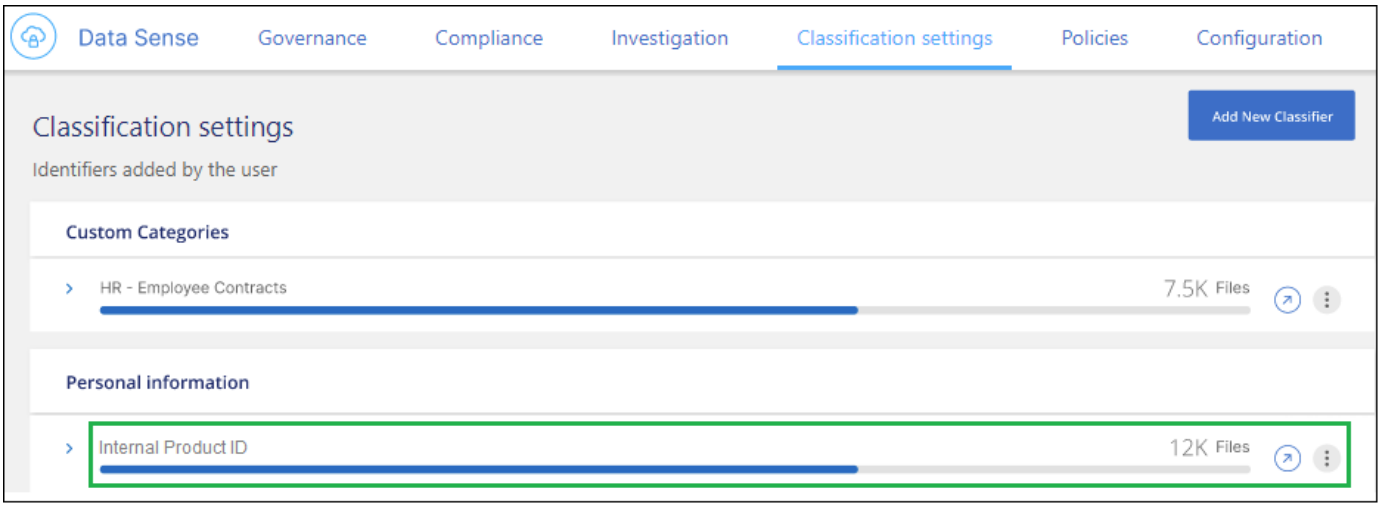


4. Nella pagina *Create Logic*, immettere l'espressione regolare e le parole di prossimità, quindi fare clic su **Done**.
   a. È possibile immettere qualsiasi espressione regolare legale. Fare clic sul pulsante **Validate** (convalida) per verificare che la classificazione BlueXP sia valida e che non sia troppo ampia, il che significa che restituirà troppi risultati.
   b. In alternativa, è possibile inserire alcune parole di prossimità per migliorare la precisione dei risultati. Si tratta di parole che in genere si trovano entro 300 caratteri del modello che si sta cercando (prima o dopo il modello trovato). Inserire ciascuna parola o frase su una riga separata.



Risultati

Il classificatore viene aggiunto e la classificazione BlueXP inizia a ripetere la scansione di tutte le origini dati. Viene visualizzata nuovamente la pagina Custom Classifier (classificatori personalizzati) in cui è possibile visualizzare il numero di file corrispondenti al nuovo classificatore. I risultati della scansione di tutte le origini dati richiederanno del tempo a seconda del numero di file da sottoporre a scansione.



Aggiungere categorie personalizzate

La classificazione BlueXP prende i dati che scansionano e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi di intelligenza artificiale del contenuto e dei metadati di ciascun file. "Vedere

l'elenco delle categorie predefinite".

Le categorie possono aiutarti a capire cosa accade con i tuoi dati mostrando i tipi di informazioni di cui disponi. Ad esempio, una categoria come *resumes* o *contratti dipendente* può includere dati sensibili. Quando si analizzano i risultati, è possibile che i contratti dei dipendenti siano memorizzati in una posizione non sicura. A questo punto, è possibile correggere il problema.

È possibile aggiungere categorie personalizzate alla classificazione BlueXP in modo da identificare dove si trovano le categorie di informazioni uniche per il proprio data estate nei dati. È possibile aggiungere ciascuna categoria creando file di "training" che contengono le categorie di dati che si desidera identificare, quindi fare in modo che la classificazione BlueXP scansioni tali file per "apprendere" attraverso l'ai in modo che possa identificare tali dati nelle origini dati. Le categorie vengono aggiunte alle categorie predefinite esistenti già identificate dalla classificazione BlueXP e i risultati sono visibili nella sezione Categorie.

Ad esempio, è possibile vedere dove si trovano i file di installazione compressi in formato .gz nei file in modo da poterli rimuovere, se necessario.

Dopo aver aggiornato le categorie personalizzate, la classificazione BlueXP riavvia la scansione di tutte le origini dati. Una volta completata la scansione, i nuovi risultati verranno visualizzati nella dashboard di conformità della classificazione BlueXP nella sezione "Categorie" e nella pagina delle indagini nel filtro "Categoria". "Scopri come visualizzare i file in base alle categorie".

Di cosa hai bisogno

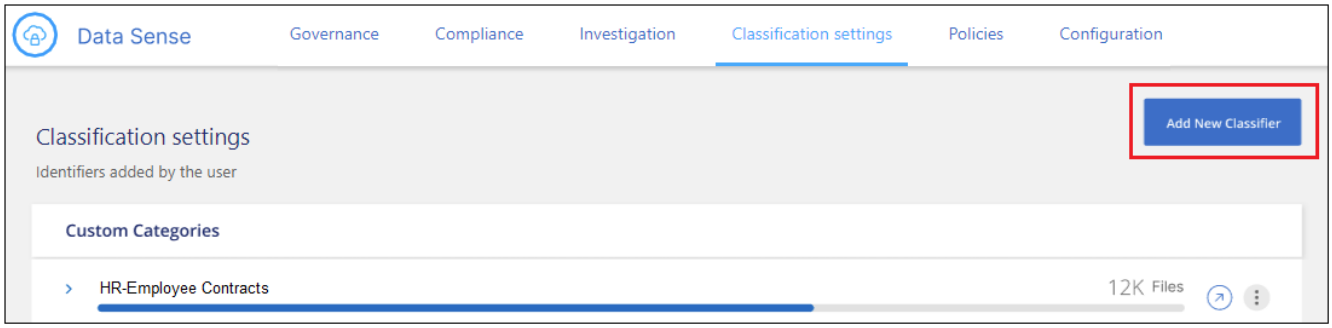
È necessario creare un minimo di 25 file di training contenenti esempi delle categorie di dati che si desidera vengano riconosciute dalla classificazione BlueXP. Sono supportati i seguenti tipi di file:

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

I file devono essere di almeno 100 byte e devono trovarsi in una cartella accessibile dalla classificazione BlueXP.

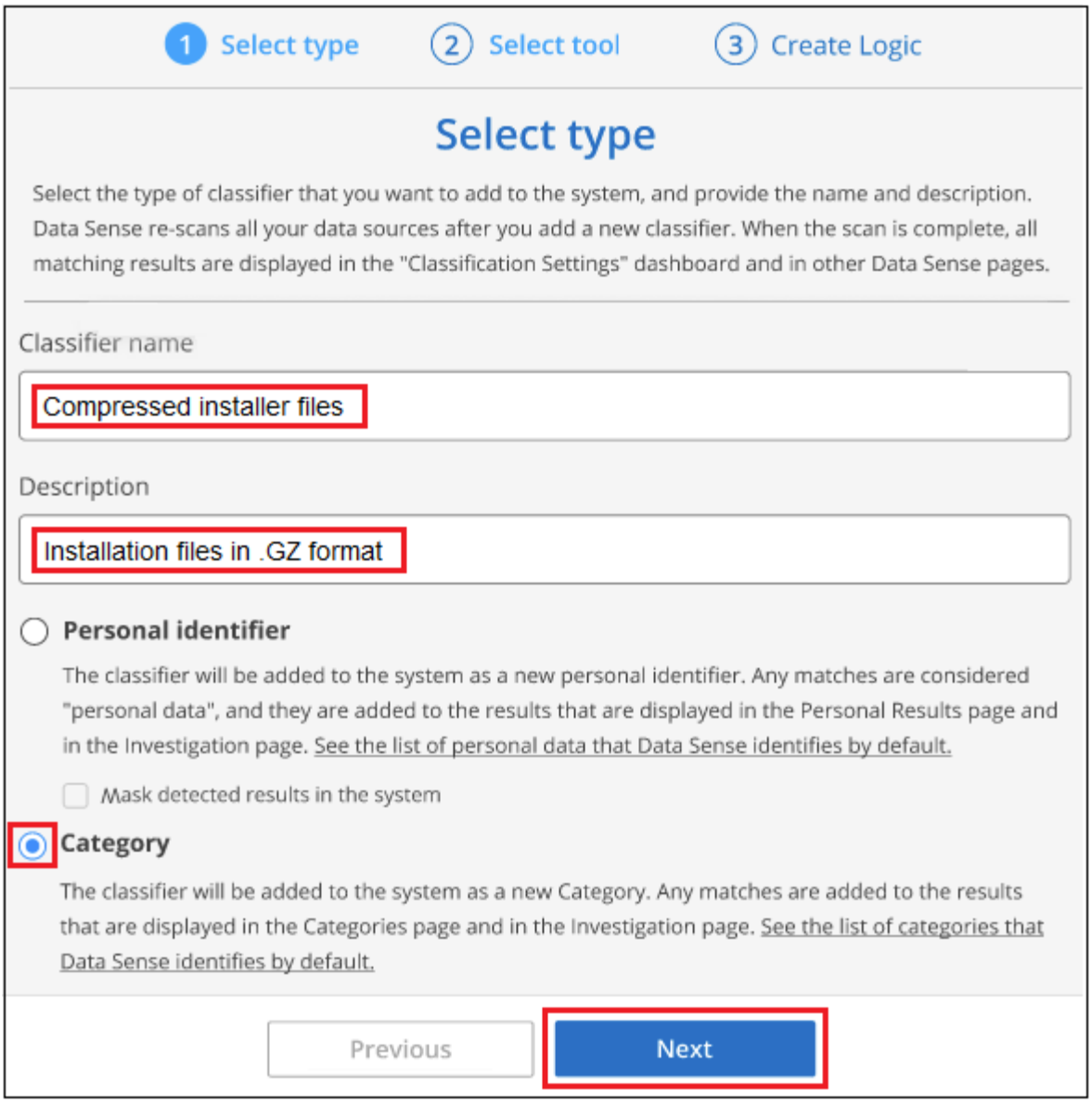
Fasi

1. Dalla scheda *Impostazioni classificazione*, fare clic su **Aggiungi nuovo classificatore** per avviare la procedura guidata *Aggiungi classificatore personalizzato*.

