Documentazione sulla classificazione BlueXP

BlueXP classification

NetApp
August 11, 2025

This PDF was generated from https://docs.netapp.com/it-it/bluexp-classification/index.html on August 11, 2025. Always check docs.netapp.com for the latest.

Sommario

Documentazione sulla classificazione BlueXP . . . 1
Note di rilascio . . . 2
Novità della classificazione BlueXP . . . 2
11 agosto 2025 . . . 2
14 luglio 2025 . . . 2
10 giugno 2025 . . . 3
12 maggio 2025 . . . 3
14 aprile 2025 . . . 4
10 marzo 2025 . . . 5
19 febbraio 2025 . . . 5
22 gennaio 2025 . . . 6
16 dicembre 2024 . . . 7
4 novembre 2024 . . . 7
10 ottobre 2024 . . . 7
2 settembre 2024 . . . 7
05 agosto 2024 . . . 8
01 luglio 2024 . . . 8
05 giugno 2024 . . . 9
15 maggio 2024 . . . 9
01 aprile 2024 . . . 9
04 marzo 2024 . . . 10
10 gennaio 2024 . . . 10
14 dicembre 2023 . . . 11
06 novembre 2023 . . . 11
04 ottobre 2023 . . . 11
05 settembre 2023 . . . 11
17 luglio 2023 . . . 12
06 giugno 2023 . . . 12
03 aprile 2023 . . . 13
07 marzo 2023 . . . 13
05 febbraio 2023 . . . 14
09 gennaio 2023 . . . 15
Limitazioni note nella classificazione BlueXP . . . 16
Opzioni disabilitate per la classificazione BlueXP . . . 16
Scansione della classificazione BlueXP . . . 16
Inizia subito . . . 18
Scopri di più sulla classificazione BlueXP . . . 18
Caratteristiche . . . 18
Ambienti di lavoro e origini dati supportati . . . 19
Costo . . . 19
L’istanza di classificazione BlueXP . . . 20
Come funziona la scansione della classificazione BlueXP . . . 21
Qual è la differenza tra le scansioni di mappatura e classificazione . . . 22

Informazioni classificate dalla classificazione BlueXP . . . 22
Panoramica delle reti . . . 23
Accedi BlueXP classification . . . 23
Implementare la classificazione BlueXP . . . 24
Quale implementazione della classificazione BlueXP dovresti utilizzare? . . . 24
Implementare la classificazione BlueXP nel cloud utilizzando BlueXP . . . 25
Installare la classificazione BlueXP su un host con accesso a Internet . . . 34
Installare la classificazione BlueXP su un host Linux senza accesso Internet . . . 45
Verificare che l'host Linux sia pronto per installare la classificazione BlueXP . . . 54
Attivare la scansione sulle origini dati . . . 60
Panoramica delle origini dati di scansione con classificazione BlueXP . . . 60
Esegui la scansione dei volumi Azure NetApp Files con classificazione BlueXP . . . 64
Esegui la scansione di Amazon FSX per volumi ONTAP con classificazione BlueXP . . . 67
Esegui la scansione di Cloud Volumes ONTAP e dei volumi ONTAP on-premise con classificazione BlueXP . . . 72
Eseguire la scansione degli schemi del database con classificazione BlueXP . . . 76
Eseguire la scansione delle condivisioni di file con classificazione BlueXP . . . 79
Eseguire la scansione dei dati StorageGRID con classificazione BlueXP . . . 85
Integra Active Directory con la classificazione BlueXP . . . 87
Origini dati supportate . . . 87
Connettersi al server Active Directory . . . 88
Gestire l'integrazione di Active Directory . . . 89
Utilizzare la classificazione BlueXP . . . 90
Visualizza i dettagli di governance sui dati archiviati nell'organizzazione con la classificazione BlueXP . . . 90
Rivedere il dashboard Governance . . . 90
Creare il report di valutazione per il rilevamento dei dati . . . 93
Creare il rapporto Panoramica mappatura dati . . . 93
Visualizza i dettagli di conformità sui dati privati archiviati nell'organizzazione con la classificazione BlueXP . . . 96
Consente di visualizzare i file che contengono dati personali . . . 97
Consente di visualizzare i file che contengono dati personali sensibili . . . 99
Visualizzare i file per categorie . . . 101
Visualizzare i file in base ai tipi di file . . . 102
Categorie di dati privati nella classificazione BlueXP . . . 103
Tipi di dati personali . . . 103
Tipi di dati personali sensibili . . . 108
Tipi di categorie . . . 109
Tipi di file . . . 110
Accuratezza delle informazioni rilevate . . . 110
Creare una classificazione personalizzata nella classificazione BlueXP . . . 111
Creare una classificazione personalizzata . . . 111
Esaminare i dati memorizzati nella propria organizzazione con la classificazione BlueXP . . . 112
Filtrare i dati nella pagina analisi dati . . . 113
Visualizzare i metadati dei file . . . 116
Visualizzare le autorizzazioni degli utenti per file e directory . . . 117

Verificare la presenza di file duplicati nei sistemi di storage . . . 118
Creare il rapporto analisi dati . . . 119
Crea una ricerca salvata in base ai filtri selezionati . . . 122
Gestire le ricerche salvate con la classificazione BlueXP . . . 123
Visualizzare i risultati delle ricerche salvate nella pagina di analisi . . . 123
Creare ricerche salvate personalizzate . . . 123
Modificare le ricerche salvate . . . 125
Eliminare le ricerche salvate . . . 127
Ricerche predefinite . . . 127
Modificare le impostazioni di scansione della classificazione BlueXP per gli archivi . . . 128
Consente di visualizzare lo stato della scansione per i repository . . . 128
Modificare il tipo di scansione per un repository . . . 129
Assegnare priorità alle scansioni . . . 130
Interrompere la ricerca di un repository . . . 131
Sospendere e riprendere la scansione di un repository . . . 132
Visualizza i report sulla conformità della classificazione BlueXP . . . 132
Selezionare gli ambienti di lavoro per i rapporti . . . 133
Report di richiesta di accesso ai soggetti dei dati . . . 134
Report HIPAA (Health Insurance Portability and Accountability Act) . . . 136
Report PCI DSS (Payment Card Industry Data Security Standard) . . . 137
Report sulla valutazione dei rischi per la privacy . . . 138
Gestire la classificazione BlueXP . . . 140
Escludere directory specifiche dalle scansioni di classificazione BlueXP . . . 140
Origini dati supportate . . . 140
Definire le directory da escludere dalla scansione . . . 140
Esempi . . . 141
Escape di caratteri speciali nei nomi delle cartelle . . . 142
Consente di visualizzare l’elenco di esclusione corrente . . . 143
Definire altri ID di gruppo come aperti all’organizzazione nella classificazione BlueXP . . . 143
Aggiungere l’autorizzazione "Apri all’organizzazione" agli ID gruppo . . . 143
Consente di visualizzare l’elenco corrente degli ID di gruppo . . . 144
Rimuovere le origini dati dalla classificazione BlueXP . . . 144
Disattivare le scansioni di conformità per un ambiente di lavoro . . . 144
Rimozione di un database dalla classificazione BlueXP . . . 145
Rimozione di un gruppo di condivisioni di file dalla classificazione BlueXP . . . 145
Disinstallare la classificazione BlueXP . . . 146
Disinstallare la classificazione BlueXP da un’implementazione cloud . . . 146
Disinstallare la classificazione BlueXP da un’implementazione on-premise . . . 146
Funzioni obsolete . . . 148
Funzionalità obsolete di classificazione BlueXP . . . 148
Origini dati supportate . . . 148
Funzionalità di conformità . . . 148
Funzioni per la gestione dei dati . . . 149
Implementa le deprecazioni di classificazione BlueXP . . . 150
Installare la classificazione BlueXP su host multipli per configurazioni di grandi dimensioni senza

accesso a Internet . . . 150
Deprecazioni dei dati di scansione . . . 151
Esegui la scansione dei bucket Amazon S3 con classificazione BlueXP . . . 151
Eseguire la scansione degli account OneDrive con classificazione BlueXP . . . 159
Eseguire la scansione degli account SharePoint con la classificazione BlueXP . . . 162
Eseguire la scansione degli account Google Drive con classificazione BlueXP . . . 167
Eseguire la scansione dei dati StorageGRID con classificazione BlueXP . . . 169
Gestire le deprecazioni dei dati . . . 173
Visualizza i dettagli di governance dei tuoi dati utilizzando il dashboard di governance della classificazione BlueXP . . . 173
Organizza i tuoi dati privati con la classificazione BlueXP . . . 174
Gestisci i tuoi dati privati con la classificazione BlueXP . . . 183
Aggiungi identificatori di dati personali alle scansioni di classificazione BlueXP . . . 194
Visualizzare lo stato delle azioni di conformità nella classificazione BlueXP . . . 210
Controllare la cronologia delle azioni di classificazione di BlueXP . . . 211
Riduzione della velocità di scansione della classificazione BlueXP . . . 212
Rimuovere un account OneDrive, SharePoint o Google Drive dalla classificazione BlueXP . . . 213
Riferimento . . . 215
Tipi di istanze di classificazione BlueXP supportati . . . 215
Tipi di istanze AWS . . . 215
Tipi di istanze di Azure . . . 215
Tipi di istanze GCP . . . 215
Metadati raccolti dalle origini dei dati nella classificazione BlueXP . . . 216
Data e ora dell'ultimo accesso . . . 216
Accedi al sistema di classificazione BlueXP . . . 217
API di classificazione BlueXP . . . 218
Panoramica . . . 218
Accesso al riferimento API Swagger . . . 219
Esempio di utilizzo delle API . . . 219
Conoscenza e supporto . . . 229
Registrati al supporto BlueXP . . . 229
Panoramica sulla registrazione del supporto . . . 229
Registrare BlueXP per ricevere assistenza NetApp . . . 229
Associare le credenziali NSS per il supporto Cloud Volumes ONTAP . . . 232
Assistenza per la classificazione BlueXP . . . 233
Ottieni supporto per un file service del cloud provider . . . 233
Utilizzare le opzioni di supporto automatico . . . 234
Crea un caso con il supporto NetApp . . . 234
Gestire i casi di supporto (anteprima) . . . 236
Domande frequenti sulla classificazione BlueXP . . . 239
Servizio di classificazione BlueXP . . . 239
Come funziona la classificazione BlueXP? . . . 239
La classificazione BlueXP dispone di un'API REST e funziona con strumenti di terze parti? . . . 239
La classificazione BlueXP è disponibile attraverso i marketplace del cloud? . . . 239
Analisi e scansione della classificazione BlueXP . . . 239

Con quale frequenza la classificazione BlueXP esegue la scansione dei dati? 239
Le prestazioni di scansione variano? 240
Posso cercare i miei dati usando la classificazione BlueXP? 240
Gestione e privacy della classificazione BlueXP 240
Come si attiva o disattiva la classificazione BlueXP ? 240
Il servizio può escludere la scansione dei dati in determinate directory? 241
Le snapshot che risiedono su volumi ONTAP vengono sottoposte a scansione? 241
Cosa succede se il tiering dei dati è attivato sui volumi ONTAP? 241
Tipi di sistemi di origine e tipi di dati 241
Esistono restrizioni quando viene implementato in un'area governativa? 241
Quali origini dati è possibile eseguire la scansione se si installa la classificazione BlueXP in un sito senza accesso a Internet? 241
Quali tipi di file sono supportati? 241
Quali tipi di dati e metadati cattura la classificazione BlueXP? 242
Posso limitare le informazioni di classificazione di BlueXP a utenti specifici? 242
Qualcuno può accedere ai dati privati inviati tra il browser e la classificazione BlueXP? 242
Come vengono gestiti i dati sensibili? 243
Dove sono memorizzati i dati? 243
Come si accede ai dati? 243
Licenze e costi 243
Quanto costa la classificazione BlueXP? 243
Implementazione del connettore 243
Che cos'è il connettore? 243
Dove deve essere installato il connettore? 243
La classificazione BlueXP richiede l'accesso alle credenziali? 244
La comunicazione tra il servizio e il connettore utilizza il protocollo HTTP? 244
Implementazione della classificazione BlueXP 244
Quali modelli di implementazione supporta la classificazione BlueXP? 244
Quale tipo di istanza o macchina virtuale è richiesto per la classificazione BlueXP? 244
È possibile implementare la classificazione BlueXP sul proprio host? 244
E i siti sicuri senza accesso a Internet? 244
Note legali 245
Copyright 245
Marchi 245
Brevetti 245
Direttiva sulla privacy 245
Open source 245

Documentazione sulla classificazione BlueXP

Note di rilascio

Novità della classificazione BlueXP

Scopri le novità della classificazione BlueXP.

11 agosto 2025

Versione 1.46

Questa versione BlueXP classification include correzioni di bug e i seguenti aggiornamenti:

Informazioni dettagliate sugli eventi di scansione nella cronologia BlueXP

La cronologia BlueXP ora supporta approfondimenti avanzati sugli eventi di scansione per la BlueXP classification. La cronologia ora mostra quando inizia la scansione di un ambiente di lavoro, lo stato degli ambienti di lavoro e gli eventuali problemi. Gli stati delle condivisioni e degli ambienti di lavoro sono disponibili solo per le scansioni di mappatura.

Per ulteriori informazioni sulla cronologia BlueXP , vedere"Monitorare le operazioni BlueXP" .

Supporto per RHEL 9.6

Questa versione aggiunge il supporto per Red Hat Enterprise Linux v9.6 per l'installazione manuale in sede della BlueXP classification, comprese le distribuzioni di siti oscuri.

I seguenti sistemi operativi richiedono l'utilizzo del motore del contenitore Podman e richiedono la classificazione BlueXP versione 1,30 o superiore: Red Hat Enterprise Linux versione 8,8, 8,10, 9,0, 9,1, 9,2, 9,3, 9,4 e 9,5.

14 luglio 2025

Versione 1,45

Questa versione BlueXP classification include modifiche al codice che ottimizzano l'utilizzo delle risorse e:

Flusso di lavoro migliorato per aggiungere condivisioni di file per la scansione

Il flusso di lavoro per aggiungere condivisioni file a un gruppo di condivisione file è stato semplificato. Il processo ora differenzia anche il supporto del protocollo CIFS in base al tipo di autenticazione (Kerberos o NTLM).

Per ulteriori informazioni, vedere "Eseguire la scansione delle condivisioni dei file".

Informazioni avanzate sul proprietario del file

Ora puoi visualizzare maggiori informazioni sui proprietari dei file acquisiti nella scheda Indagine. Quando visualizzi i metadati di un file nella scheda Indagine, individua il proprietario del file, quindi seleziona **Visualizza dettagli** per vedere il nome utente, l'e-mail e il nome dell'account SAM. Puoi anche visualizzare altri elementi di proprietà di questo utente. Questa funzionalità è disponibile solo per gli ambienti di lavoro con Active Directory.

Per ulteriori informazioni, vedere "Esaminare i dati memorizzati nella propria organizzazione".

10 giugno 2025

Versione 1,44

Questa versione di classificazione BlueXP include:

Tempi di aggiornamento migliorati per la dashboard di Governance

I tempi di aggiornamento per i singoli componenti della dashboard di Governance sono stati migliorati. La tabella seguente mostra la frequenza degli aggiornamenti per ciascun componente.

Componente	Tempi di aggiornamento
Età dei dati	24 ore
Categorie	24 ore
Panoramica dei dati	5 minuti
File duplicati	2 ore
Tipi di file	24 ore
Dati non aziendali	2 ore
Aprire permessi	24 ore
Ricerche salvate	2 ore
Dati sensibili e permessi estesi	24 ore
Dimensione dei dati	24 ore
Dati obsoleti	2 ore
Principali repository di dati per livello di sensibilità	2 ore

È possibile visualizzare l'ora dell'ultimo aggiornamento e aggiornare manualmente i componenti File duplicati, Dati non aziendali, Ricerche salvate, Dati obsoleti e Repository dati principali per livello di sensibilità. Per ulteriori informazioni sulla dashboard di Governance, consultare "Visualizzare i dettagli di governance sui dati archiviati nell'organizzazione" .

Miglioramenti delle prestazioni e della sicurezza

Sono stati apportati miglioramenti per ottimizzare le prestazioni, il consumo di memoria e la sicurezza della classificazione BlueXP.

Correzioni dei bug

Redis è stato aggiornato per migliorare l'affidabilità della classificazione BlueXP. La classificazione BlueXP ora utilizza Elasticsearch per migliorare l'accuratezza del reporting del conteggio dei file durante le scansioni.

12 maggio 2025

Versione 1,43

Questa versione di classificazione BlueXP include:

Assegnare la priorità alle scansioni di classificazione

La classificazione BlueXP supporta la possibilità di assegnare priorità alle scansioni Map & Classify oltre alle scansioni Mapping-only, consentendo di selezionare le scansioni da completare per prime. La prioritizzazione

delle scansioni Map & Classify è supportata durante e prima dell'inizio delle scansioni. Se si sceglie di assegnare la priorità a una scansione mentre è in corso, vengono assegnate priorità sia alla scansione di mappatura che alla scansione di classificazione.

Per ulteriori informazioni, vedere "Assegnare priorità alle scansioni".

Supporto per categorie di dati canadesi per l'identificazione personale (PII)

Le scansioni di classificazione BlueXP identificano le categorie di dati PII canadesi. Queste categorie includono informazioni bancarie, numeri di passaporto, numeri di assicurazione sociale, numeri di patente di guida e numeri di carta sanitaria per tutte le province e territori canadesi.

Per ulteriori informazioni, vedere "Categorie di dati personali".

Classificazione personalizzata (anteprima)

La classificazione BlueXP supporta classificazioni personalizzate per le scansioni Map & Classify. Grazie alle classificazioni personalizzate, è possibile personalizzare le scansioni BlueXP per acquisire dati specifici dell'organizzazione utilizzando espressioni regolari. Questa funzione è attualmente in anteprima.

Per ulteriori informazioni, vedere "Aggiungere classificazioni personalizzate".

Scheda ricerche salvate

La scheda **Policies** è stata rinominata **"Ricerche salvate"**. La funzionalità rimane invariata.

Inviare gli eventi di scansione alla timeline BlueXP

La classificazione BlueXP supporta l'invio di eventi di classificazione (quando viene avviata e terminata una scansione) a "Tempistiche di BlueXP ".

Aggiornamenti di protezione

- Il pacchetto keras è stato aggiornato, attenuando le vulnerabilità (BDSA-2025-0107 e BDSA-2025-1984).
- La configurazione dei container Docker è stata aggiornata. Il contenitore non ha più accesso alle interfacce di rete dell'host per la creazione di pacchetti di rete grezzi. Riducendo gli accessi non necessari, l'aggiornamento riduce i potenziali rischi di protezione.

Miglioramenti delle performance

I miglioramenti del codice sono stati implementati per ridurre l'utilizzo della RAM e migliorare le prestazioni complessive della classificazione BlueXP .

Correzioni dei bug

Sono stati corretti i bug che hanno causato il mancato funzionamento delle scansioni StorageGRID, il mancato caricamento delle opzioni del filtro della pagina di analisi e la valutazione del rilevamento dati per le valutazioni di volumi elevati.

14 aprile 2025

Versione 1,42

Questa versione di classificazione BlueXP include:

Scansione in blocco per ambienti di lavoro

La classificazione BlueXP supporta le operazioni bulk per gli ambienti di lavoro. È possibile scegliere di attivare le scansioni di mappatura, attivare le scansioni di mappatura e classificazione, disattivare le scansioni o creare una configurazione personalizzata tra i volumi in ambiente di lavoro. Se si effettua una selezione per

un singolo volume, questa sovrascrive la selezione in blocco. Per eseguire un'operazione bulk, accedere alla pagina **Configurazione** ed effettuare la selezione.

Scaricare il rapporto di indagine localmente

La classificazione BlueXP supporta la possibilità di scaricare localmente i report di analisi dei dati da visualizzare nel browser. Se si sceglie l'opzione locale, l'analisi dei dati è disponibile solo nel formato CSV e visualizza solo le prime 10.000 righe di dati.

Per ulteriori informazioni, vedere "Esaminare i dati memorizzati nella propria organizzazione con la classificazione BlueXP ".

10 marzo 2025

Versione 1,41

Questa versione di classificazione BlueXP include miglioramenti generali e correzioni dei bug. Include inoltre:

Stato scansione

La classificazione BlueXP tiene traccia dell'avanzamento in tempo reale delle scansioni di mappatura e classificazione *iniziali* su un volume. Le barre progressive separate tengono traccia delle scansioni di mappatura e classificazione, presentando una percentuale di file totali sottoposti a scansione. È inoltre possibile passare il mouse su una barra di avanzamento per visualizzare il numero di file sottoposti a scansione e il numero totale di file. Il monitoraggio dello stato delle scansioni consente di ottenere informazioni più approfondite sull'avanzamento della scansione, consentendo di pianificare meglio le scansioni e di comprendere l'allocazione delle risorse.

Per visualizzare lo stato delle scansioni, accedere a **Configurazione** nella classificazione BlueXP , quindi selezionare **Configurazione ambiente di lavoro**. L'avanzamento viene visualizzato in linea per ogni volume.

19 febbraio 2025

Versione 1,40

Questa versione di classificazione BlueXP include i seguenti aggiornamenti.

Supporto per RHEL 9,5

Questa versione fornisce il supporto per Red Hat Enterprise Linux v9,5 oltre alle versioni precedentemente supportate. Ciò è applicabile a qualsiasi installazione manuale in loco della classificazione BlueXP , comprese le implementazioni in ambienti oscuri.

I seguenti sistemi operativi richiedono l'utilizzo del motore del contenitore Podman e richiedono la classificazione BlueXP versione 1,30 o superiore: Red Hat Enterprise Linux versione 8,8, 8,10, 9,0, 9,1, 9,2, 9,3, 9,4 e 9,5.

Assegnare priorità alle scansioni di sola mappatura

Quando si eseguono scansioni solo mapping, è possibile assegnare la priorità alle scansioni più importanti. Questa funzione è utile quando si hanno molti ambienti di lavoro e si desidera garantire che le scansioni ad alta priorità vengano completate per prime.

Per impostazione predefinita, le scansioni vengono accodate in base all'ordine in cui vengono avviate. Con la possibilità di assegnare priorità alle scansioni, è possibile spostare le scansioni in primo piano nella coda. È possibile assegnare priorità a più scansioni. La priorità viene indicata in un ordine di primo ingresso e primo uscita, ovvero la prima scansione assegnata all'utente viene spostata in primo piano nella coda; la seconda

scansione assegnata all'utente diventa seconda nella coda e così via.

La priorità viene concessa una tantum. Le riscansioni automatiche dei dati di mappatura vengono eseguite nell'ordine predefinito.

La prioritizzazione è limitata a "scansioni di sola mappatura"; non è disponibile per le scansioni mappa e classificazione.

Per ulteriori informazioni, vedere "Assegnare priorità alle scansioni".

Riprovare tutte le scansioni

La classificazione BlueXP supporta la possibilità di ripetere in batch tutte le scansioni non riuscite.

È possibile ripetere le scansioni in un'operazione batch con la funzione **Riprova tutto**. Se le scansioni di classificazione non vengono eseguite correttamente a causa di un problema temporaneo, ad esempio un'interruzione della rete, è possibile riprovare tutte le scansioni contemporaneamente con un solo pulsante invece di riprovare singolarmente. Le scansioni possono essere riavviate tutte le volte necessarie.

Per riprovare tutte le scansioni:

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Per riprovare tutte le scansioni non riuscite, selezionare **Riprova tutte le scansioni**.

Migliore precisione del modello di categorizzazione

La precisione del modello di machine learning per "categorie predefinite" è migliorata del 11%.

22 gennaio 2025

Versione 1,39

Questa versione di classificazione BlueXP aggiorna il processo di esportazione per il rapporto analisi dati. Questo aggiornamento per l'esportazione è utile per eseguire analisi aggiuntive sui dati, creare visualizzazioni aggiuntive sui dati o condividere con altri i risultati dell'analisi dei dati.

In precedenza, l'esportazione del rapporto Data Investigation era limitata a 10.000 righe. Con questa versione, il limite è stato rimosso in modo da poter esportare tutti i dati. Questa modifica consente di esportare più dati dai report di analisi dei dati, offrendo maggiore flessibilità nell'analisi dei dati.

È possibile scegliere l'ambiente di lavoro, i volumi, la cartella di destinazione e il formato JSON o CSV. Il nome file esportato include un indicatore data e ora che consente di identificare quando i dati sono stati esportati.

Gli ambienti di lavoro supportati includono:

- Cloud Volumes ONTAP
- FSX per ONTAP
- ONTAP
- Gruppo di condivisione

L'esportazione dei dati dal rapporto di analisi dei dati presenta le seguenti limitazioni:

- Il numero massimo di record da scaricare è di 500 milioni. Per tipo (file, directory e tabelle)
- Si prevede che l'esportazione di un milione di record richiederà circa 35 minuti.

Per informazioni dettagliate sull'analisi dei dati e sul rapporto, vedere "Esaminare i dati memorizzati nella propria organizzazione".

16 dicembre 2024

Versione 1,38

Questa versione di classificazione BlueXP include miglioramenti generali e correzioni dei bug.

4 novembre 2024

Versione 1,37

Questa versione di classificazione BlueXP include i seguenti aggiornamenti.

Supporto per RHEL 8,10

Questa versione fornisce il supporto per Red Hat Enterprise Linux v8,10 oltre alle versioni precedentemente supportate. Ciò è applicabile a qualsiasi installazione manuale in loco della classificazione BlueXP , comprese le implementazioni in ambienti oscuri.

I seguenti sistemi operativi richiedono l'utilizzo del motore del contenitore Podman e richiedono la classificazione BlueXP versione 1,30 o superiore: Red Hat Enterprise Linux versione 8,8, 8,10, 9,0, 9,1, 9,2, 9,3 e 9,4.

Ulteriori informazioni su "Classificazione BlueXP".

Supporto di NFS v4,1

Questa release fornisce supporto per NFS v4,1 oltre alle versioni precedentemente supportate.

Ulteriori informazioni su "Classificazione BlueXP".

10 ottobre 2024

Versione 1,36

Supporto per RHEL 9,4

Questa versione fornisce il supporto per Red Hat Enterprise Linux v9,4 oltre alle versioni precedentemente supportate. Ciò è applicabile a qualsiasi installazione manuale in loco della classificazione BlueXP , comprese le implementazioni in ambienti oscuri.

I seguenti sistemi operativi richiedono l'utilizzo del motore del contenitore Podman e richiedono la classificazione BlueXP versione 1,30 o superiore: Red Hat Enterprise Linux versione 8,8, 9,0, 9,1, 9,2, 9,3 e 9,4.

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

Prestazioni di scansione migliorate

Questa versione offre prestazioni di scansione migliorate.

2 settembre 2024

Versione 1,35

Eseguire la scansione dei dati StorageGRID

La classificazione BlueXP supporta la scansione dei dati in StorageGRID.

Per ulteriori informazioni, fare riferimento alla "Eseguire la scansione dei dati StorageGRID".

05 agosto 2024

Versione 1,34

Questa versione di classificazione BlueXP include il seguente aggiornamento.

Passare da CentOS a Ubuntu

La classificazione BlueXP ha aggiornato il proprio sistema operativo Linux per Microsoft Azure e Google Cloud Platform (GCP) da CentOS 7,9 a Ubuntu 22,04.

Per informazioni dettagliate sulla distribuzione, fare riferimento a "Installare su un host Linux con accesso a Internet e preparare il sistema host Linux".

01 luglio 2024

Versione 1,33

Ubuntu supportato

Questa versione supporta la piattaforma Linux Ubuntu 24,04.

Le scansioni di mappatura raccolgono i metadati

I seguenti metadati vengono estratti dai file durante le scansioni di mappatura e visualizzati nelle dashboard Governance, Compliance e Investigation:

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

Dati aggiuntivi nelle dashboard

Questa versione aggiorna i dati visualizzati nei dashboard Governance, Compliance e Investigation durante le scansioni di mappatura.

Per ulteriori informazioni, vedere "Qual è la differenza tra la mappatura e la classificazione delle scansioni".

05 giugno 2024

Versione 1,32

Nuova colonna Stato mapping nella pagina di configurazione

In questa versione viene ora visualizzata una nuova colonna Stato mapping nella pagina di configurazione. La nuova colonna consente di identificare se la mappatura è in esecuzione, in coda, in pausa o superiore.

Per la spiegazione degli stati, vedere "Modificare le impostazioni di scansione".

15 maggio 2024

Versione 1,31

La classificazione è disponibile come servizio core all'interno di BlueXP

La BlueXP classification è ora disponibile come funzionalità principale di BlueXP senza costi aggiuntivi per un massimo di 500 TiB di dati scansionati per connettore. Non è richiesta alcuna licenza di classificazione o abbonamento a pagamento. Mentre concentriamo la funzionalità di classificazione BlueXP sulla scansione dei sistemi storage NetApp con questa nuova versione, alcune funzionalità legacy saranno disponibili solo per i clienti che avevano precedentemente pagato per una licenza. L'utilizzo di tali funzioni legacy scadrà quando il contratto a pagamento avrà raggiunto la data di fine.

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

"Ulteriori informazioni sulle funzioni obsolete".

01 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".

La classificazione BlueXP è supportata se installi il connettore su un host RHEL 8 o 9 che risiede on-premise. Non è supportato se l'host RHEL 8 o 9 si trova in AWS, Azure o Google Cloud.

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".

04 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 visualizzano le dimensioni totali oltre al numero totale di elementi

I risultati filtrati nella pagina di analisi visualizzano 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.

La release ha inoltre 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. Fare riferimento alla "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".

06 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.

04 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.

05 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".

06 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 anche possibile immettere nomi giapponesi in "Filtro "Data Subject" nella pagina Data Investigation" per identificare i file che contengono il nome del soggetto.

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.

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.

03 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 di sensibilizzare i clienti sulle problematiche di governance dei dati, sulle esposizioni alla sicurezza dei dati e sulle lacune di conformità dei dati del 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, ci sono 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".

07 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 dispone di molti "categorie predefinite", quindi questa funzione consente di aggiungere categorie personalizzate per identificare la posizione in cui vengono trovate le informazioni univoche dell'organizzazione.

"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`.

05 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)".

09 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. Questo può aiutare a capire dove si possono avere alcuni rischi con i 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). Ciò include sia il numero personale che il numero aziendale. "Scopri tutti i tipi di dati personali che la classificazione BlueXP può identificare nei tuoi dati".

Limitazioni note nella classificazione BlueXP

Le limitazioni note identificano funzioni che non sono supportate o non interagiscono correttamente in questa versione. Esaminare attentamente queste limitazioni.

Opzioni disabilitate per la classificazione BlueXP

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

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

Scansione della classificazione BlueXP

Le scansioni delle classificazioni BlueXP presentano le seguenti limitazioni.

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.

In questa configurazione, vengono scansionati solo i dati in /A. I dati in /C e /D non vengono scansionati.

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:

   Filtra i dati in base a "Nome dell’ambiente di lavoro" e "Tipo di directory = Condivisione" per vedere quale condivisione viene scansionata.

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".

   Aggiungi tutte le azioni singolarmente, ad esempio:

   ```
   /C
   /D
   ```

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

Ultimo timestamp di accesso

Quando la classificazione BlueXP esegue una scansione di una directory, la scansione influisce sul campo **Ultimo accesso** della directory. Quando si visualizza il campo **Ultimo accesso**, i metadati riflettono la data e l’ora della scansione o l’ultimo accesso dell’utente alla directory.

Inizia subito

Scopri di più sulla classificazione BlueXP

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

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

Caratteristiche

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

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

Mantenere la conformità

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

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

Rafforzare la sicurezza

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

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

Ottimizzare l'utilizzo dello storage

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

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

Ambienti di lavoro e origini dati supportati

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

Ambienti di lavoro

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

Origini dati

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

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

Costo

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

Costi delle infrastrutture

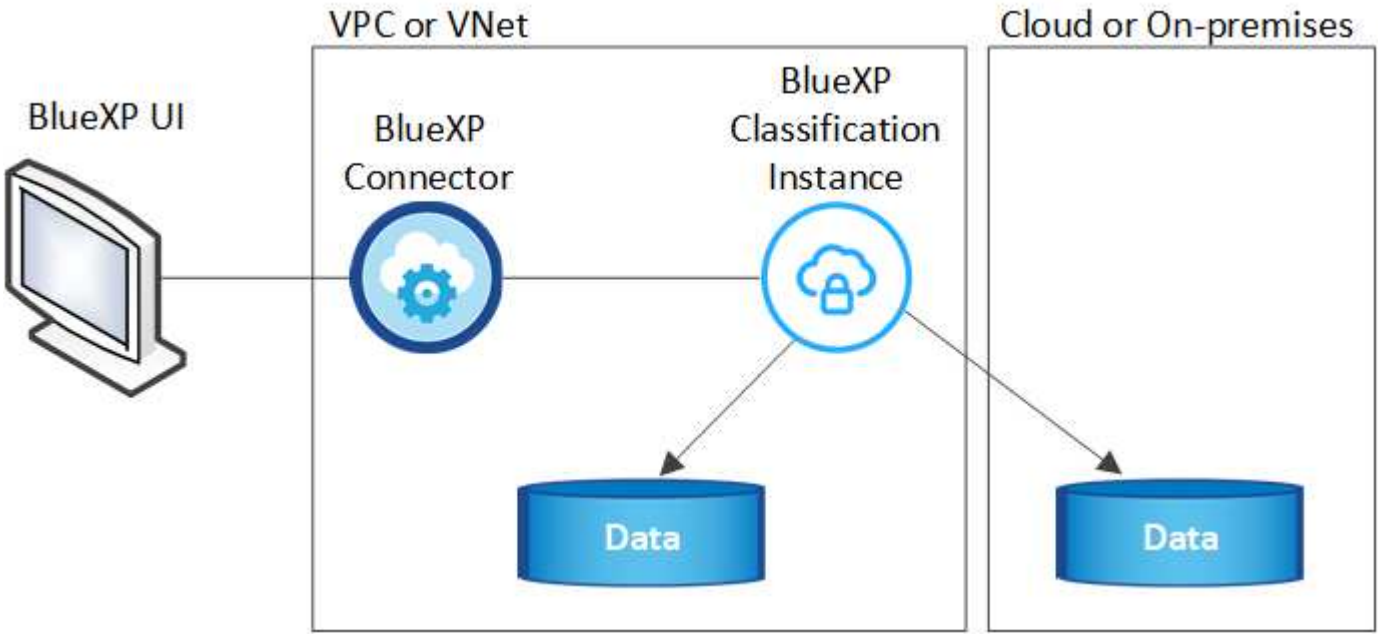
- L'installazione della classificazione BlueXP nel cloud richiede l'implementazione di un'istanza di cloud, con conseguente addebito da parte del provider di cloud in cui viene implementata. Vedere il tipo di istanza implementata per ciascun cloud provider. L'installazione della classificazione BlueXP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

Costi di trasferimento dei dati

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

L'istanza di classificazione BlueXP

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



Tenere presente quanto segue sull'istanza predefinita:

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

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

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

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

Distribuire su diversi tipi di istanza

Esaminare le seguenti specifiche per i tipi di istanza:

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

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

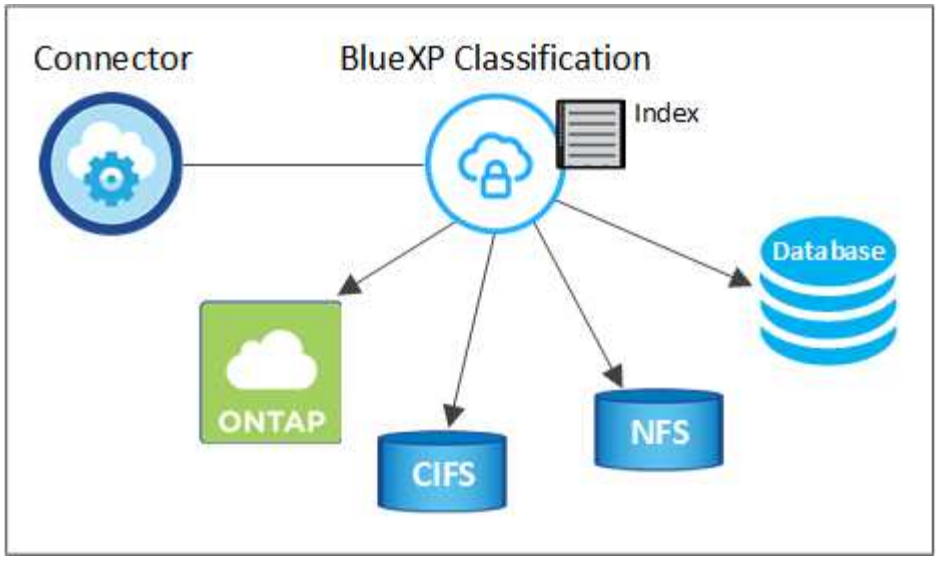
Come funziona la scansione della classificazione BlueXP

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

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

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

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



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

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

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

Qual è la differenza tra le scansioni di mappatura e classificazione

È possibile eseguire due tipi di scansioni nella classificazione BlueXP :

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

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

Informazioni classificate dalla classificazione BlueXP

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

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

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

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

Panoramica delle reti

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

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

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

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

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

Accedi BlueXP classification

È possibile accedere al servizio BlueXP classification tramite NetApp BlueXP.

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

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

Prima di iniziare

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

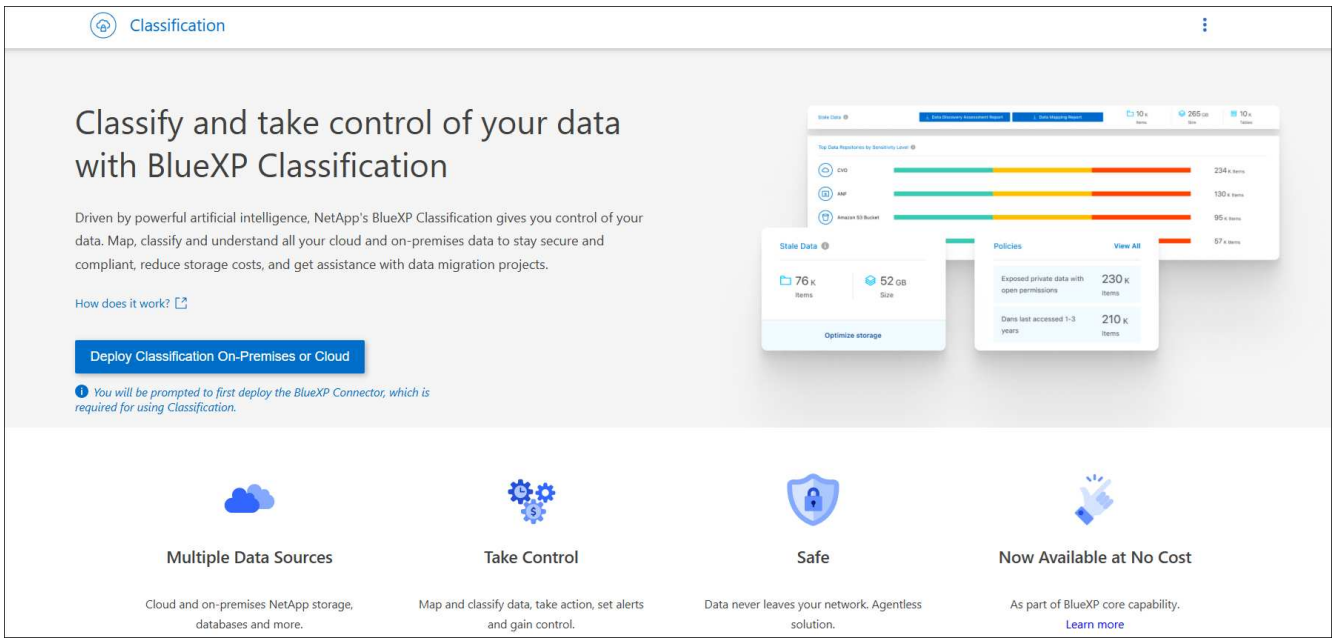
Fasi

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

   Viene visualizzata la pagina di accesso a NetApp BlueXP.

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

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



In caso contrario, viene visualizzata la Dashboard BlueXP classification .

Implementare la classificazione BlueXP

Quale implementazione della classificazione BlueXP dovresti utilizzare?

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

La classificazione BlueXP può essere implementata nei seguenti modi:

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

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

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

Implementare la classificazione BlueXP nel cloud utilizzando BlueXP

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

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

Avvio rapido

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

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.

Creare un connettore

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

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

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

sottoporre a scansione.