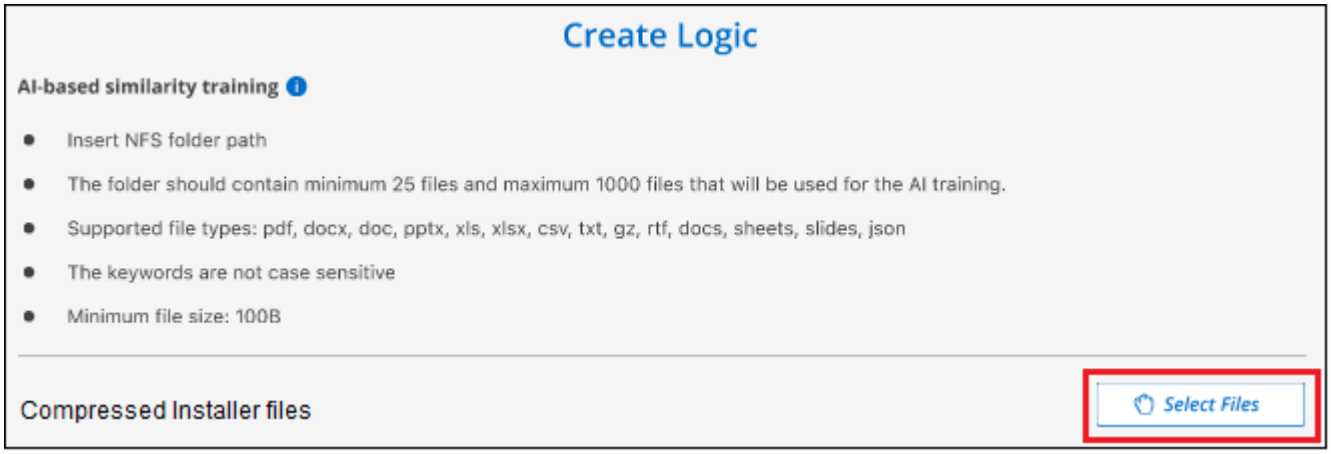


2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Category**, quindi fare clic su **Next**.

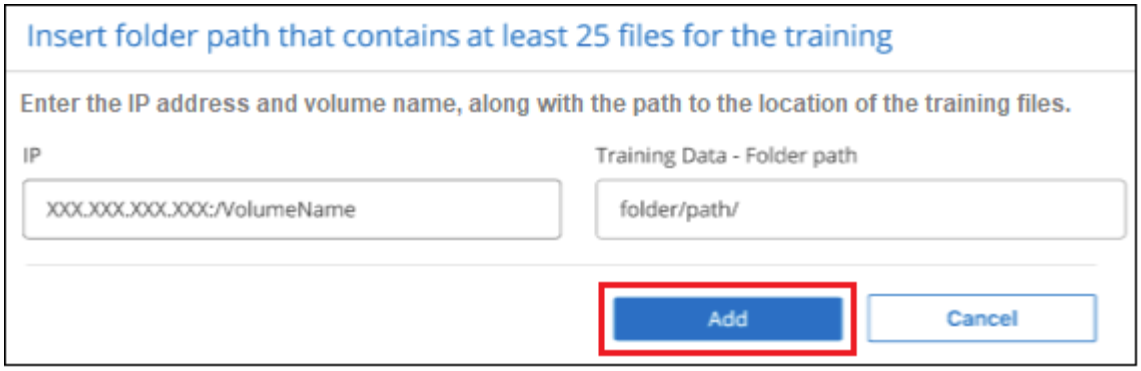
   Il nome immesso viene visualizzato nell'interfaccia utente di classificazione BlueXP come intestazione per i file sottoposti a scansione che corrispondono alla categoria di dati che si sta definendo e come nome del filtro nella pagina di analisi.



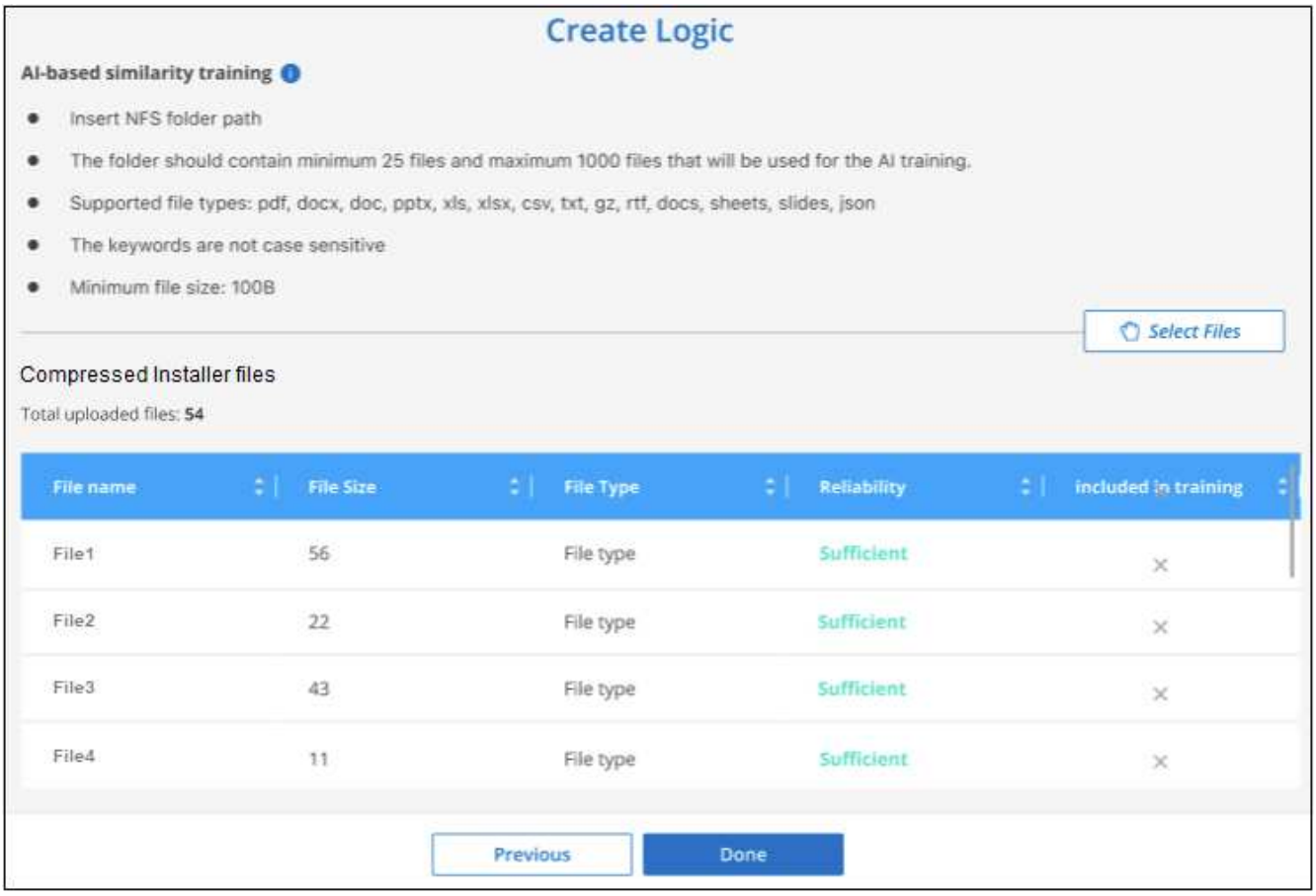
3. Nella pagina *Create Logic*, assicurarsi di aver preparato i file di apprendimento, quindi fare clic su **Select Files** (Seleziona file).



4. Inserire l'indirizzo IP del volume e il percorso in cui si trovano i file di training, quindi fare clic su **Aggiungi**.



5. Verificare che i file di training siano stati riconosciuti dalla classificazione BlueXP. Fare clic su **x** per rimuovere i file di training che non soddisfano i requisiti. Quindi fare clic su **fine**.



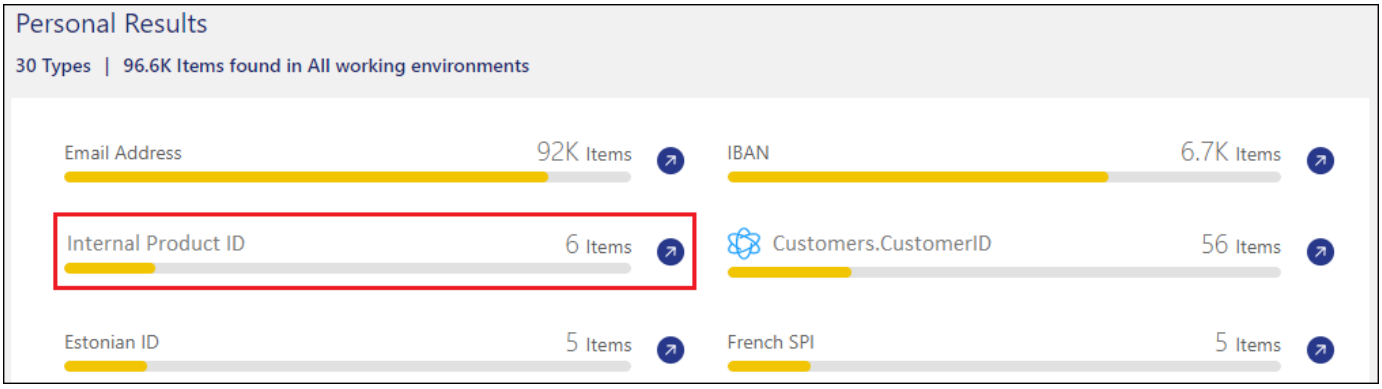
Risultati

La nuova categoria viene creata in base alla definizione dei file di training e aggiunta alla classificazione BlueXP. Quindi, la classificazione BlueXP inizia a ripetere la scansione di tutte le origini dati per identificare i file che rientrano in questa nuova categoria. Viene visualizzata nuovamente la pagina Custom Classifier (classificatori personalizzati) in cui è possibile visualizzare il numero di file corrispondenti alla nuova categoria. I risultati della scansione di tutte le origini dati richiederanno del tempo a seconda del numero di file da sottoporre a scansione.

Visualizzare i risultati dei classificatori personalizzati

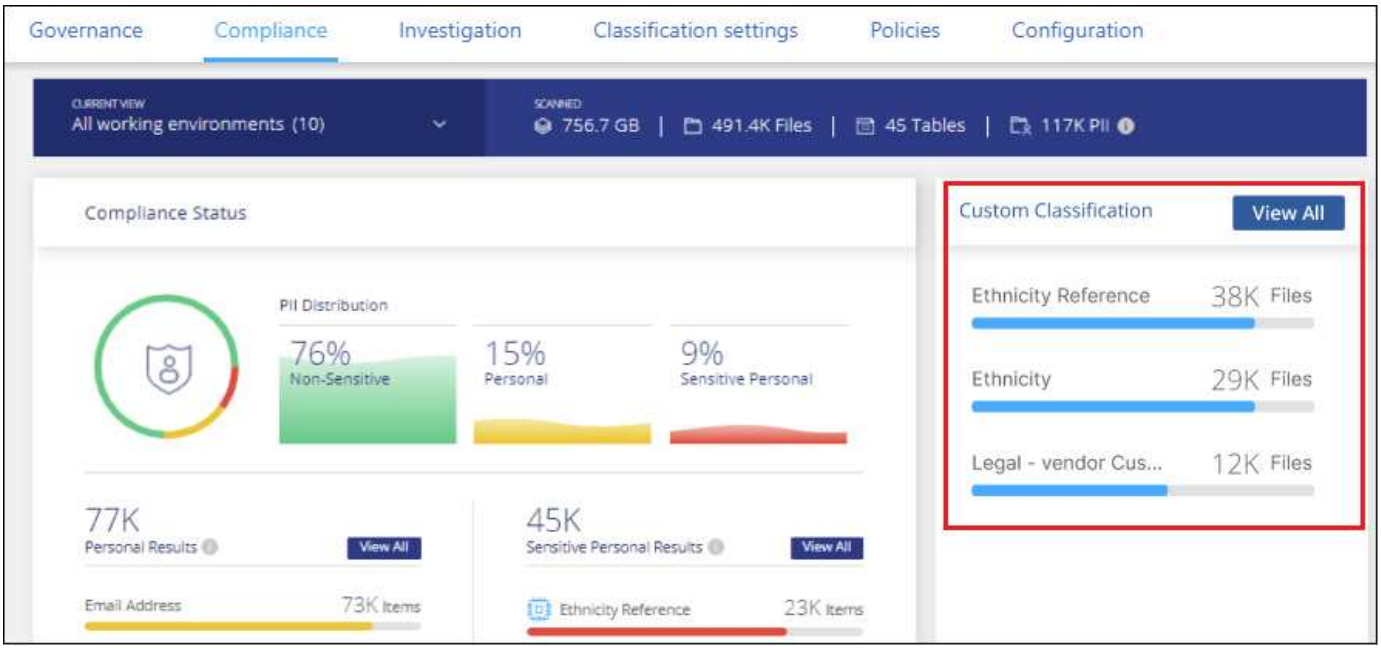
È possibile visualizzare i risultati da qualsiasi classificatore personalizzato nella dashboard di conformità e nella pagina di analisi. Ad esempio, questa schermata mostra le informazioni corrispondenti nella dashboard di

conformità nella sezione "risultati personali".



Fare clic su Per visualizzare i risultati dettagliati nella pagina delle analisi.

Inoltre, tutti i risultati del classificatore personalizzato vengono visualizzati nella scheda classificatori personalizzati e i primi 6 risultati del classificatore personalizzato vengono visualizzati nella dashboard di conformità, come mostrato di seguito.

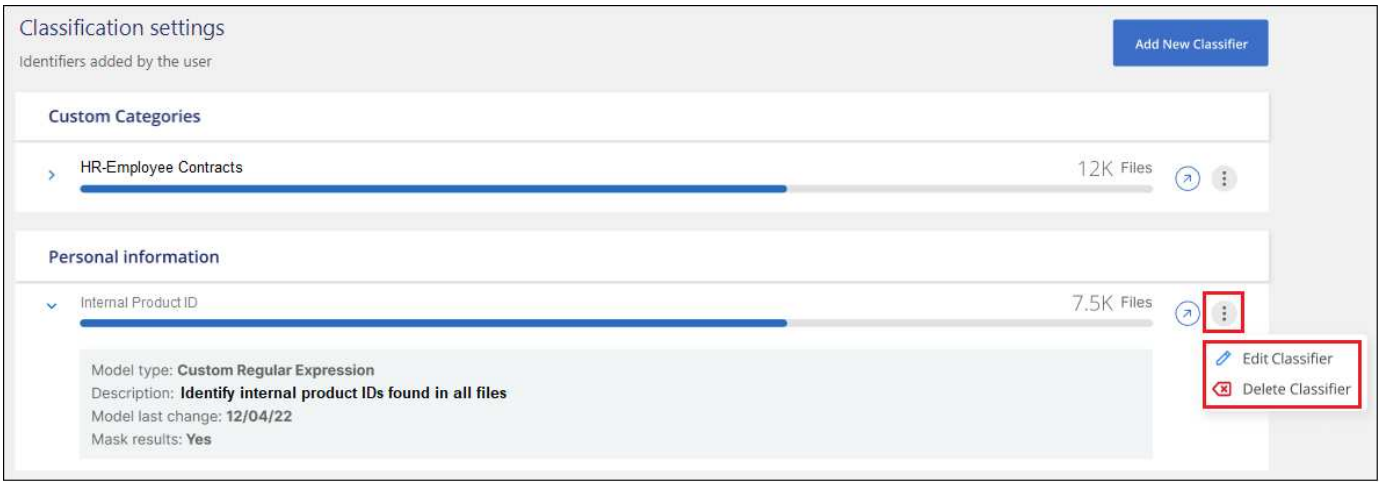


Gestire classificatori personalizzati

È possibile modificare qualsiasi classificatore personalizzato creato utilizzando il pulsante **Edit Classifier** (Modifica classificatore).

Al momento non è possibile modificare i classificatori Data Fusion.

Se poi decidi di non aver bisogno della classificazione BlueXP per identificare i modelli personalizzati aggiunti, puoi utilizzare il pulsante **Delete Classifier** (Elimina classificatore) per rimuovere ogni elemento.



Escludere directory specifiche dalle scansioni di classificazione BlueXP

Se si desidera che la classificazione BlueXP escluda la scansione dei dati che risiedono in determinate directory di origine dati, è possibile aggiungere questi nomi di directory a un file di configurazione. Dopo aver applicato questa modifica, il motore di classificazione BlueXP escluderà la scansione dei dati in tali directory.

La classificazione BlueXP è configurata per impostazione predefinita in modo da escludere la scansione dei dati snapshot del volume perché tale contenuto è identico al contenuto del volume.

Questa funzionalità è disponibile con la classificazione BlueXP versione 1,29 e successive (a partire da marzo 2024).

Origini dati supportate

L'esclusione di directory specifiche dalle scansioni di classificazione BlueXP è supportata per le condivisioni NFS e CIFS nelle seguenti origini dati:

- ONTAP on-premise
- Cloud Volumes ONTAP
- Amazon FSX per NetApp ONTAP
- Azure NetApp Files
- Condivisioni di file generiche

Definire le directory da escludere dalla scansione

Prima di poter escludere le directory dalla scansione della classificazione, è necessario accedere al sistema di classificazione BlueXP in modo da poter modificare un file di configurazione ed eseguire uno script. Scopri come "Accedi al sistema di classificazione BlueXP" A seconda che il software sia stato installato manualmente su una macchina Linux o se l'istanza è stata distribuita nel cloud.

- È possibile escludere un massimo di 50 percorsi di directory per sistema di classificazione BlueXP.
- L'esclusione dei percorsi di directory può influire sui tempi di scansione.

Fasi

1. Nel sistema di classificazione BlueXP, vai a "/opt/netapp/config/custom_Configuration" e apri il file `data_provider.yaml`.
2. Nella sezione "data_providers", sotto la riga "exclude:", immettere i percorsi di directory da escludere. Ad esempio:

   ```
   exclude:
   - "folder1"
   - "folder2"
   ```

   Non modificare altro contenuto in questo file.

3. Salvare le modifiche apportate al file.
4. Andare a "/opt/netapp/Datasense/tools/customer_Configuration/data_provider" ed eseguire il seguente script:

   ```
   update_data_providers_from_config_file.sh
   ```

   Questo comando commette le directory da escludere dalla scansione al motore di classificazione.

Risultato

Tutte le scansioni successive dei dati escluderanno la scansione di quelle directory specificate.

È possibile aggiungere, modificare o eliminare elementi dall'elenco Escludi utilizzando gli stessi passaggi. L'elenco di esclusione rivisto verrà aggiornato dopo l'esecuzione dello script per confermare le modifiche.

Esempi

Configurazione 1:

Ogni cartella che contiene "folder1" in qualsiasi punto del nome sarà esclusa da tutte le origini dati.

```
data_providers:
   exclude:
   - "folder1"
```

Risultati previsti per i percorsi che saranno esclusi:

- /CVO1/folder1
- /CVO1/folder1name
- /CVO1/folder10

- /CVO1/*folder1
- /CVO1/+folder1name
- /CVO1/notfolder10
- /CVO22/folder1
- /CVO22/folder1name
- /CVO22/folder10

Esempi di percorsi che non verranno esclusi:

- /CVO1/*cartella
- /CVO1/nome cartella
- /CVO22/*folder20

Configurazione 2:

Ogni cartella che contiene "*folder1" solo all'inizio del nome sarà esclusa.

```
data_providers:
   exclude:
   - "\\*folder1"
```

Risultati previsti per i percorsi che saranno esclusi:

- /CVO/*folder1
- /CVO/*folder1name
- /CVO/*folder10

Esempi di percorsi che non verranno esclusi:

- /CVO/folder1
- /CVO/folder1name
- /CVO/NOT*folder10

Configurazione 3:

Ogni cartella dell'origine dati "CVO22" che contiene "folder1" in qualsiasi punto del nome sarà esclusa.

```
data_providers:
   exclude:
   - "CVO22/folder1"
```

Risultati previsti per i percorsi che saranno esclusi:

- /CVO22/folder1
- /CVO22/folder1name
- /CVO22/folder10

Esempi di percorsi che non verranno esclusi:

- /CVO1/folder1
- /CVO1/folder1name
- /CVO1/folder10

Escape di caratteri speciali nei nomi delle cartelle

Se si dispone di un nome di cartella che contiene uno dei seguenti caratteri speciali e si desidera escludere la scansione dei dati contenuti in tale cartella, sarà necessario utilizzare la sequenza di escape \\ prima del nome della cartella.

```
 ., +, *, ?, ^, $, (, ), [, ], {, }, |
Ad esempio:
```

Percorso in origine: `/project/*not_to_scan`

Sintassi nel file di esclusione: `"\\*not_to_scan"`

Consente di visualizzare l'elenco di esclusione corrente

È possibile per i contenuti di `data_provider.yaml` il file di configurazione deve essere diverso da quello che è stato effettivamente eseguito dopo l'esecuzione di `update_data_providers_from_config_file.sh` script. Per visualizzare l'elenco corrente delle directory che hai escluso dalla scansione della classificazione BlueXP, esegui il seguente comando da "/opt/netapp/Datasense/tools/customer_Configuration/data_provider":

```
get_data_providers_configuration.sh
```

Visualizzazione dello stato delle azioni di compliance

Quando si esegue un'azione asincrona dal riquadro dei risultati dell'analisi su molti file, ad esempio, spostando o eliminando 100 file, il processo può richiedere del tempo. Puoi monitorare lo stato di queste azioni nel pannello *Action Status* per sapere quando sono state applicate a tutti i file.