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

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

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

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

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

Supporto per le regioni governative

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

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

Esaminare i prerequisiti

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

Abilitare l'accesso a Internet in uscita dalla classificazione BlueXP

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

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

Endpoint richiesti per AWS

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

Endpoint richiesti per Azure

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

Endpoint richiesti per GCP

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

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

Assicurarsi che BlueXP disponga delle autorizzazioni necessarie

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

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

Assicurarsi che BlueXP Connector possa accedere alla classificazione BlueXP

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

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

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

Assicurarsi che sia possibile mantenere in esecuzione la classificazione BlueXP

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

Garantire la connettività del browser Web alla classificazione BlueXP

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

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

Controllare i limiti della vCPU

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

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

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

Implementare la classificazione BlueXP nel cloud

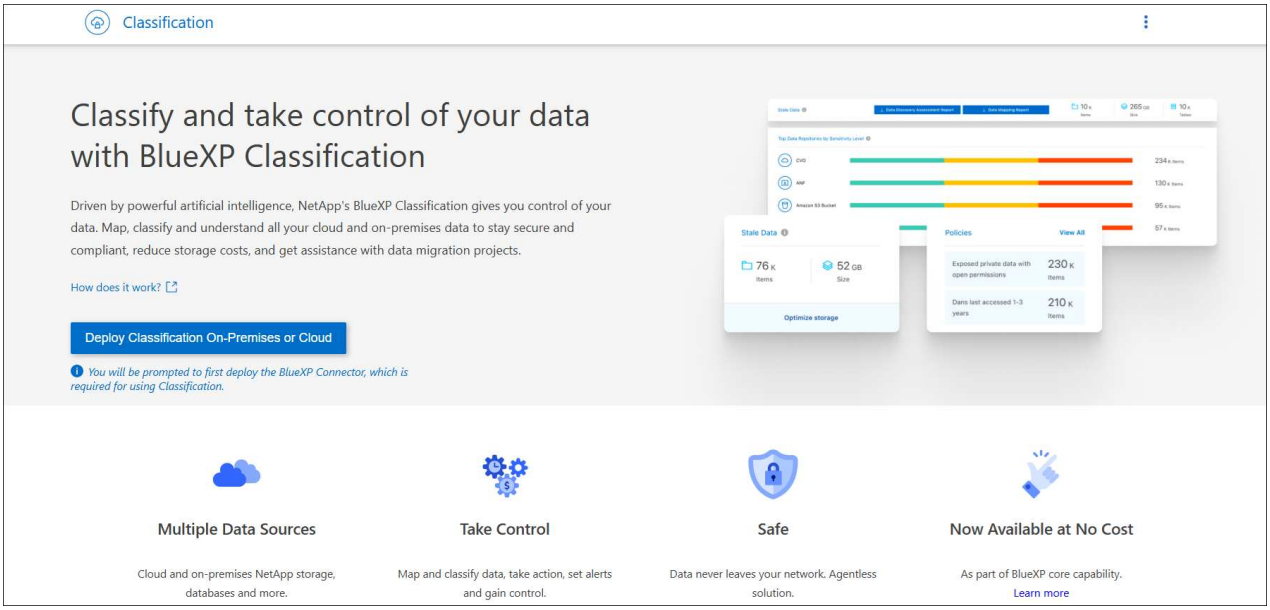
Seguire questi passaggi per implementare un'istanza della classificazione BlueXP nel cloud. Il connettore implementerà l'istanza nel cloud, quindi installerà il software di classificazione BlueXP su tale istanza.

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

Implementazione in AWS

Fasi

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



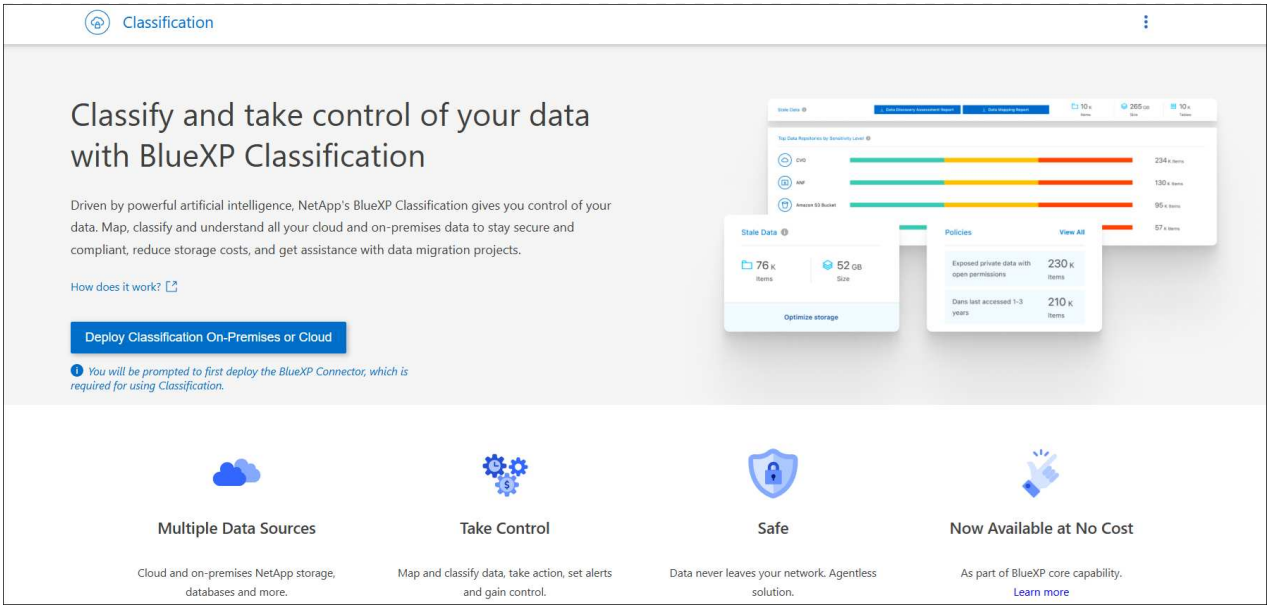
3. Dalla pagina *Installazione*, seleziona **Distribuisci > Distribuisci** per utilizzare la dimensione dell'istanza "Grande" e avviare la procedura guidata di distribuzione nel cloud.
4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi,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

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

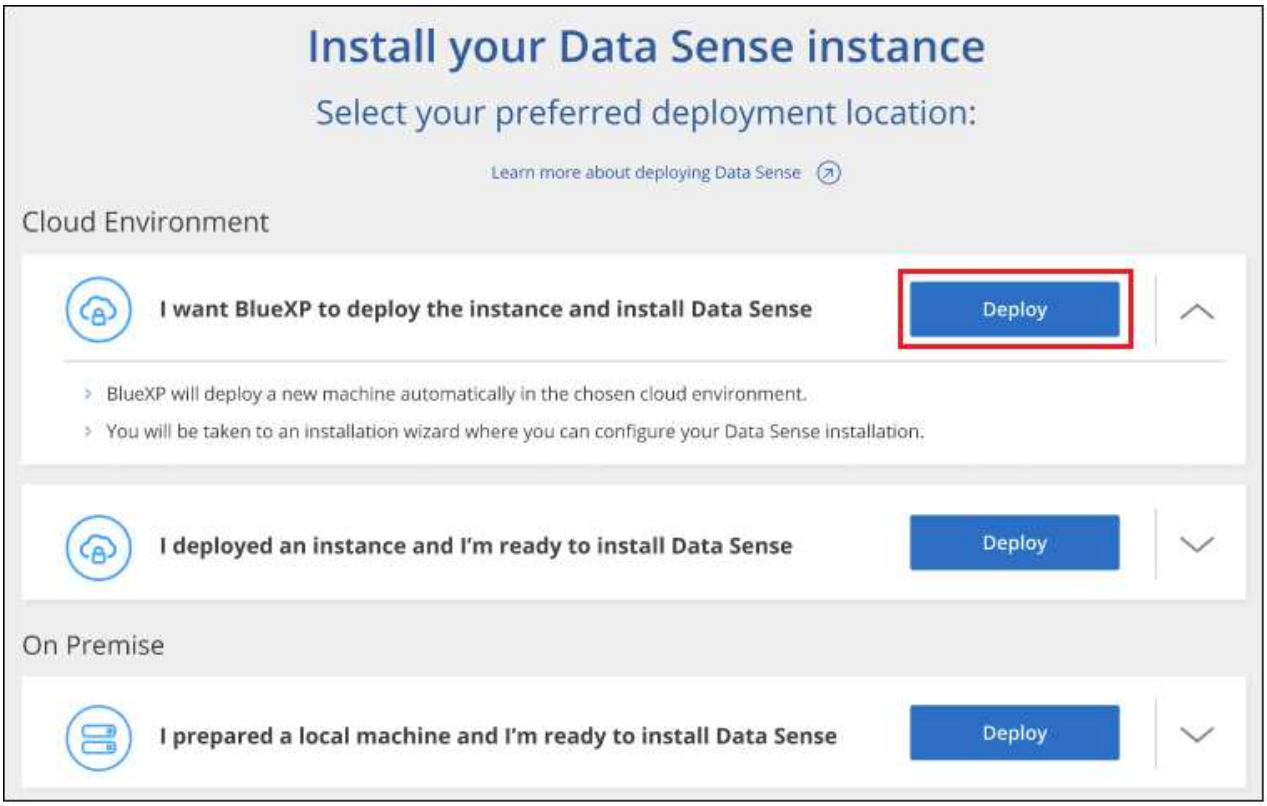
Implementazione in Azure

Fasi

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



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



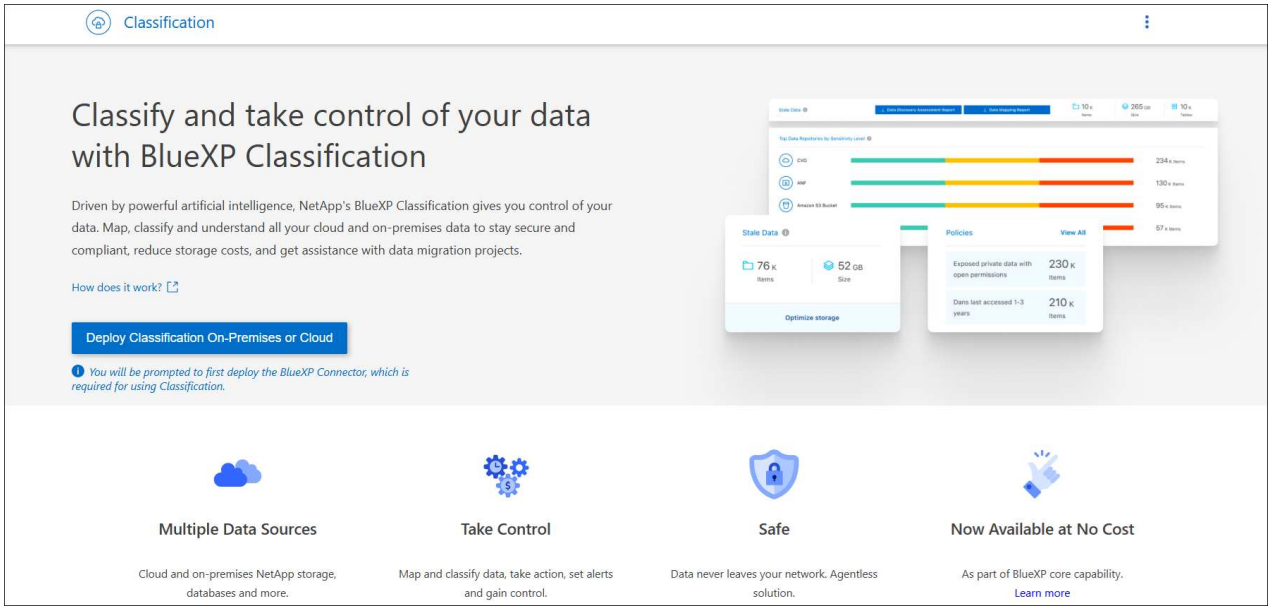
4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.

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

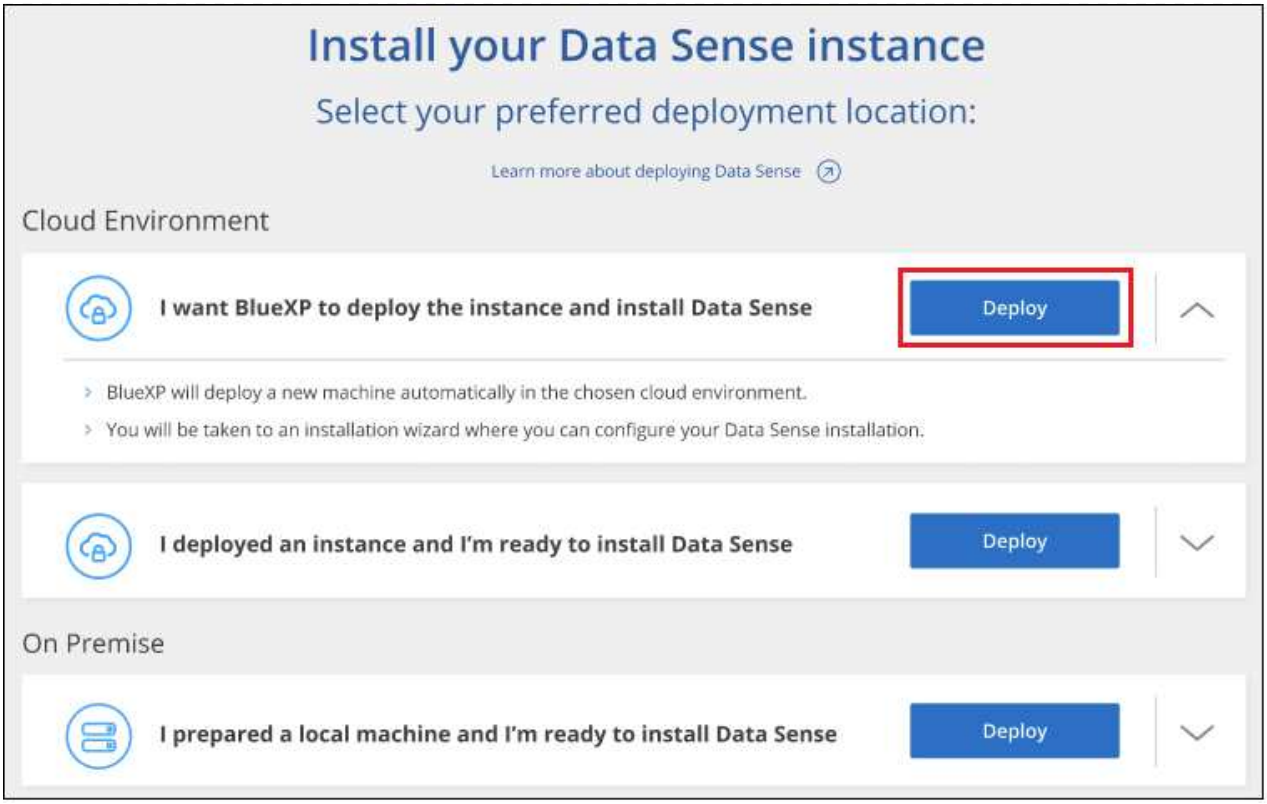
Implementazione in Google Cloud

Fasi

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



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



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

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

Risultato

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

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

Cosa c'è di nuovo

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

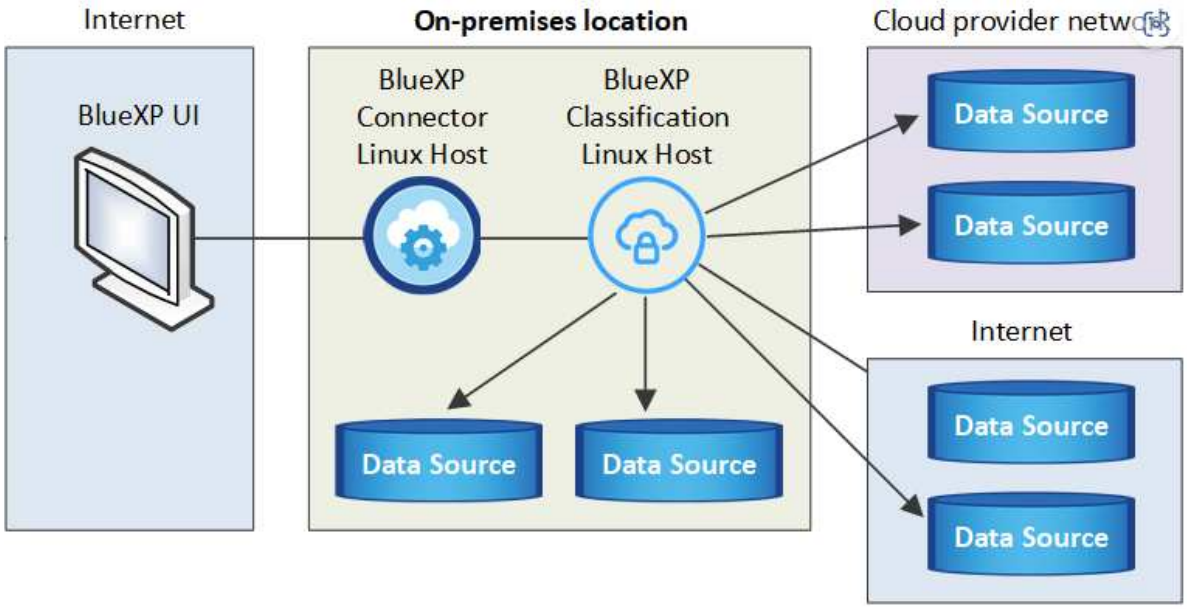
Installare la classificazione BlueXP su un host con accesso a Internet

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

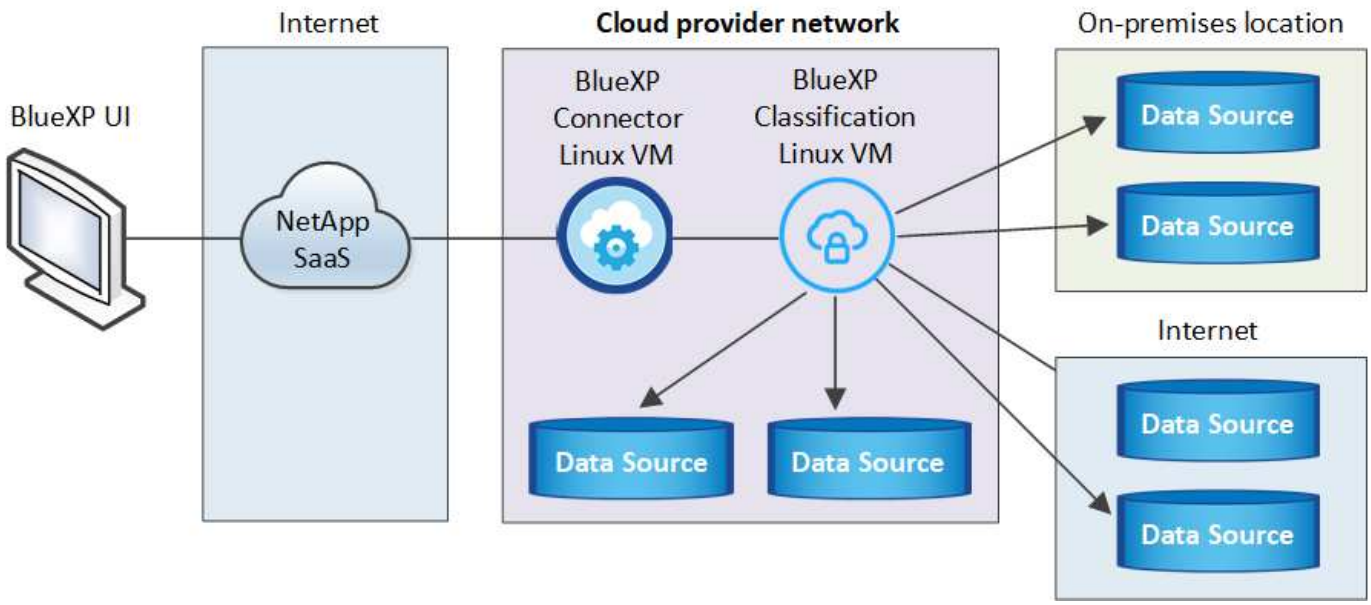
L'installazione in sede può essere una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP in sede utilizzando un'istanza di classificazione BlueXP che si trova anche in loco, ma questo non è un requisito. Il software funziona esattamente allo stesso modo, indipendentemente dal metodo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

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

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



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



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

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

Avvio rapido

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

1 **Creare un connettore**

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

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

2 **Esaminare i prerequisiti**

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

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

3 **Scarica e implementa la classificazione BlueXP**

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

Creare un connettore

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

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

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

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

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

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

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

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

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

Preparare il sistema host Linux

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

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

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

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

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

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

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

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

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

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

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

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

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

Abilitare l'accesso a Internet in uscita dalla classificazione BlueXP

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

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

Verificare che tutte le porte richieste siano attivate

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

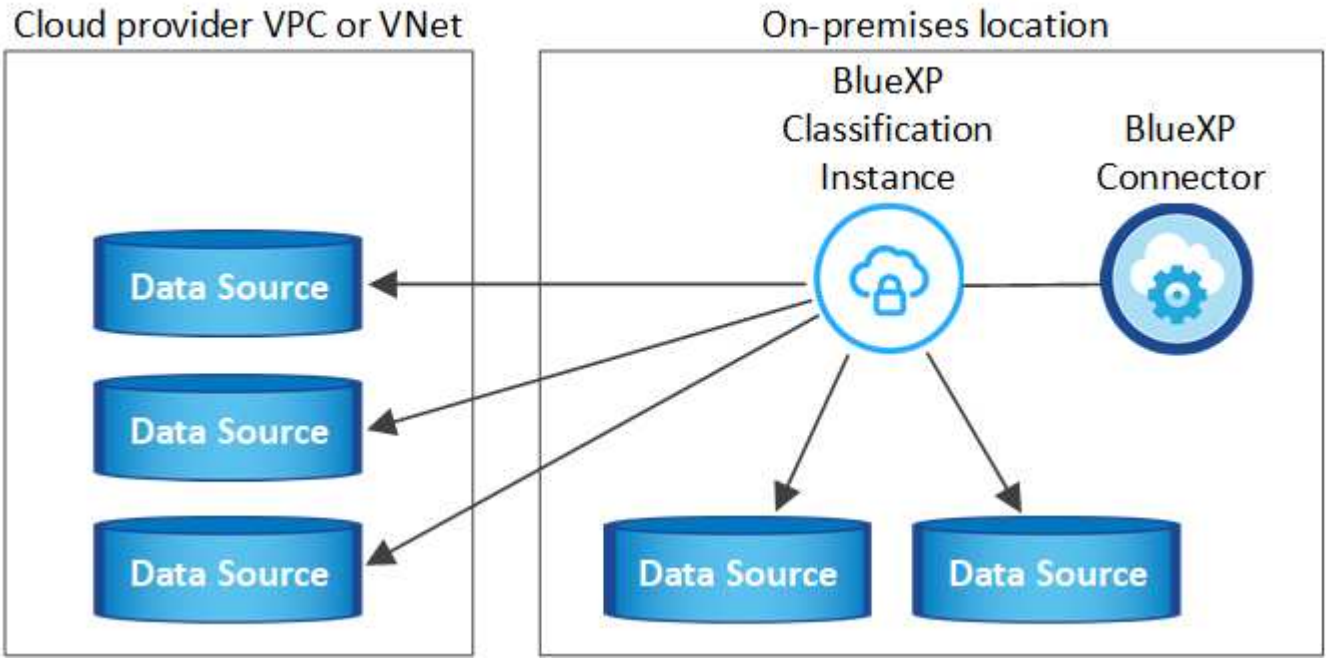
Tipo di connessione	Porte	Descrizione
Connettore <> classificazione BlueXP	8080 (TCP), 443 (TCP) e 80. 9000	Il firewall o le regole di routing per il connettore devono consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione BlueXP. Assicurarsi che la porta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

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

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

Installare la classificazione BlueXP sull'host Linux

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



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

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

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

Installazione a host singolo per configurazioni tipiche

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

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

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

Prima di iniziare

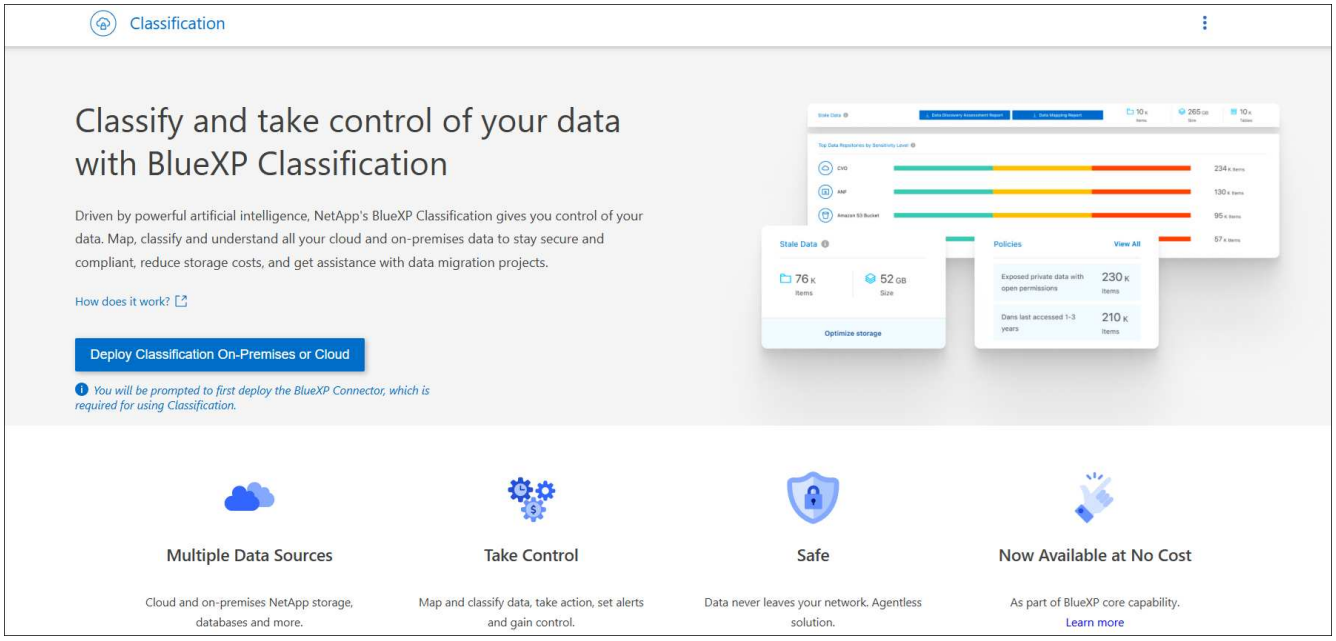
- Verificare che il sistema Linux soddisfi i requisiti requisiti dell'host.
- Verificare che sul sistema siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sul sistema Linux.
- Se si utilizza un proxy per l'accesso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

Fasi

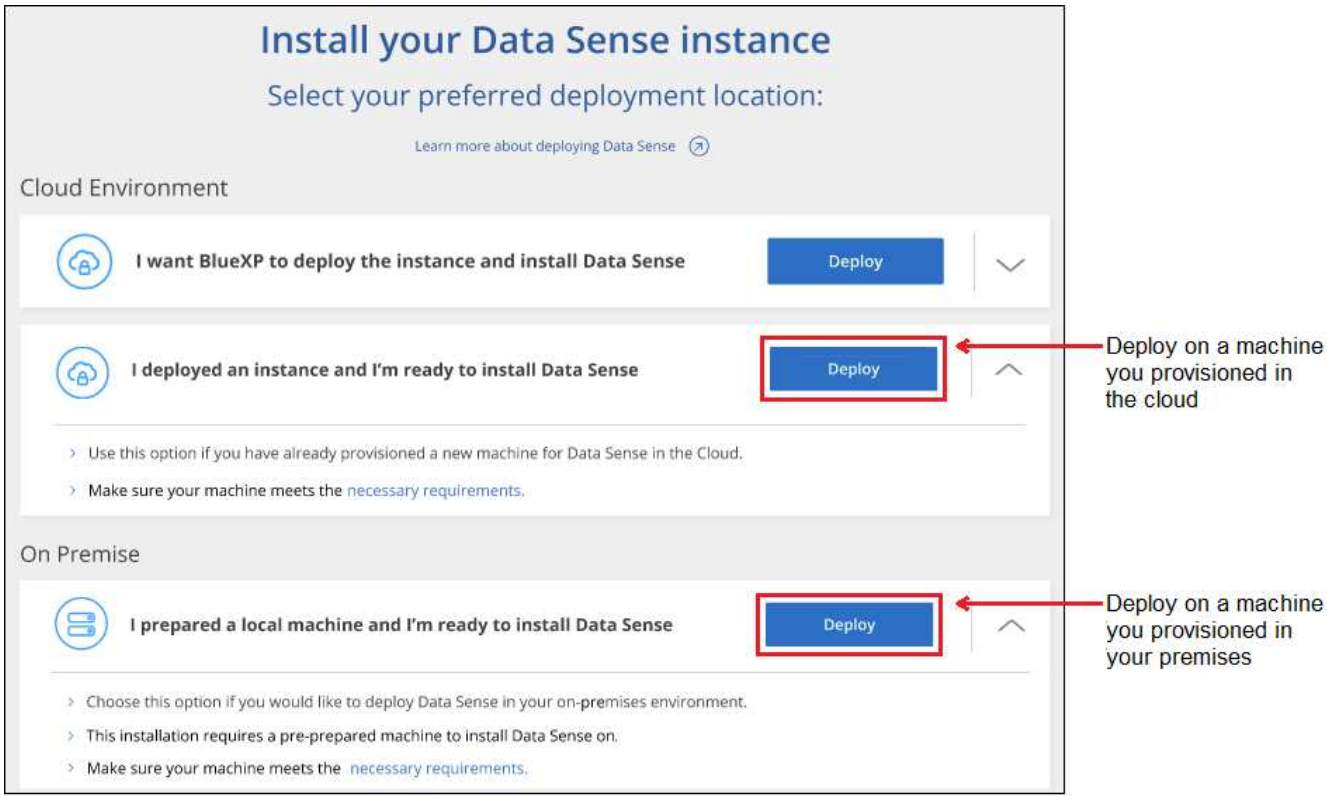
1. Scaricare il software di classificazione BlueXP dal "Sito di supporto NetApp". Il file da selezionare è **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copiare il file del programma di installazione sull'host Linux che si desidera utilizzare (utilizzando `scp` o qualche altro metodo).
3. Decomprimere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

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

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



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



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

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

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

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

Valori variabili:

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

Risultato

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

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

Cosa c'è di nuovo

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

Installare la classificazione BlueXP su un host Linux senza accesso Internet

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

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

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

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

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

Origini dati supportate

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

- Sistemi ONTAP on-premise
- Schemi di database

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

Limitazioni

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

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

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

Avvio rapido

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

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.

Installare il connettore BlueXP

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

Preparare il sistema host Linux

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

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

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

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

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

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

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

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

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

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

Verificare i prerequisiti di classificazione di BlueXP e BlueXP

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

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

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

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

Verificare che tutte le porte richieste siano attivate

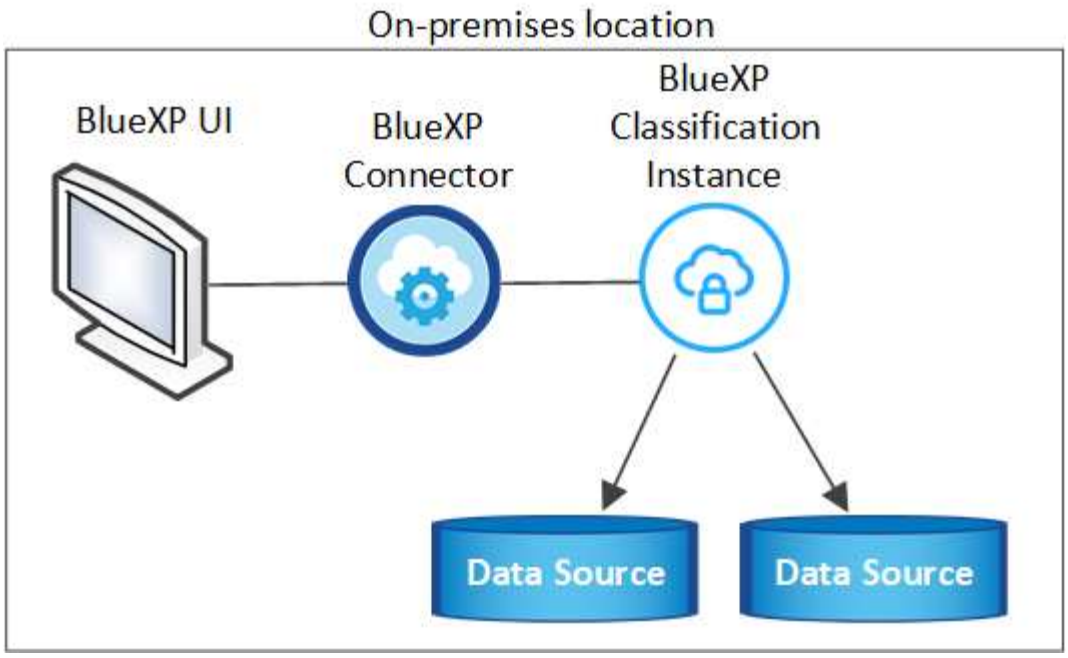
Assicurarsi che tutte le porte richieste siano aperte per la comunicazione tra il connettore, la classificazione BlueXP, Active Directory e le origini dati.

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

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

Installare la classificazione BlueXP sull'host Linux on-premise

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



Installazione a host singolo per configurazioni tipiche

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

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

Prima di iniziare

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

Fasi

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

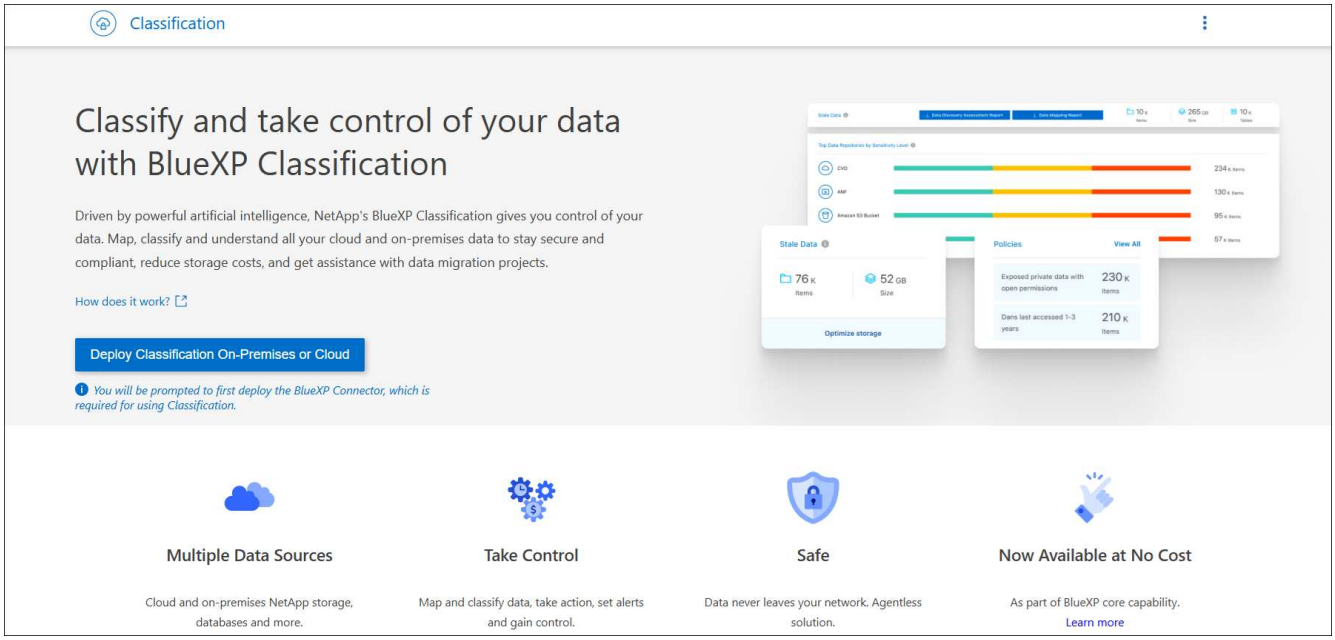
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

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

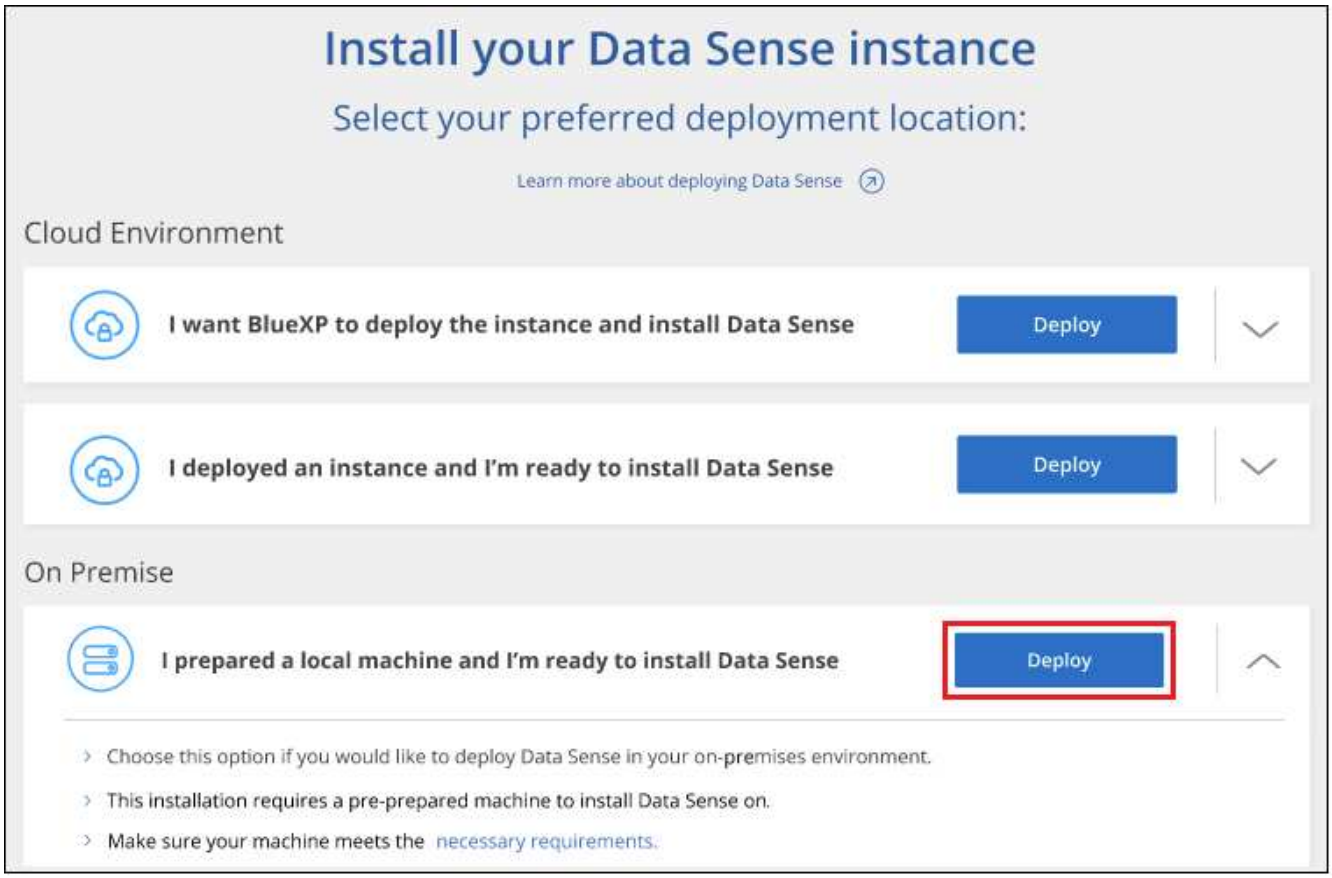
4. Decomprimere il file di installazione sul computer host, ad esempio:

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

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



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



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

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

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

   Valori variabili:

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

Risultato

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

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

Cosa c'è di nuovo

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

Aggiornare il software di classificazione BlueXP

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

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

Prima di iniziare

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

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

Fasi

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

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

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

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

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

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

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

   ```
   start_darksite_upgrade.sh
   ```

Risultato

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

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

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

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

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

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

Per iniziare

Eseguire le seguenti operazioni.

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

Creare un connettore

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

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

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

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

Verificare i requisiti dell'host

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

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

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

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

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

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

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

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

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

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

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

Abilitare l'accesso a Internet in uscita dalla classificazione BlueXP

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

Internet in uscita per contattare i seguenti endpoint.

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

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

Verificare che tutte le porte richieste siano attivate

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

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

Eseguire lo script dei prerequisiti di classificazione BlueXP

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

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

Prima di iniziare

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

Fasi

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

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

4. Eseguire lo script utilizzando il seguente comando.

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

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

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

Risultato

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

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

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

Attivare la scansione sulle origini dati

Panoramica delle origini dati di scansione con classificazione BlueXP

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

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

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

Qual è la differenza tra le scansioni di mappatura e classificazione

È possibile eseguire due tipi di scansioni nella classificazione BlueXP :

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

La tabella seguente mostra alcune delle differenze:

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

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

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

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

Differenze del dashboard di governance:

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

Differenze del dashboard di conformità:

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

Differenze tra i filtri di analisi:

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

Con quale rapidità la classificazione BlueXP esegue la scansione dei dati

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

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

100-150 tibs di dati al giorno.

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

Esegui la scansione dei volumi Azure NetApp Files con classificazione BlueXP

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

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

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

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

Distribuire l'istanza di classificazione BlueXP

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

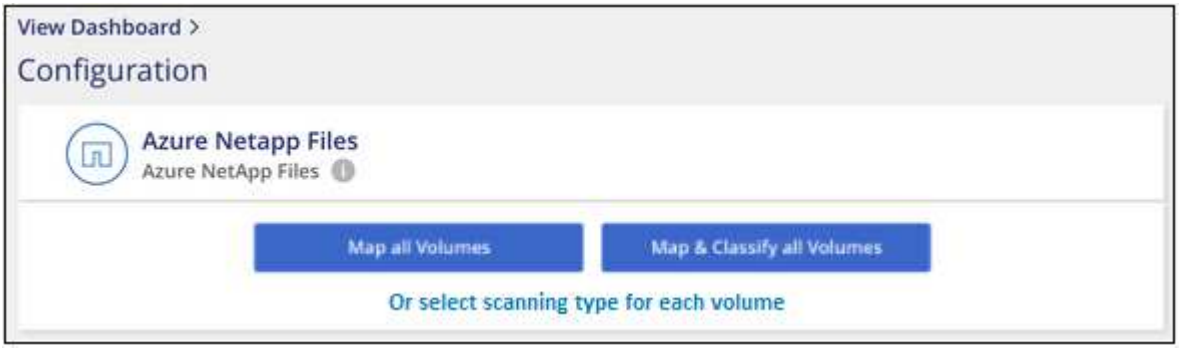
La classificazione BlueXP deve essere implementata nel cloud durante la scansione dei volumi Azure NetApp Files e deve essere implementata nella stessa regione dei volumi che si desidera sottoporre a scansione.