In questo modo è possibile visualizzare le azioni che sono state completate correttamente, quelle attualmente in corso e quelle che hanno avuto esito negativo, in modo da poter diagnosticare e risolvere eventuali problemi. Tenere presente che le brevi operazioni che vengono completate rapidamente, ad esempio lo spostamento di un singolo file, non vengono visualizzate nel riquadro Stato azioni.

Lo stato può essere:

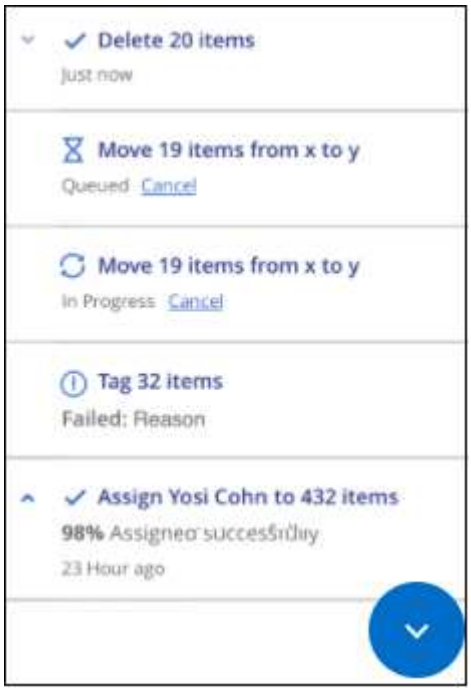
- Operazione riuscita - un'azione di classificazione BlueXP è terminata e tutti gli elementi sono riusciti.
- Successo parziale - Un'azione di classificazione BlueXP è terminata e alcuni elementi non sono riusciti e altri sono riusciti.
- In corso - l'azione è ancora in corso.
- Accodato - l'azione non è stata avviata.

- Annullato - l'azione è stata annullata.
- Non riuscito - l'azione non è riuscita.

Nota: È possibile annullare le azioni con stato "in coda" o "in corso".

Fasi

1. Nella parte inferiore destra dell'interfaccia utente di classificazione di BlueXP, viene visualizzato il pulsante **Actions Status** (Stato azioni) .
2. Fare clic su questo pulsante per visualizzare le 20 azioni più recenti.



È possibile fare clic sul nome di un'azione per visualizzare i dettagli corrispondenti a tale operazione.

Definire altri ID di gruppo come aperti all'organizzazione

Quando gli ID di gruppo (GID) sono allegati a file o cartelle nelle condivisioni di file NFS, definiscono le autorizzazioni per il file o la cartella, ad esempio se sono "aperti all'organizzazione". Se alcuni ID gruppo (GID) non sono inizialmente impostati con il livello di autorizzazione "Apri all'organizzazione", è possibile aggiungere tale autorizzazione al GID in modo che tutti i file e le cartelle che hanno quel GID allegato saranno considerati "aperti all'organizzazione".

Dopo aver apportato questa modifica e aver eseguito nuovamente la classificazione BlueXP per i file e le cartelle, tutti i file e le cartelle con questi ID di gruppo allegati mostreranno questa autorizzazione nella pagina Dettagli analisi e verranno visualizzati anche nei report in cui vengono visualizzate le autorizzazioni dei file.

Per attivare questa funzionalità, devi accedere al sistema di classificazione BlueXP in modo da poter modificare un file di configurazione ed eseguire uno script. Scopri come "Accedi al sistema di classificazione BlueXP" A seconda che il software sia stato installato manualmente su una macchina Linux o se l'istanza è

stata distribuita nel cloud.

Aggiungere l’autorizzazione "Apri all’organizzazione" agli ID gruppo

È necessario disporre dei numeri ID gruppo (GID) prima di iniziare questa attività.

Fasi

1. Nel sistema di classificazione BlueXP, vai a "/opt/netapp/config/custom_Configuration" e apri il file `data_provider.yaml`.
2. Nella riga "organization_group_ids: []" aggiungere gli ID del gruppo. Ad esempio:

   ```
   organization_group_ids: [1014, 1015, 21, 2021, 1013, 2020, 1018, 1019]
   ```

   Non modificare altro contenuto in questo file.

3. Salvare le modifiche apportate al file.
4. Andare a "/opt/netapp/Datasense/tools/customer_Configuration/data_provider" ed eseguire il seguente script:

   ```
   update_data_providers_from_config_file.sh
   ```

   Questo comando assegna le autorizzazioni ID gruppo modificate al motore di classificazione.

Risultato

Tutte le successive scansioni dei dati identificheranno i file o le cartelle che hanno questi ID di gruppo allegati come "aperti all’organizzazione".

È possibile modificare l’elenco degli ID di gruppo ed eliminare gli ID di gruppo aggiunti in passato utilizzando la stessa procedura. L’elenco rivisto degli ID di gruppo verrà aggiornato dopo l’esecuzione dello script per confermare le modifiche.

Consente di visualizzare l’elenco corrente degli ID di gruppo

È possibile per i contenuti di `data_provider.yaml` il file di configurazione deve essere diverso da quello che è stato effettivamente eseguito dopo l’esecuzione di `update_data_providers_from_config_file.sh` script. Per visualizzare l’elenco corrente degli ID di gruppo che hai aggiunto alla classificazione BlueXP, esegui il seguente comando da "/opt/netapp/Datasense/tools/customer_Configuration/data_provider":

```
get_data_providers_configuration.sh
```

Controllare la cronologia delle azioni di classificazione di BlueXP

La classificazione BlueXP registra le attività di gestione eseguite sui file di tutti gli ambienti di lavoro e le origini dati che la classificazione BlueXP sta eseguendo. La

classificazione BlueXP registra anche le attività durante l'implementazione dell'istanza di classificazione BlueXP.

È possibile visualizzare il contenuto dei file di registro di controllo della classificazione BlueXP o scaricarli per verificare quali modifiche sono state apportate e quando. Ad esempio, è possibile visualizzare la richiesta emessa, l'ora della richiesta e i dettagli, ad esempio la posizione di origine nel caso in cui un file sia stato cancellato o la posizione di origine e destinazione nel caso in cui un file sia stato spostato.

Contenuto del file di log

Ogni riga del registro di controllo contiene informazioni in questo formato:

```
<full date> | <status> | ds_audit_logger | <module> | 0 | 0 | File <full file
path> deleted from device <device path> - <result>
```

- Data e ora - indicatore orario completo dell'evento
- Stato - INFORMAZIONI, AVVISO
- Tipo di azione (eliminare, copiare, spostare, creare policy, aggiornare policy, Eseguire nuovamente la scansione dei file, scaricare il report JSON, ecc.)
- Nome del file (se l'azione è rilevante per un file)
- Dettagli dell'azione - cosa è stato fatto: Dipende dall'azione
  - Nome policy
  - Per lo spostamento - origine e destinazione
  - Per la copia - origine e destinazione
  - Per tag - nome tag
  - Per assegnare a - nome utente
  - Per avvisi e-mail - indirizzo e-mail/account

Ad esempio, le seguenti righe del file di log mostrano un'operazione di copia riuscita e un'operazione di copia non riuscita.

```
2022-06-06 15:23:08,910 | INFO | ds_audit_logger | es_scanned_file | 237 |
49 | Copy file /CIFS_share/data/dop1/random_positives.tsv from device
10.31.133.183 (type: SMB_SHARE) to device 10.31.130.133:/export_reports
(NFS_SHARE) - SUCCESS
2022-06-06 15:23:08,968 | WARNING | ds_audit_logger | es_scanned_file |
239 | 153 | Copy file /CIFS_share/data/compliance-netapp.tar.gz from
device 10.31.133.183 (type: SMB_SHARE) to device
10.31.130.133:/export_reports (NFS_SHARE) - FAILURE
```

Posizioni dei file di registro

I file di log dell'audit di gestione si trovano sulla macchina di classificazione BlueXP in: `/opt/netapp/audit_logs/`

I file di log dell'audit dell'installazione vengono scritti in `/opt/netapp/install_logs/`

Ogni file di log può avere una dimensione massima di 10 MB. Una volta raggiunto questo limite, viene avviato un nuovo file di log. I file di log sono denominati "DataSense_audit.log", "DataSense_audit.log.1", "DataSense_audit.log.2" e così via. Sul sistema vengono conservati al massimo 100 file di registro - i file di registro meno recenti vengono eliminati automaticamente dopo aver raggiunto il limite massimo consentito.

Accedere ai file di registro

Sarà necessario accedere al sistema di classificazione BlueXP per accedere ai file di log. Scopri come "Accedi al sistema di classificazione BlueXP" A seconda che il software sia stato installato manualmente su una macchina Linux o se l'istanza è stata distribuita nel cloud.

Riduzione della velocità di scansione della classificazione BlueXP

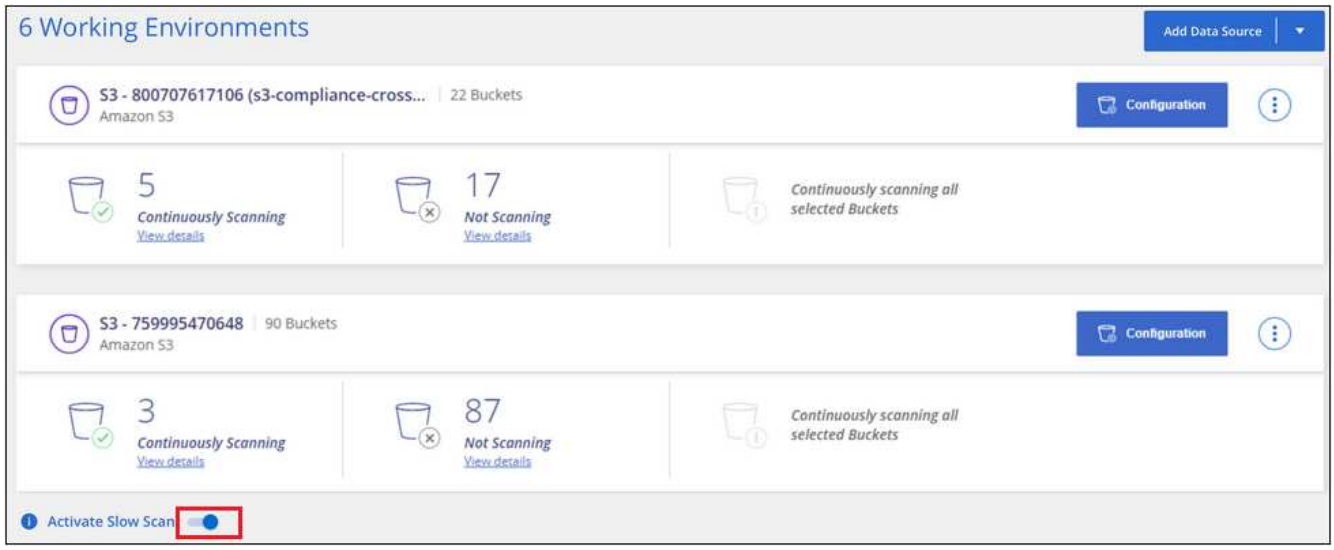
Le scansioni dei dati hanno un impatto trascurabile sui sistemi storage e sui dati. Tuttavia, se si è preoccupati anche di un impatto molto ridotto, è possibile configurare la classificazione BlueXP per eseguire scansioni "lente".

Se attivata, la scansione lenta viene utilizzata su tutte le origini dati, non è possibile configurare la scansione lenta per un singolo ambiente di lavoro o un'origine dati.

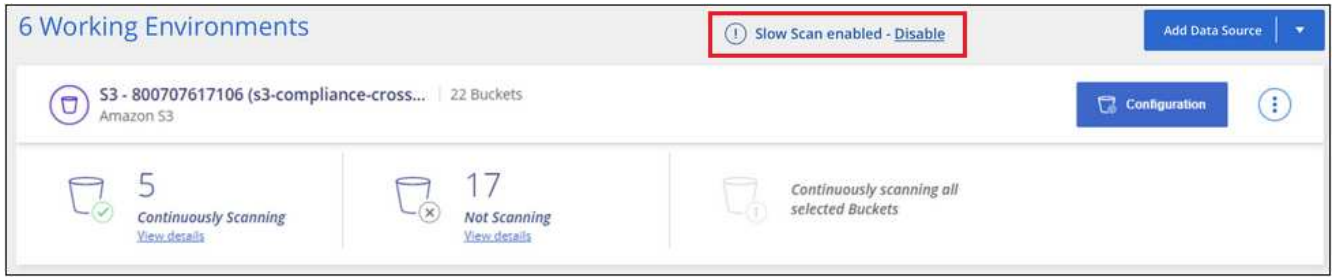
La velocità di scansione non può essere ridotta durante la scansione dei database.

Fasi

1. Nella parte inferiore della pagina *Configuration*, spostare il dispositivo di scorrimento verso destra per attivare la scansione lenta.



La parte superiore della pagina di configurazione indica che la scansione lenta è attivata.



2. È possibile disattivare la scansione lenta facendo clic su **Disable** (Disattiva) da questo messaggio.

Rimozione delle origini dati dalla classificazione BlueXP

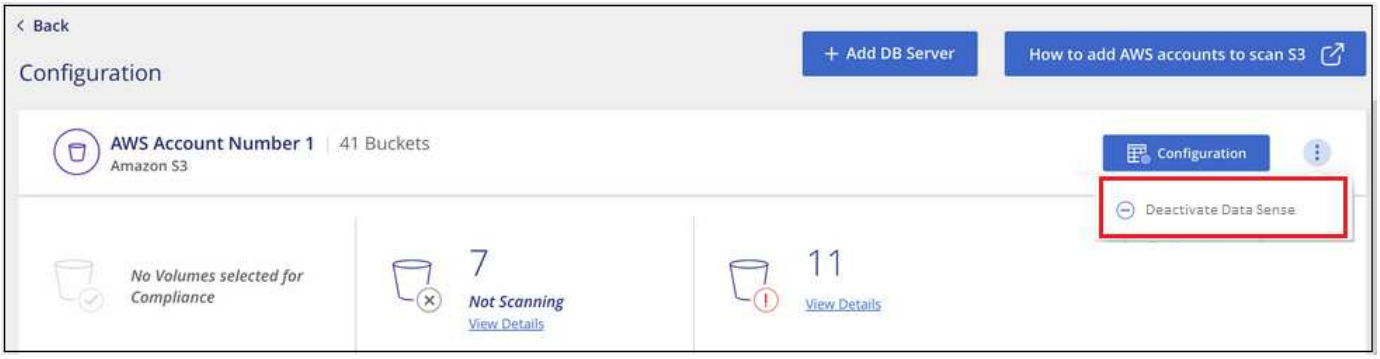
Se necessario, è possibile impedire alla classificazione BlueXP di eseguire la scansione di uno o più ambienti di lavoro, database, gruppi di condivisione file, account OneDrive, account Google Drive, O SharePoint.

La ricarica per la scansione dei dati viene interrotta quando l'origine dati viene rimossa.

Disattivazione delle scansioni di compliance per un ambiente di lavoro

Quando si disattivano le scansioni, la classificazione BlueXP non esegue più la scansione dei dati nell'ambiente di lavoro e rimuove le informazioni indicizzate sulla conformità dall'istanza di classificazione BlueXP (i dati dell'ambiente di lavoro stesso non vengono cancellati).

1. Dalla pagina *Configuration*, fare clic su ⋮ Nella riga dell'ambiente di lavoro, quindi fare clic su **Disattiva rilevamento dati**.



È inoltre possibile disattivare le scansioni di conformità per un ambiente di lavoro dal pannello servizi quando si seleziona l'ambiente di lavoro.

Rimozione di un database dalla classificazione BlueXP

Se non si desidera più eseguire la scansione di un determinato database, è possibile eliminarlo dall'interfaccia di classificazione di BlueXP e interrompere tutte le scansioni.

1. Dalla pagina *Configuration*, fare clic su ⋮ Nella riga del database, quindi fare clic su **Remove DB Server** (Rimuovi server DB).

Rimozione di un account OneDrive, SharePoint o Google Drive dalla classificazione BlueXP

Se non si desidera più eseguire la scansione dei file utente da un determinato account OneDrive, da un account SharePoint specifico o da un account Google Drive, è possibile eliminare l'account dall'interfaccia di classificazione BlueXP e interrompere tutte le scansioni.

Fasi

1. Dalla pagina *Configuration*, fare clic su ⋮ Nella riga dell'account OneDrive, SharePoint o Google Drive, quindi fare clic su **Rimuovi account OneDrive**, **Rimuovi account SharePoint** o **Rimuovi account Google Drive**.

2. Fare clic su **Delete account** (Elimina account) nella finestra di dialogo di conferma.

Rimozione di un gruppo di condivisioni di file dalla classificazione BlueXP

Se non si desidera più eseguire la scansione dei file utente da un gruppo di condivisioni file, è possibile eliminare il gruppo di condivisioni file dall'interfaccia di classificazione BlueXP e interrompere tutte le scansioni.

Fasi

1. Dalla pagina *Configuration*, fare clic su ⋮ Nella riga del gruppo condivisioni file, quindi fare clic su **Rimuovi gruppo condivisioni file**.

2. Fare clic su **Delete Group of shares** (Elimina gruppo di condivisioni) nella finestra di dialogo di conferma

Disinstallazione della classificazione BlueXP

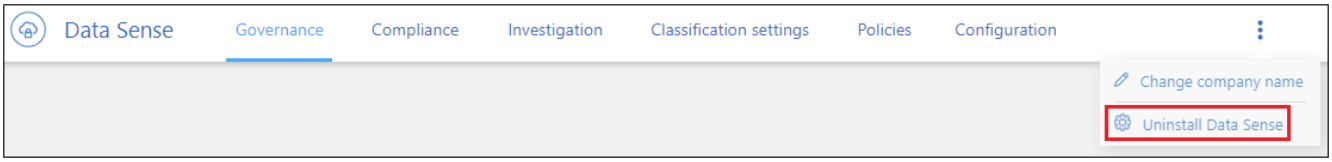
È possibile disinstallare il software di classificazione BlueXP per risolvere i problemi o per rimuovere in modo permanente il software dall'host. L'eliminazione dell'istanza comporta anche l'eliminazione dei dischi associati in cui risiedono i dati indicizzati. Tutte le informazioni sottoposte a scansione della classificazione BlueXP verranno eliminate in modo permanente.

I passaggi da utilizzare dipendono dal fatto che sia stata implementata la classificazione BlueXP nel cloud o su un host on-premise.

Disinstallare la classificazione BlueXP da un'implementazione cloud

Se non si desidera più utilizzare la classificazione BlueXP, è possibile disinstallare ed eliminare l'istanza di classificazione BlueXP dall'ambiente del provider cloud.

1. Nella parte superiore della pagina di classificazione di BlueXP, fare clic su ⋮ Quindi fare clic su **Uninstall Data Sense** (Disinstalla rilevamento dati).



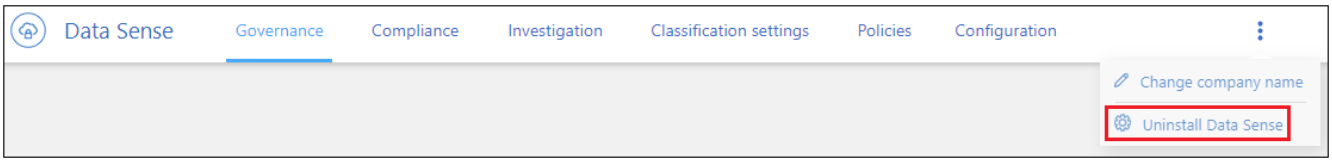
2. Nella finestra di dialogo *Uninstall Data Sense*, digitare **uninstall** per confermare che si desidera disconnettere l'istanza di classificazione BlueXP dal connettore BlueXP, quindi fare clic su **Uninstall** (Disinstalla).
3. Accedere alla console del provider di servizi cloud ed eliminare l'istanza di classificazione BlueXP. L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*

   In questo modo si eliminano l'istanza e tutti i dati associati raccolti dalla classificazione BlueXP.

Disinstallare la classificazione BlueXP da un'implementazione on-premise

È possibile disinstallare la classificazione BlueXP da un host se non si desidera più utilizzare la classificazione BlueXP o se si è verificato un problema che richiede la reinstallazione.