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

Abilita la classificazione BlueXP nei tuoi ambienti di lavoro

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

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



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

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

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

Risultato

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

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

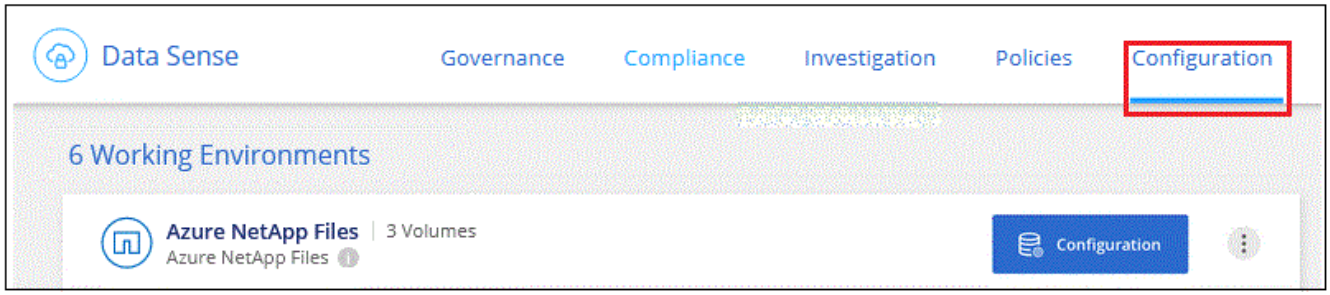
Verificare che la classificazione BlueXP abbia accesso ai volumi

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

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

Fasi

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

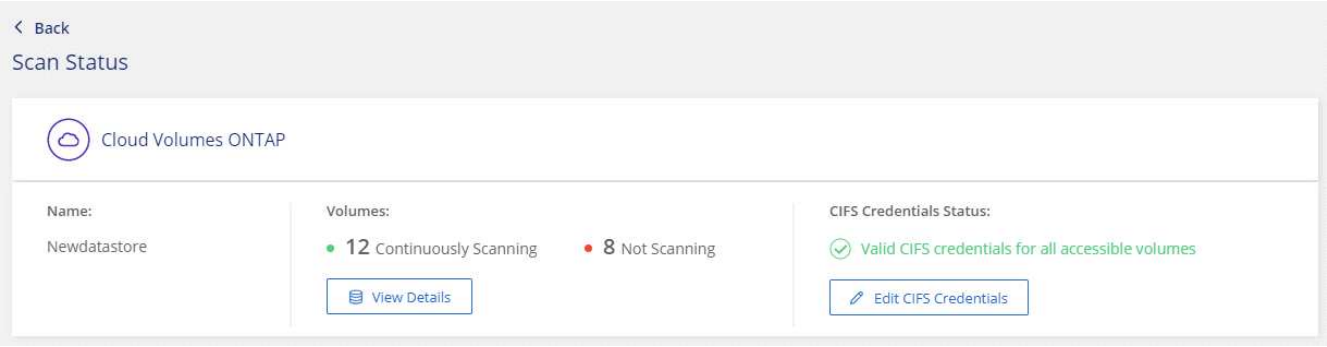


a. Per ogni ambiente di lavoro, selezionare **Modifica credenziali CIFS** e immettere il nome utente e la password necessari per la classificazione BlueXP per accedere ai volumi CIFS sul sistema.

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

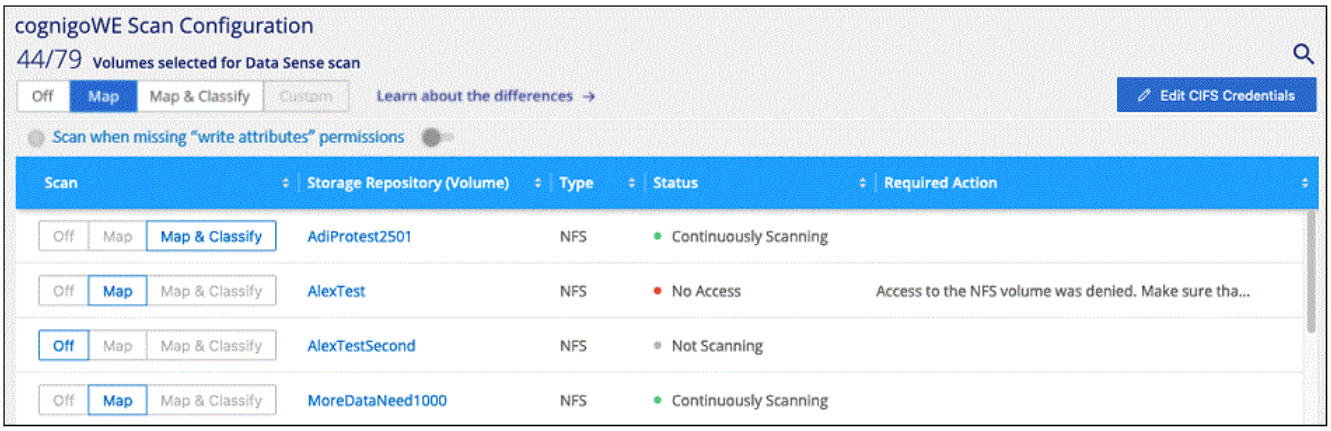
   Per assicurarsi che gli "ultimi accessi" dei file non vengano modificati dalle scansioni BlueXP classification , si consiglia che l'utente disponga delle autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS. Se possibile, configurare l'utente di Active Directory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

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



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

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

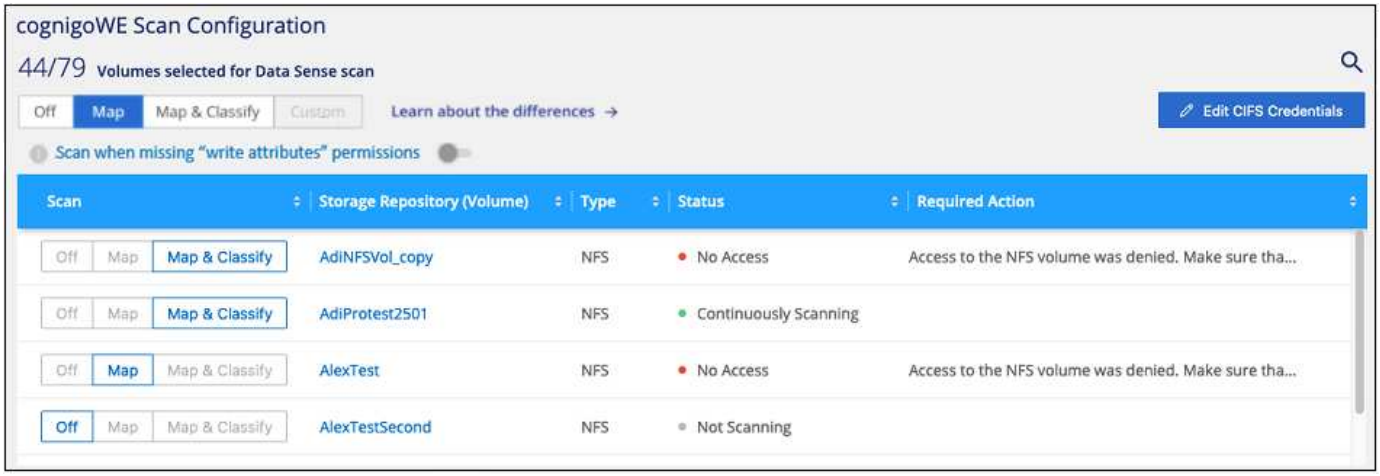


Abilitare e disabilitare le scansioni di conformità sui volumi

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

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

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



Fasi

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

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

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

Prima di iniziare

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

  "Gruppi di sicurezza AWS per istanze Linux"

  "Gruppi di sicurezza AWS per le istanze di Windows"

  "AWS Elastic Network Interface (ENI)"

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

Distribuire l'istanza di classificazione BlueXP

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

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

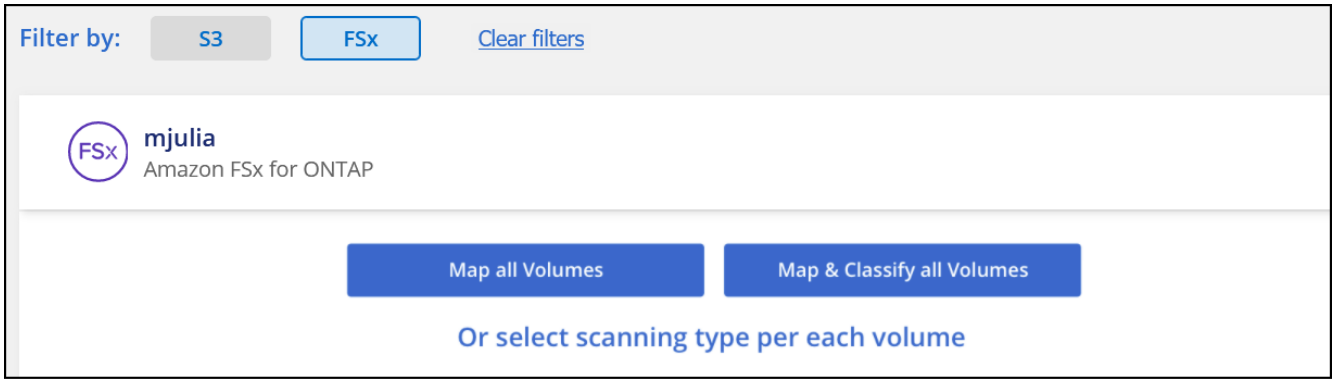
Nota: l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei volumi FSX.

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

Abilita la classificazione BlueXP nei tuoi ambienti di lavoro

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

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



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

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

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

Risultato

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

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

Verificare che la classificazione BlueXP abbia accesso ai volumi

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

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

Fasi

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

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

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

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

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

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

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

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

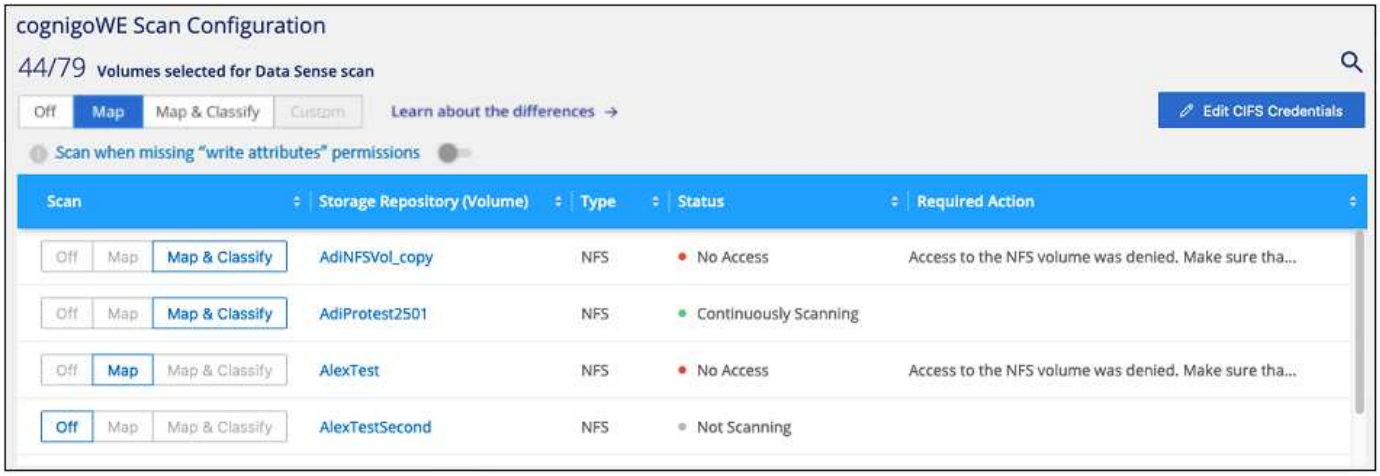
      Per assicurarsi che gli "ultimi accessi" dei file non vengano modificati dalle scansioni BlueXP classification , si consiglia che l'utente disponga delle autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS. Se possibile, configurare l'utente di Active Directory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

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

Abilitare e disabilitare le scansioni di conformità sui volumi

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

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



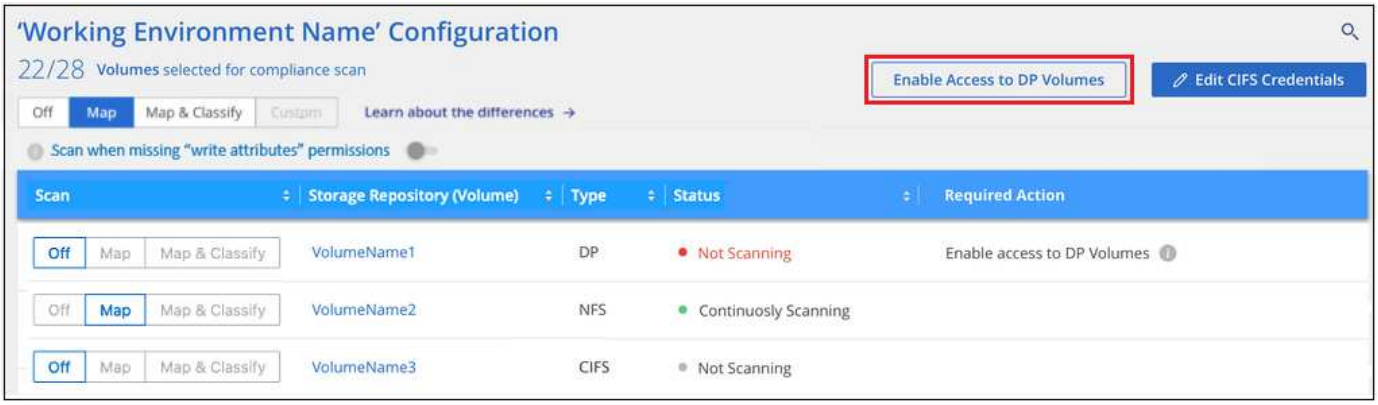
1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Nella pagina di configurazione, individuare l'ambiente di lavoro con i volumi da sottoporre a scansione.
3. Effettuare una delle seguenti operazioni:
    - Per attivare le scansioni di sola mappatura su un volume, nell'area del volume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

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

Eseguire la scansione dei volumi di protezione dei dati

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

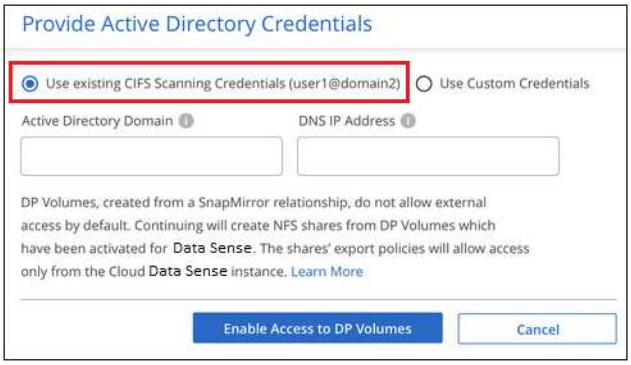
Inizialmente, l'elenco dei volumi identifica questi volumi come *Type* **DP** con *Status* **Not Scanning** e *Required Action* **Enable Access to DP Volumes**.

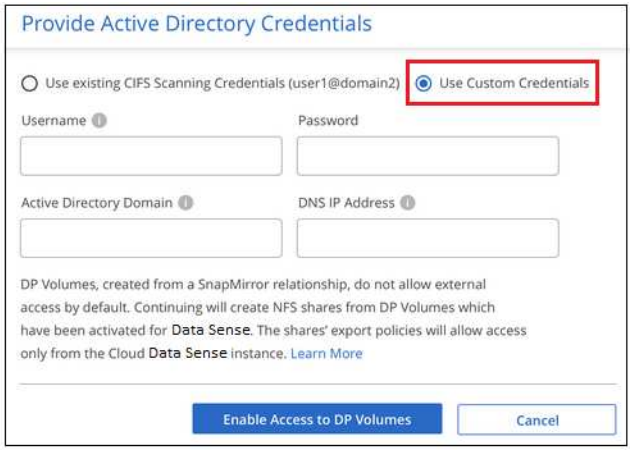


Fasi

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

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





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

Risultato

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

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

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

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

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

Prerequisiti

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

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

Abilitare la scansione della classificazione BlueXP negli ambienti di lavoro

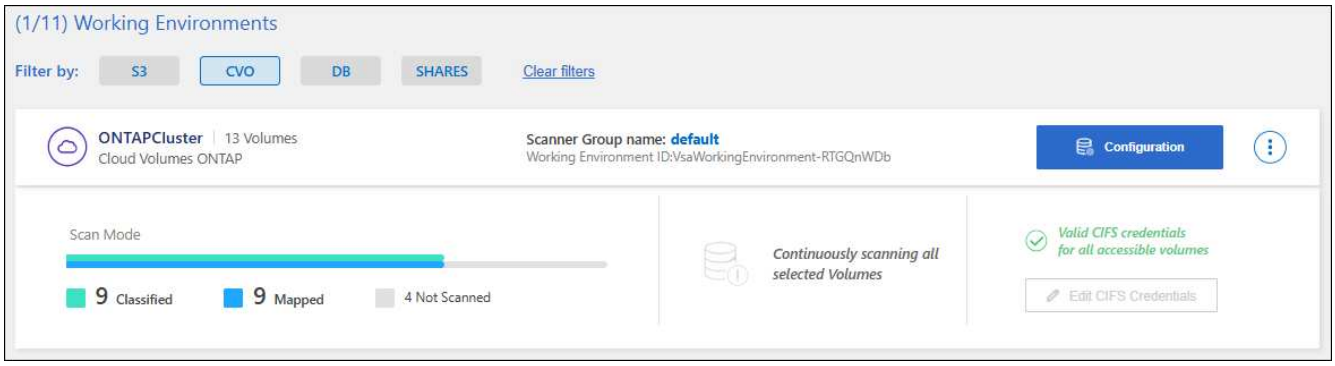
Puoi abilitare la scansione della classificazione BlueXP sui sistemi Cloud Volumes ONTAP in qualsiasi cloud

provider supportato e sui cluster ONTAP on-premise.

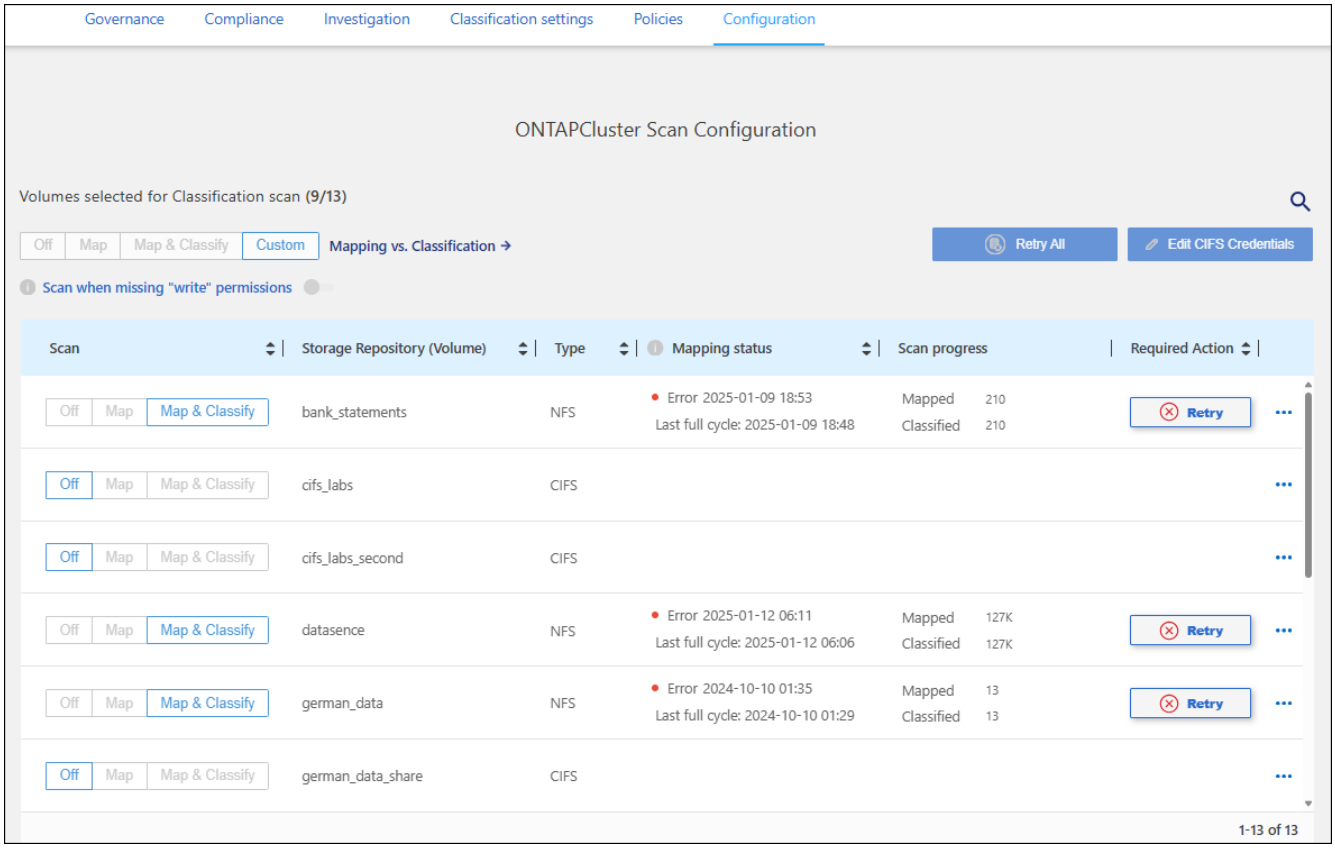
Fasi

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

   La pagina di configurazione mostra più ambienti di lavoro.



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



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

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

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

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

Risultato

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

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

Verificare che la classificazione BlueXP abbia accesso ai volumi

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

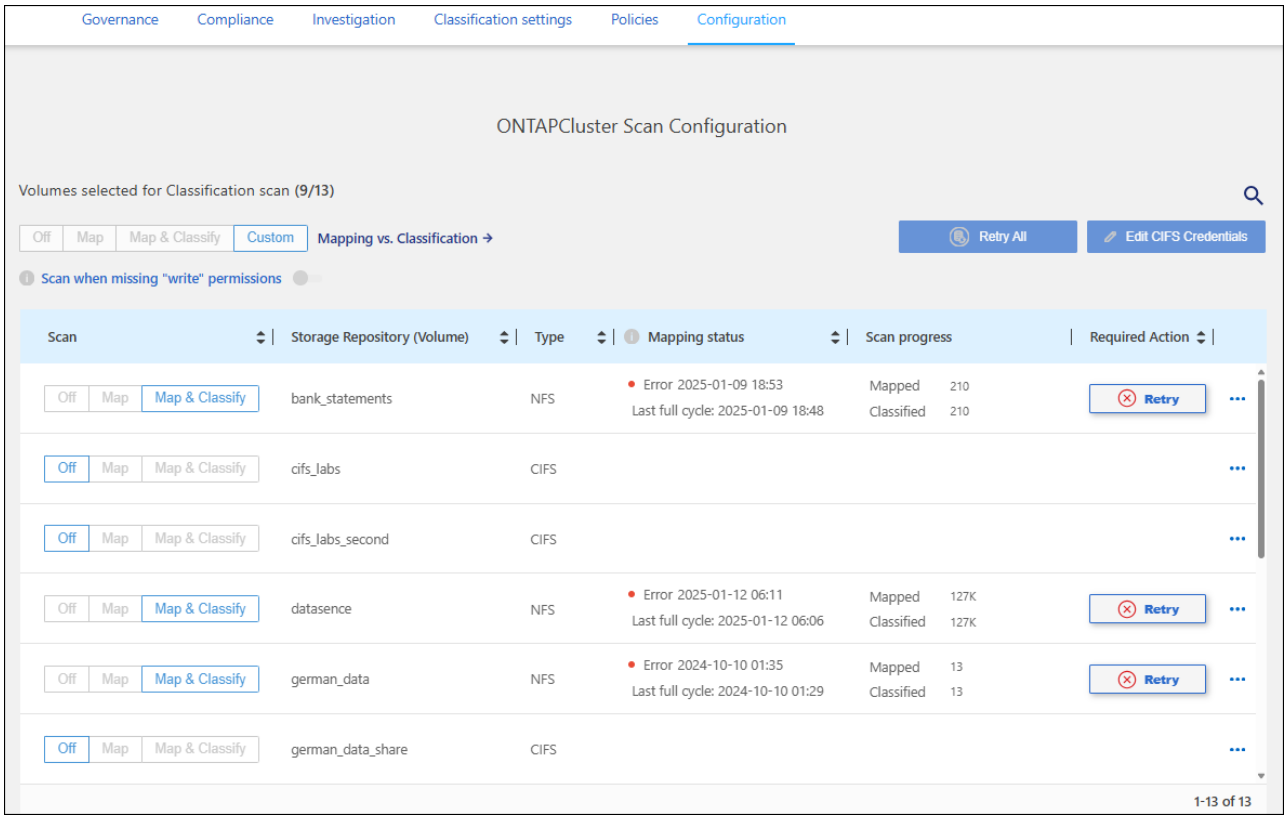
Fasi

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

   È possibile aprire il gruppo di protezione per il traffico dall'indirizzo IP dell'istanza di classificazione BlueXP oppure aprire il gruppo di protezione per tutto il traffico dall'interno della rete virtuale.

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

   a. Dal menu di navigazione sinistro di BlueXP , selezionare **Governance > classificazione**.
   b. Dal menu classificazione BlueXP , selezionare **Configurazione**.



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

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

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

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

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

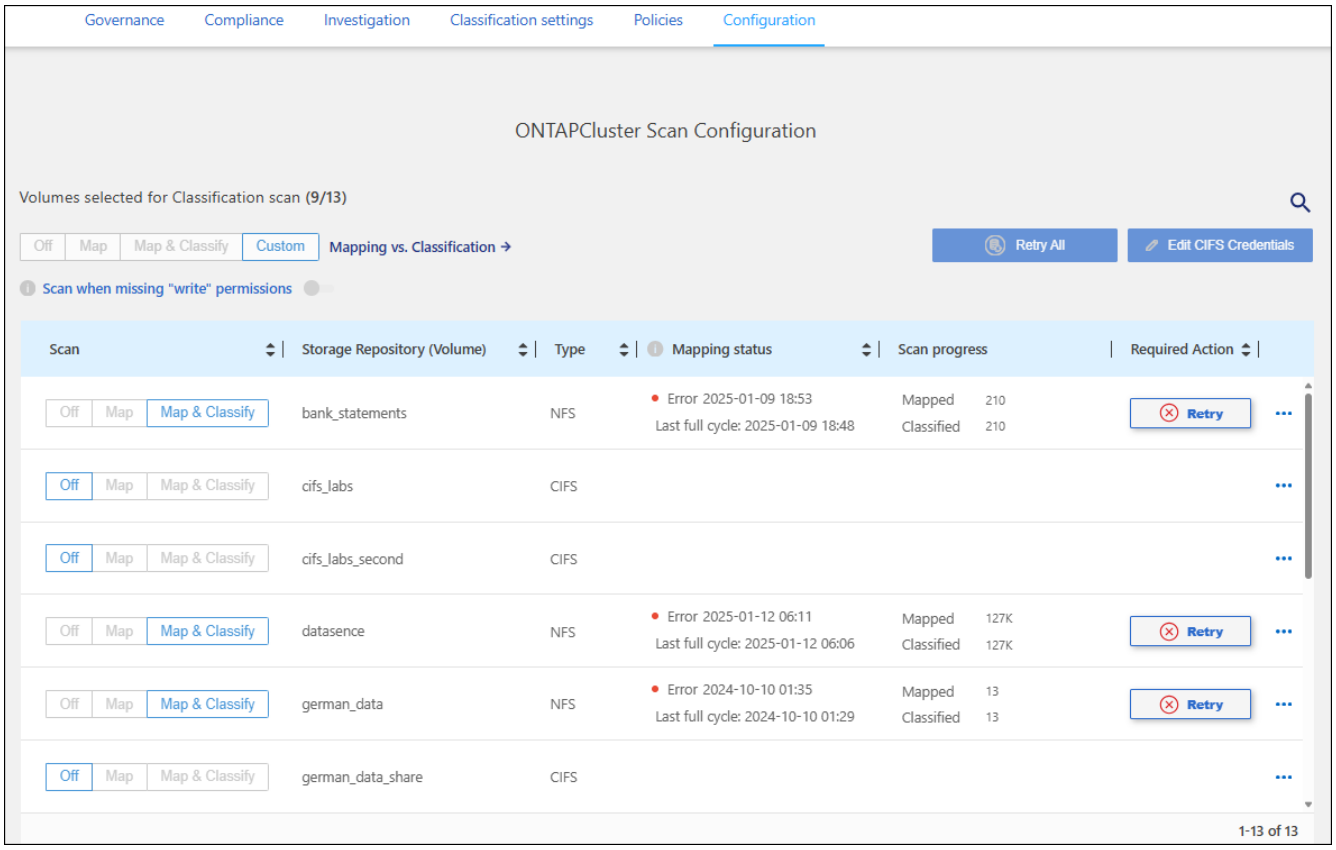
Disattivare le scansioni di conformità sui volumi

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

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

Fasi

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



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

Eseguire la scansione degli schemi del database con classificazione BlueXP

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

Esaminare i prerequisiti

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

Database supportati

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

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

- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

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

Requisiti del database

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

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

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

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

Distribuire l'istanza di classificazione BlueXP

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

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

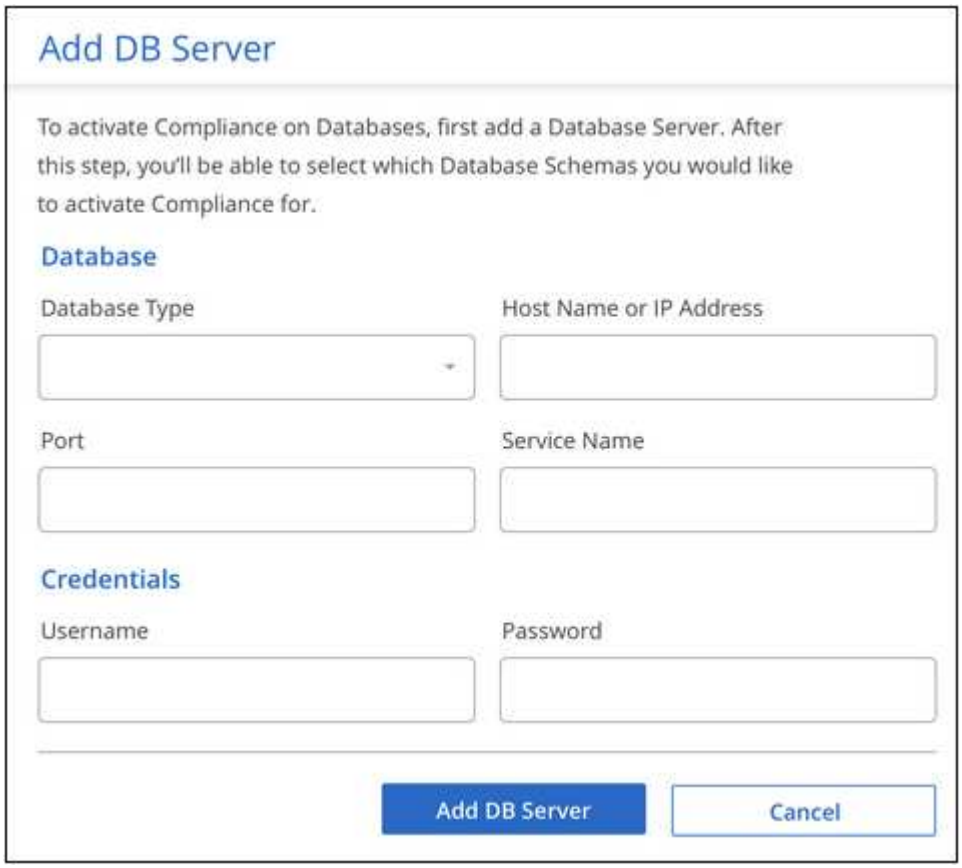
Se si eseguono scansioni di schemi di database installati in un sito buio che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella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

Aggiungere il server database

Aggiungere il server di database in cui risiedono gli schemi.

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

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



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

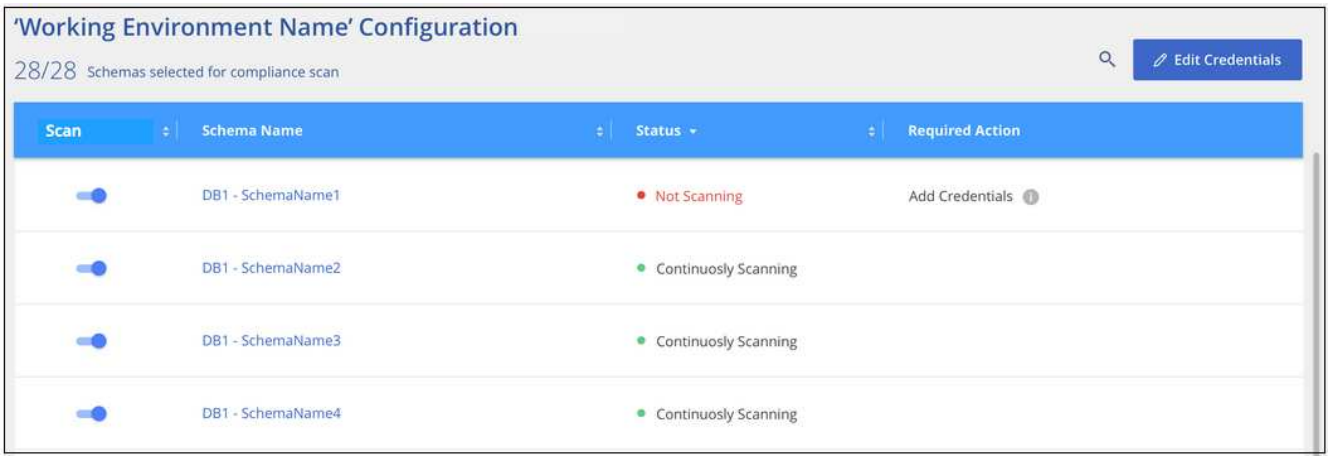
Abilitare e disabilitare le scansioni di conformità sugli schemi di database

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

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

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

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



Risultato

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

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

Eseguire la scansione delle condivisioni di file con classificazione BlueXP

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

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

Prerequisiti

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

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

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

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

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

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

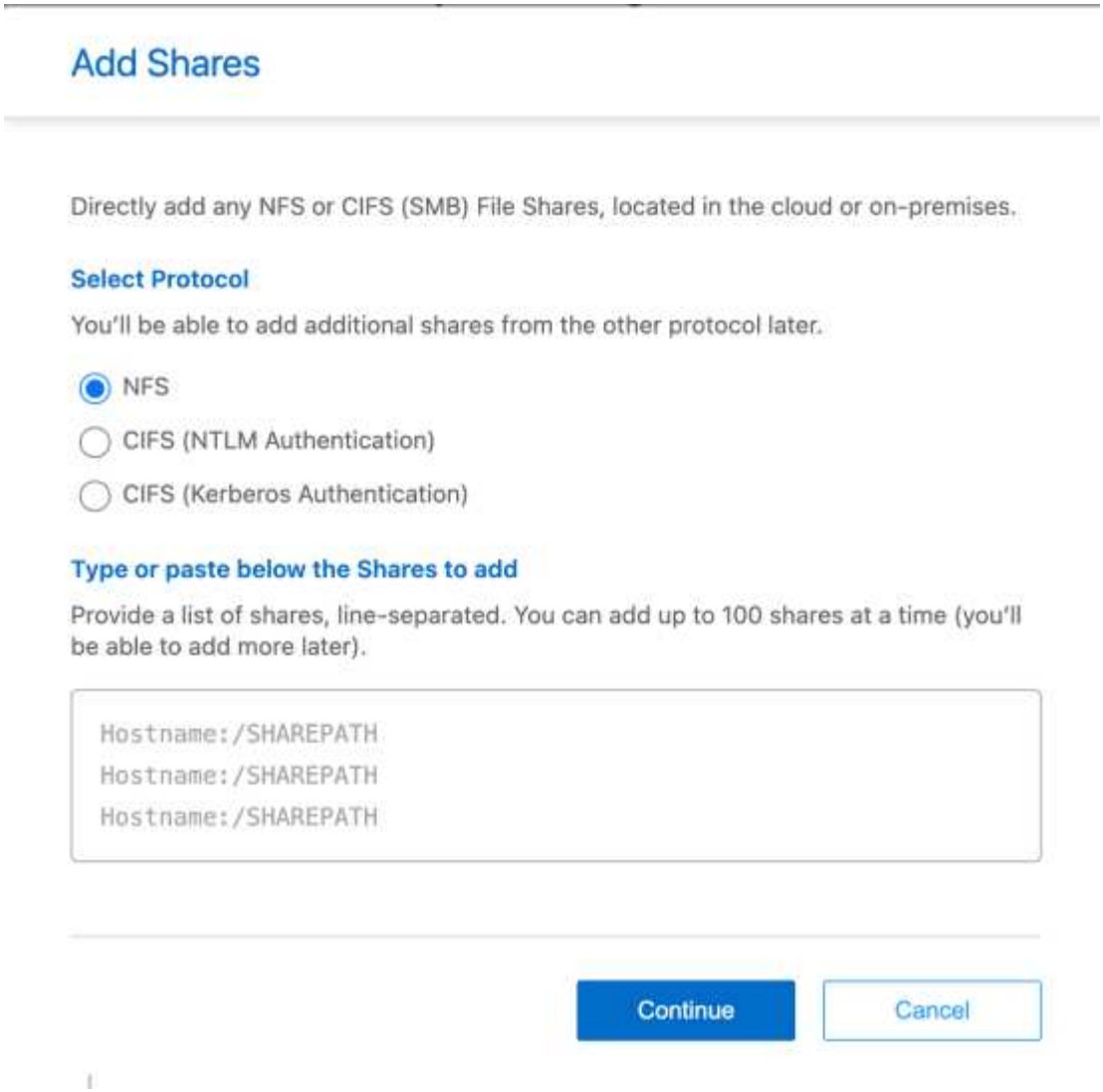
Crea un gruppo di condivisione file

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

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

Fasi

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



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

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

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

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

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

Risultato

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

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

Modifica un gruppo di condivisione file

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

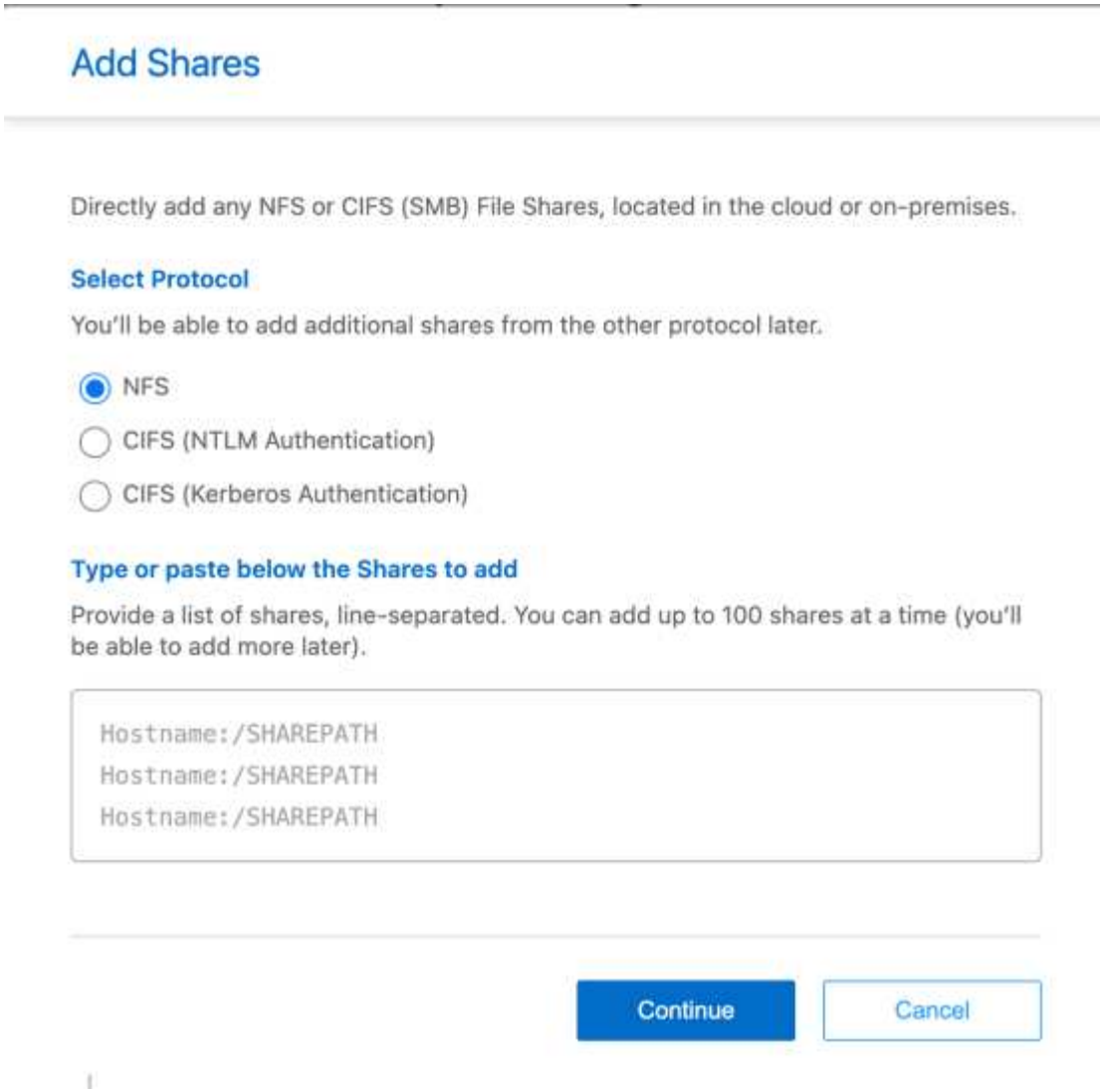
Modifica la configurazione del protocollo CIFS

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

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

Aggiungere condivisioni di file alle scansioni di conformità

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



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

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

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

Rimuovere una condivisione di file dalle scansioni di conformità

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

Tenere traccia dell'avanzamento della scansione

È possibile tenere traccia dell'avanzamento della scansione iniziale.