1. Nella parte superiore della pagina di classificazione di BlueXP, fare clic su ⋮ Quindi fare clic su **Uninstall Data Sense** (Disinstalla rilevamento dati).



2. Nella finestra di dialogo *Uninstall Data Sense*, digitare **uninstall** per confermare che si desidera

disconnettere l'istanza di classificazione BlueXP dal connettore BlueXP, quindi fare clic su **Uninstall** (Disinstalla).

3. Per disinstallare il software dall'host, eseguire `cleanup.sh` script sul computer host, ad esempio:

```
cleanup.sh
```

Scopri come "Accedere al computer host di classificazione BlueXP".

Riferimento

Tipi di istanze di classificazione BlueXP supportati

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. Quando si implementa la classificazione BlueXP nel cloud, si consiglia di utilizzare un sistema con le caratteristiche "grandi" per una funzionalità completa.

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. "Scopri queste limitazioni".

Nelle tabelle seguenti, se il sistema contrassegnato come "predefinito" non è disponibile nella regione in cui si sta installando la classificazione BlueXP, verrà implementato il sistema successivo nella tabella.

Tipi di istanze AWS

Dimensioni del sistema	Specifiche	Tipo di istanza
Extra large	32 CPU, 128 GB di RAM, 1 TiB SSD GP3	"m6i.8xlarge" (impostazione predefinita)
Grande	16 CPU, 64 GB di RAM, SSD da 500 GiB	"m6i.4xlarge" (impostazione predefinita) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Medio	8 CPU, 32 GB di RAM, SSD da 200 GiB	"m6i.2xlarge" (impostazione predefinita) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Piccolo	8 CPU, 16 GB di RAM, SSD da 100 GiB	"c6a.2xlarge" (impostazione predefinita) c5a.2xlarge c5.2xlarge c4.2xlarge

Tipi di istanze di Azure

Dimensioni del sistema	Specifiche	Tipo di istanza
Extra large	32 CPU, 128 GB di RAM, disco OS (2.048 GiB, throughput minimo 250 MB/s) e disco dati (SSD 1 TiB, throughput minimo 750 MB/s)	"Standard_D32_v3" (impostazione predefinita)
Grande	16 CPU, 64 GB di RAM, SSD da 500 GiB	"Standard_D16s_v3" (impostazione predefinita)

Tipi di istanze GCP

Dimensioni del sistema	Specifiche	Tipo di istanza
Grande	16 CPU, 64 GB di RAM, SSD da 500 GiB	"n2-standard-16" (impostazione predefinita) n2d-standard-16 n1-standard-16

Metadati raccolti dalle origini dati

La classificazione BlueXP raccoglie determinati metadati quando si eseguono scansioni di classificazione sui dati provenienti dalle origini dati e dagli ambienti di lavoro. La classificazione BlueXP può accedere alla maggior parte dei metadati necessari per classificare i tuoi dati, ma esistono alcune fonti in cui non siamo in grado di accedere ai dati di cui abbiamo bisogno.

	Metadati	CIFS	NFS
Indicatori di data e ora	*Tempo di creazione*	Disponibile	Non disponibile (non supportato in Linux)
	Ora ultimo accesso	Disponibile	Disponibile
	Ora ultima modifica	Disponibile	Disponibile
Autorizzazioni	*Autorizzazioni aperte*	Se il gruppo "EVERYONE" ha accesso al file, viene considerato "aperto all'organizzazione"	Se "altri" hanno accesso al file, viene considerato "aperto all'organizzazione"
	Accesso utenti/gruppi	Le informazioni relative a utenti e gruppi provengono da LDAP	Non disponibile (gli utenti NFS sono generalmente gestiti localmente sul server, pertanto la stessa persona può avere un UID diverso in ciascun server)

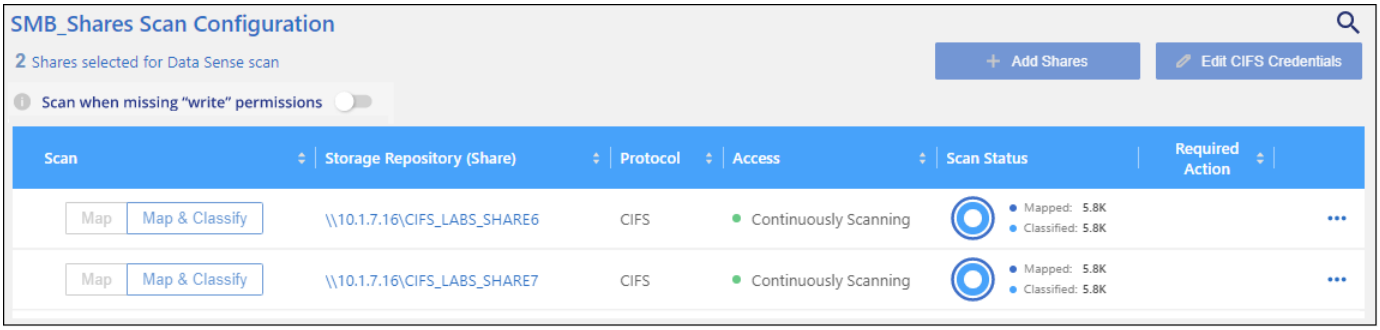
- La classificazione BlueXP non estrae l'ultimo tempo a cui si accede dalle seguenti origini dati: SharePoint Online, SharePoint on-premise (SharePoint Server), OneDrive, Google Drive, Amazon S3 e Database.
- Le versioni precedenti del sistema operativo Windows (ad esempio, Windows 7 e Windows 8) disattivano per impostazione predefinita la raccolta dell'attributo "ultimo tempo di accesso" perché può influire sulle prestazioni del sistema. Quando questo attributo non viene raccolto, le analisi di classificazione BlueXP basate sull'ultimo tempo di accesso verranno influenzate. È possibile abilitare la raccolta dell'ultimo tempo di accesso su questi sistemi Windows meno recenti, se necessario.

Data e ora dell'ultimo accesso

Quando la classificazione BlueXP estrae i dati dalle condivisioni di file, il sistema operativo li considera come utenti che accedono ai dati e modifica di conseguenza il "tempo di accesso ultimo". Dopo la scansione, la classificazione BlueXP tenta di riportare l'ultimo tempo di accesso all'indicatore data e ora originale. Se la classificazione BlueXP non dispone delle autorizzazioni per gli attributi di scrittura in CIFS o di scrittura in NFS, il sistema non può ripristinare l'ultimo orario di accesso all'indicatore data e ora originale. I volumi ONTAP configurati con SnapLock dispongono di autorizzazioni di sola lettura e non possono riportare l'ultimo orario di

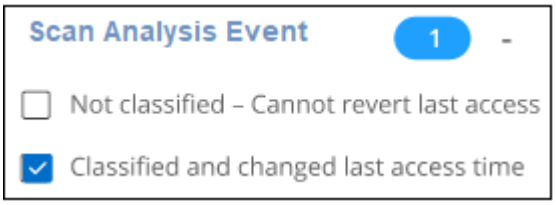
accesso all'indicatore data e ora originale.

Per impostazione predefinita, se la classificazione BlueXP non dispone di queste autorizzazioni, il sistema non esegue la scansione dei file nei volumi perché la classificazione BlueXP non può riportare l'ultimo tempo di accesso all'indicatore data e ora originale. Tuttavia, se non si ha alcun problema se l'ultimo tempo di accesso viene reimpostato sull'ora originale nei file, è possibile fare clic sull'opzione **scansione quando mancano i permessi di "scrittura attributi"** nella parte inferiore della pagina di configurazione in modo che la classificazione BlueXP scansiona i volumi indipendentemente dalle autorizzazioni.



Questa funzionalità è applicabile a sistemi ONTAP on-premise, Cloud Volumes ONTAP, Azure NetApp Files, FSX per ONTAP e file share non NetApp.

Si noti che nella pagina di analisi è presente un filtro denominato *Scan Analysis Event* che consente di visualizzare i file non classificati perché la classificazione BlueXP non ha potuto ripristinare l'ultimo tempo di accesso, Oppure i file classificati anche se la classificazione BlueXP non ha potuto ripristinare l'ultimo tempo di accesso.



Le selezioni dei filtri sono:

- "Non classificato — Impossibile ripristinare l'ultimo tempo di accesso" - Mostra i file che non sono stati classificati a causa di autorizzazioni di scrittura mancanti.
- "Classified and updated last access time" (tempo di accesso ultimo classificato e aggiornato) - Mostra i file classificati e la classificazione BlueXP non è stata in grado di ripristinare l'ultimo tempo di accesso alla data originale. Questo filtro è valido solo per gli ambienti in cui è stata attivata l'OPZIONE **Scan when missing "write attribtributes" permissions**.

Se necessario, è possibile esportare questi risultati in un report in modo da visualizzare i file sottoposti o meno a scansione a causa delle autorizzazioni. "Scopri di più sul Data Investigation Report".

Accedi al sistema di classificazione BlueXP

A volte potrebbe essere necessario accedere al sistema di classificazione BlueXP in modo da poter accedere ai file di log o modificare i file di configurazione.

Quando la classificazione BlueXP è installata su una macchina Linux on-premise o su una macchina Linux implementata nel cloud, puoi accedere direttamente al file di configurazione e allo script.

Quando la classificazione BlueXP viene implementata nel cloud, è necessario eseguire l'SSH nell'istanza di classificazione BlueXP. Si accede al sistema inserendo l'utente e la password oppure utilizzando la chiave SSH fornita durante l'installazione di BlueXP Connector. Il comando SSH è:

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = posizione delle chiavi di autenticazione ssh
* <machine_user>:
```

+
Per AWS: Utilizzare <ec2-user>
Per Azure: Utilizzare l'utente creato per l'istanza di BlueXP
** Per GCP: Utilizzare l'utente creato per l'istanza di BlueXP

- <datasense_ip> = indirizzo IP dell'istanza della macchina virtuale

Nota: Per accedere al sistema nel cloud, è necessario modificare le regole in entrata del gruppo di sicurezza. Per ulteriori informazioni, vedere:

- "Regole del gruppo di sicurezza in AWS"
- "Regole del gruppo di sicurezza in Azure"
- "Regole del firewall in Google Cloud"

API di classificazione BlueXP

Le funzionalità di classificazione BlueXP che sono disponibili tramite l'interfaccia utente web sono anche disponibili tramite l'API Swagger.

Esistono quattro categorie definite nella classificazione BlueXP che corrispondono alle schede dell'interfaccia utente:

- Indagine
- Conformità
- Governance
- Configurazione

Le API nella documentazione di Swagger consentono di cercare, aggregare dati, monitorare le scansioni e creare azioni come copia, spostamento e altro ancora.

Panoramica

L'API consente di eseguire le seguenti funzioni:

- Informazioni sull'esportazione
  - Tutto ciò che è disponibile nell'interfaccia utente può essere esportato tramite l'API (ad eccezione dei report)
  - I dati vengono esportati in formato JSON (semplice da analizzare e inviare ad applicazioni di 3rd parti, come Splunk)

- Creare query utilizzando le istruzioni "AND" e "OR", includere ed escludere informazioni e altro ancora.

  Ad esempio, è possibile individuare i file *senza* informazioni personali identificabili (PII) specifiche (funzionalità non disponibile nell'interfaccia utente). È inoltre possibile escludere campi specifici per l'operazione di esportazione.

- Eseguire le azioni
  - Aggiornare le credenziali CIFS
  - Visualizzare e annullare le azioni
  - Eseguire nuovamente la scansione delle directory
  - Eliminare, copiare, etichettare e assegnare gli utenti ai dati
  - Clona e copia i file
  - Esportare i dati

L'API è protetta e utilizza lo stesso metodo di autenticazione dell'interfaccia utente. Le informazioni sull'autenticazione sono disponibili in: https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html

Accesso al riferimento API Swagger

Per accedere a Swagger, è necessario l'indirizzo IP dell'istanza di classificazione BlueXP. Nel caso di un'implementazione cloud, verrà utilizzato l'indirizzo IP pubblico. Quindi, è necessario accedere a questo endpoint:

https://<classification_ip>/documentazione

Esempio di utilizzo delle API

Nell'esempio seguente viene illustrata una chiamata API per copiare i file.

Richiesta API

Inizialmente, per visualizzare tutti i filtri nella scheda analisi, è necessario ottenere tutti i campi e le opzioni pertinenti per un ambiente di lavoro.

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… " -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients"
```

Risposta

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
```

```
      "name": "string",
      "operators": [
        "EQUALS"
      ],
      "optional_values": [
        {}
      ],
      "secondary": {},
      "server_data": false,
      "type": "TEXT"
    }
  ]
}
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "POLICIES",
      "name": "Policies",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "EXTRACTION_STATUS_RANGE",
      "name": "Scan Analysis Status",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "SCAN_ANALYSIS_ERROR",
      "name": "Scan Analysis Event",
      "operators": [
        "IN"
      ],
```

```
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "PUBLIC_ACCESS",
      "name": "Open Permissions",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USERS_PERMISSIONS_COUNT_RANGE",
      "name": "Number of Users with Access",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USER_GROUP_PERMISSIONS",
      "name": "User / Group Permissions",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_OWNER",
      "name": "File Owner",
      "operators": [
        "EQUALS",
        "CONTAINS"
```

```
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT_TYPE",
      "name": "Working Environment Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT",
      "name": "Working Environment",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "SCAN_TASK",
      "name": "Storage Repository",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_PATH",
      "name": "File / Directory Path",
      "operators": [
```

```
        "MULTI_CONTAINS",
        "MULTI_EXCLUDE"
      ],
      "server_data": true,
      "type": "MULTI_TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
      "field": "CATEGORY",
      "name": "Category",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVITY_LEVEL",
      "name": "Sensitivity Level",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "NUMBER_OF_IDENTIFIERS",
      "name": "Number of identifiers",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_PERSONAL",
      "name": "Personal Data",
```

```
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVE",
      "name": "Sensitive Personal Data",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DATA_SUBJECT",
      "name": "Data Subject",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "DIRECTORIES",
      "field": "DIRECTORY_TYPE",
      "name": "Directory Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
```

```
      "field": "FILE_TYPE",
      "name": "File Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_SIZE_RANGE",
      "name": "File Size",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_CREATION_RANGE_RETENTION",
      "name": "Created Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DISCOVERED_TIME_RANGE",
      "name": "Discovered Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
```

```
      "field": "FILE_LAST_MODIFICATION_RETENTION",
      "name": "Last Modified",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
      "name": "Last Accessed",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "IS_DUPLICATE",
      "name": "Duplicates",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "FILE_HASH",
      "name": "File Hash",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
```

```
      "field": "USER_DEFINED_STATUS",
      "name": "Tags",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ASSIGNED_TO",
      "name": "Assigned to",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    }
  ]
}
```

Useremo questa risposta nei nostri parametri di richiesta per filtrare i file desiderati che vogliamo copiare.

È possibile applicare un'azione a più elementi. I tipi di azione supportati comprendono: Spostamento, eliminazione, copia, assegnazione a, FlexClone, esportazione di dati, nuova scansione ed etichetta.

Creeremo l'azione di copia:

Richiesta API

Questa API successiva è quella Action API e consente di creare più azioni.

```
curl -X POST "http://
{classification_ip}/api//{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
"{ontap_ip}:/{share_name} " },
\"requested_query\":{"condition":"AND","rules":[{"field":"ENVIRONMENT_TYPE
","operator":"IN","value":["ONPREM"]},{"field":"CATEGORY","operator":"IN",
"value":["21"]}]}}"
```

Risposta

La risposta restituirà l'oggetto azione, in modo da poter utilizzare le API Get ed DELETE per ottenere lo stato dell'azione o per annullarla.


```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```

Conoscenza e supporto

Registrati per ricevere assistenza

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

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

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

Panoramica sulla registrazione del supporto

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

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

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

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

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

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

Registrare l'account BlueXP per il supporto NetApp

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

Cliente esistente con un account NSS

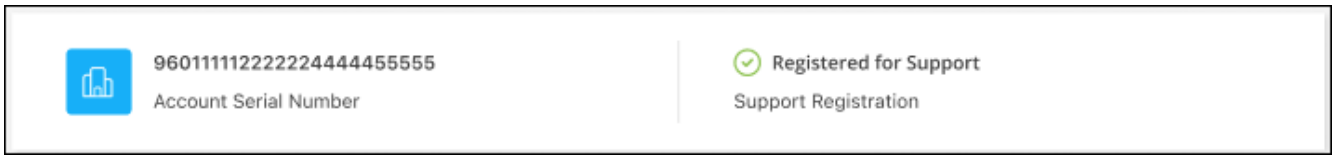
Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite BlueXP.

Fasi

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

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

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

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

Cliente esistente ma nessun account NSS

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

Fasi

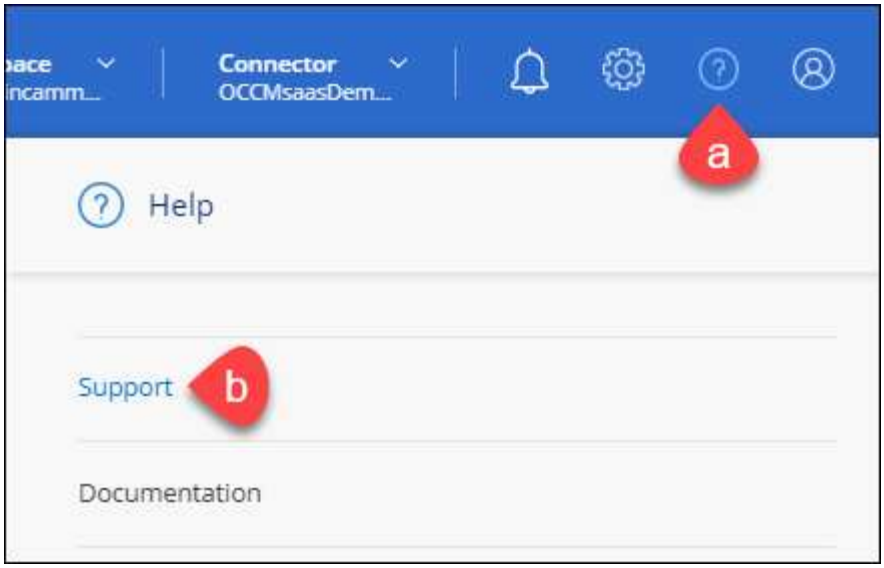
1. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account BlueXP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

Novità di NetApp

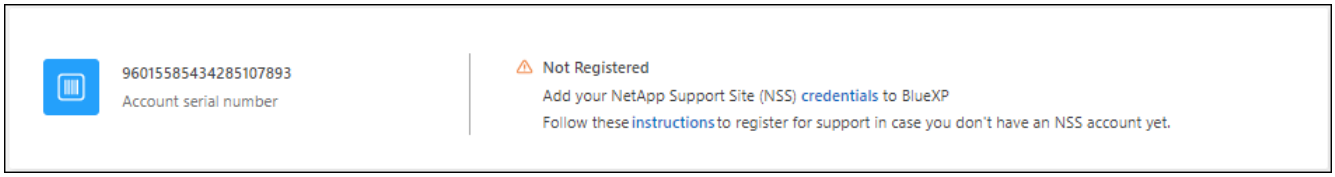
Se sei nuovo di NetApp e non disponi di un account NSS, segui i passaggi riportati di seguito.

Fasi

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



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



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

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

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

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

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

Al termine

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

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

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

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

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

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

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

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

- Aggiornamento del software Cloud Volumes ONTAP alla versione più recente

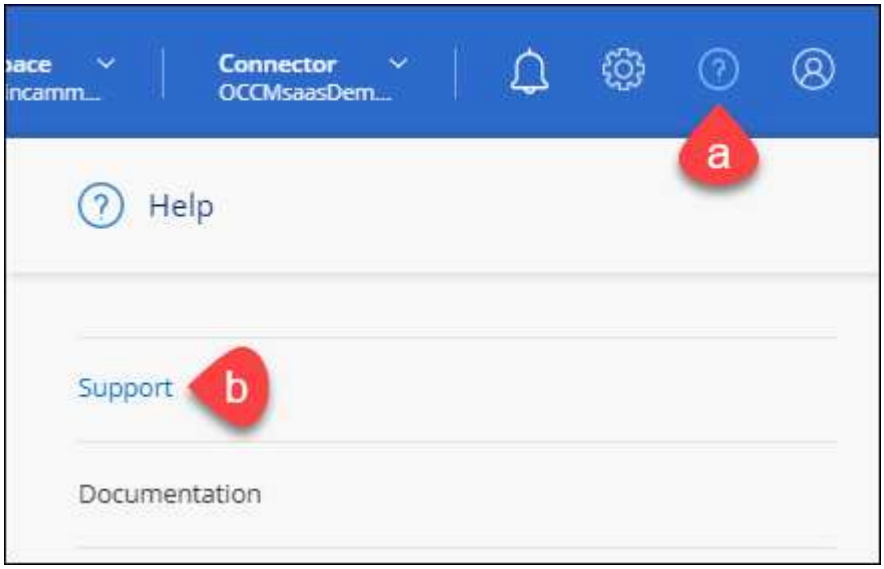
L'associazione delle credenziali NSS all'account BlueXP è diversa dall'account NSS associato a un account utente BlueXP.