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

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

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

Eseguire la scansione dei dati StorageGRID con classificazione BlueXP

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

Consulta i requisiti delle StorageGRID

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

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

Distribuire l'istanza di classificazione BlueXP

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

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

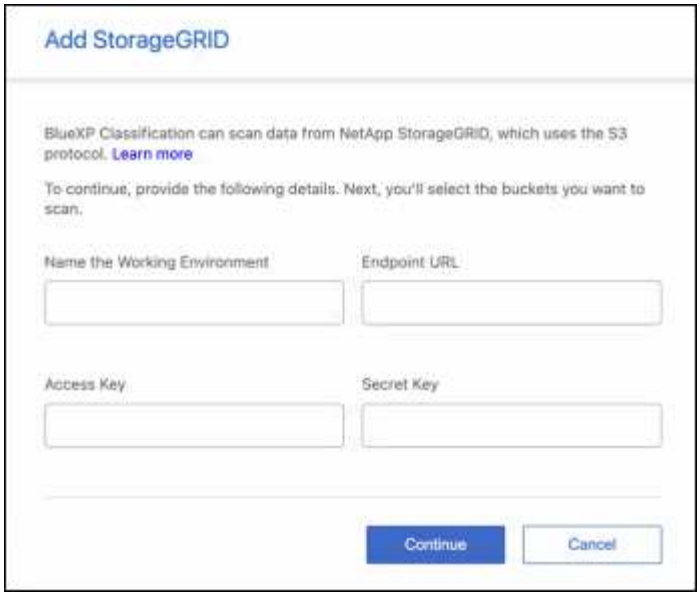
Se si esegue la scansione di dati da StorageGRID installati in un sito oscuro che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato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

Aggiungere il servizio StorageGRID alla classificazione BlueXP

Aggiungere il servizio StorageGRID.

Fasi

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



Risultato

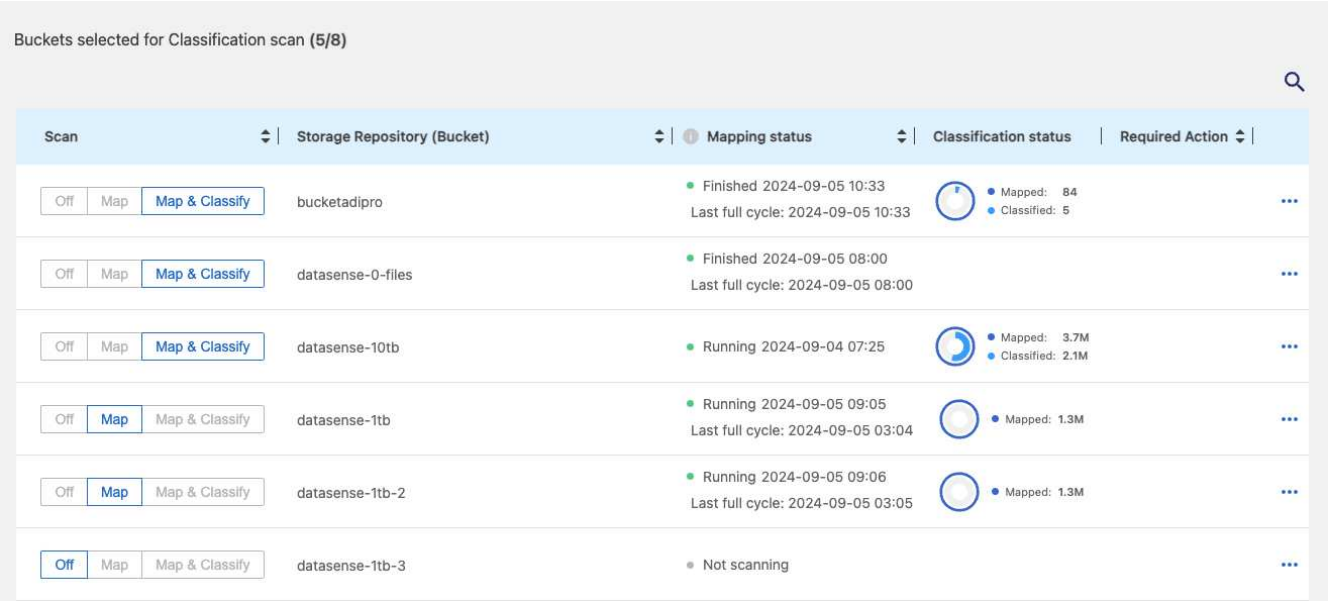
StorageGRID viene aggiunto all'elenco degli ambienti di lavoro.

Abilitare e disabilitare le scansioni di conformità sui bucket StorageGRID

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

Fasi

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



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

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

Risultato

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

Integra Active Directory con la classificazione BlueXP

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

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

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

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

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

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

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

Origini dati supportate

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

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

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

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

Connettersi al server Active Directory

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

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

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

Requisiti

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

    oppure

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

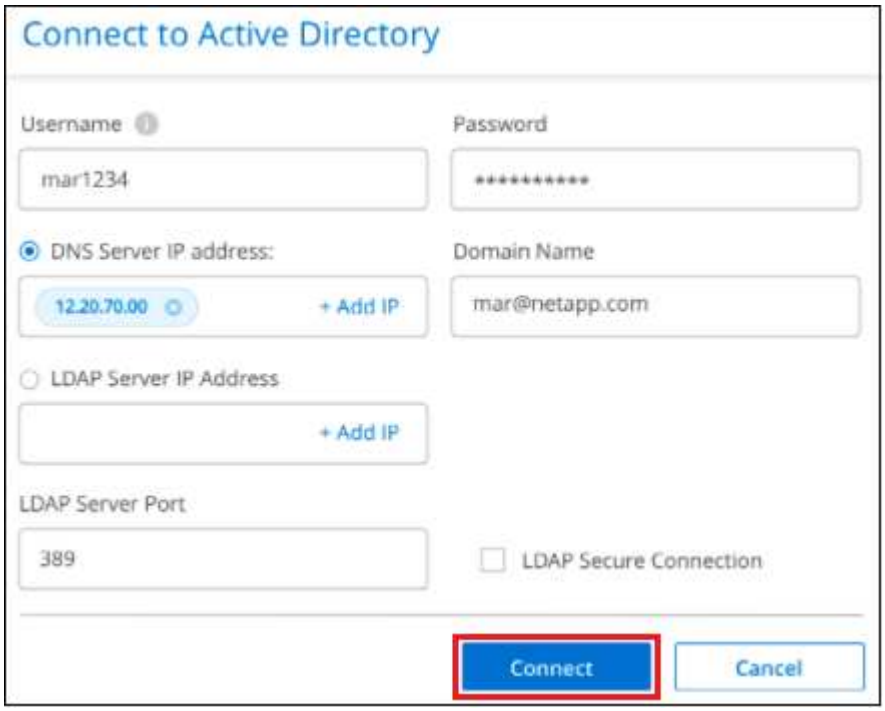
Protocollo	Porta	Destinazione	Scopo
TCP E UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP su SSL
TCP	3268	Active Directory	Catalogo globale
TCP	3269	Active Directory	Catalogo globale su SSL

Fasi

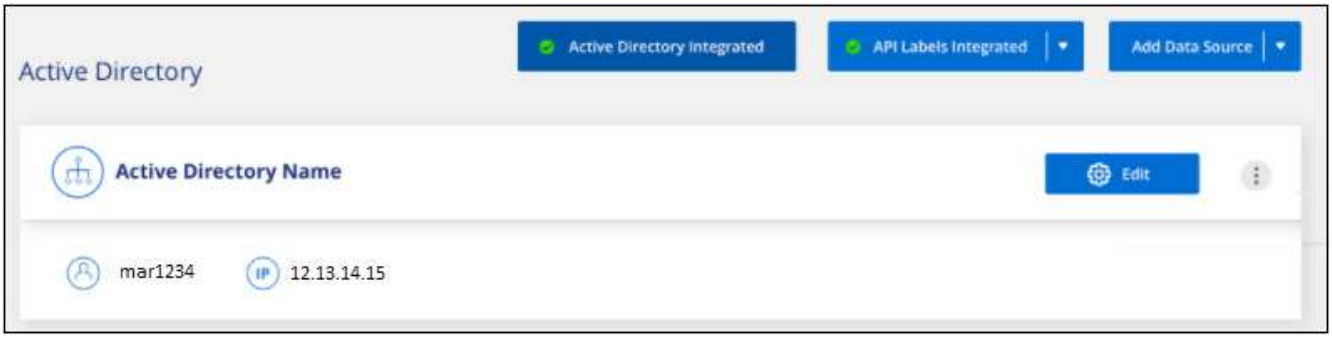
1. Dalla pagina di configurazione della classificazione BlueXP, fare clic su **Add Active Directory** (Aggiungi Active Directory).

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

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



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



Gestire l'integrazione di Active Directory

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

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

Utilizzare la classificazione BlueXP

Visualizza i dettagli di governance sui dati archiviati nell’organizzazione con la classificazione BlueXP

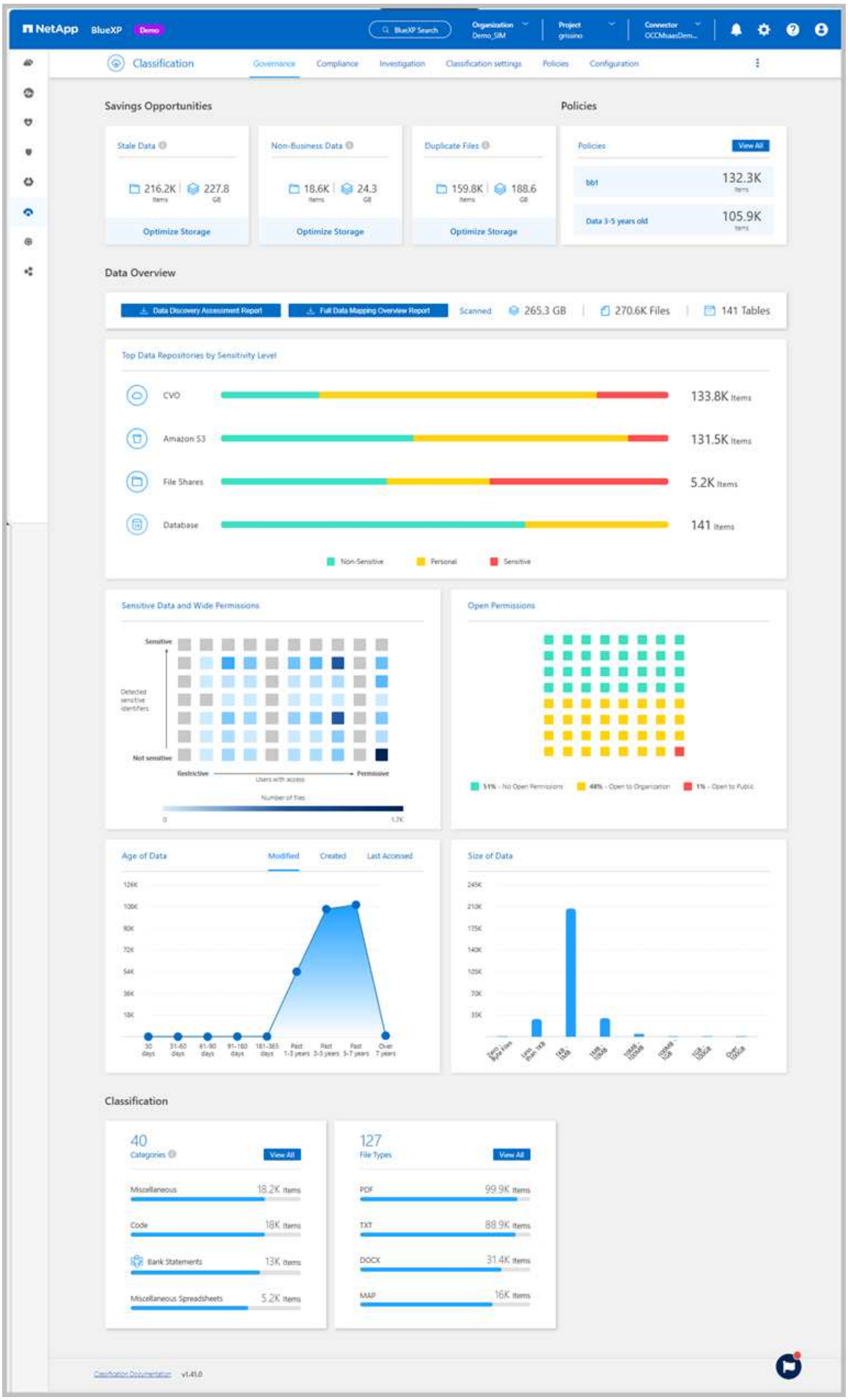
Ottieni il controllo dei costi relativi ai dati sulle risorse di storage della tua organizzazione. La classificazione BlueXP identifica la quantità di dati obsoleti, dati non aziendali, file duplicati e file molto grandi nei sistemi, in modo da poter decidere se rimuovere o tierare alcuni file in uno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

Questo è dove dovreste cominciare la vostra ricerca. Dal dashboard Governance, è possibile selezionare un’area per ulteriori indagini.

Inoltre, se hai in programma di migrare i dati da posizioni on-premise nel cloud, puoi vedere le dimensioni dei dati e se alcuni di essi contengono informazioni sensibili prima di spostarli.

Rivedere il dashboard 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.


NetApp
BlueXP
Demo
BlueXP Search
Organization
Demo_SIM
Project
grisino
Connector
Classification
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Policies
Stale Data
216.2K Items
227.8 GB
Optimize Storage
Non-Business Data
18.6K Items
24.3 GB
Optimize Storage
Duplicate Files
159.8K Items
188.6 GB
Optimize Storage
Policies
View All
bb1
132.3K Items
Data 3-5 years old
105.9K Items
Data Overview
Data Discovery Assessment Report
Full Data Mapping Overview Report
Scanned
265.3 GB
270.6K Files
141 Tables
Top Data Repositories by Sensitivity Level
CVO
133.8K Items
Amazon S3
131.5K Items
File Shares
5.2K Items
Database
141 Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detected sensitive identifiers
Not sensitive
Restrictive
Users with access
Permissive
Number of files
Open Permissions
51% - No Open Permissions
48% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
Size of Data
Classification
40
Categories
View All
Miscellaneous
18.2K Items
Code
18K Items
Bank Statements
13K Items
Miscellaneous Spreadsheets
5.2K Items
127
File Types
View All
PDF
99.9K Items
TXT
88.9K Items
DOCX
31.4K Items
MAP
16K Items
Classification Documentation
v1.41.0

Fasi

1. Dal menu BlueXP , selezionare **Governance > classificazione**.
2. Selezionare **Governance**.

   Viene visualizzato il dashboard Governance.

Rivedere le opportunità di risparmio

Il componente *Opportunità di risparmio* mostra i dati che è possibile eliminare o spostare in un archivio oggetti meno costoso. I dati in *Opportunità di risparmio* vengono aggiornati ogni 2 ore e possono essere aggiornati manualmente.

Fasi

1. Dal menu classificazione BlueXP , selezionare **Governance**.
2. All'interno di ogni riquadro opportunità di risparmio del dashboard Governance, selezionare **Ottimizza archiviazione** per visualizzare i risultati filtrati nella pagina di analisi. Per scoprire quali dati dovresti eliminare o spostare in un archivio meno costoso, esamina le *Opportunità di risparmio*.
   - **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".

> 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*.

Esaminare le ricerche salvate con il maggior numero di risultati

Nella scheda *ricerche salvate*, le ricerche con il maggior numero di risultati vengono visualizzate in cima all'elenco. Questi dati vengono aggiornati ogni due ore.

Per informazioni dettagliate sulle ricerche salvate, vedere "Creare ricerche salvate".

Fasi

1. Dal menu classificazione BlueXP , selezionare **Governance**.
2. Nella dashboard Governance, individua il riquadro Ricerche salvate. Selezionare il nome di una ricerca salvata per visualizzare i risultati nella pagina di analisi.
3. Selezionare **Visualizza tutto** per visualizzare l'elenco di tutte le ricerche salvate disponibili. Nell'area *ricerche salvate*, le ricerche con il maggior numero di risultati vengono visualizzate all'inizio dell'elenco.

Creare il report di valutazione per il rilevamento dei dati

Il report di valutazione del rilevamento dei dati fornisce un'analisi di alto livello dell'ambiente sottoposto a scansione per 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 i clienti su tre aspetti significativi del set di dati:

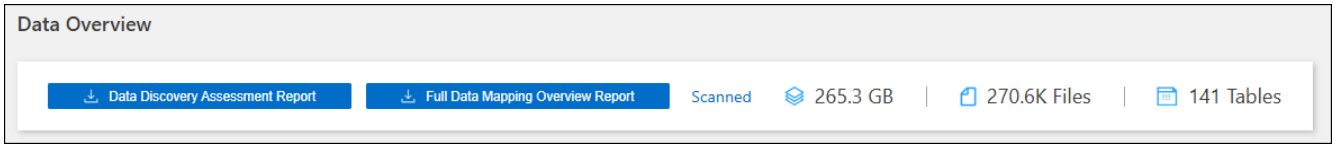
Funzione	Descrizione
Problemi di governance dei dati	Un'immagine dettagliata di tutti i dati in tuo possesso e delle aree in cui puoi ridurre la quantità di dati per risparmiare sui costi.
Esposizioni alla sicurezza dei dati	Aree in cui i dati sono accessibili ad attacchi interni o esterni a causa di 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).

Utilizzando questo rapporto, è possibile effettuare le seguenti operazioni:

- 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

Fasi

1. Dal menu BlueXP , selezionare **Governance > classificazione**.
2. Selezionare **Governance**.
3. Selezionare **Report valutazione rilevamento dati**.



Risultato

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

Creare il rapporto Panoramica mappatura dati

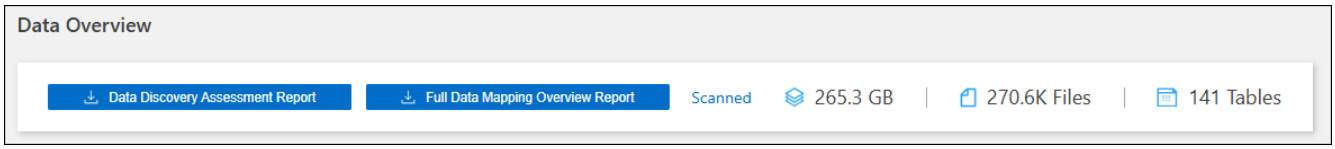
Il rapporto di panoramica sulla mappatura dei dati fornisce una panoramica dei dati archiviati nelle origini dati aziendali per assistere l'utente nelle decisioni relative ai processi di migrazione, backup, sicurezza e conformità. Il report riassume tutti gli ambienti di lavoro e le fonti di dati, fornendo anche un'analisi 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.

Fasi

1. Dal menu BlueXP , selezionare **Governance > classificazione**.
2. Selezionare **Governance**.
3. Selezionare **rapporto completo Panoramica mappatura dati**.



4. Per personalizzare il nome della società visualizzato nella prima pagina del report, in alto a destra della pagina classificazione BlueXP , selezionare ⋮. Quindi selezionare **Modifica nome società**. La volta successiva che si genera il rapporto, questo includerà il nuovo nome.

Risultato

La classificazione BlueXP genera un report in formato .pdf che puoi esaminare e inviare ad altri gruppi, se necessario.

Se il report è più grande di 1 MB, il file .pdf viene conservato nell'istanza di classificazione BlueXP e viene visualizzato un messaggio a comparsa sulla posizione esatta. Quando la classificazione BlueXP è installata su una macchina Linux locale o su una macchina Linux implementata nel cloud, puoi accedere direttamente al file .pdf. Quando la classificazione BlueXP viene distribuita nel cloud, sarà necessario connettersi tramite SSH all'istanza della classificazione BlueXP per scaricare il file .pdf.

Esaminare i principali repository di dati elencati in base alla sensibilità dei dati

L'area *Top Data Repository by Sensitivity Level* del rapporto Panoramica mappatura dati elenca i quattro principali 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

Questi dati vengono aggiornati ogni due ore e possono essere aggiornati manualmente.

Fasi

1. Per visualizzare il numero totale di elementi in ciascuna categoria, posizionare il cursore su ciascuna sezione della barra.
2. Per filtrare i risultati che appariranno nella pagina Indagine, seleziona ogni area nella barra e prosegui nella ricerca.

Esaminare i dati sensibili e le autorizzazioni estese

L'area *dati sensibili e autorizzazioni ampie* del report Panoramica mappatura dati mostra la percentuale di file che contengono dati riservati e hanno autorizzazioni ampie. Il grafico mostra i seguenti tipi di autorizzazioni:

- Dai permessi più restrittivi alle restrizioni più permissive sull'asse orizzontale.
- Dai dati meno sensibili a quelli più sensibili sull'asse verticale.

Fasi

1. Per visualizzare il numero totale di file in ciascuna categoria, posizionare il cursore su ciascuna casella.
2. Per filtrare i risultati che verranno visualizzati nella pagina di analisi, selezionare una casella e analizzare ulteriormente.

Esaminare i dati elencati in base ai tipi di autorizzazioni aperte

L'area *autorizzazioni aperte* del rapporto Panoramica mappatura dati mostra la percentuale per ciascun tipo di autorizzazioni 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

Fasi

1. Per visualizzare il numero totale di file in ciascuna categoria, posizionare il cursore su ciascuna casella.
2. Per filtrare i risultati che verranno visualizzati nella pagina di analisi, selezionare una casella e analizzare ulteriormente.

Controllare l'età e le dimensioni dei dati

È possibile esaminare gli elementi nei grafici *Age* e *Size* del rapporto Panoramica mappatura dati per verificare se vi sono dati da eliminare o da assegnare a livelli di archiviazione a oggetti meno costosi.

Fasi

1. Nel grafico Età dei dati, per visualizzare i dettagli relativi all'età dei dati, posizionare il cursore su un punto del grafico.
2. Per filtrare in base all'età o all'intervallo di dimensioni, selezionare l'età o la dimensione.
   - **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.

> Se un'origine dati implementa il tiering dei dati, è possibile identificare i dati vecchi che risiedono già nello storage a oggetti nel grafico *Age of Data*.

Esamina le classificazioni dei dati più identificate nei tuoi dati

L'area *Classification* del rapporto Panoramica mappatura dati fornisce un elenco dei dati più identificati "Categorie" e "Tipi di file"acquisiti.

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 esaminano i risultati, è possibile che i contratti dei dipendenti siano memorizzati in una posizione non sicura. A questo punto, è possibile correggere il problema.

Per ulteriori informazioni, vedere "Visualizzazione dei file in base alle categorie" .

Fasi

1. Dal menu BlueXP , selezionare **Governance > classificazione**.
2. Selezionare **Governance**, quindi il pulsante **Data Discovery Assessment Report**.

Risultato

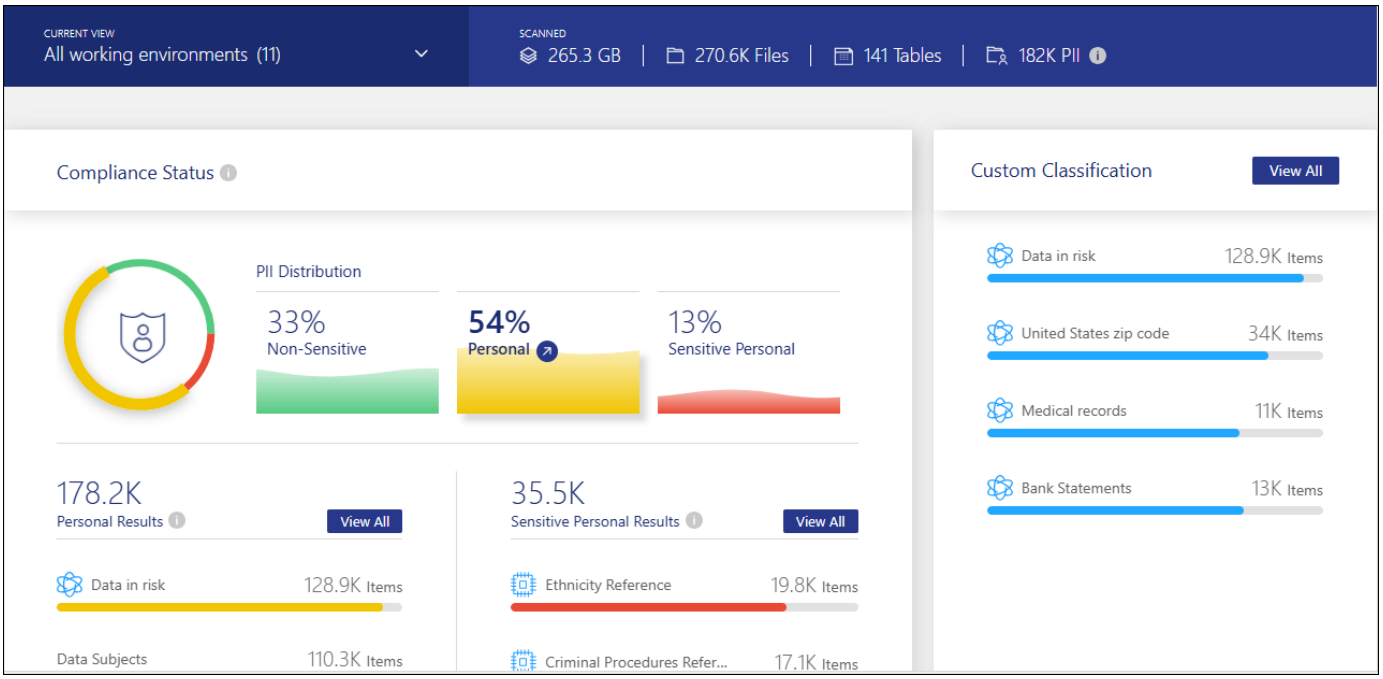
La classificazione BlueXP genera un report in formato .pdf che puoi esaminare e inviare ad altri gruppi, se necessario.

Visualizza i dettagli di conformità sui dati privati archiviati nell'organizzazione con la classificazione BlueXP

Ottenete il controllo dei vostri dati privati visualizzando i dettagli sui dati personali (PII) e sui dati personali sensibili (SPII) della vostra 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. Per visualizzare i dati relativi solo ad alcuni ambienti di lavoro, selezionarli.



Filtrare i risultati dalla pagina analisi dati e scaricare un rapporto dei risultati come file CSV. Per ulteriori informazioni, vedere "Filtraggio dei dati nella pagina Data Investigation" .

Consente di visualizzare i file che contengono dati personali

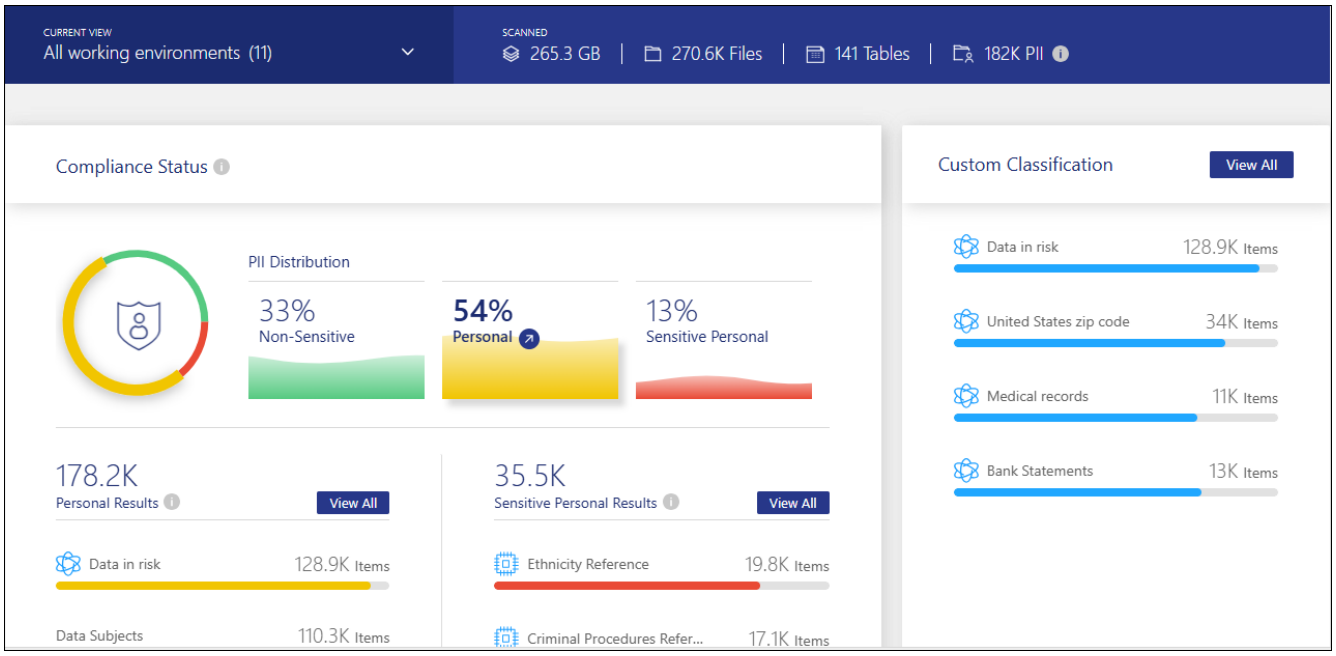
La classificazione BlueXP identifica automaticamente parole, stringhe e modelli specifici (Regex) all'interno dei dati. Ad esempio, informazioni di identificazione personale (PII), numeri di carta di credito, numeri di previdenza sociale, numeri di conto bancario, password, e molto altro ancora. "Consulta 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.

È inoltre possibile creare termini di ricerca personalizzati per identificare i dati personali specifici dell'organizzazione. Per ulteriori informazioni, vedere "Creare una classificazione personalizzata".

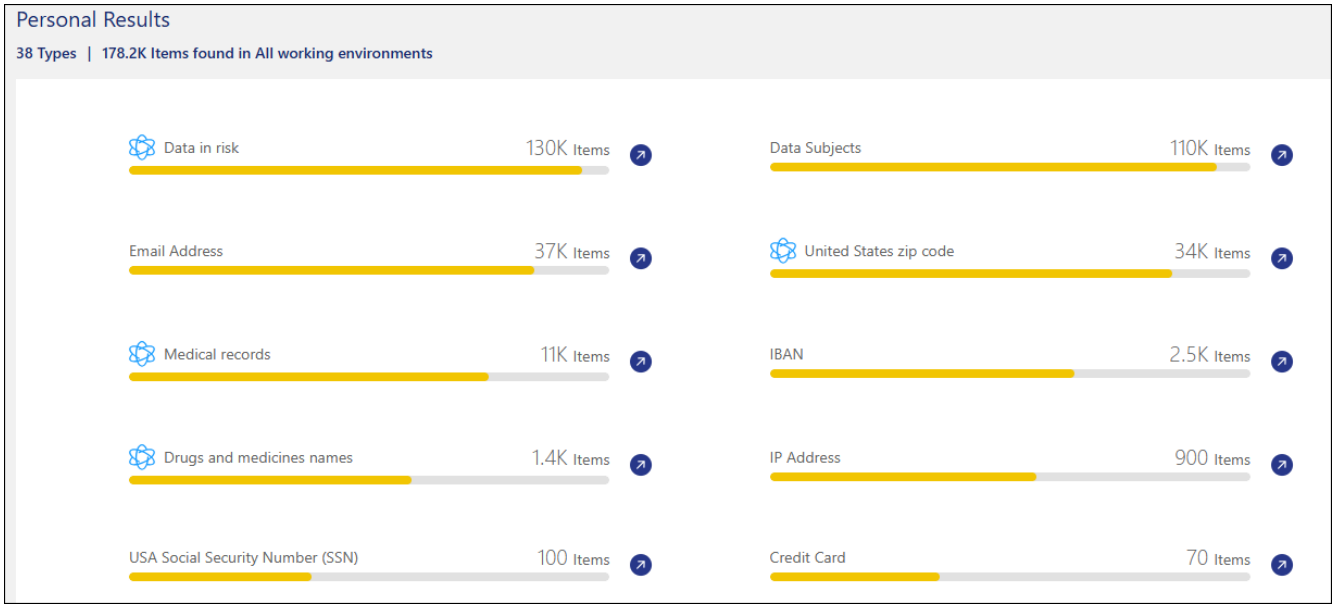
Per alcuni tipi di dati personali, la classificazione BlueXP utilizza *Proximity Validation* per validarne i risultati. La convalida avviene cercando una o più parole chiave predefinite in prossimità dei dati personali trovati. Ad esempio, la classificazione BlueXP identifica un numero SSN (Social Security Number) statunitense come un SSN se vede accanto una parola 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 classificazione BlueXP , selezionare la scheda **conformità**.
2. Per esaminare i dettagli di tutti i dati personali, selezionare l'icona accanto alla percentuale dei dati personali.

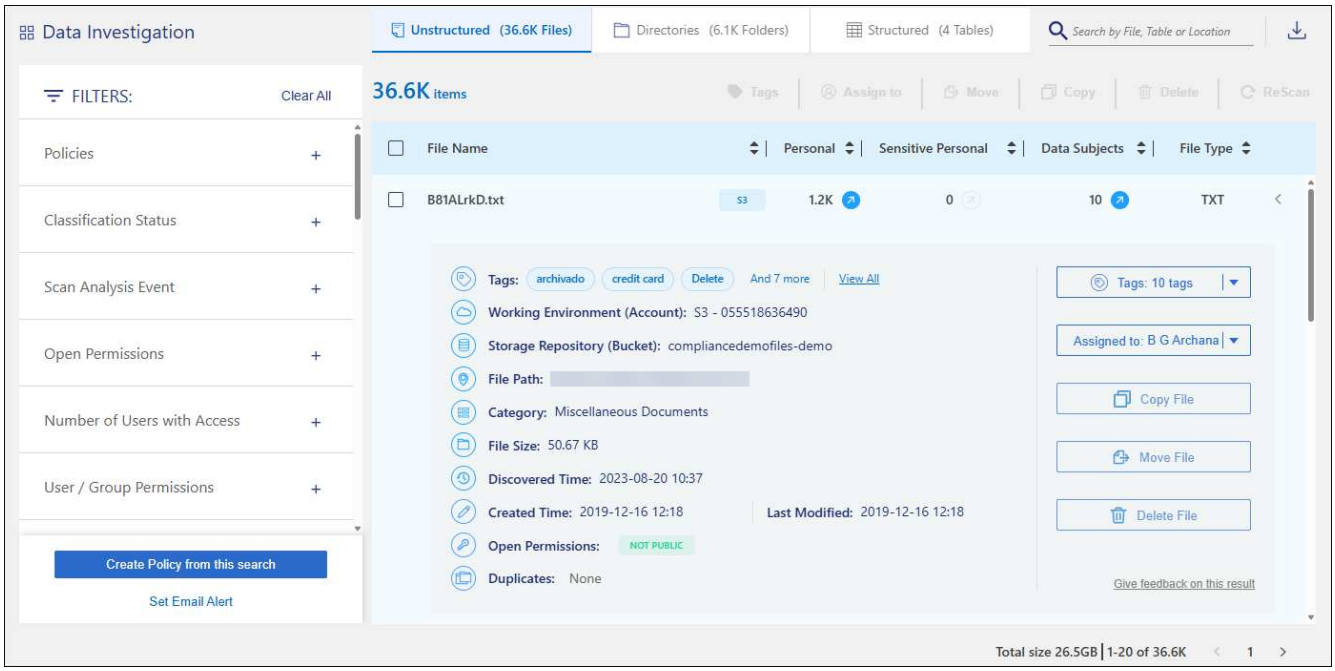


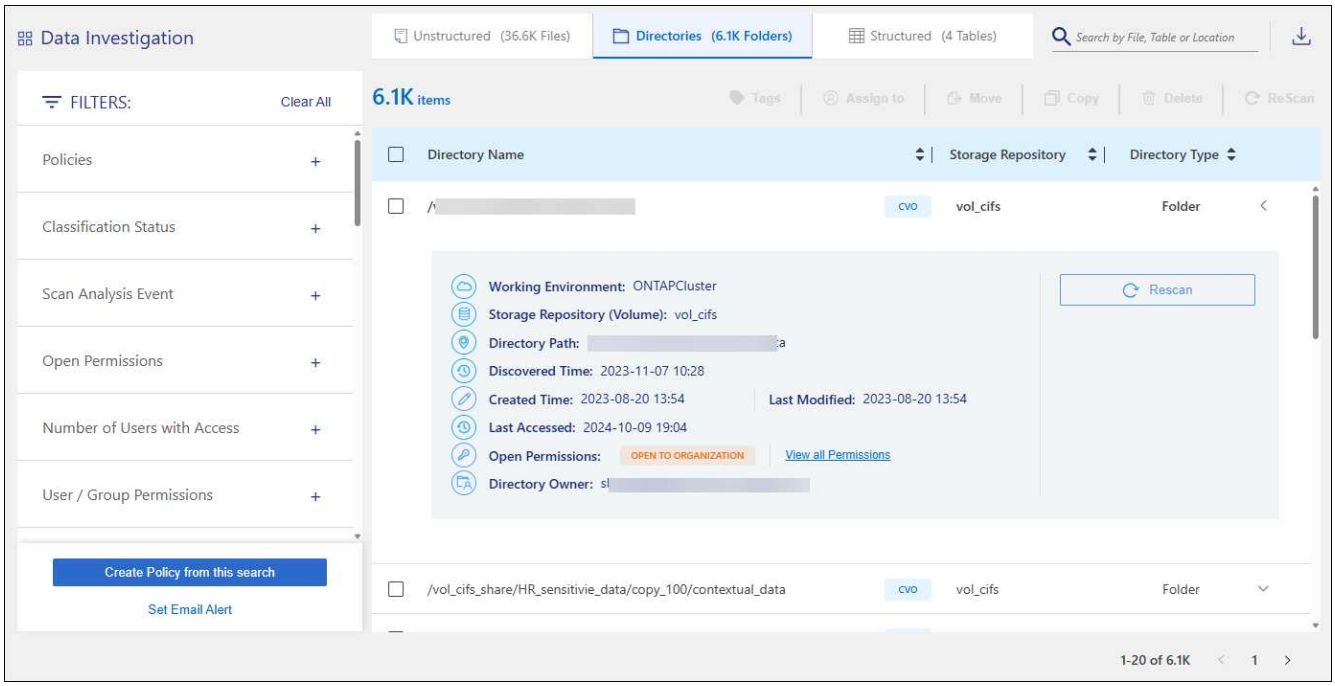
3. Per esaminare i dettagli di un tipo specifico di dati personali, selezionare **Visualizza tutto**, quindi selezionare l'icona a freccia **esamina risultati** per un tipo specifico di dati personali, ad esempio gli indirizzi e-mail.



4. Analizzare i dati cercando, ordinando, espandendo i dettagli di un file specifico, selezionando la freccia **indaga risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

   Le due schermate seguenti mostrano i dati personali trovati nei singoli file e trovati 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 i tipi speciali di informazioni personali sensibili, come definito dalle normative sulla privacy come "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.

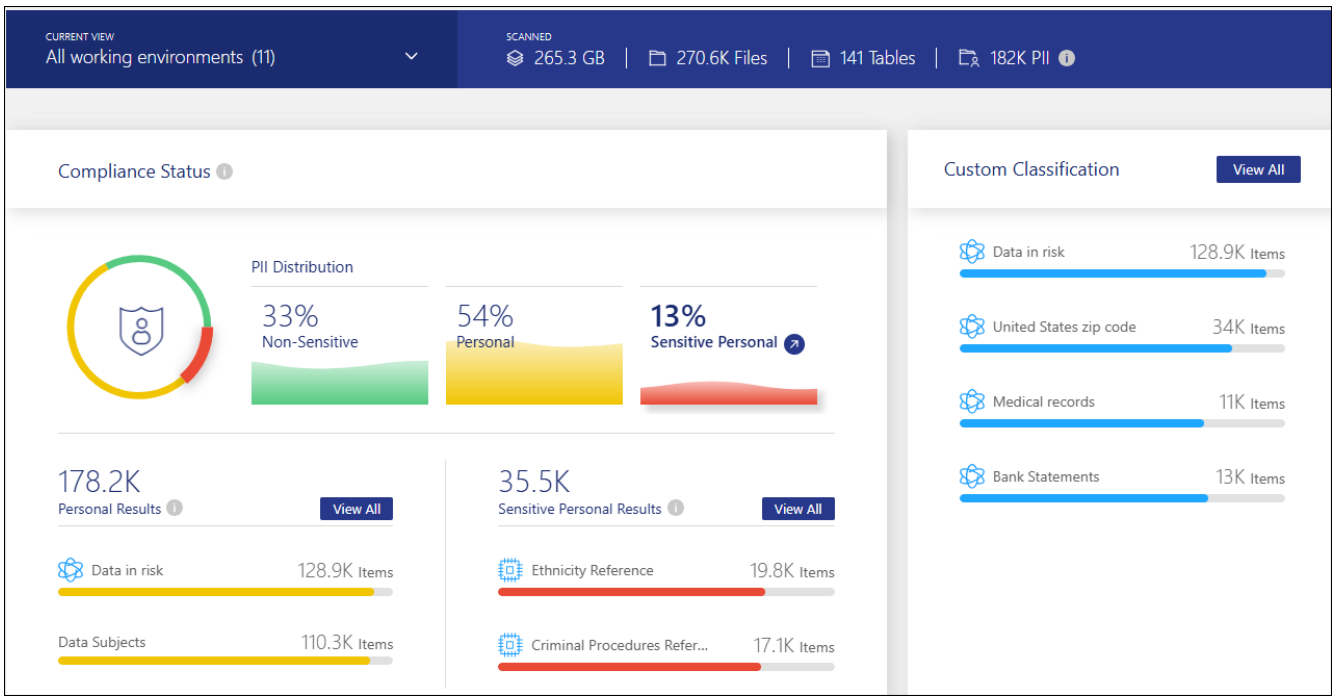
Ad esempio, una categoria di dati GDPR sensibili è l'origine etnica. Grazie alle sue capacità NLP, la

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).

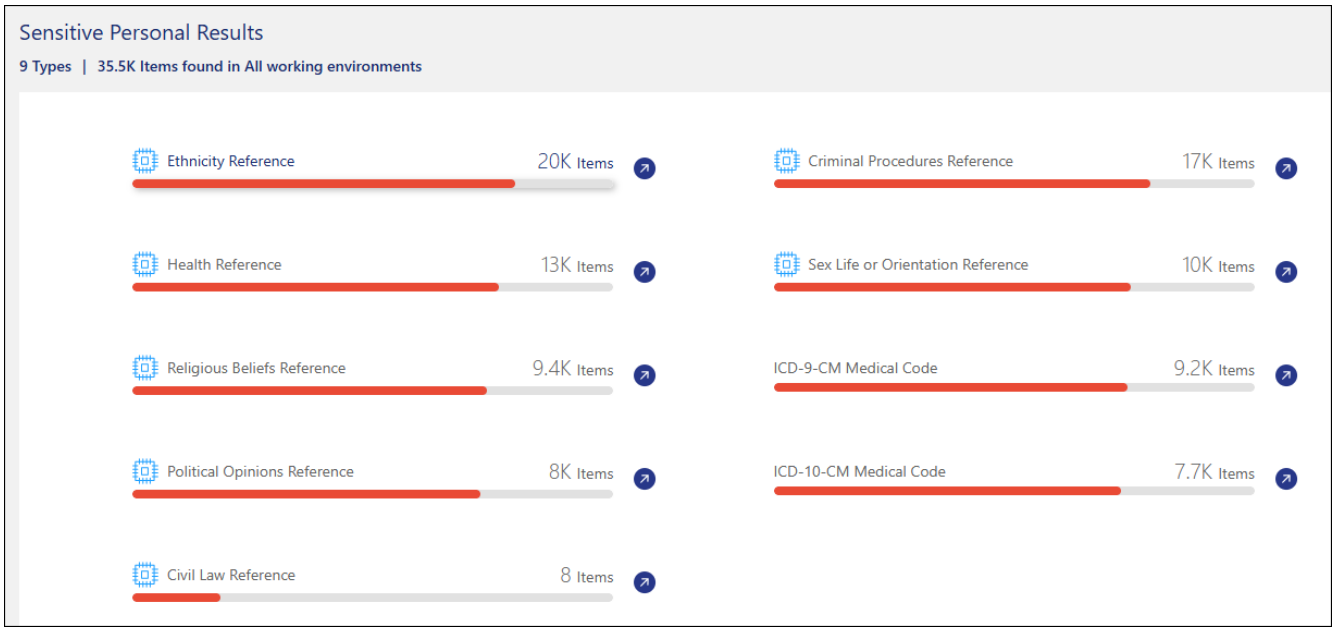
> Quando si esegue la scansione di dati personali sensibili, è supportata solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Fasi

1. Dal menu classificazione BlueXP , selezionare **conformità**.
2. Per esaminare i dettagli di tutti i dati personali sensibili, selezionare l'icona accanto alla percentuale di dati personali sensibili.



3. Per esaminare i dettagli relativi a un tipo specifico di dati personali sensibili, selezionare **Visualizza tutto**, quindi selezionare l'icona con la freccia **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

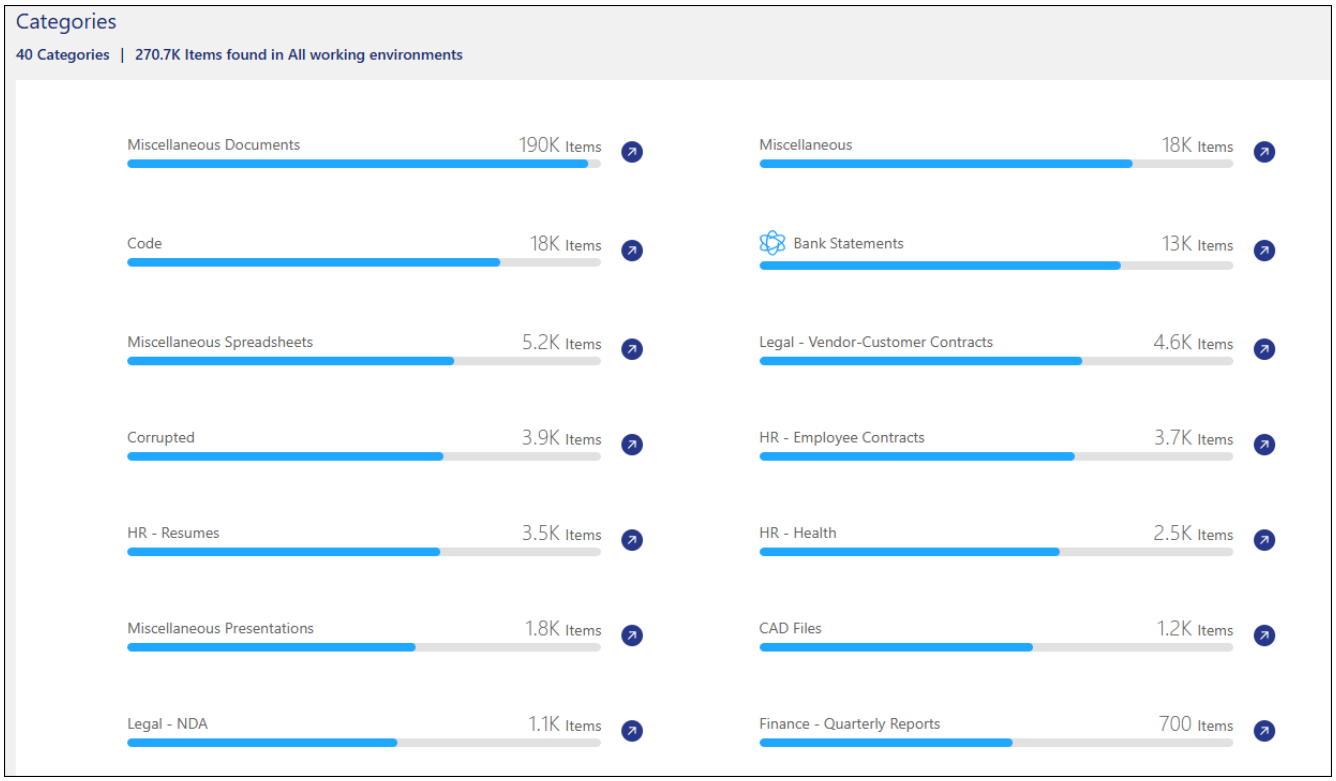
La classificazione BlueXP prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. "Vedere l'elenco delle categorie".

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 esaminano 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 classificazione BlueXP , selezionare la scheda **conformità**.
2. Selezionare l'icona con la freccia **risultati analisi** per una delle 4 categorie principali direttamente dalla schermata principale oppure selezionare **Visualizza tutto**, quindi selezionare l'icona per una delle categorie.



3. Analizzare i dati cercando, ordinando, espandendo i dettagli di un file specifico, selezionando la freccia **indaga risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

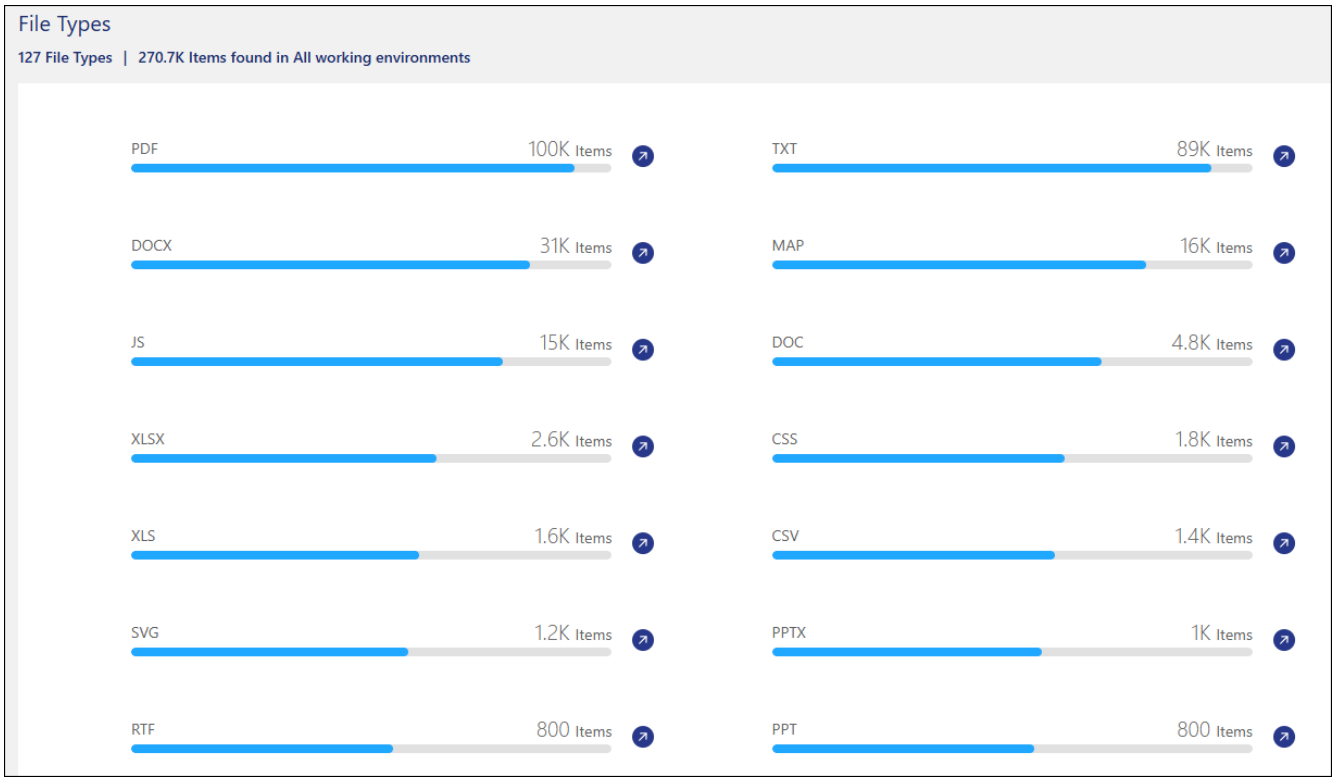
Visualizzare i file in base ai tipi di file

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. Dalla memo di classificazione BlueXP , selezionare la scheda **conformità**.
2. Selezionare l'icona con la freccia **esamina risultati** per uno dei 4 tipi di file principali direttamente dalla schermata principale, oppure selezionare **Visualizza tutto**, quindi selezionare l'icona per qualsiasi tipo di file.



3. Analizzare i dati cercando, ordinando, espandendo i dettagli di un file specifico, selezionando la freccia **indaga risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

Categorie di dati privati nella classificazione BlueXP

Esistono molti tipi di dati privati che la classificazione BlueXP può identificare nei volumi e nei database.

La classificazione BlueXP identifica due tipi di dati personali:

- **Informazioni di identificazione personale (PII)**
- **Dati personali sensibili (SPII)**

> Se è necessaria la classificazione BlueXP per identificare altri tipi di dati privati, ad esempio numeri ID nazionali aggiuntivi o identificativi sanitari, contattare il proprio account manager.

Tipi di dati personali

I dati personali, o *informazioni di identificazione personale* (PII), contenuti nei file possono essere dati personali generici o identificatori nazionali. La terza colonna della tabella riportata di seguito 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.

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese
Generale	Numero della carta di credito	Sì	✓	✓	✓		✓
	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

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese
	ID maltese	Sì	✓	✓	✓		
	Numero NHS (National Health Service)	Sì	✓	✓	✓		
	Conto bancario della Nuova Zelanda	Sì	✓	✓	✓		
	Patente di guida della Nuova Zelanda	Sì	✓	✓	✓		
	Numero IRD Nuova Zelanda (ID fiscale)	Sì	✓	✓	✓		
	New Zealand NHI (National Health Index)	Sì	✓	✓	✓		
	Numero di passaporto per la Nuova Zelanda	Sì	✓	✓	✓		
	ID polacco (PESEL)	Sì	✓	✓	✓		
	Portoghese Tax Identification Number (NIF)	Sì	✓	✓	✓		
	ID rumeno (CNP)	Sì	✓	✓	✓		
	Singapore National Registration Identity Card (NRIC)	Sì	✓	✓	✓		
	ID sloveno (EMSO)	Sì	✓	✓	✓		
	ID sudafricano	Sì	✓	✓	✓		
	Codice fiscale spagnolo	Sì	✓	✓	✓		
	ID svedese	Sì	✓	✓	✓		
	ID REGNO UNITO (NINO)	Sì	✓	✓	✓		
	USA California driver’s License	Sì	✓	✓	✓		
	USA, Indiana driver’s License	Sì	✓	✓	✓		
	USA New York driver’s License	Sì	✓	✓	✓		
	Patente di guida USA Texas	Sì	✓	✓	✓		
	Numero di previdenza sociale (SSN) USA	Sì	✓	✓	✓		

Tipi di dati personali sensibili

La classificazione BlueXP può trovare nei file le seguenti informazioni personali sensibili (SPII).

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

- **Procedura penale riferimento**: Dati relativi alle condanne penali e ai reati di una persona fisica.
- **Riferimento etnico**: Dati relativi all’origine razziale o etnica di una persona fisica.
- **Health Reference**: Dati relativi alla salute di una persona fisica.
- **ICD-9-CM codici medici**: Codici utilizzati nell’industria medica e sanitaria.
- **ICD-10-CM codici medici**: Codici utilizzati nell’industria medica e sanitaria.
- **Principi filosofici riferimento**: Dati riguardanti le credenze filosofiche di una persona fisica.
- **Pareri politici riferimento**: Dati relativi alle opinioni politiche di una persona fisica.
- **Religious credences Reference**: Dati relativi alle credenze religiose di una persona fisica.

- **Sex Life o Orientation Reference**: 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	✓	✓	✓

Anche i seguenti metadati sono categorizzati e identificati nelle stesse lingue supportate:

- Dati dell'applicazione
- Archiviare i file
- Audio
- Breadcrumb dalla classificazione BlueXP
  Dati delle applicazioni di business