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

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

Fasi

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



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

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

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

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

   Tenere presente quanto segue:

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

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

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

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

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

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

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

Richiedi assistenza

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

Ottieni supporto per un file service del cloud provider

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

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

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

Utilizzare le opzioni di supporto automatico

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

- Documentazione

  La documentazione BlueXP attualmente visualizzata.

- "Knowledge base"

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

- "Community"

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

Crea un caso con il supporto NetApp

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

Prima di iniziare

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

Fasi

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

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

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

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

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

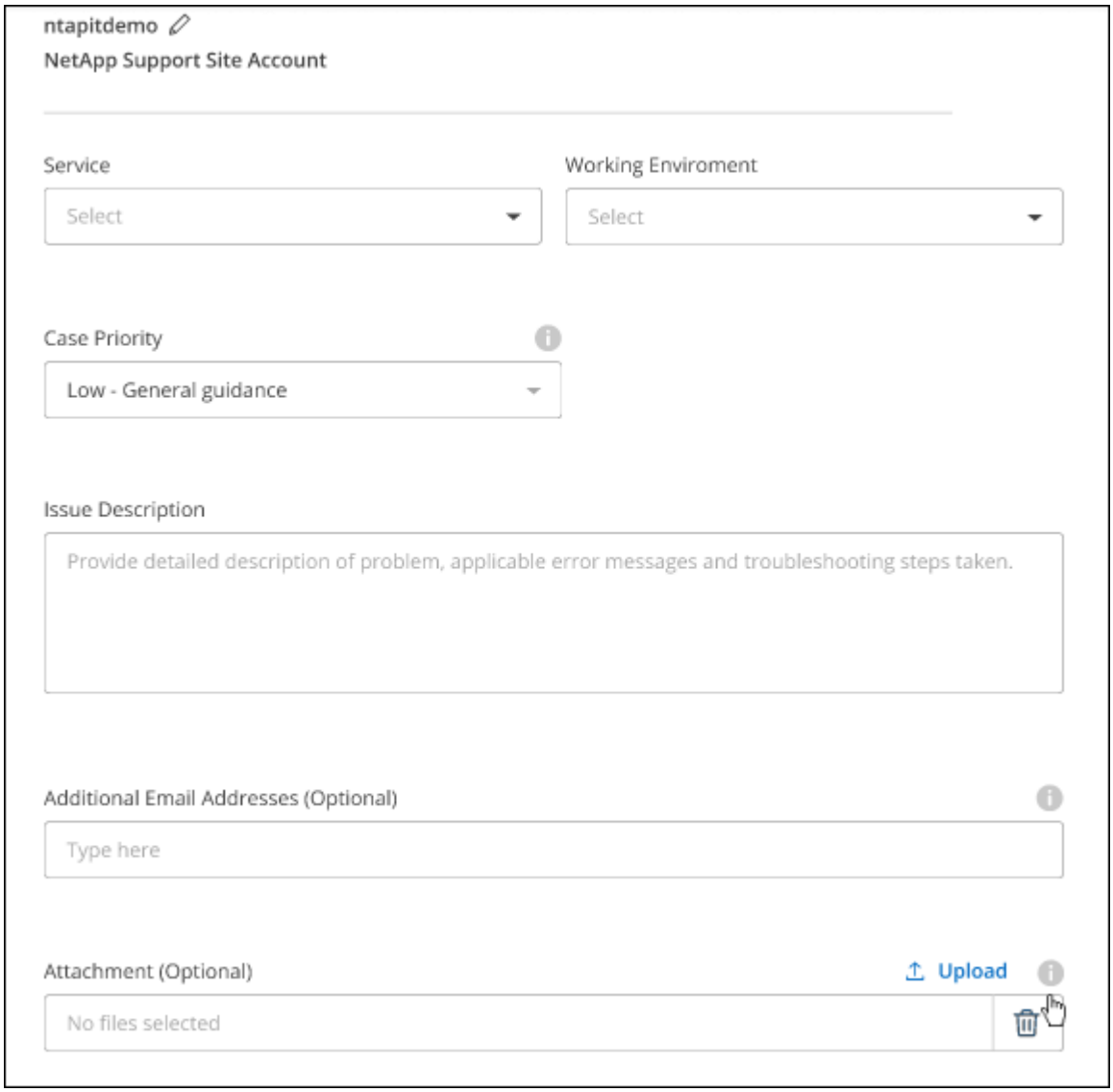
      - **Priorità caso**: Scegliere la priorità per il caso, che può essere bassa, Media, alta o critica.

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

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

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

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



Al termine

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

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

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

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

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

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

Gestire i casi di supporto (anteprima)

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

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

Tenere presente quanto segue:

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

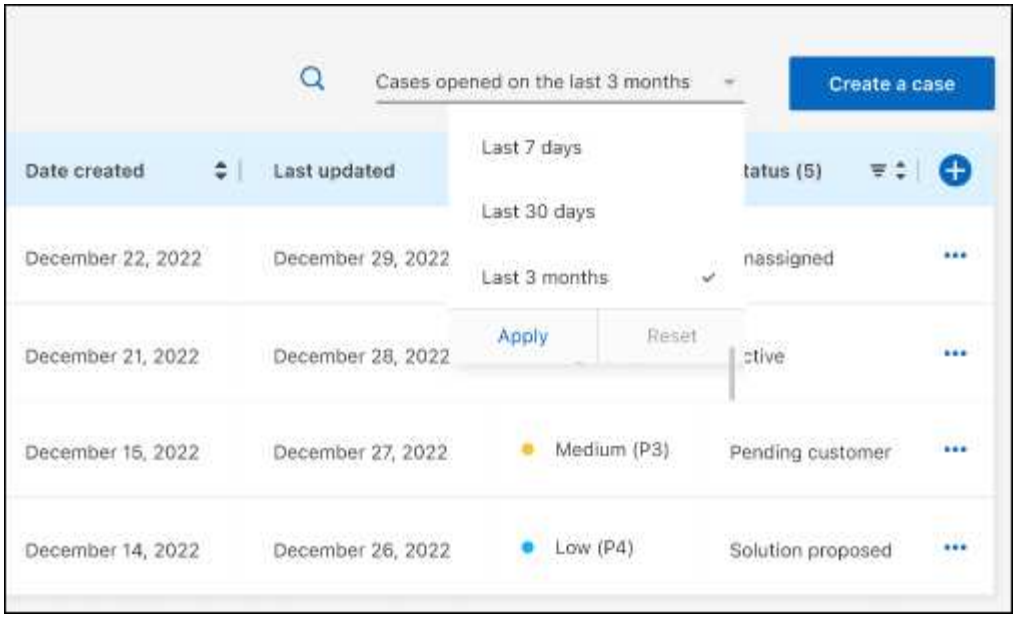
  I risultati della tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come priorità e Stato. Altre colonne offrono funzionalità di ordinamento.

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

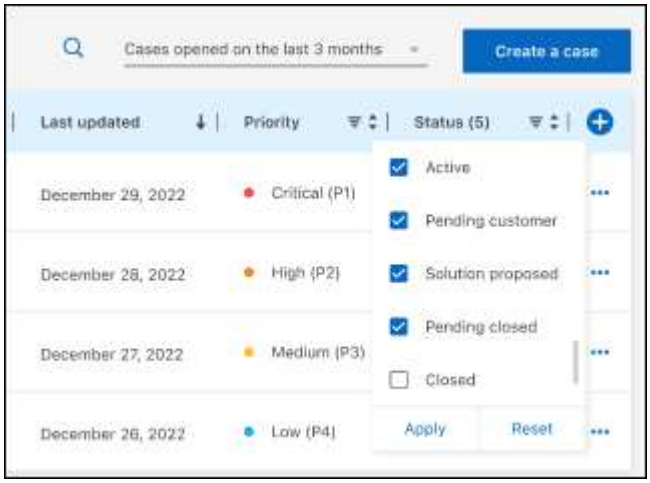
Fasi

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

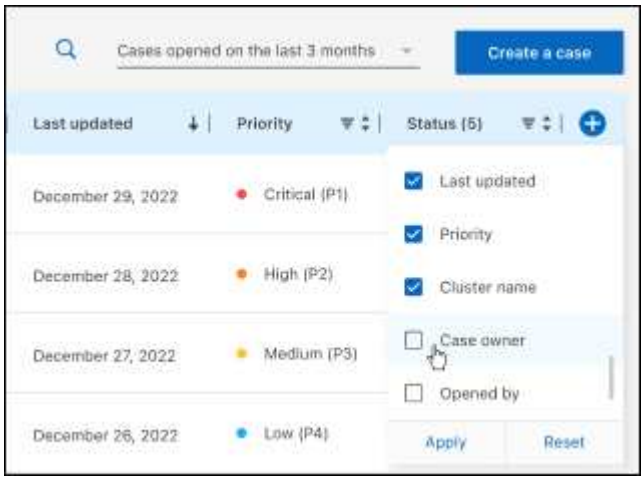
   La pagina **Gestione del caso** mostra i casi aperti relativi all'account NSS associato all'account utente BlueXP. Si tratta dello stesso account NSS visualizzato nella parte superiore della pagina **gestione NSS**.
3. Se si desidera, modificare le informazioni visualizzate nella tabella:
   - In **Organization's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



- Filtrare il contenuto delle colonne.



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

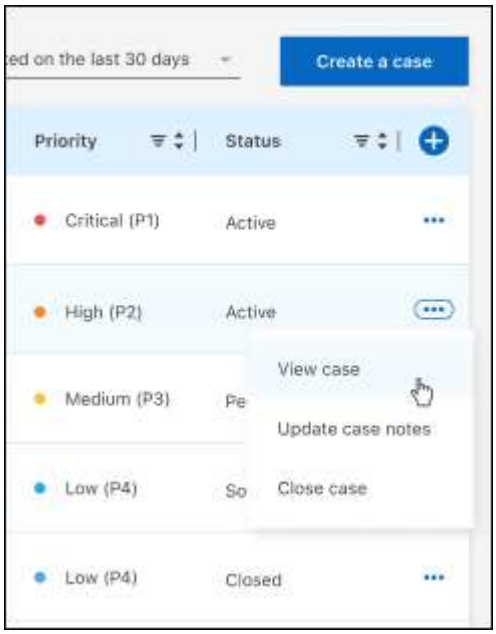


4. Gestire un caso esistente selezionando ••• e selezionando una delle opzioni disponibili:

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

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

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



Note legali

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

Copyright

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

Marchi

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

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

Brevetti

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

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

Direttiva sulla privacy

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

Open source

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

- "Avviso per BlueXP"
- "Avviso per la classificazione BlueXP"