- File CAD
- Codice
- Corrotto
- Database e file di indice
- 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. Quando la classificazione BlueXP rileva informazioni personali identificabili (PII) o quando esegue una ricerca DSAR, sono supportati solo i seguenti formati di file:

```
.CSV, .DCM, .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%

Creare una classificazione personalizzata nella classificazione BlueXP

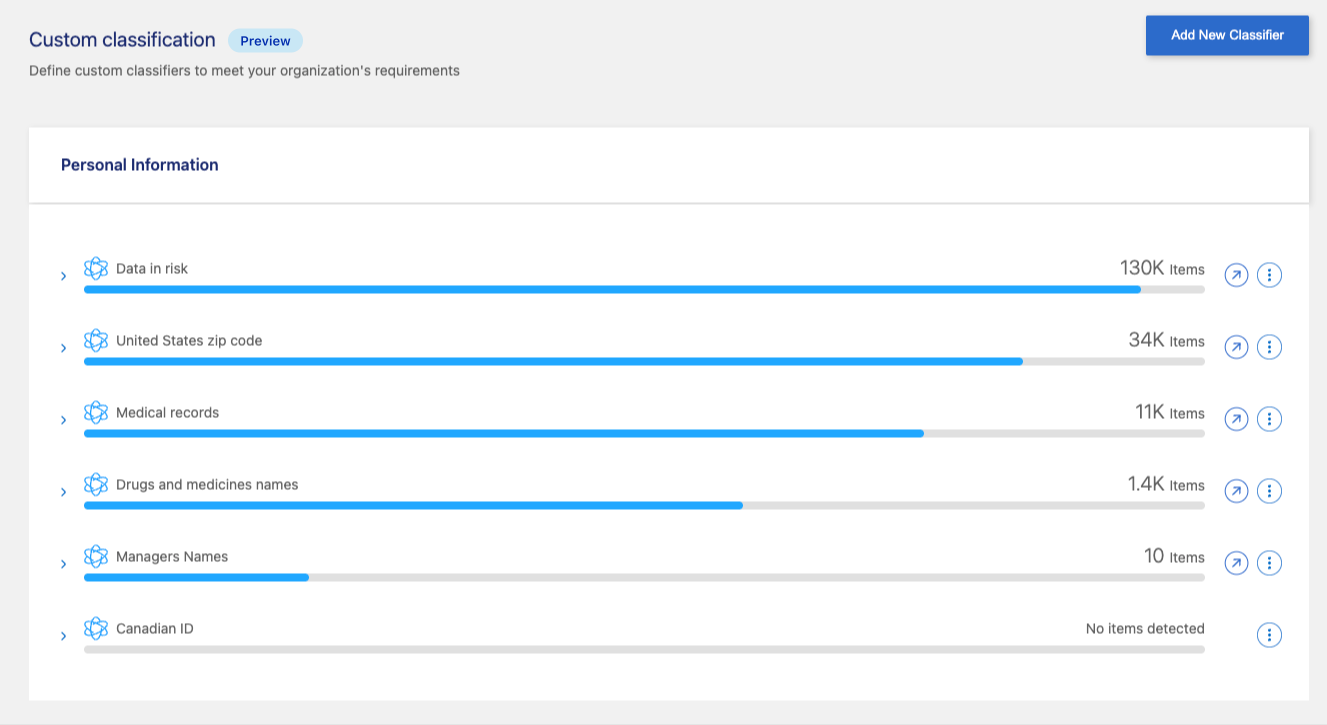
Con la classificazione BlueXP , è possibile creare una ricerca personalizzata per le informazioni riservate. La ricerca può essere definita come espressione regolare (regex).

Creare una classificazione personalizzata

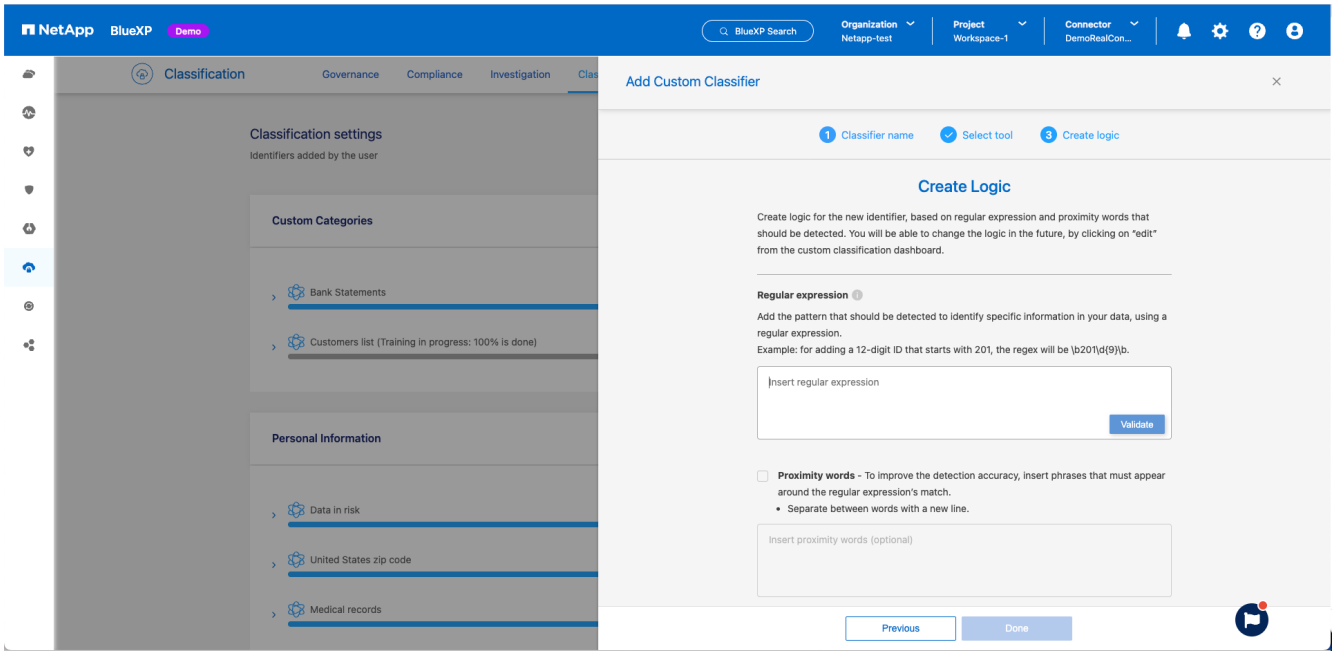
La classificazione personalizzata è disponibile solo per le scansioni Map & Classify, non solo per le scansioni mapping. Questa funzione è attualmente in anteprima.

Fasi

1. Selezionare la scheda **classificazione personalizzata**.



2. Selezionare il pulsante **Aggiungi nuovo classificatore**.
3. Aggiungere un Nome e una Descrizione per il nuovo classificatore.
4. Per aggiungere la personalizzazione come espressione regolare, selezionare **espressione regolare personalizzata** quindi **Avanti**.
5. Aggiungere un modello per rilevare le informazioni specifiche dei dati. Selezionare **convalida** per confermare la sintassi della voce.



6. Selezionare **fatto** per creare la classificazione personalizzata.

La nuova personalizzazione viene acquisita nella successiva scansione pianificata. Per visualizzare i risultati, vedere Generare report sulla conformità.

Esaminare i dati memorizzati nella propria organizzazione con la classificazione BlueXP

Esamina i dati della tua organizzazione visualizzandone i dettagli nella pagina Indagine sui dati. Qui è possibile continuare la ricerca dopo aver esaminato il dashboard Governance. Nella pagina di analisi, è possibile filtrare i dati utilizzando uno dei numerosi filtri per visualizzare solo i risultati desiderati. Puoi anche vedere i metadati dei file, le autorizzazioni per file e directory e controllare i file duplicati nei tuoi sistemi storage.

È possibile accedere a questa pagina da molte aree dell'interfaccia utente di classificazione BlueXP , tra cui i dashboard Governance e Compliance con i filtri già selezionati in quelle pagine. È possibile esportare i dati in un file CSV o JSON per ulteriori analisi o per condividerli con altri utenti.

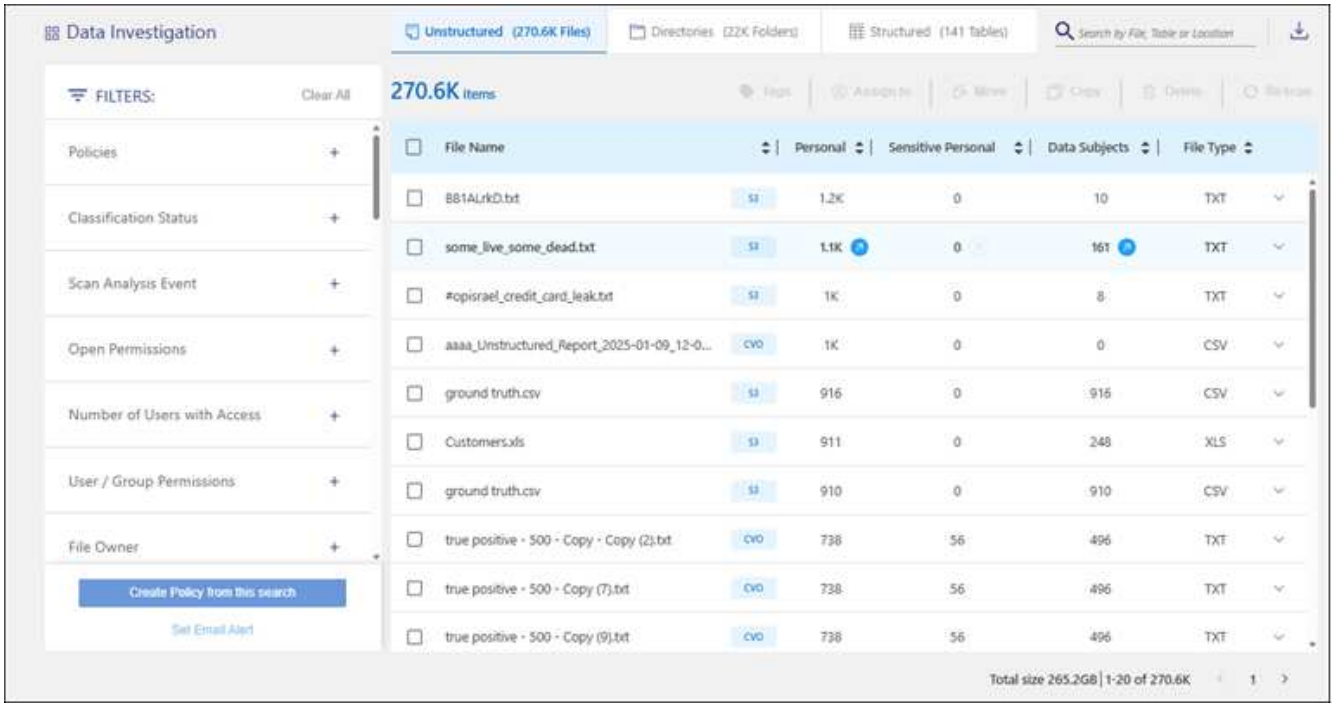
> Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.

Filtrare i dati nella pagina analisi dati

È possibile filtrare il contenuto della pagina di analisi per visualizzare solo i risultati desiderati.

Fasi

1. Dal menu classificazione BlueXP , selezionare **analisi**.
2. Nella pagina analisi dati, effettuare una delle seguenti operazioni:
3. Per scaricare il contenuto della pagina come report dopo averlo rifinito, selezionare il pulsante.



4. Per visualizzare i dati provenienti da file (dati non strutturati), directory (cartelle e condivisioni di file) o da database (dati strutturati), selezionare una delle schede in alto.
5. Per ordinare i risultati in ordine numerico o alfabetico, selezionare il controllo nella parte superiore di ciascuna colonna.
6. Per restringere ulteriormente i risultati, seleziona uno dei filtri nel riquadro Filtro.

> È possibile visualizzare solo i primi 10.000 risultati, o 500 pagine, per una scansione nella pagina analisi dati.

Filtrare 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).

Filtro	Dettagli
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 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 e alle autorizzazioni 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.

Filtra dati per 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.
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.

Filtro	Dettagli
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. 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 dati per 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.

Filtra dati per tipo di archiviazione

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

Filtrare i dati in base alle ricerche salvate

Utilizzare il seguente filtro per visualizzare i dati in base alle ricerche salvate.

Filtro	Dettagli
Ricerca salvata	Selezionare una o più ricerche salvate. Accedere a "scheda ricerche salvate"per visualizzare l'elenco delle ricerche salvate esistenti e crearne di nuove.

Filtra dati per stato 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 mediante l'evento di analisi scansione.

Filtra dati per duplicati

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

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

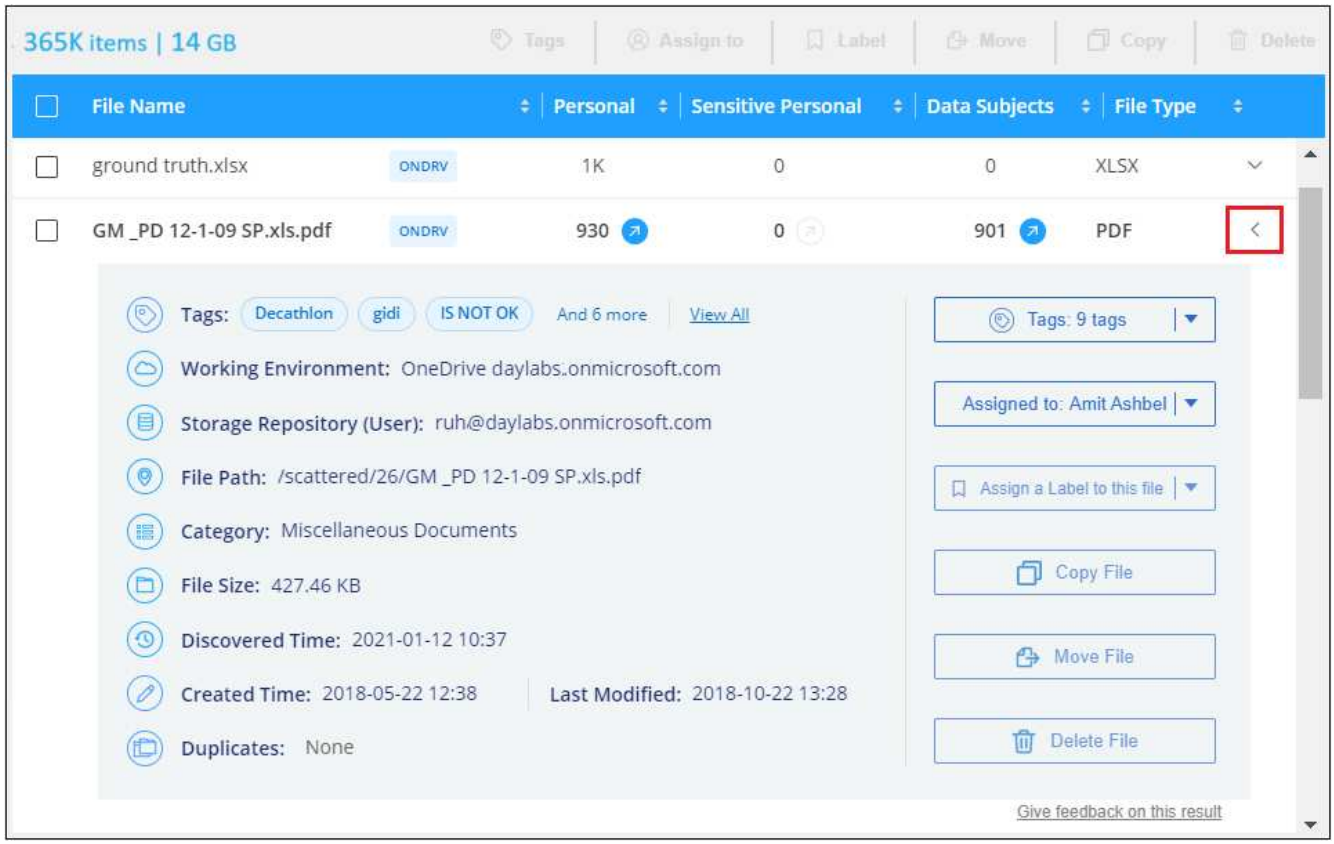
Visualizzare i metadati dei file

Oltre a mostrare l'ambiente di lavoro e il volume in cui si trova il file, i metadati mostrano molte più informazioni, incluse le autorizzazioni per i file, il proprietario del file e l'eventuale presenza di duplicati di questo file. Queste informazioni sono utili se si prevede di "creare ricerche salvate"visualizzare tutte le informazioni che è possibile utilizzare per filtrare i dati.

La disponibilità delle informazioni dipende dall'origine dati. Ad esempio, il nome del volume e le autorizzazioni non sono condivisi per i file di database.

Fasi

1. Dal menu classificazione BlueXP , selezionare **analisi**.
2. Nell'elenco Data Investigation (analisi dati) a destra, selezionare il pulsante freccia giù ⌄ a destra per ogni singolo file per visualizzare i metadati del file.



Visualizzare le autorizzazioni degli utenti per file e directory

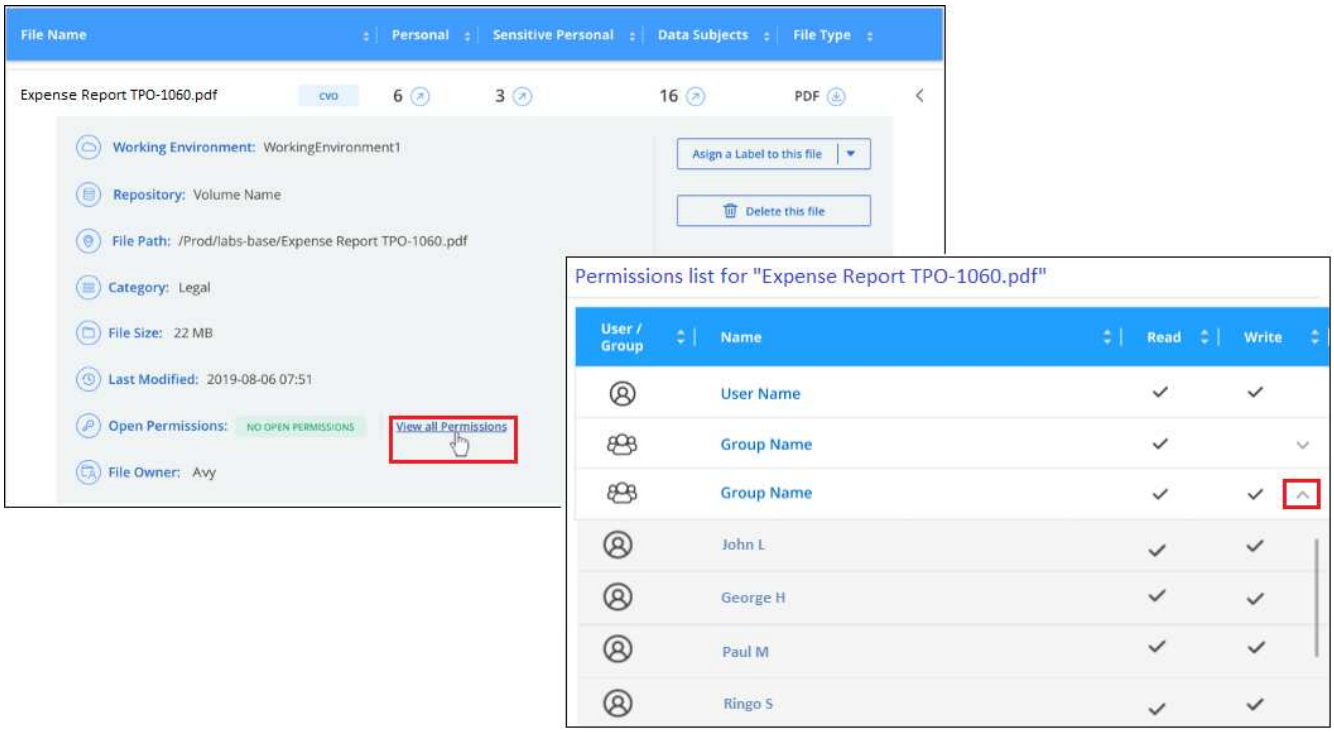
Per visualizzare un elenco di tutti gli utenti o gruppi che hanno accesso a un file o a una directory e i tipi di autorizzazioni di cui dispongono, selezionare **Visualizza tutte le autorizzazioni**. Questo pulsante è disponibile solo per i dati nelle condivisioni CIFS.

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".

Fasi

1. Dal menu classificazione BlueXP , selezionare **analisi**.
2. Nell'elenco Data Investigation (analisi dati) a destra, selezionare il pulsante freccia giù ⌄ a destra per ogni singolo file per visualizzare i metadati del file.
3. Per visualizzare un elenco di tutti gli utenti o gruppi che hanno accesso a un file o a una directory e ai tipi di autorizzazioni di cui dispongono, nel campo autorizzazioni aperte, selezionare **Visualizza tutte le autorizzazioni**.

> ⓘ La classificazione BlueXP mostra fino a 100 utenti nell'elenco.



4. Selezionare il pulsante freccia giù ⌄ per qualsiasi gruppo per visualizzare l'elenco degli utenti che fanno parte del gruppo.

> È possibile espandere un livello del gruppo per visualizzare gli utenti che fanno parte del gruppo.

5. Selezionare il nome di un utente o di un gruppo per aggiornare la pagina di analisi 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

Puoi verificare se nei tuoi sistemi di archiviazione sono presenti file duplicati. Ciò è utile se si desidera identificare le aree in cui è possibile risparmiare spazio di storage. È inoltre opportuno assicurarsi che determinati file con autorizzazioni specifiche o informazioni sensibili non vengano duplicati inutilmente nei tuoi sistemi di archiviazione.

Tutti i file (esclusi i database) di dimensioni pari o superiori a 1 MB o contenenti informazioni personali o riservate vengono confrontati per verificare se sono presenti duplicati.

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, puoi essere sicuro al 100% che i file sono duplicati esatti, anche se i nomi dei file sono diversi.

Fasi

1. Dal menu classificazione BlueXP , selezionare **analisi**.
2. Nel pannello filtri della pagina di analisi a sinistra, selezionare "dimensione file" insieme a "duplicati" ("ha duplicati") per vedere quali file di un determinato intervallo di dimensioni sono duplicati nell'ambiente.
3. Facoltativamente, scaricare l'elenco di file duplicati e inviarlo all'amministratore dello storage in modo da poter decidere quali file, se presenti, possono essere eliminati.
4. Facoltativamente, "eliminare il file"se si è certi che non è necessaria una versione specifica del file.

Visualizza se un file specifico è duplicato

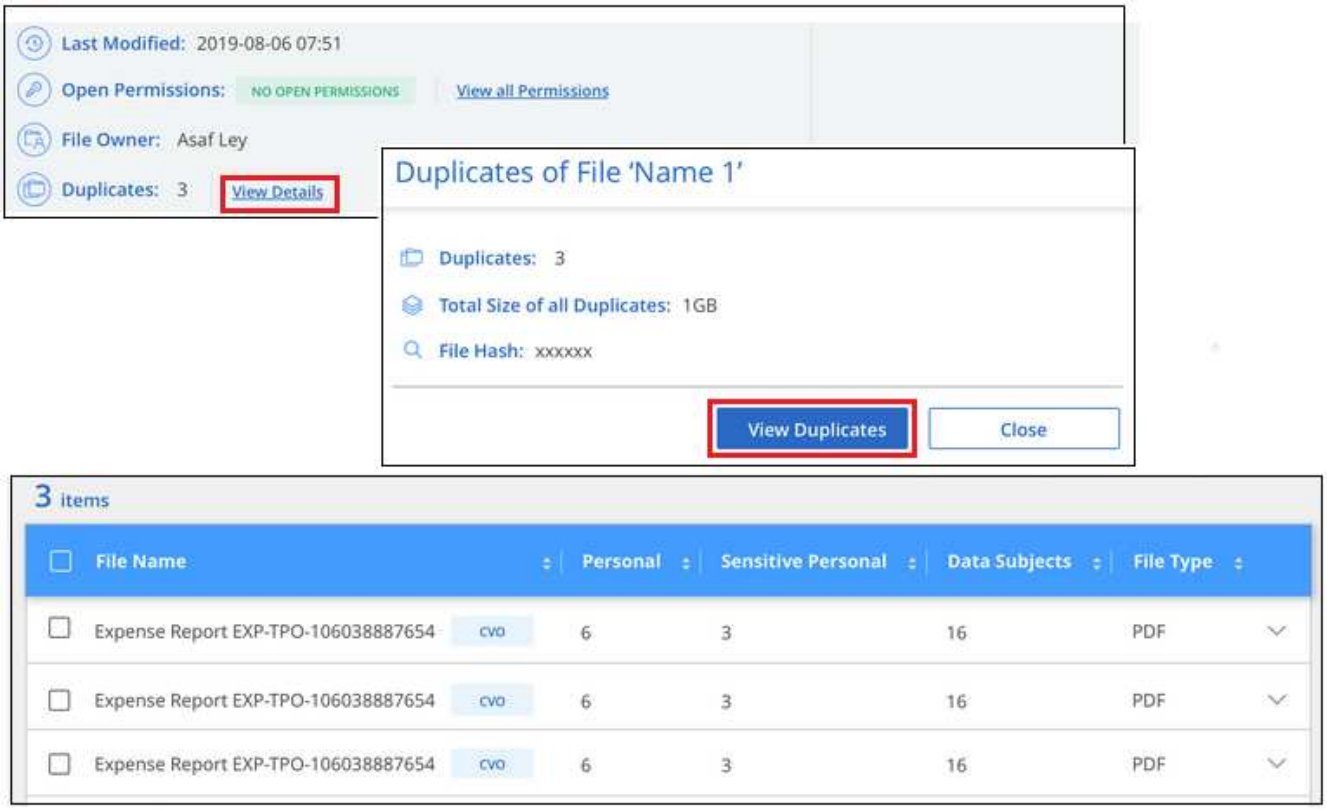
È possibile verificare se un singolo file contiene duplicati.

Fasi

1. Dal menu classificazione BlueXP , selezionare **analisi**.
2. Nell'elenco analisi dati, selezionare ⌄ a destra un singolo file per visualizzare i metadati del file.

   Se esistono duplicati per un file, queste informazioni vengono visualizzate accanto al campo *duplicati*.

3. Per visualizzare l'elenco dei file duplicati e la loro posizione, selezionare **Visualizza dettagli**.
4. Nella pagina successiva selezionare **Visualizza duplicati** per visualizzare i file nella pagina di analisi.



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

Creare il rapporto analisi dati

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

Il report è disponibile come file CSV o JSON e puoi salvarlo sul tuo computer locale.

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.

I file sono suddivisi in file con un numero fisso di righe o record:

- JSON - 100.000 record per report, la cui generazione richiede circa 5 minuti
- CSV - 200.000 record per report, la cui generazione richiede circa 4 minuti

> È possibile scaricare una versione del file CSV da visualizzare in questo browser. Questa versione è limitata a 10.000 record.

Cosa è incluso nel rapporto 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
  - I dati del proprietario del file comprendono il nome dell'account, il nome dell'account SAM e l'indirizzo e-mail quando Active Directory è configurato.
- Categoria
- Informazioni personali
- Informazioni personali sensibili
- Autorizzazioni aperte
- Errore analisi scansione
- Data di rilevamento dell'eliminazione

  La data di rilevamento dell'eliminazione identifica la data in cui il file è stato eliminato o spostato. In questo modo è possibile identificare quando sono stati spostati file sensibili. I file eliminati non contribuiscono al conteggio dei file visualizzato nella dashboard o nella pagina Indagine. 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:

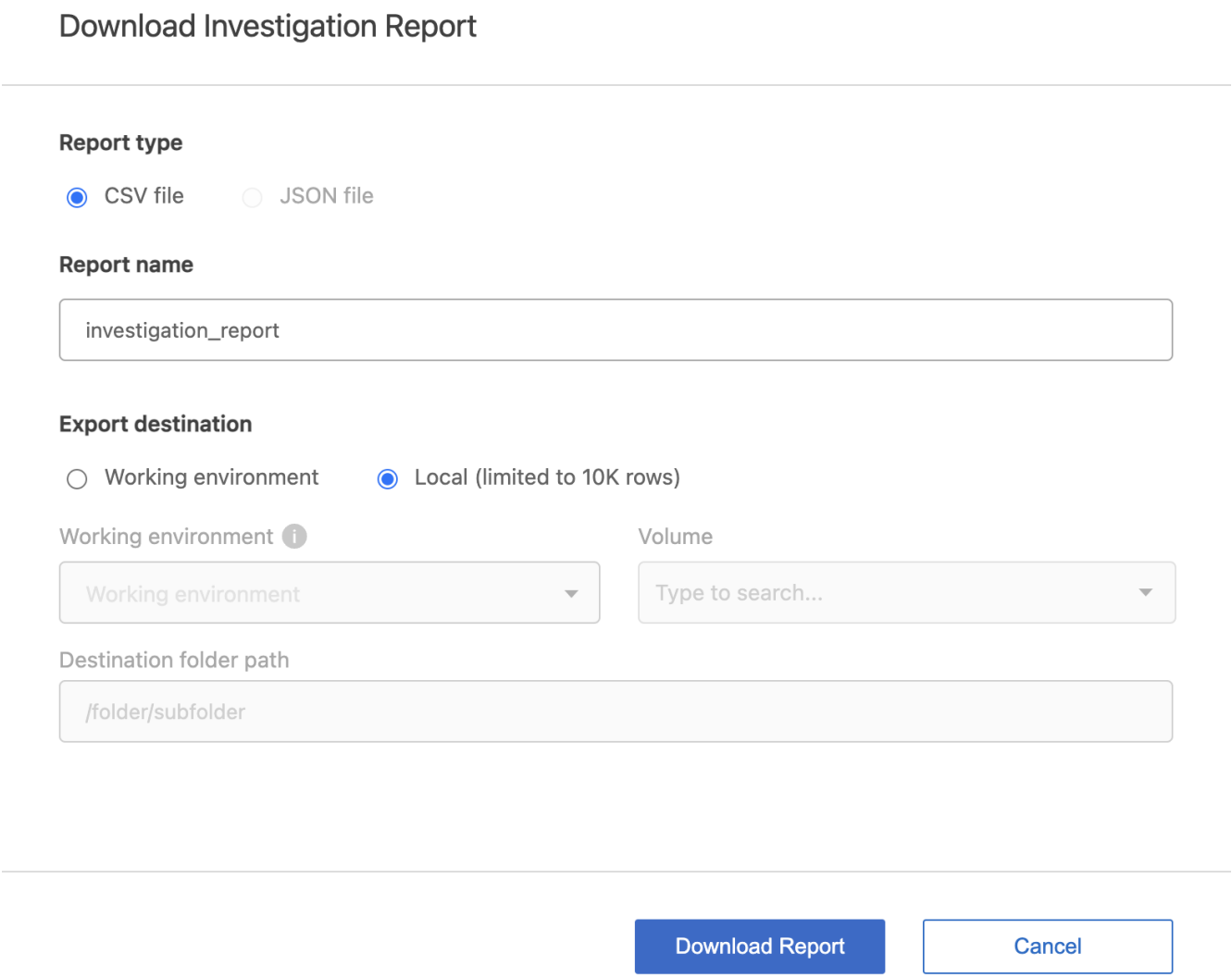
- DB Nome tabella
- Tipo di ubicazione
- Nome dell'ambiente di lavoro
- Repository di storage (ad esempio, uno schema)
- Numero di colonne
- Numero di righe
- Informazioni personali
- Informazioni personali sensibili

Procedura per generare il rapporto

1. Nella pagina analisi dati, selezionare il pulsante in alto a destra della pagina.
2. Scegliere il tipo di rapporto: CSV o JSON.
3. Immettere un **Nome rapporto**.
4. Per scaricare il report completo, selezionare **ambiente di lavoro** quindi scegliere **ambiente di lavoro** e **Volume** dai rispettivi menu a discesa. Fornire un percorso della cartella di destinazione **.

   Per scaricare il report nel browser, selezionare **locale** . Nota questa opzione limita il rapporto alle prime 10.000 righe ed è limitata al formato **CSV**. Non è necessario completare altri campi se si seleziona **locale**.

5. Selezionare **Scarica rapporto**.



Risultato

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

Crea una ricerca salvata in base ai filtri selezionati

È possibile creare una ricerca salvata per i filtri di ricerca utilizzati di frequente nella pagina analisi dati per replicare facilmente le query di ricerca.

Fasi

1. Dal menu classificazione BlueXP , selezionare **analisi**.
2. Nella pagina analisi dati, selezionare i filtri che si desidera utilizzare per creare una ricerca salvata.
3. Nella parte inferiore del pannello filtro, selezionare **Crea ricerca salvata da questa ricerca**.
4. Immettere un nome e una descrizione per la ricerca salvata.
5. Scegli una delle seguenti opzioni:
6. Selezionare **Crea ricerca salvata**.

La visualizzazione dei risultati nella pagina Ricerche salvate potrebbe richiedere fino a 15 minuti.

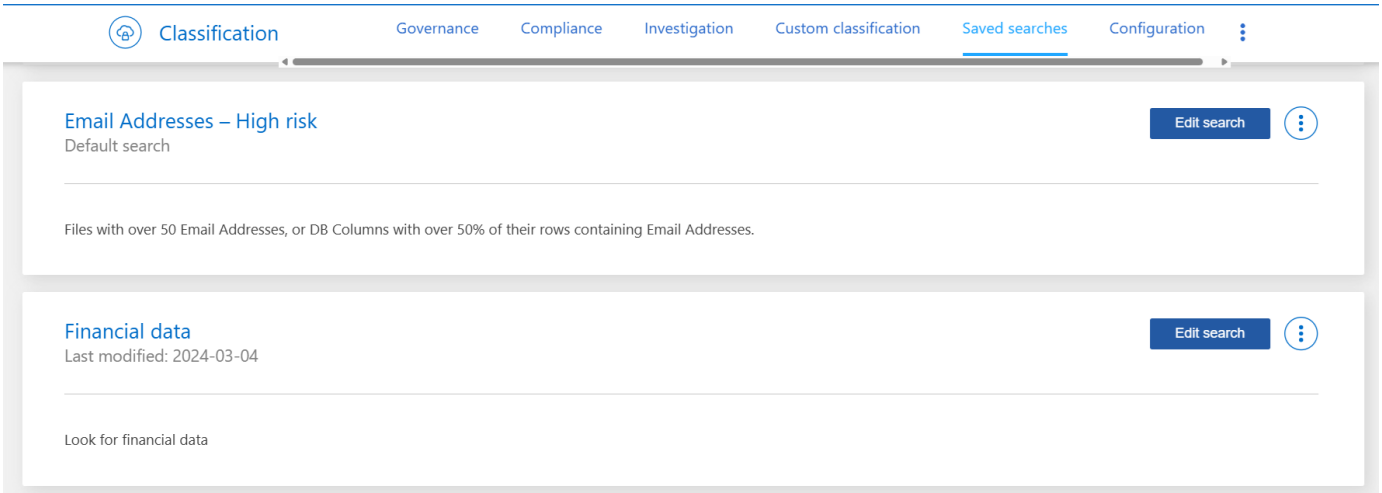
Gestire le ricerche salvate con la classificazione BlueXP

La classificazione BlueXP supporta il salvataggio delle query di ricerca. Con una ricerca salvata, è possibile creare filtri personalizzati per ordinare le query frequenti della pagina di analisi dei dati. La classificazione BlueXP include anche ricerche salvate predefinite basate su richieste comuni.

Nelle versioni di classificazione BlueXP precedenti alla 1,43, le ricerche salvate sono state chiamate policy.

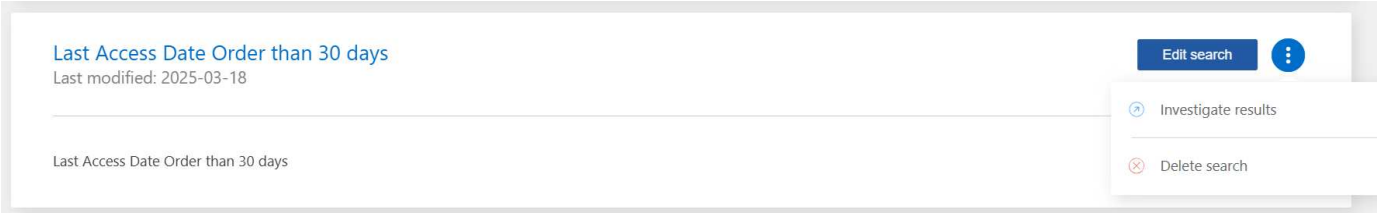
La scheda **ricerche salvate** nel dashboard conformità elenca tutte le ricerche salvate predefinite e personalizzate disponibili in questa istanza della classificazione BlueXP .

Le ricerche salvate vengono visualizzate anche nell'elenco dei filtri nella pagina di analisi.



Visualizzare i risultati delle ricerche salvate nella pagina di analisi

Per visualizzare i risultati di una ricerca salvata nella pagina di analisi, selezionare il pulsante per una ricerca specifica, quindi selezionare **risultati analisi**.

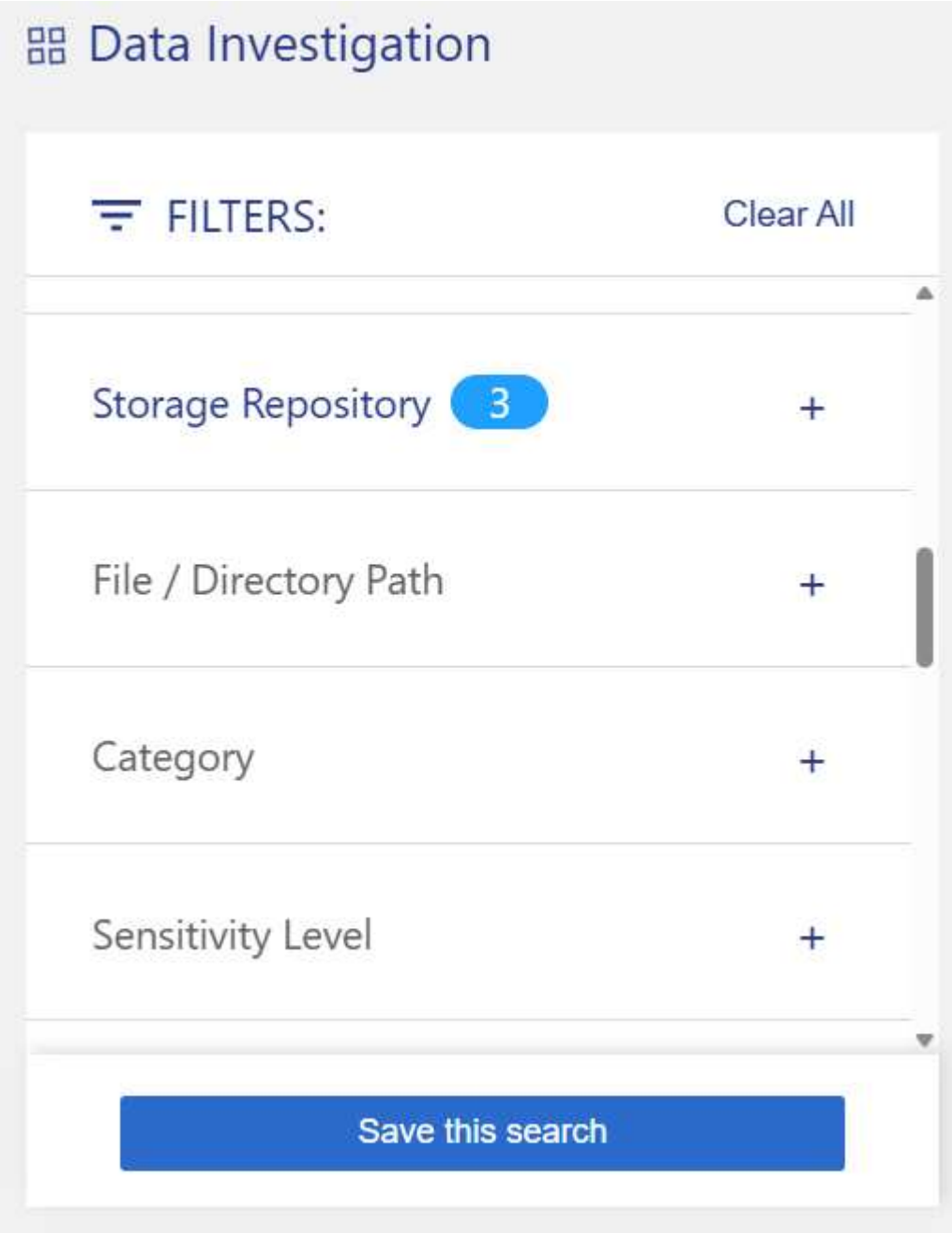


Creare ricerche salvate personalizzate

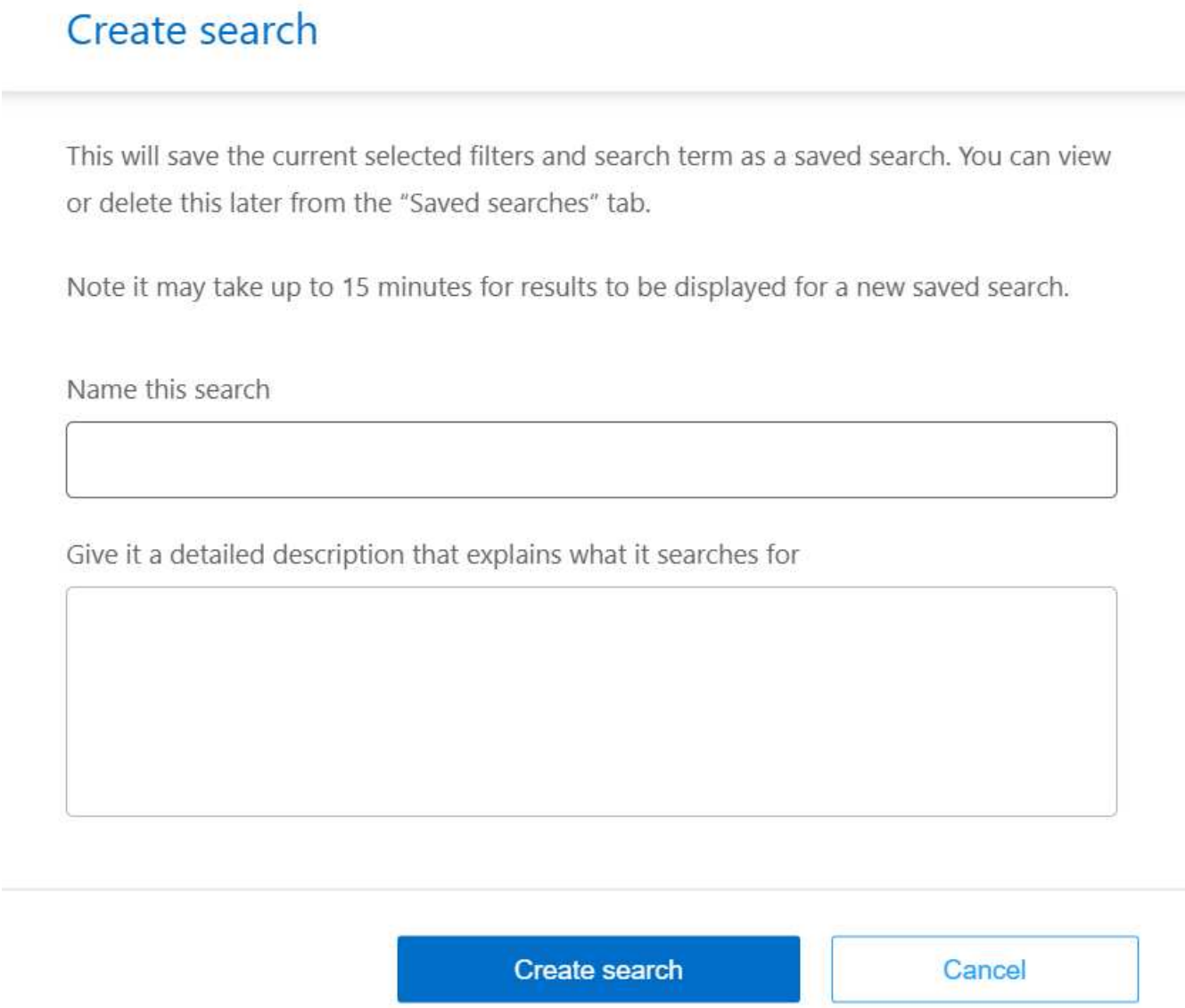
È possibile creare ricerche salvate personalizzate che forniscono risultati per le query specifiche dell'organizzazione. I risultati vengono restituiti per tutti i file e le directory (condivisioni e cartelle) che corrispondono ai criteri di ricerca.

Fasi

1. Nella scheda analisi, definire una ricerca selezionando i filtri che si desidera utilizzare. Per ulteriori informazioni, vedere "Filtraggio dei dati nella pagina di analisi" .
2. Una volta impostate tutte le caratteristiche del filtro a tuo piacimento, seleziona **Crea ricerca salvata**.



3. Assegnare un nome alla ricerca salvata e aggiungere una descrizione. Il nome deve essere univoco.
4. Selezionare **Crea ricerca salvata**.



Una volta creata la ricerca, è possibile visualizzarla nella scheda **ricerche salvate**.

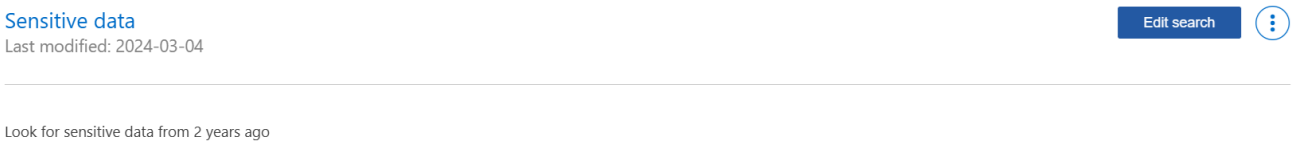
Modificare le ricerche salvate

È possibile modificare i criteri di query per una ricerca salvata (ovvero i filtri definiti) per aggiungere o rimuovere determinati parametri.

Non è possibile modificare le ricerche salvate predefinite.

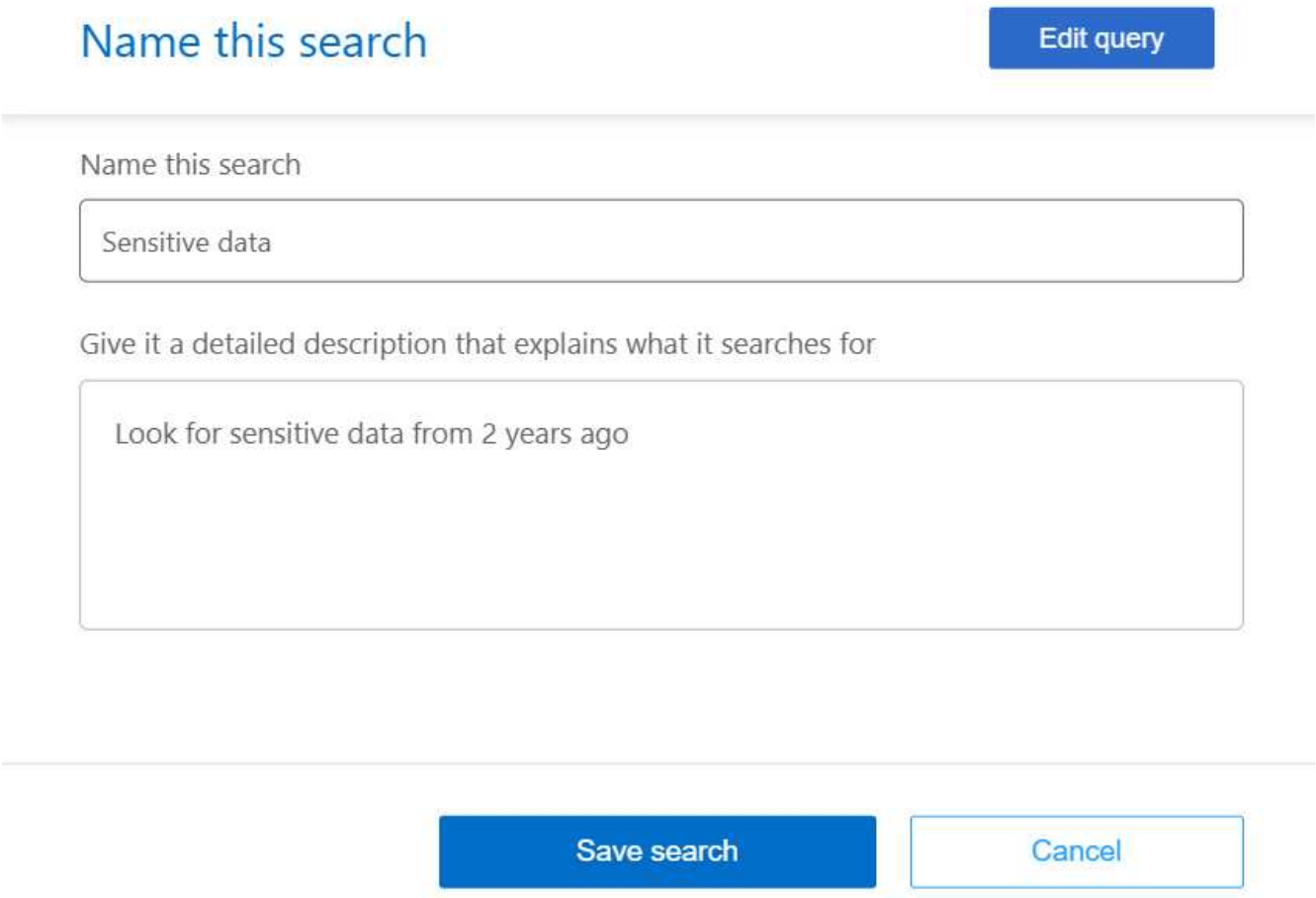
Fasi

1. Nella pagina ricerche salvate, selezionare **Modifica ricerca** per la ricerca che si desidera modificare.

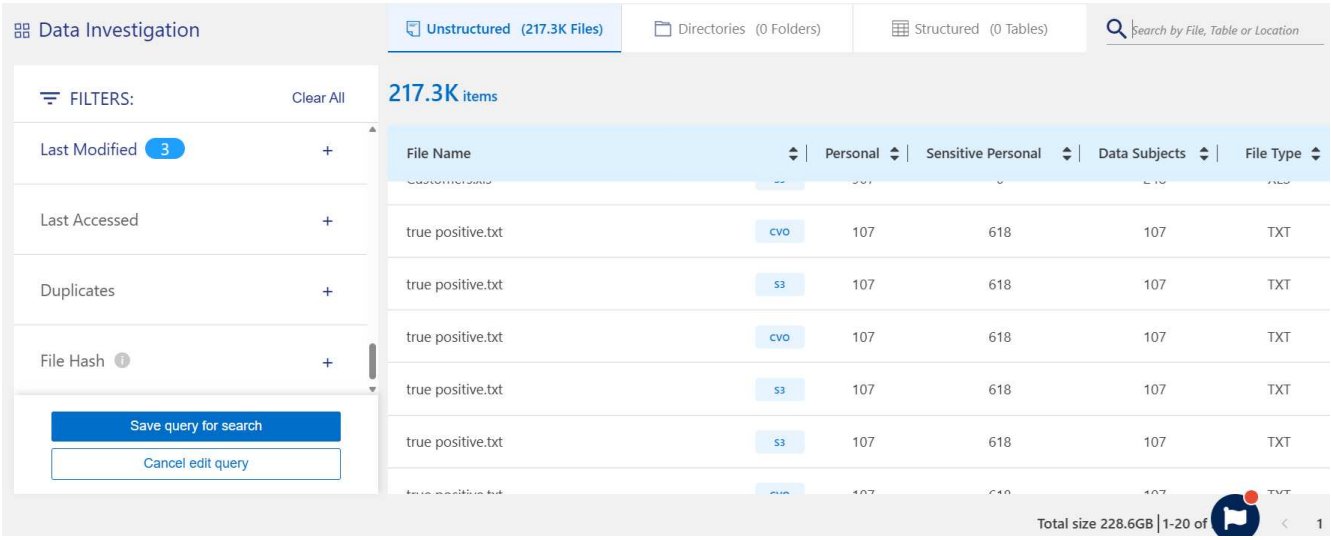


2. Apportare le modifiche ai campi nome e descrizione. Per modificare solo i campi nome e descrizione, selezionare **Salva ricerca**.

   Per modificare i filtri per la ricerca salvata, selezionare **Modifica query**.



3. Nella pagina di analisi, modificare la query. È possibile aggiungere, rimuovere o modificare i filtri. Per completare le modifiche, selezionare **Salva query per questa ricerca**.



Eliminare le ricerche salvate

È possibile eliminare qualsiasi ricerca salvata personalizzata se non è più necessaria. Non è possibile eliminare le ricerche salvate predefinite.

Per eliminare una ricerca salvata, selezionare il pulsante per una ricerca specifica, selezionare **Elimina ricerca**, quindi selezionare nuovamente **Elimina ricerca** nella finestra di dialogo di conferma.

Ricerche predefinite

La classificazione BlueXP fornisce le seguenti query di ricerca definite dal sistema:

- **Denominazione delle persone - rischio elevato**

  File con più di 50 nomi di soggetti di dati

- **Indirizzi e-mail - rischio elevato**

  File con più di 50 indirizzi e-mail o colonne di database con più del 50% delle righe contenenti indirizzi e-mail

- **Dati personali - rischio elevato**

  File con più di 20 identificatori di dati personali o colonne di database con oltre il 50% delle righe contenenti identificatori di dati personali

- **Dati privati - obsoleti oltre 7 anni**

  File contenenti informazioni personali o sensibili, ultima modifica più di 7 anni fa

- **Protezione - alta**

  File o colonne di database contenenti una password, informazioni sulla carta di credito, numero IBAN o numero di previdenza sociale

- **Protezione - bassa**

  File a cui non si accede da più di 3 anni

- **Proteggi - Medio**

  File che contengono file o colonne di database con identificatori di dati personali, inclusi numeri di identificazione, numeri di identificazione fiscale, numeri di patente di guida, ID medicinali o numeri di passaporto

- **Dati personali sensibili - rischio elevato**

  File con più di 20 identificatori di dati personali sensibili o colonne di database con più del 50% delle righe contenenti dati personali sensibili

Modificare le impostazioni di scansione della classificazione BlueXP per gli archivi

È possibile gestire la modalità di scansione dei dati in ciascuno degli ambienti di lavoro e delle origini dati. È possibile apportare le modifiche in base al "repository", ovvero apportare modifiche per ogni volume, schema, utente e così via, a seconda del tipo di origine dati che si sta eseguendo la scansione.

Alcune delle cose che è possibile modificare sono se un repository viene sottoposto a scansione o meno e se la classificazione BlueXP sta eseguendo un "scansione di mappatura o scansione di classificazione di mappatura". È inoltre possibile sospendere e riprendere la scansione, ad esempio se è necessario interrompere la scansione di un volume per un determinato periodo di tempo.

Consente di visualizzare lo stato della scansione per i repository

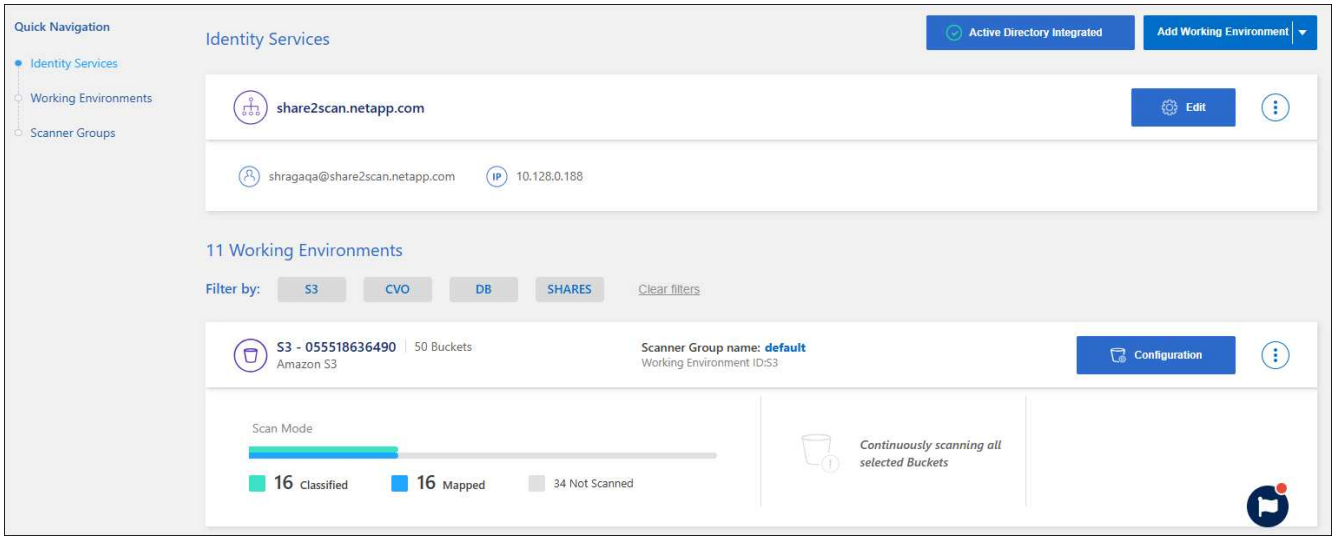
È possibile visualizzare i singoli repository che la classificazione BlueXP sta analizzando (volumi, bucket, ecc.) per ogni ambiente di lavoro e origine dati. Inoltre, puoi vedere quanti sono stati "mappati" e quanti sono stati "classificati". La classificazione richiede più tempo poiché l'identificazione ai completa viene eseguita su tutti i dati.

È possibile visualizzare lo stato di scansione di ciascun ambiente di lavoro nella pagina di configurazione:

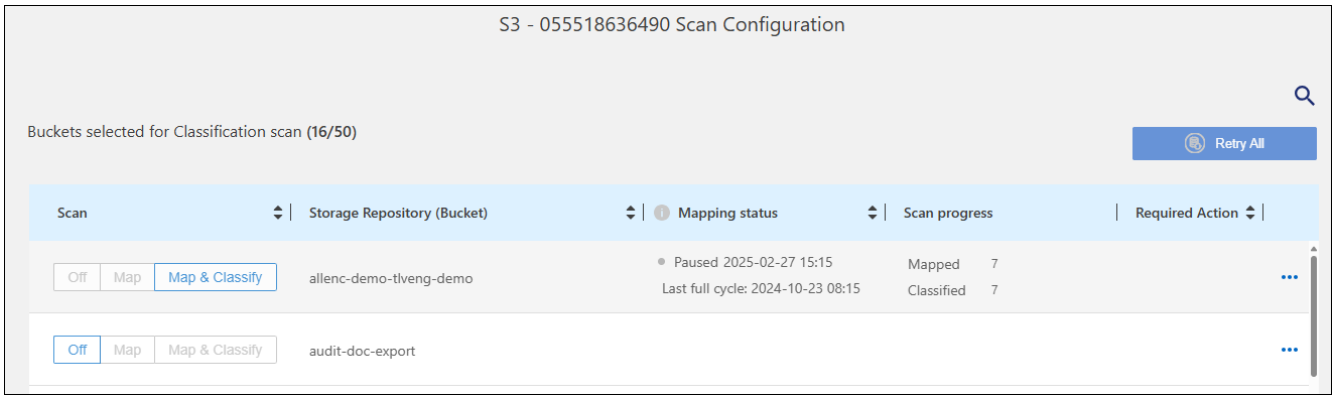
- **Inizializzazione** (punto azzurro): La configurazione mappa o classificazione è attivata. Viene visualizzato per alcuni secondi prima di avviare lo stato "coda in sospeso".
- **Coda in sospeso** (punto arancione): L'attività di scansione è in attesa di essere elencata nella coda di scansione.
- **In coda** (punto arancione): L'attività è stata aggiunta correttamente alla coda di scansione. Il sistema avvia il mapping o la classificazione del volume all'arrivo del turno nella coda.
- **In esecuzione** (punto verde): L'attività di scansione, che si trovava nella coda, è in corso attivo nell'archivio di archiviazione selezionato.
- **Terminato** (punto verde): La scansione del repository di archiviazione è completa.
- **In pausa** (punto grigio): È stata selezionata l'opzione "Pausa" per sospendere la scansione. Mentre le modifiche del volume non vengono visualizzate nel sistema, le informazioni acquisite vengono comunque visualizzate.
- **Errore** (punto rosso): Impossibile completare la scansione perché si sono verificati problemi. Se è necessario completare un'azione, l'errore viene visualizzato nella descrizione comandi sotto la colonna "azione richiesta". In caso contrario, il sistema visualizza uno stato di "errore" e tenta di eseguire il ripristino. Al termine, lo stato cambia.
- **Non scansione**: È stata selezionata la configurazione del volume "Off" e il sistema non sta eseguendo la scansione del volume.

Fasi

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.



2. Dalla scheda Configurazione, selezionare il pulsante **Configurazione** per l'ambiente di lavoro.
3. Nella pagina Configurazione scansione, visualizzare le impostazioni di scansione per tutti gli archivi.



4. Posizionare il cursore sul grafico nella colonna *Mapping Status* per vedere il numero di file che rimangono da mappare o classificare in ciascun repository (bucket in questo esempio).

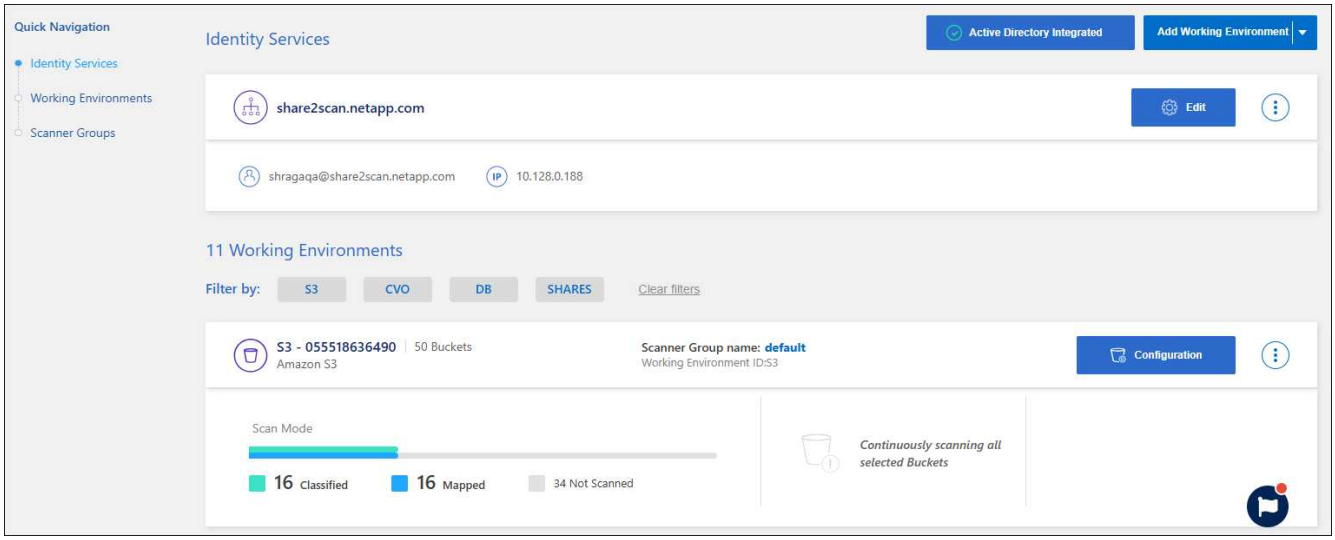
Modificare il tipo di scansione per un repository

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.

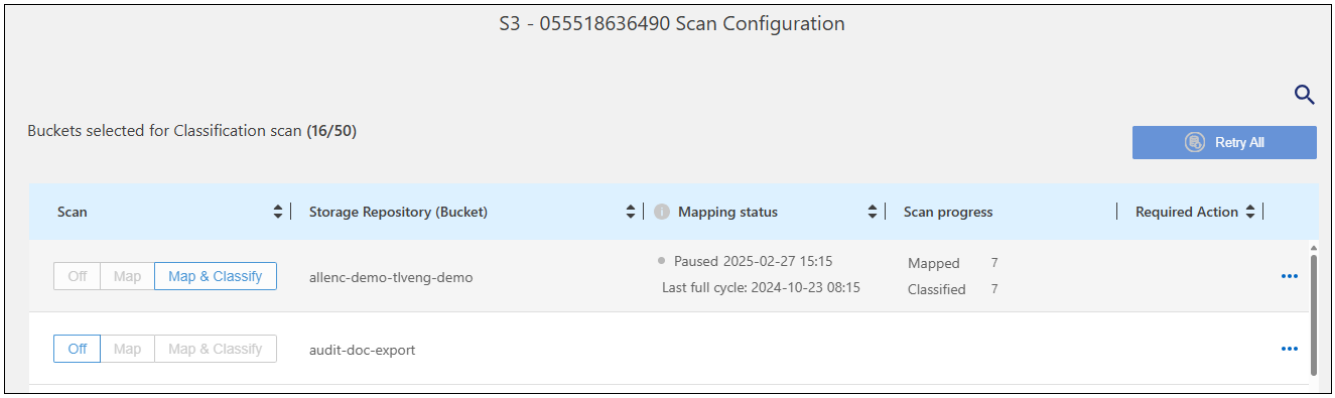
> I database non possono essere impostati su scansioni solo di mappatura. La scansione del database può essere disattivata o attivata; dove attivata equivale a Mappa e classificazione.

Fasi

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Dalla scheda Configurazione, selezionare il pulsante **Configurazione** per l'ambiente di lavoro.

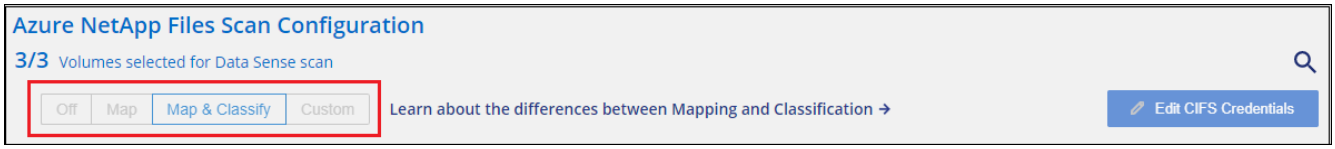


3. Nella pagina Configurazione scansione, modificare qualsiasi repository (bucket in questo esempio) per eseguire scansioni **Map** o **Map & Classify**.



Alcuni tipi di ambienti di lavoro consentono di modificare il tipo di scansione globale per tutti i repository utilizzando una barra dei pulsanti nella parte superiore della pagina. Valido per i sistemi Cloud Volumes ONTAP, on-premise ONTAP, Azure NetApp Files e Amazon FSX per ONTAP.

L'esempio seguente mostra questa barra dei pulsanti per un sistema Azure NetApp Files.



Assegnare priorità alle scansioni

È possibile assegnare la priorità alle scansioni di sola mappatura più importanti o mappare e classificare le scansioni per garantire che vengano completate per prime le scansioni ad alta priorità.

Per impostazione predefinita, le scansioni vengono accodate in base all'ordine in cui vengono avviate. Con la possibilità di assegnare priorità alle scansioni, è possibile spostare le scansioni in primo piano nella coda. È possibile assegnare priorità a più scansioni. La priorità viene indicata in un ordine di primo ingresso e primo uscita, ovvero la prima scansione assegnata all'utente viene spostata in primo piano nella coda; la seconda scansione assegnata all'utente diventa seconda nella coda e così via.

La priorità viene concessa una tantum. Le riscansioni automatiche dei dati di mappatura vengono eseguite nell'ordine predefinito.

Fasi

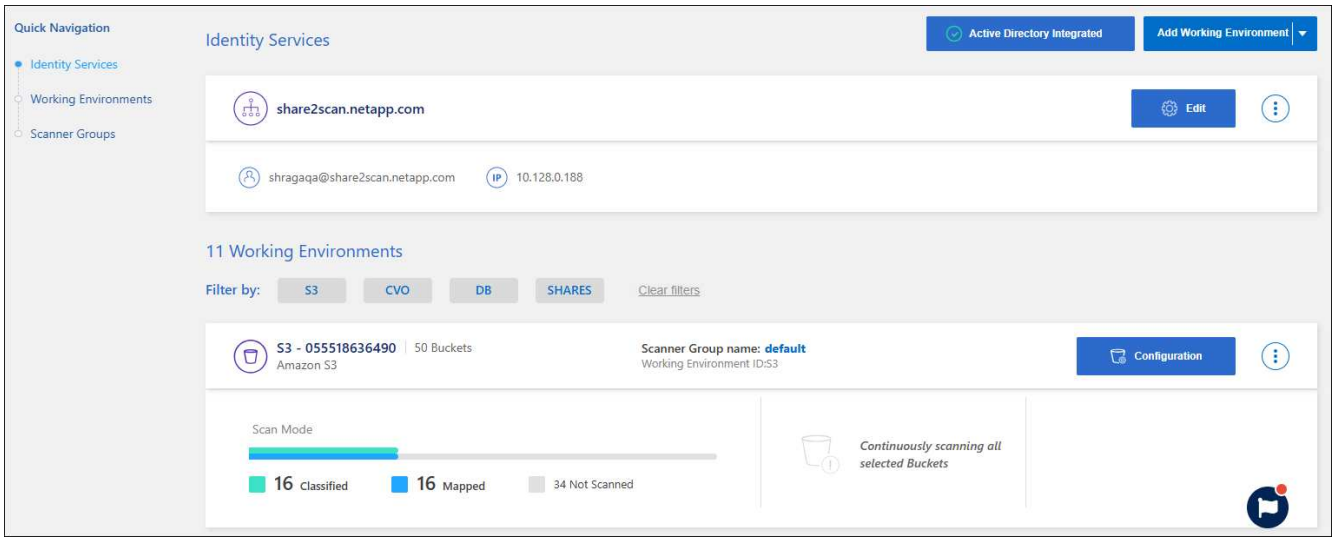
1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Selezionare le risorse a cui assegnare la priorità.
3. Dall'opzione azioni ..., selezionare **prioritizza scansione**.

Interrompere la ricerca di un repository

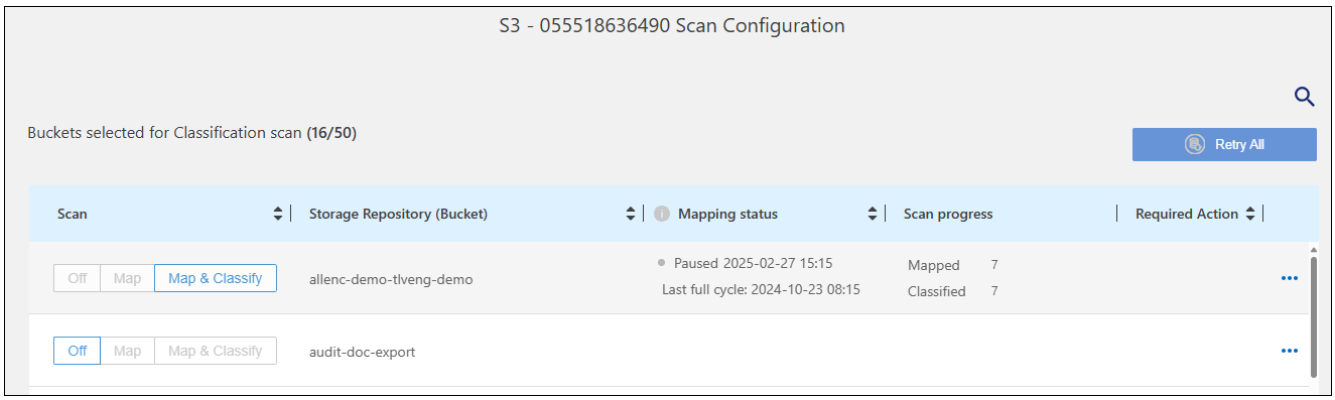
È possibile interrompere la scansione di un repository (ad esempio, un volume) se non è più necessario monitorarlo per verificarne la conformità. Per eseguire questa operazione, disattivare la scansione. Quando la scansione viene disattivata, tutte le informazioni e l'indicizzazione relative a quel volume vengono rimosse dal sistema e la ricarica per la scansione dei dati viene interrotta.

Fasi

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Dalla scheda Configurazione, selezionare il pulsante **Configurazione** per l'ambiente di lavoro.



3. Nella pagina Configurazione scansione selezionare **Off** per interrompere la scansione di un particolare bucket.



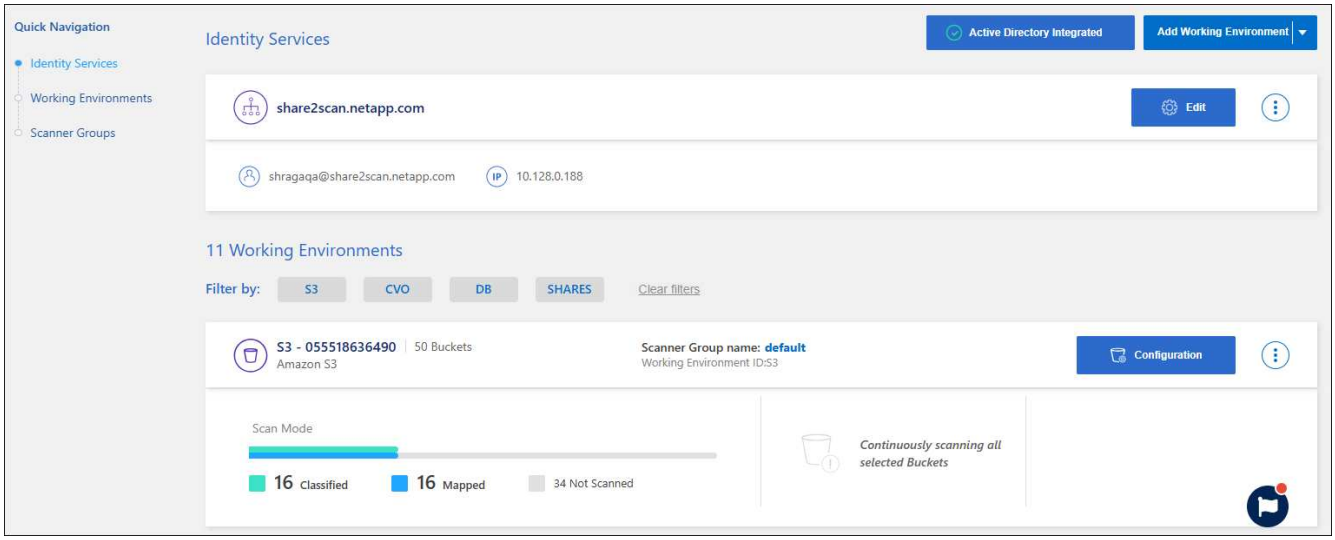
Sospendere e riprendere la scansione di un repository

È possibile "sospendere" la scansione in un repository se si desidera interrompere temporaneamente la scansione di determinati contenuti. La sospensione della scansione significa che la classificazione BlueXP non eseguirà scansioni future per modifiche o aggiunte al repository, ma che tutti i risultati correnti saranno ancora visualizzati nel sistema. La sospensione della scansione non interrompe il caricamento dei dati acquisiti perché i dati sono ancora presenti.

È possibile riprendere la scansione in qualsiasi momento.

Fasi

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Dalla scheda Configurazione, selezionare il pulsante **Configurazione** per l'ambiente di lavoro.



3. Nella pagina Configurazione scansione, selezionare l'icona azioni ▪▪▪ .
4. Selezionare **Pausa** per sospendere la scansione di un volume o selezionare **Riprendi** per riprendere la scansione di un volume precedentemente in pausa.

Visualizza i report sulla conformità della classificazione BlueXP

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 i report che contengono dati solo per alcuni ambienti di lavoro, è possibile filtrare per visualizzarli.

- 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.

Per la classificazione BlueXP sono disponibili i seguenti report:

- **Rapporto di valutazione del rilevamento dei dati**: 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 risoluzione dei problemi.
- **Rapporto mappatura dati**: Fornisce informazioni sulla dimensione e il numero di file negli ambienti di lavoro. Ciò include capacità di utilizzo, età dei dati, dimensioni dei dati e tipi di file.
- **Data Subject Access Request report**: Consente di estrarre un report di tutti i file che contengono informazioni relative al nome specifico o all'identificativo personale dell'interessato.
- **Rapporto HIPAA**: Consente di identificare la distribuzione delle informazioni sanitarie nei file.
- **Rapporto PCI DSS**: Consente di identificare la distribuzione delle informazioni sulle carte di credito nei file.
- **Privacy Risk Assessment report**: Fornisce informazioni sulla privacy dai tuoi dati e un punteggio di rischio sulla privacy.
- **Rapporti su un tipo specifico di informazioni**: Sono disponibili rapporti 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.

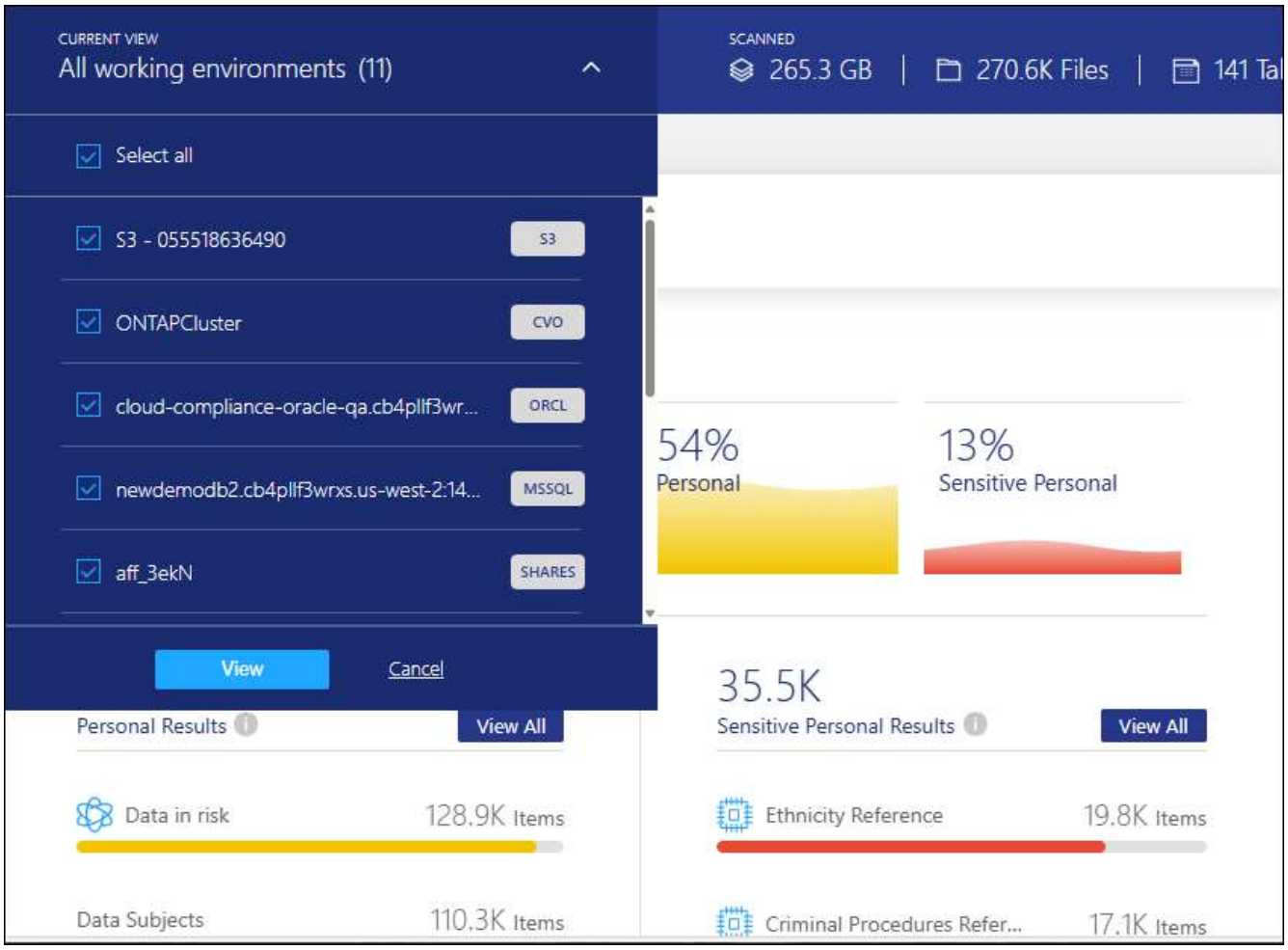
Selezionare gli ambienti di lavoro per i rapporti

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. Dal menu classificazione BlueXP , selezionare "**conformità**".
2. Selezionare l'elenco a discesa del filtro ambienti di lavoro e selezionare gli ambienti di lavoro.
3. Selezionare **Visualizza**.



Report di richiesta di accesso ai soggetti dei 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 aiutarvi a rispondere a un 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.

Cerca gli oggetti dei dati e scarica i report

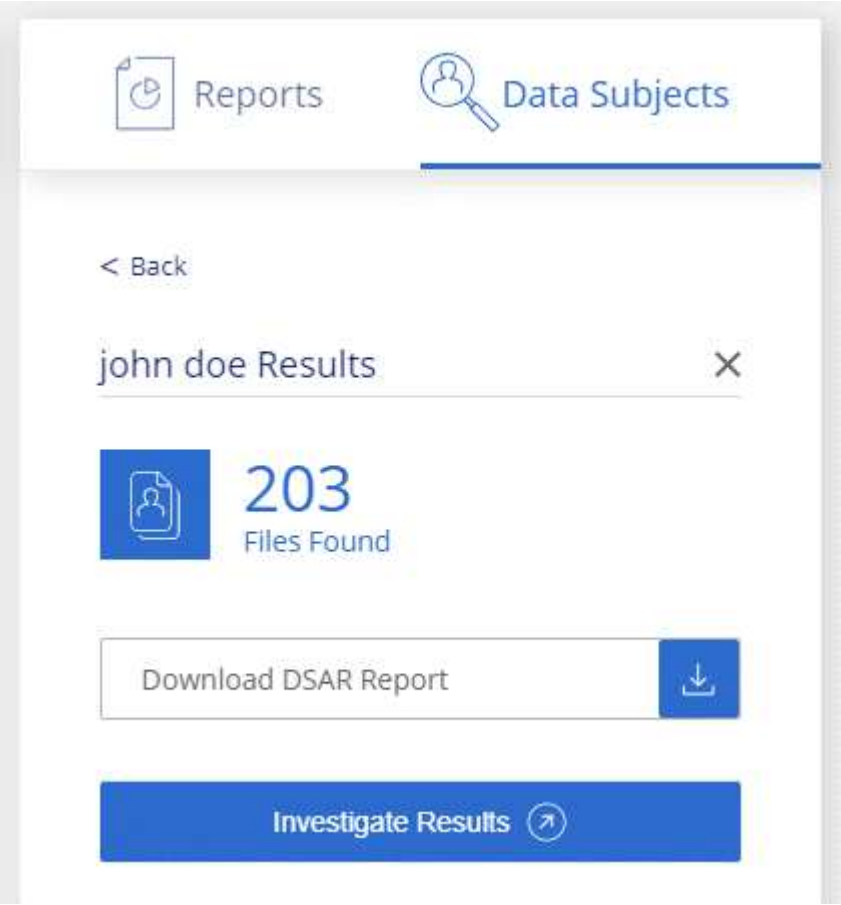
Cercare il nome completo o l'identificatore noto del soggetto interessato, quindi scaricare un report elenco file o un report DSAR. È possibile eseguire la ricerca in base a "qualsiasi tipo di informazione personale".

> 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 classificazione BlueXP , selezionare "**conformità**".
2. Dalla pagina conformità, scorrere verso il basso e selezionare **oggetti dati**.
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.

Report HIPAA (Health Insurance Portability and Accountability Act)

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:

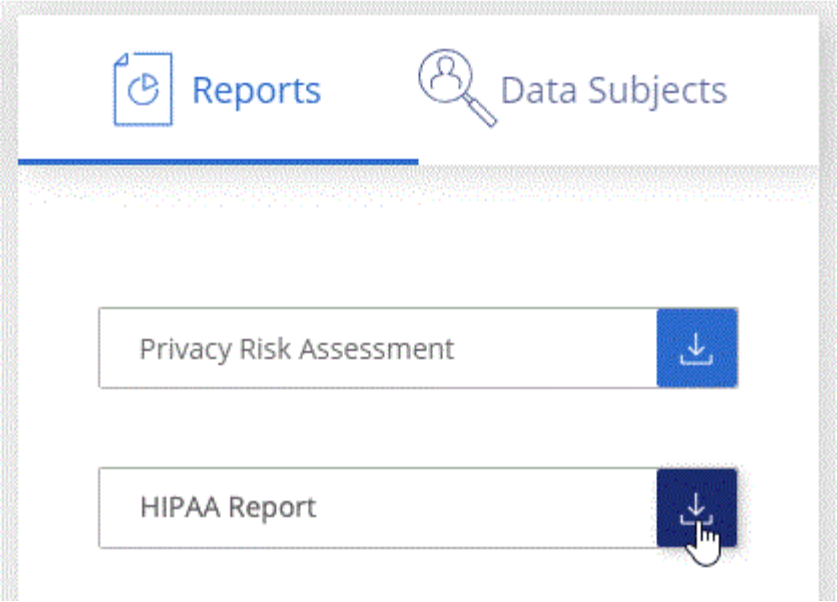
- Panoramica: Quanti file contengono informazioni sanitarie e in quali ambienti di lavoro.
- Crittografia: Percentuale di file contenenti informazioni di integrità presenti in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.
- Protezione ransomware: Percentuale di file contenenti informazioni sullo stato di salute che si trovano su ambienti di lavoro che hanno o non hanno abilitato la protezione dal ransomware. Queste informazioni sono specifiche di Cloud Volumes ONTAP.
- Retention (conservazione): L'intervallo 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 sanitarie e se la crittografia e la protezione anti-ransomware sono abilitate.

Generare il report HIPAA

Accedere alla scheda Compliance per generare il report.

Fasi

1. Dal menu classificazione BlueXP , selezionare "**conformità**".
2. Scorrere verso il basso e individuare il riquadro **rapporti**.
3. Selezionare l'icona di download accanto a **rapporto HIPAA**.



Risultato

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

Report PCI DSS (Payment Card Industry Data Security Standard)

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:

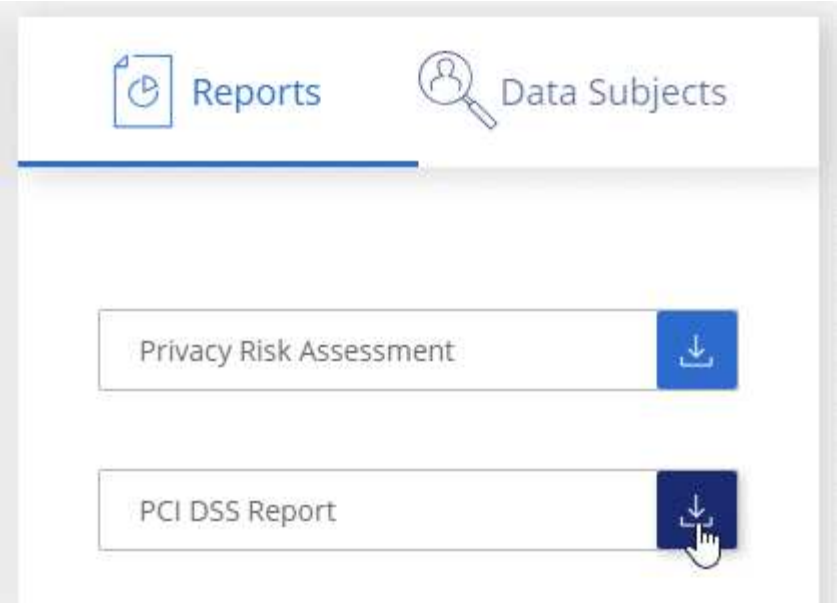
- Panoramica: Quanti file contengono informazioni sulle carte di credito e in quali ambienti di lavoro.
- Crittografia: Percentuale di file contenenti informazioni sulle carte di credito che si trovano in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.
- Protezione ransomware: Percentuale di file contenenti informazioni della carta di credito che si trovano in ambienti di lavoro che hanno o non hanno abilitato la protezione dal ransomware. Queste informazioni sono specifiche di Cloud Volumes ONTAP.
- Retention (conservazione): L'intervallo 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 della carta di credito: Ambienti di lavoro in cui sono state trovate le informazioni della carta di credito e se la crittografia e la protezione dal ransomware sono abilitate.

Generare il rapporto PCI DSS

Accedere alla scheda Compliance per generare il report.

Fasi

1. Dal menu classificazione BlueXP , selezionare "**conformità**".
2. Scorrere verso il basso e individuare il riquadro **rapporti**.
3. Selezionare l'icona di download accanto a **rapporto PCI DSS**.



Risultato

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

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:

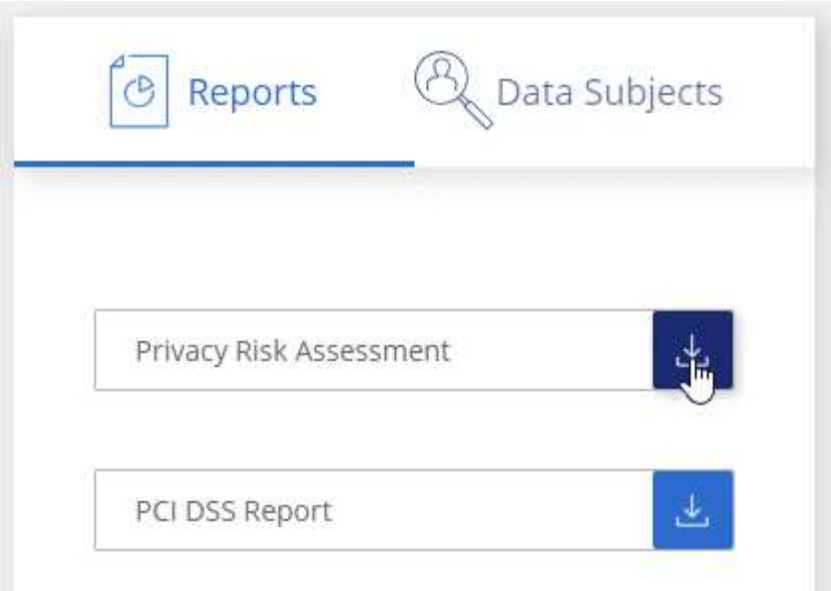
- Stato di conformità: Punteggio di gravità e distribuzione dei dati, non sensibili, personali o sensibili.
- Panoramica della valutazione: Ripartizione dei tipi di dati personali rilevati, nonché delle categorie di dati.
- Soggetti oggetto della valutazione: Il numero di persone, per località, per le quali sono stati trovati identificatori nazionali.

Generare il Privacy Risk Assessment Report

Accedere alla scheda Compliance per generare il report.

Fasi

1. Dal menu classificazione BlueXP , selezionare "**conformità**".
2. Scorrere verso il basso e individuare il riquadro **rapporti**.
3. Selezionare l'icona di download accanto a **Privacy Risk Assessment**.



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 gravità

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%

Gestire la classificazione BlueXP

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
```

Definire altri ID di gruppo come aperti all'organizzazione nella classificazione BlueXP

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 differire 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
```

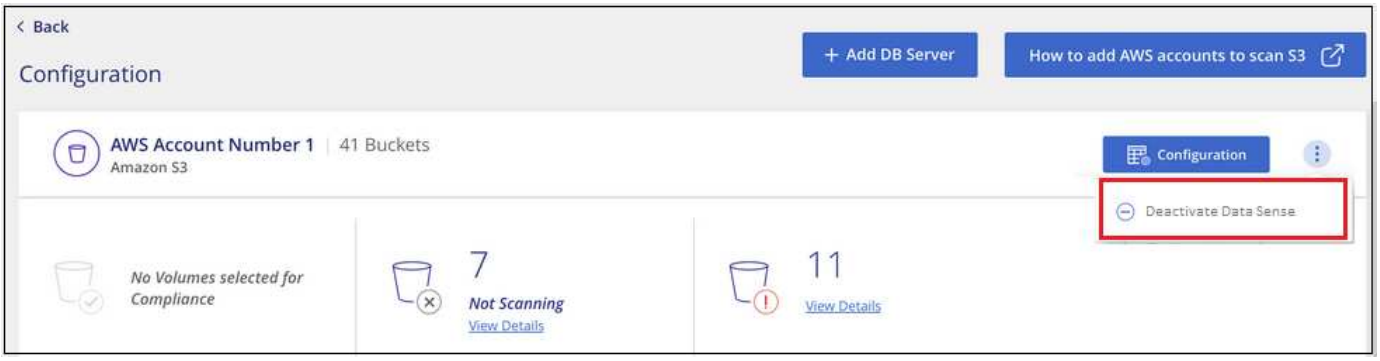
Rimuovere le origini dati dalla classificazione BlueXP

Se necessario, puoi impedire alla classificazione BlueXP di analizzare uno o più ambienti di lavoro, database o gruppi di condivisioni di file.

Disattivare le scansioni di conformità 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*, selezionare il pulsante nella riga per l'ambiente di lavoro, quindi **Deactivate Data Sense** (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. Nella pagina *Configuration*, selezionare il pulsante nella riga per il database, quindi **Remove DB Server**.

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*, selezionare il pulsante nella riga per il gruppo condivisioni file, quindi **Rimuovi gruppo condivisioni file**.

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

Disinstallare la classificazione BlueXP

È possibile disinstallare la classificazione BlueXP per risolvere i problemi o per rimuovere definitivamente il software dall'host. L'eliminazione dell'istanza comporta anche l'eliminazione dei dischi associati in cui risiedono i dati indicizzati, il che significa che tutte le informazioni acquisite dalla classificazione BlueXP verranno eliminate definitivamente.

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 classificazione BlueXP , selezionare quindi **Disinstalla classificazione**.

2. Nella finestra di dialogo *Disinstalla classificazione*, digitare **uninstall** per confermare che si desidera scollegare l'istanza di classificazione BlueXP dal connettore BlueXP , quindi selezionare **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 classificazione BlueXP , selezionare quindi **Disinstalla classificazione**.

2. Nella finestra di dialogo *Disinstalla classificazione*, digitare **uninstall** per confermare che si desidera scollegare l'istanza di classificazione BlueXP dal connettore BlueXP , quindi selezionare **Disinstalla**.
3. Per disinstallare il software dall'host, eseguire `cleanup.sh` lo script sul computer host di classificazione

BlueXP , ad esempio:

```
cleanup.sh
```

Lo script si trova nella `/install/light_probe/onprem_installer/cleanup.sh` directory.

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

Funzioni obsolete

Funzionalità obsolete di classificazione BlueXP

La classificazione BlueXP è disponibile come funzionalità core all'interno di BlueXP senza costi aggiuntivi. Includendo la classificazione BlueXP come funzionalità BlueXP essenziale disponibile per tutti i clienti, NetApp ti permette di accedere a una gestione dei dati personalizzata con funzionalità chiave.

Ci sono alcune funzionalità e caratteristiche deprecate nella versione core di BlueXP a partire dalla versione 1,31 e successive e sono ancora supportate nelle versioni legacy 1,30 e precedenti.

Origini dati supportate

Origine dei dati	Versioni precedenti 1,30 e precedenti	Versioni di base di BlueXP 1,31 e versioni successive
Cloud Volumes ONTAP (implementato in AWS, Azure o GCP)	Sì	Sì
Cluster ONTAP on-premise	Sì	Sì
StorageGRID	Sì	Sì
Azure NetApp Files	Sì	Sì
Amazon FSX per ONTAP	Sì	Sì
Google Cloud NetApp Volumes	Sì	Sì
Cloud Volumes Service per Google Cloud	Sì	Sì
Database	Sì	Sì
Amazon S3	Sì	No
Storage Google Cloud	Sì	No
OneDrive	Sì	No
SharePoint Online	Sì	No
SharePoint on-premise (SharePoint Server)	Sì	No
Google Drive	Sì	No

Funzionalità di conformità

Funzione	Versioni precedenti 1,30 e precedenti	Versioni di base di BlueXP 1,31 e versioni successive
Identificare le informazioni personali identificabili (PII)	Sì	Sì
Identificare le informazioni personali sensibili	Sì	Sì

Funzione	Versioni precedenti 1,30 e precedenti	Versioni di base di BlueXP 1,31 e versioni successive
Rispondere alle richieste di accesso dei soggetti a dati (DSAR)	Sì	Sì
Creare un elenco personalizzato di "dati personali" identificati	Sì	No
Notifica agli utenti tramite e-mail quando i file contengono determinati PII. (Questo criterio viene definito utilizzando "Policy".)	Sì	No
Utilizzare filtri a livello di directory	Sì	Sì
Utilizzare l'analisi PII a livello di directory	Sì	No

Funzioni per la gestione dei dati

Funzione	Versioni precedenti 1,30 e precedenti	Versioni di base di BlueXP 1,31 e versioni successive
Spostare, copiare ed eliminare i file di origine	Sì	No
Categorizzare i dati utilizzando i tag Stato	Sì	No
Categorizzare i dati utilizzando le etichette AIP	Sì	No
Assegnare i file agli utenti	Sì	No
Ripetere la scansione dei dati su richiesta	Sì	No
Creare classificatori personalizzati	Sì	No
Escludere le directory dalla scansione	Sì	Sì
Cercare i nomi all'interno dei file	Sì	Sì
Esportare dati in NFS/CIFS dall'analisi	Sì	Sì
Esportare i dati in CSV dall'analisi	Sì	Sì
Supporta più scanner	Sì	No
Integrare Active Directory	Sì	Sì
Utilizzare l'analisi delle autorizzazioni e i filtri	Sì	Sì
Utilizzare la scheda file	Sì	Sì
Utilizzare la mappa termica	Sì	Sì
Utilizzare le azioni su Dashboard e scheda file	Sì	No
Utilizzare la registrazione di controllo dell'accesso ai file	Sì	No
Attivare l'accesso al file dalla pagina di configurazione	Sì	No
Utilizzare determinati criteri predefiniti	Sì	No

Implementa le deprecazioni di classificazione BlueXP

Installare la classificazione BlueXP su host multipli per configurazioni di grandi dimensioni senza accesso a Internet

Completa alcuni passaggi per installare la classificazione BlueXP su più host 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.

Per le configurazioni molto grandi in cui si esegue la scansione di petabyte di dati in siti senza accesso a Internet, è possibile includere più host per fornire una potenza di elaborazione aggiuntiva. 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.

> Le seguenti informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

Prima di iniziare

- Verificare che tutti i sistemi Linux per i nodi Manager e scanner soddisfino i 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 le autorizzazioni e la connettività richieste.
- 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)
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.

Deprecazioni dei dati di scansione

Esegui la scansione dei bucket Amazon S3 con classificazione BlueXP

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.

> **NOTA** queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

Avvio rapido

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

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 vengono automatizzati finché l'istanza dispone di connettività Internet.

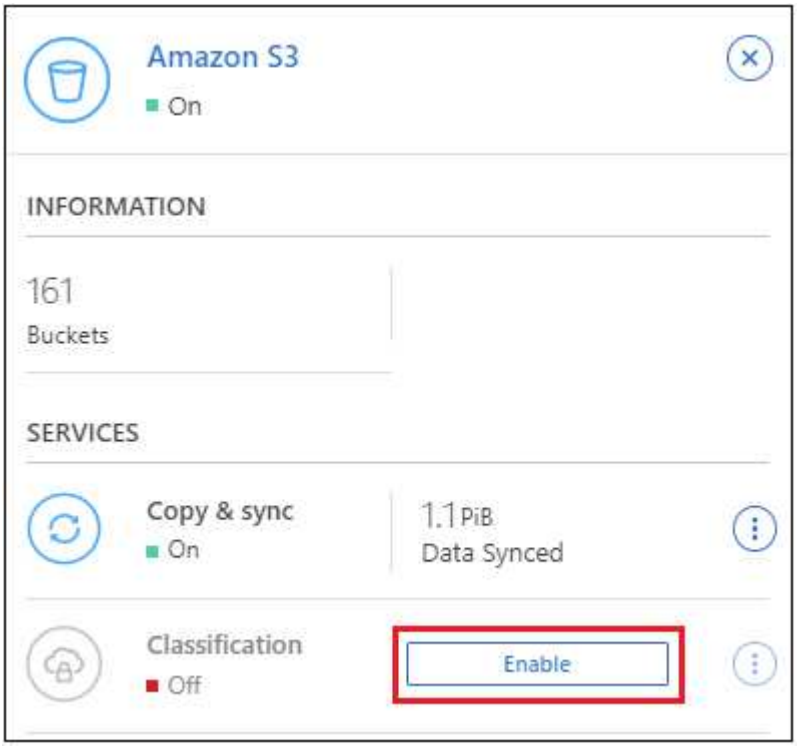
Attivazione della classificazione BlueXP nell'ambiente di lavoro S3

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

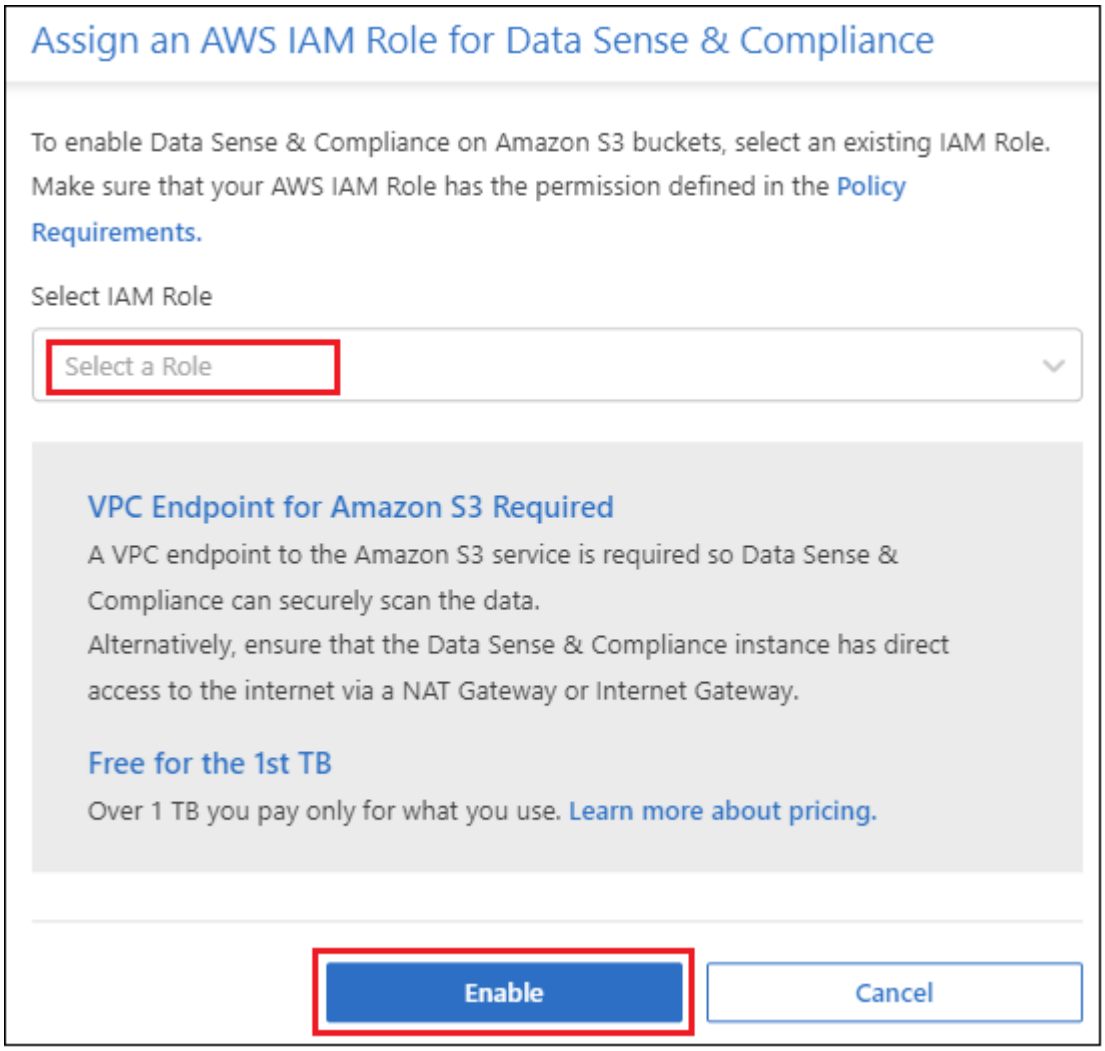
Fasi

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. Selezionare **Abilita**.

> È inoltre possibile attivare le scansioni di conformità per un ambiente di lavoro dalla pagina Configurazione selezionando il ⋮ pulsante, quindi **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.

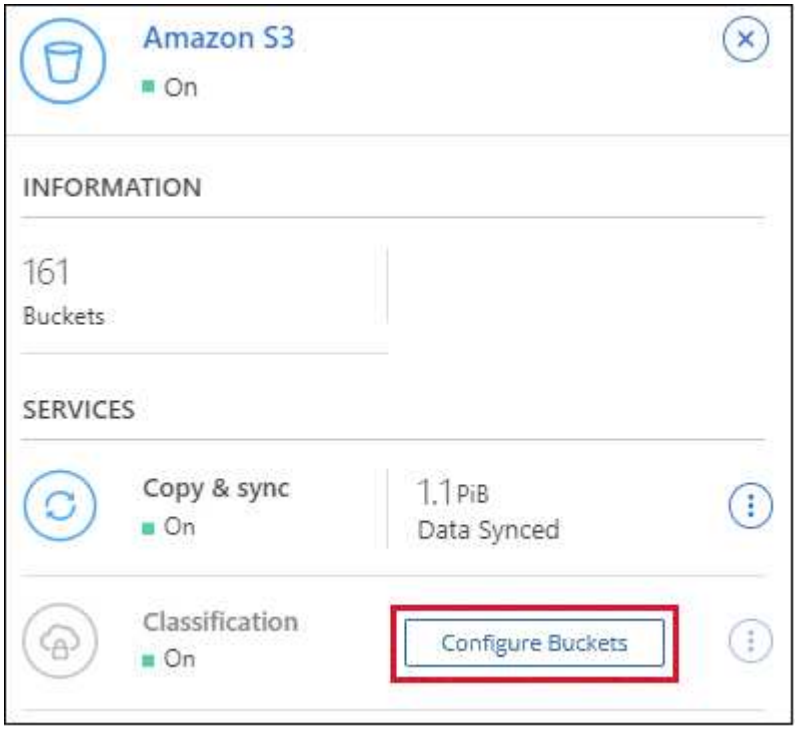
Quando BlueXP viene eseguito nell'account AWS che dispone dei bucket S3 che si desidera sottoporre a scansione, rileva tali bucket e li visualizza in un ambiente di lavoro Amazon S3.

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

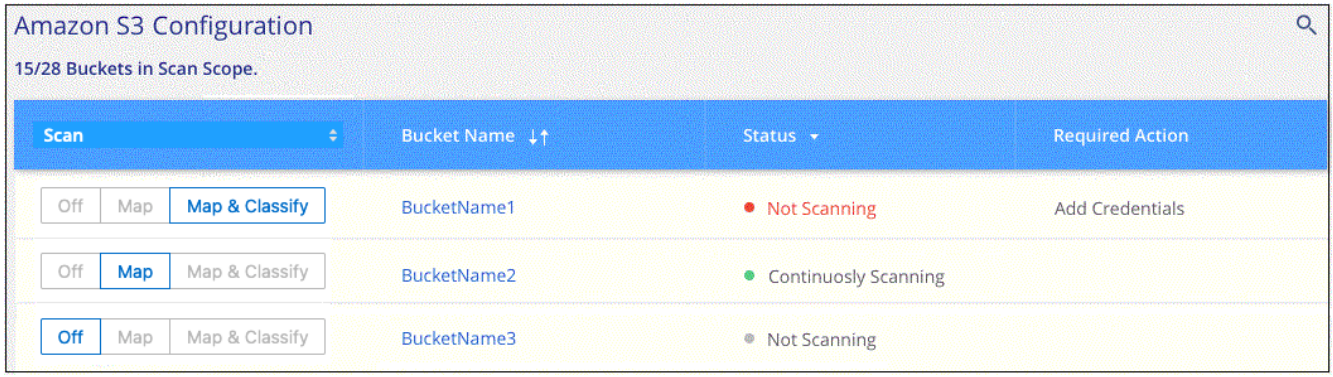
Fasi

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.

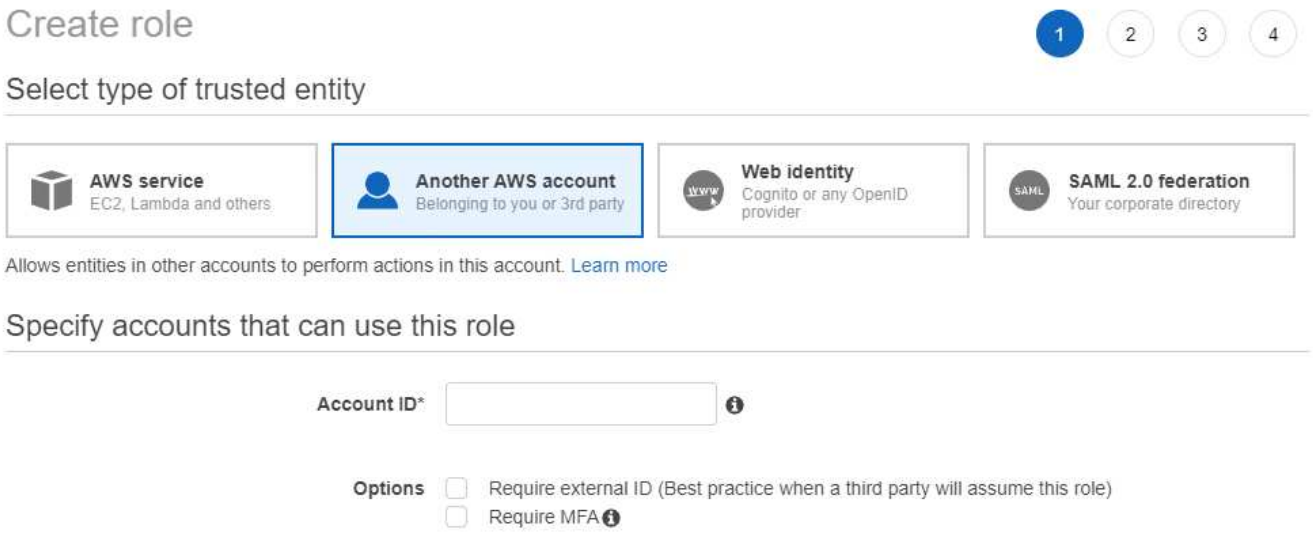
Scansione dei bucket da account AWS aggiuntivi

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. Salvare la modifica.

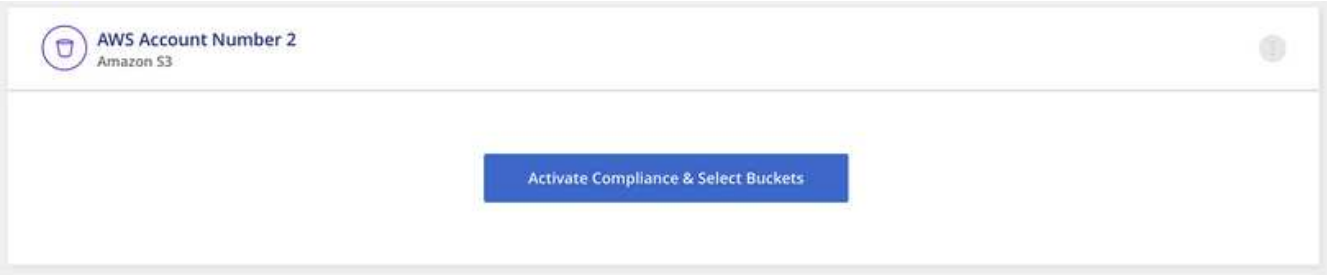
b. Selezionare **Allega criteri**, quindi **Crea criterio**.

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 riceve l'accesso all'account AWS aggiuntivo.

3. Accedere alla pagina **Amazon S3 Configuration** (Configurazione Amazon 2) 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.

Eseguire la scansione degli account OneDrive con classificazione BlueXP

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

> **NOTA** queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

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

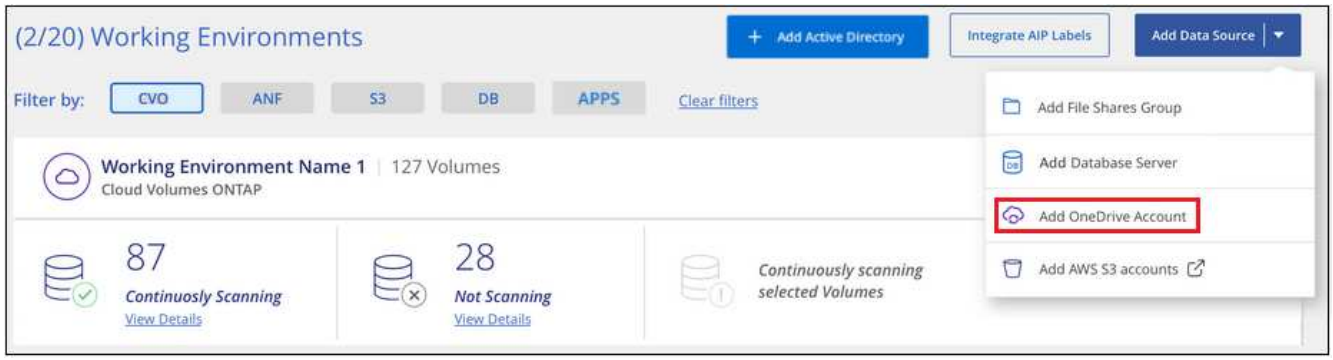
connettività Internet.

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.

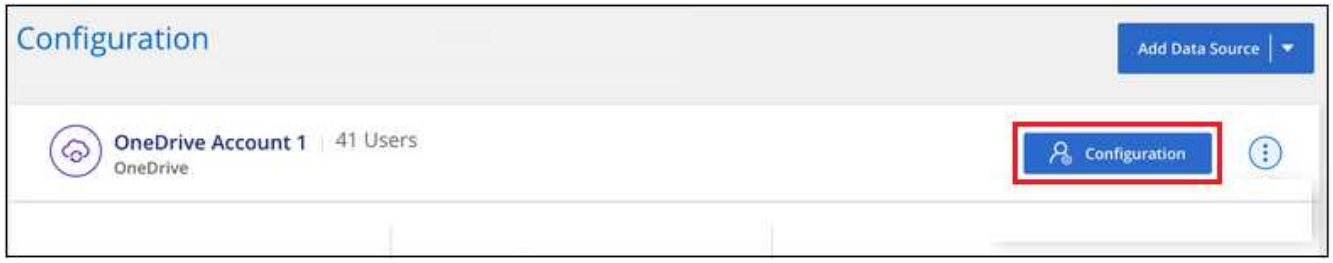
L'account OneDrive viene aggiunto all'elenco degli ambienti di lavoro.

Aggiunta di utenti OneDrive alle scansioni di conformità

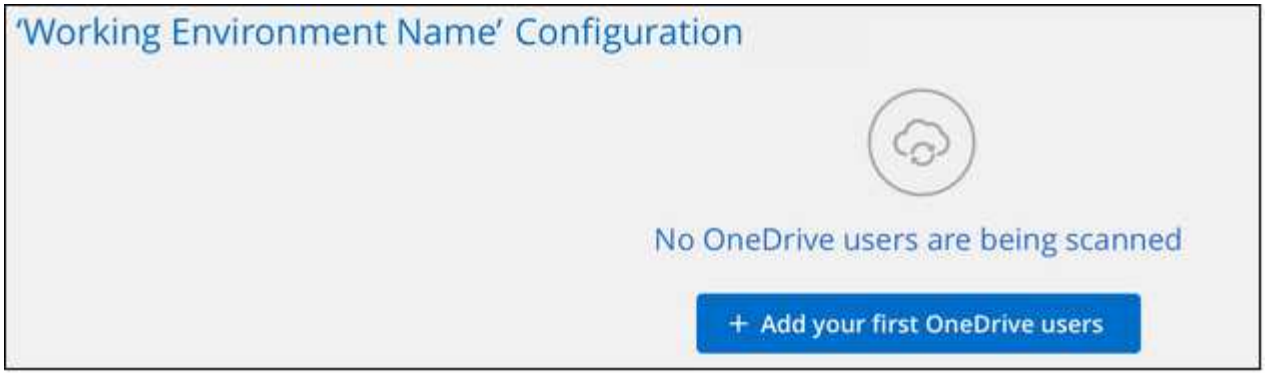
Puoi aggiungere singoli utenti OneDrive o tutti gli utenti OneDrive, in modo che i loro file vengano sottoposti a scansione in base alla classificazione BlueXP.

Fasi

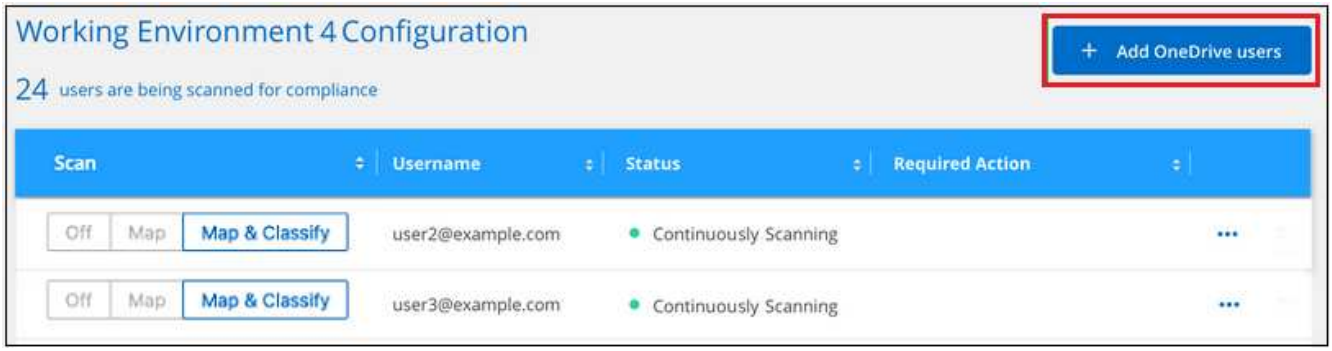
1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** dell'account OneDrive.



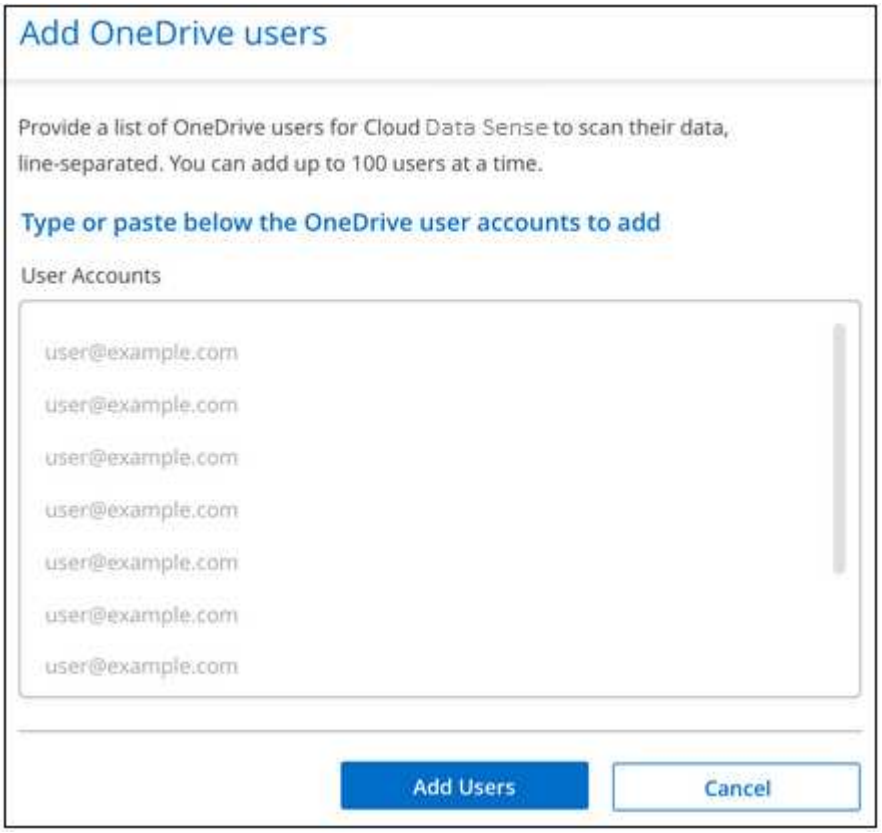
2. Se è la prima volta che si aggiungono utenti per questo account OneDrive, fare clic su **Aggiungi i primi utenti OneDrive**.



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.

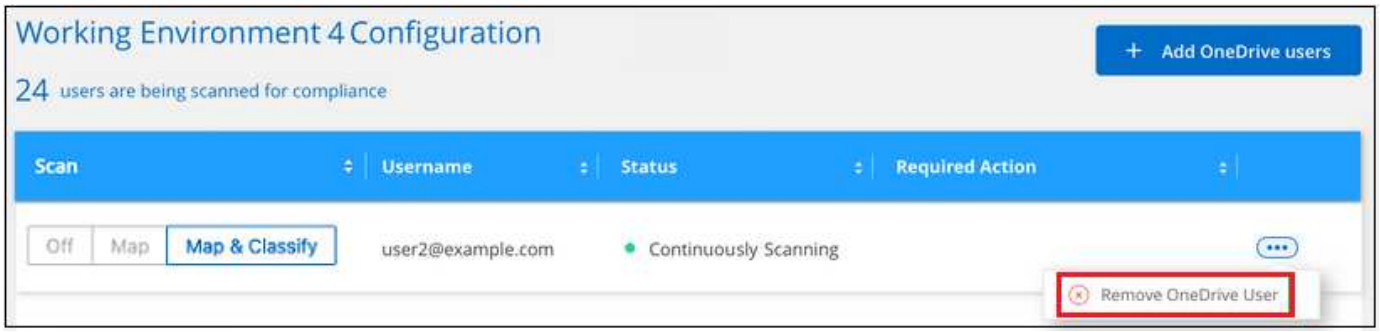
A:	Eseguire questa operazione:
Attiva scansioni solo mappatura sui file utente	Fare clic su **Map** (Mappa)
Attiva scansioni complete sui file utente	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione dei file utente	Fare clic su **Off**

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.



Eseguire la scansione degli account SharePoint con la classificazione BlueXP

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

> **NOTA** queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

Esaminare i 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.

Distribuire l'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".

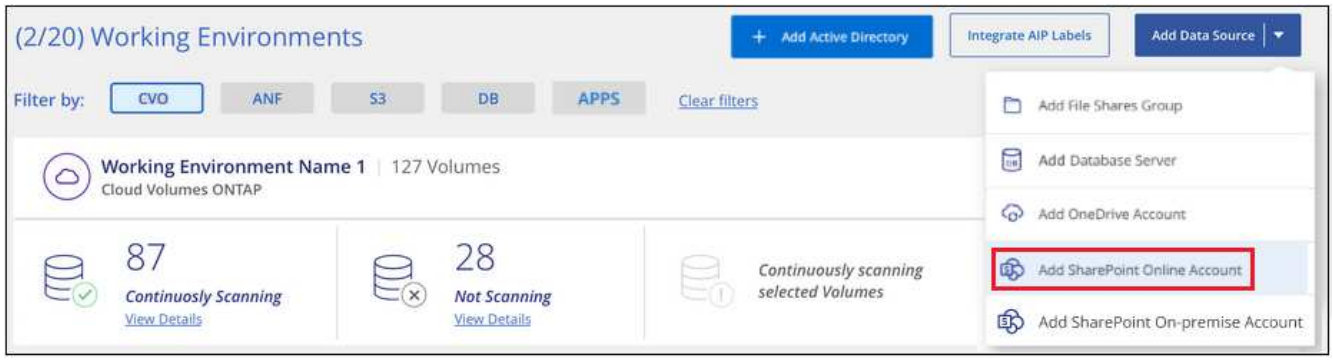
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Aggiungere 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.

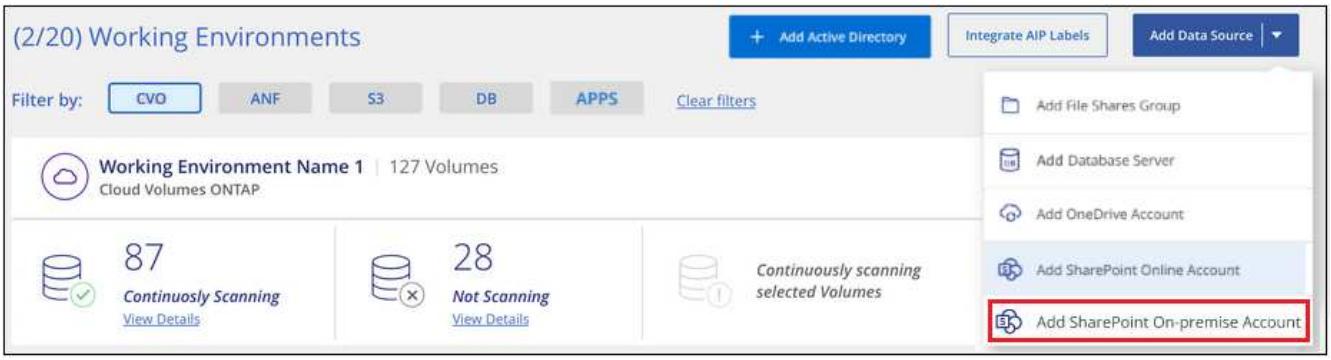
Aggiungere un account SharePoint in sede

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

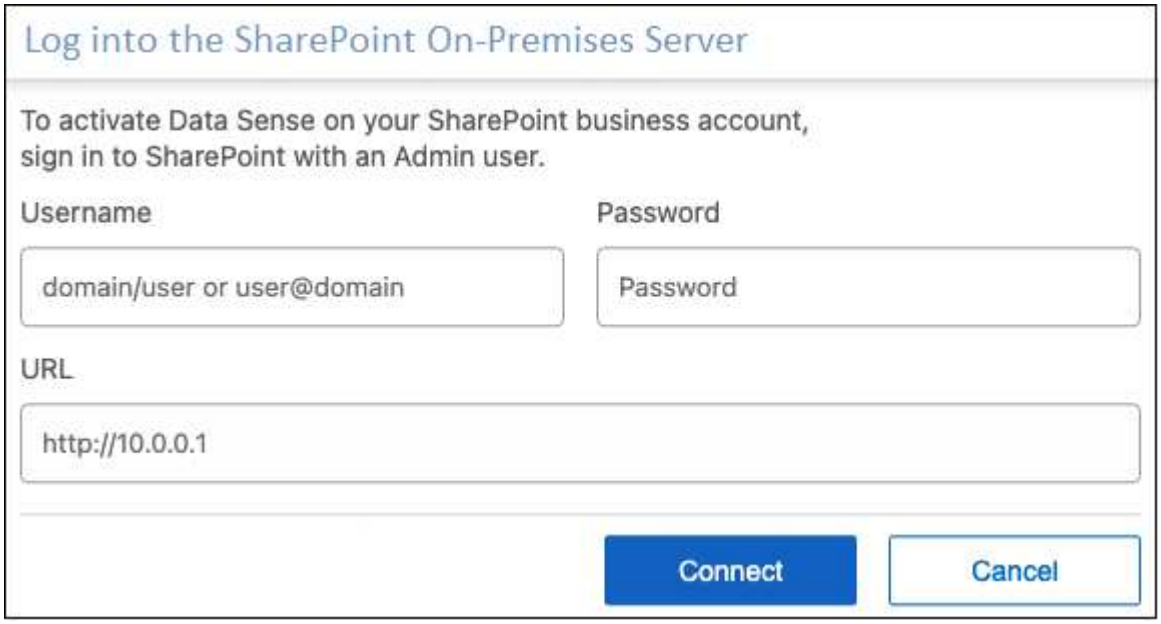
Fasi

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.

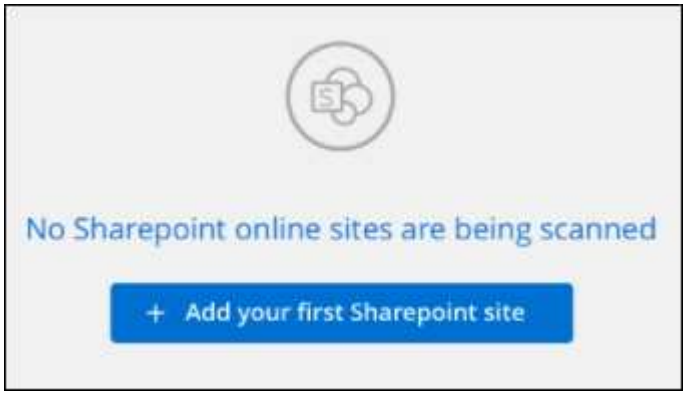
Aggiungere i siti SharePoint alle scansioni di conformità

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

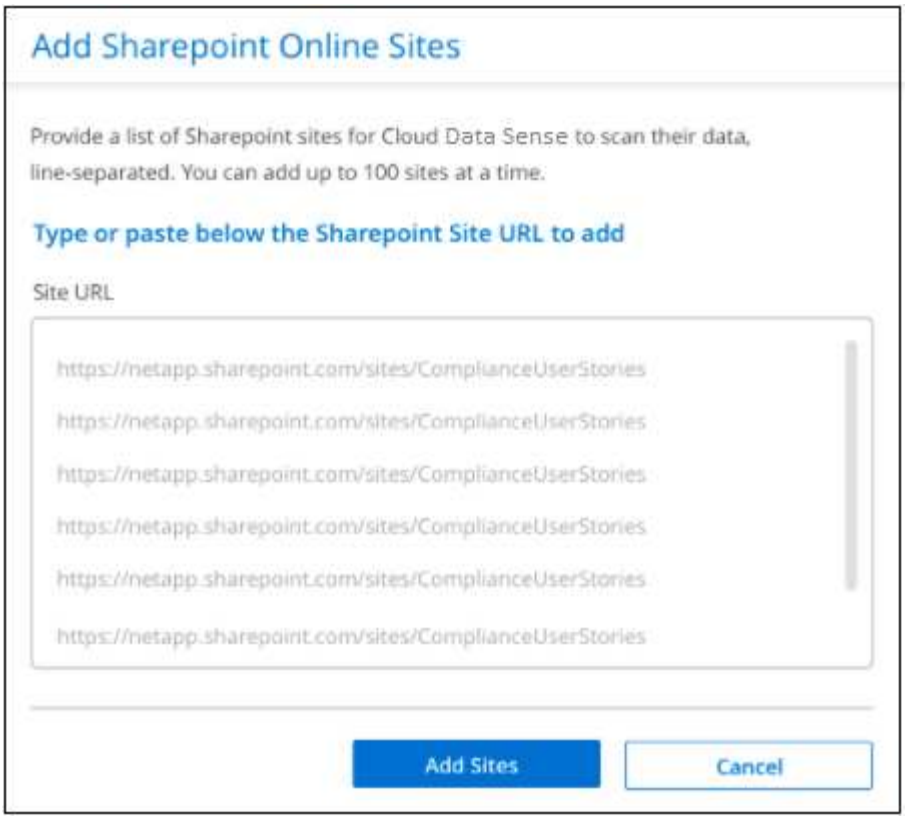
1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** dell'account SharePoint.

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.

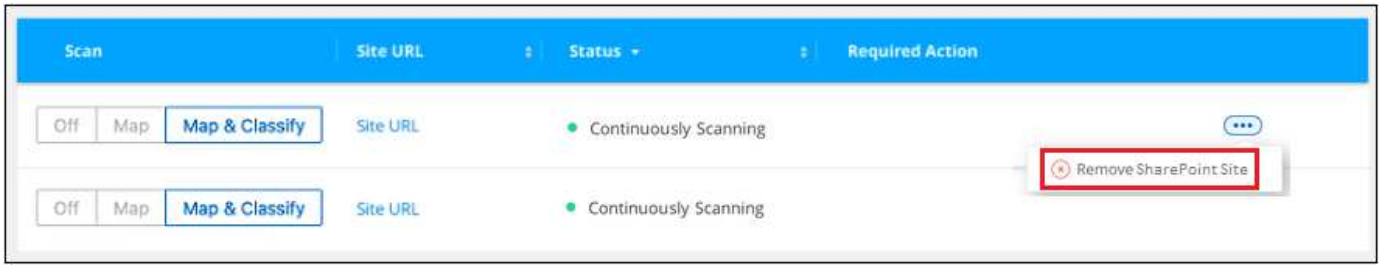
A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura sui file	Fare clic su **Map** (Mappa)
Attivare scansioni complete sui file	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione dei file	Fare clic su **Off**

Risultato

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

Rimuovere 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.

Eseguire la scansione degli account Google Drive con classificazione BlueXP

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

> **NOTA** queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

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.

Esaminare i 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.

Implementare la 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".

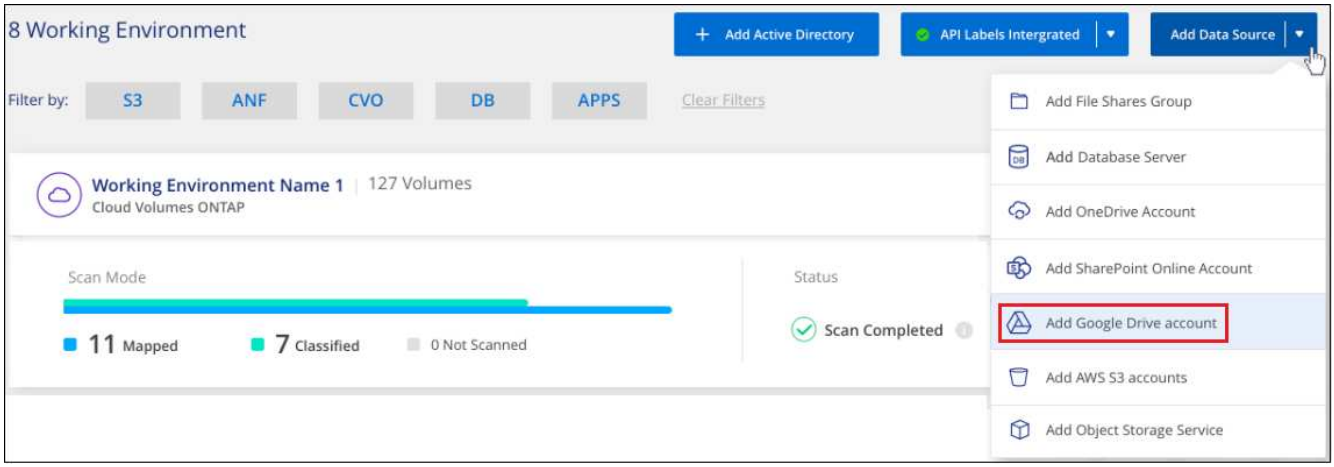
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Aggiungere l'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.

Selezionare il tipo di scansione per i dati 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.

Rimuovere 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".

Eseguire la scansione dei dati StorageGRID con classificazione BlueXP

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.

> Le seguenti informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti. + a partire dalla versione 1,31, la classificazione BlueXP fa parte dell'offerta principale di BlueXP . Per ulteriori informazioni, vedere "Eseguire la scansione dei dati StorageGRID".

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.

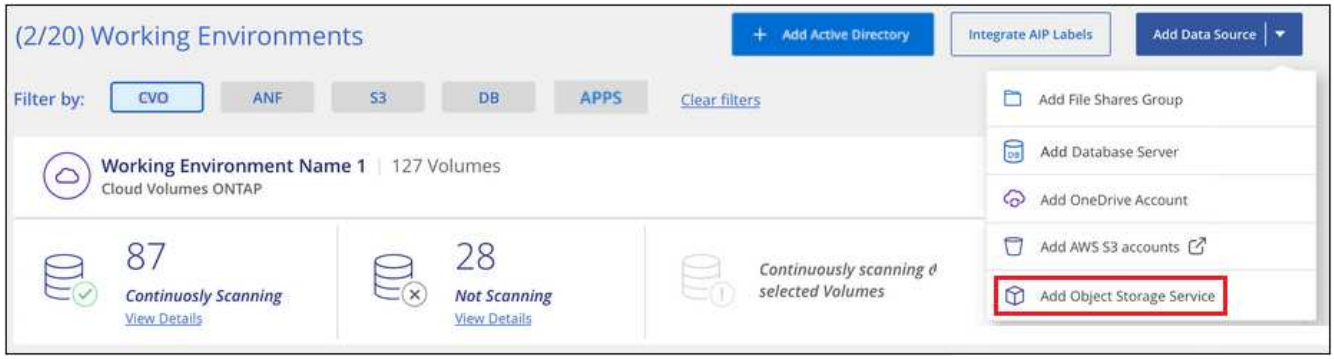
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Aggiunta del servizio di storage a oggetti alla classificazione BlueXP

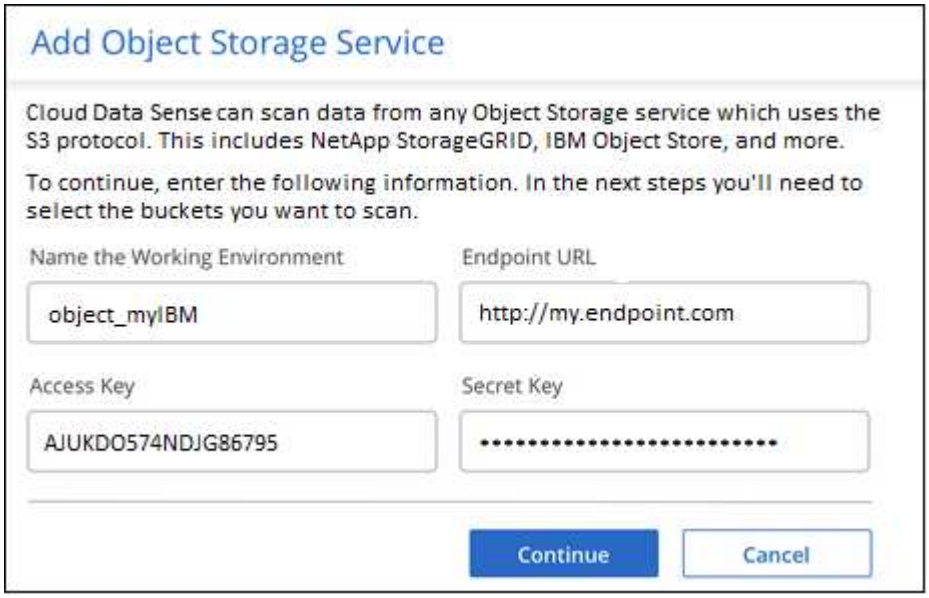
Aggiungere il servizio di storage a oggetti.

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

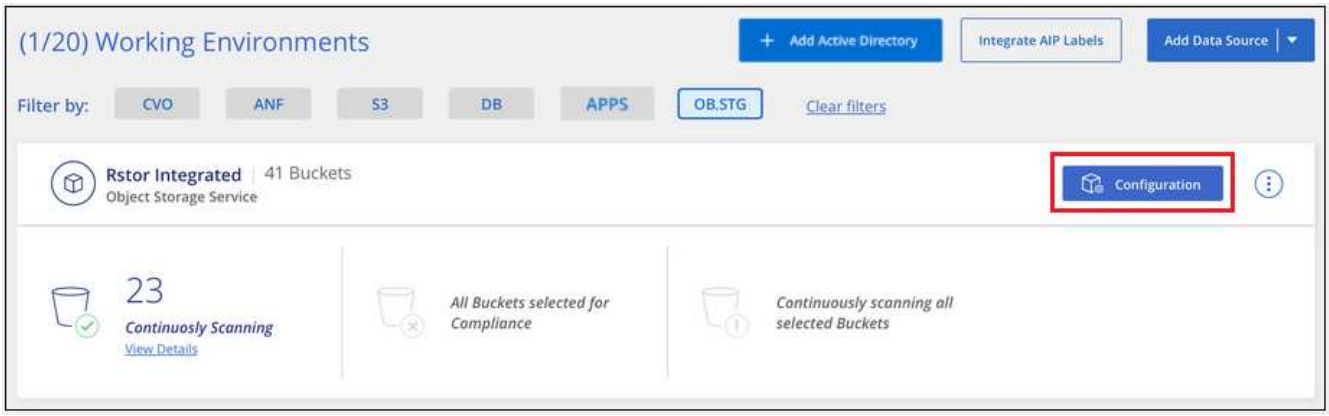
Il nuovo servizio di storage a oggetti viene aggiunto all'elenco degli ambienti di lavoro.

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

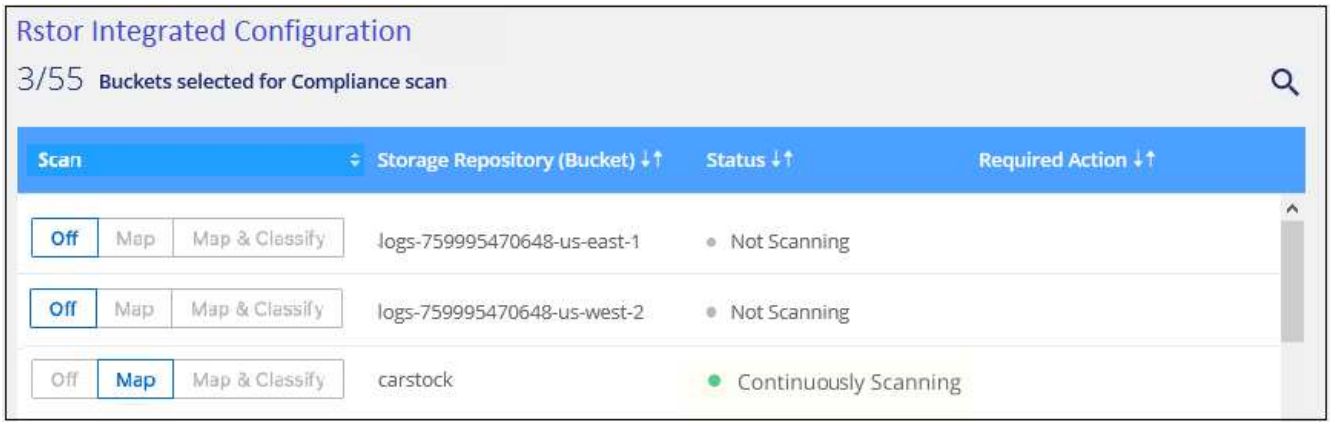
Dopo aver attivato la classificazione BlueXP sul servizio di storage a oggetti, il passaggio successivo consiste nel configurare i bucket che si desidera sottoporre a scansione. La classificazione BlueXP rileva tali bucket e li visualizza nell'ambiente di lavoro creato.

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.

Gestire le deprecazioni dei dati

Visualizza i dettagli di governance dei tuoi dati utilizzando il dashboard di governance della classificazione BlueXP

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 hai in programma di migrare i dati da posizioni on-premise nel cloud, puoi vedere le dimensioni dei dati e se alcuni di essi contengono informazioni sensibili prima di spostarli.

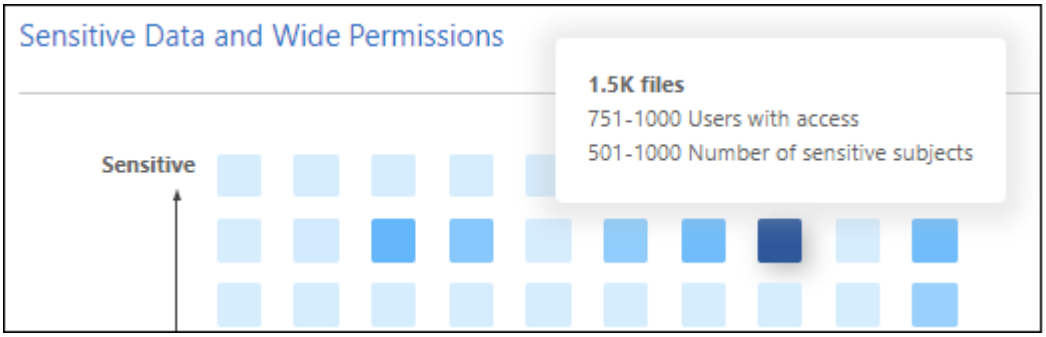
NOTA queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

Dati elencati in base alla sensibilità e alle autorizzazioni estese nel dashboard Governance

L'area *dati sensibili e permessi estesi* sul dashboard Governance fornisce una mappa 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.

Ciò si applica alla classificazione BlueXP versioni 1,30 e precedenti.

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 riportata di seguito mostra il testo della descrizione dei comandi 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.

Area di classificazione sul cruscotto che mostra le etichette AIP

L'area *Classification* sul dashboard fornisce un elenco delle etichette AIP (Azure Information Protection) più identificate nei dati sottoposti a scansione.

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.

Organizza i tuoi dati privati con la classificazione BlueXP

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.

Queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

- 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.
- 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.
- Con la funzionalità di ricerca salvata, 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).

Tag	Etichette
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.
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 nel progetto o 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" nel progetto o nell'area di lavoro BlueXP .

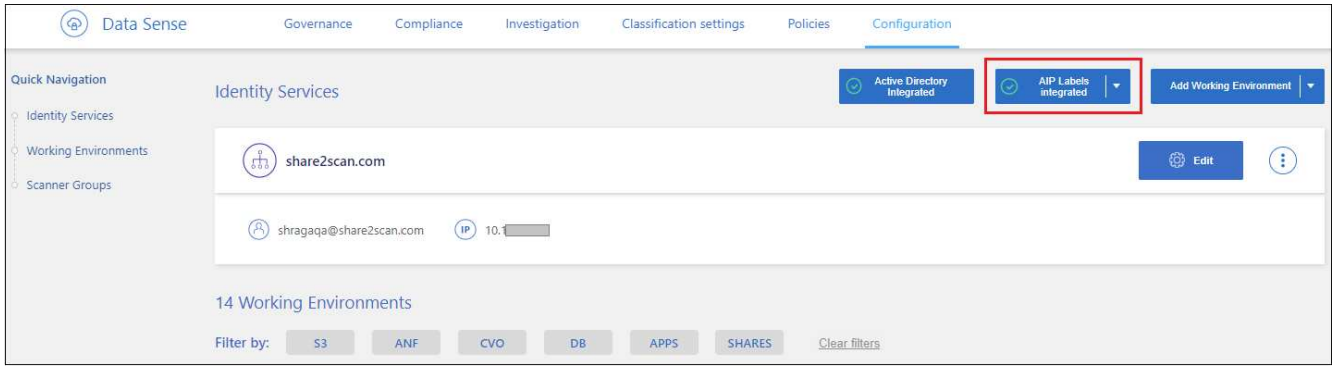
Requisiti

- 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.

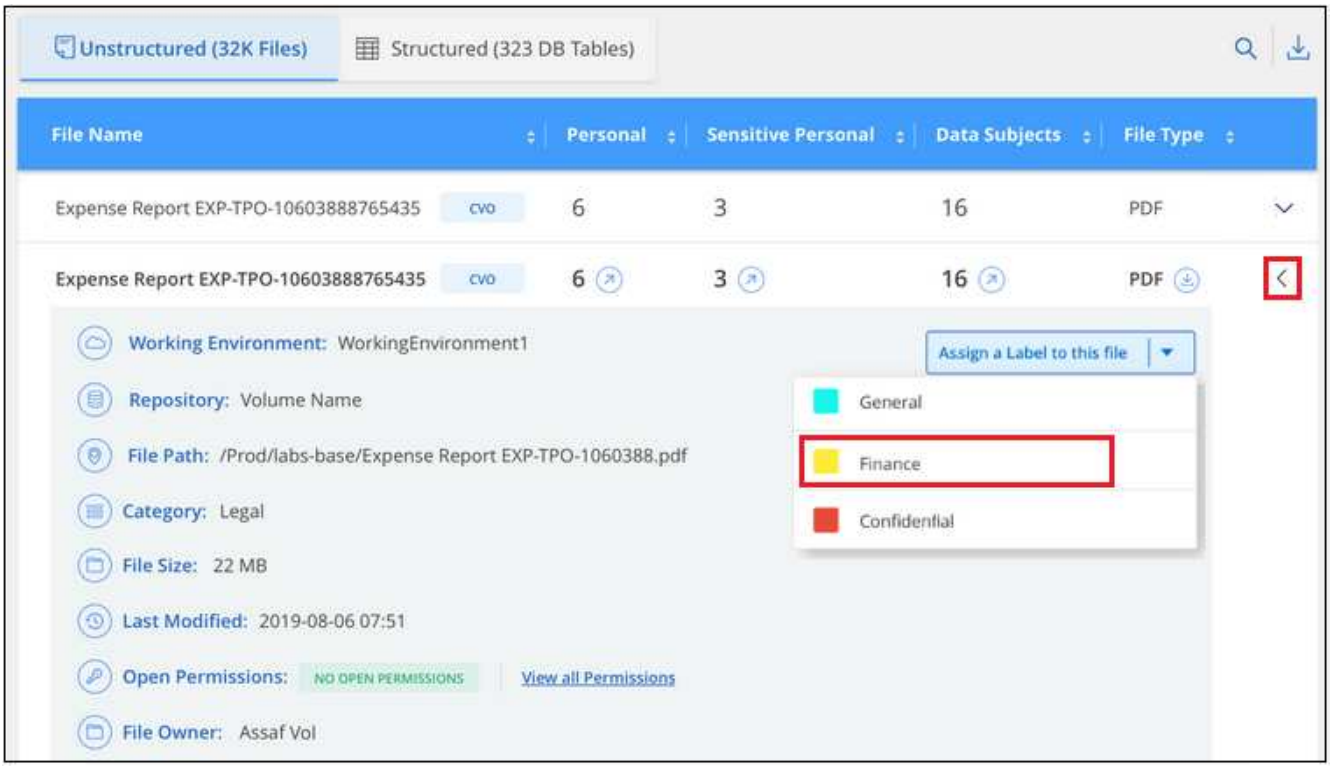
Assegnare manualmente le etichette AIP

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.

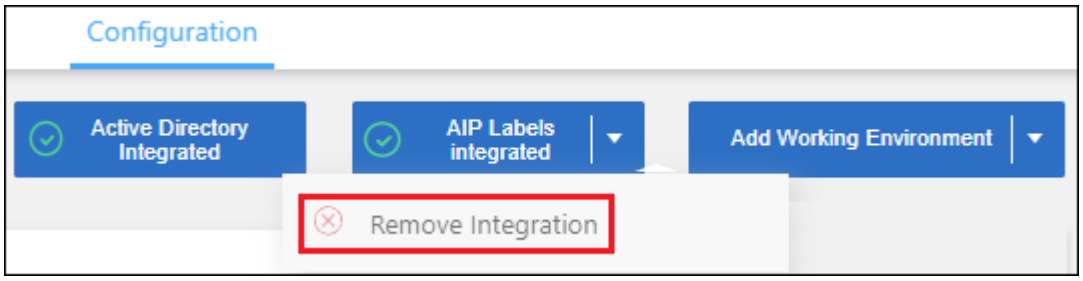
Rimuovere l'integrazione AIP

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.

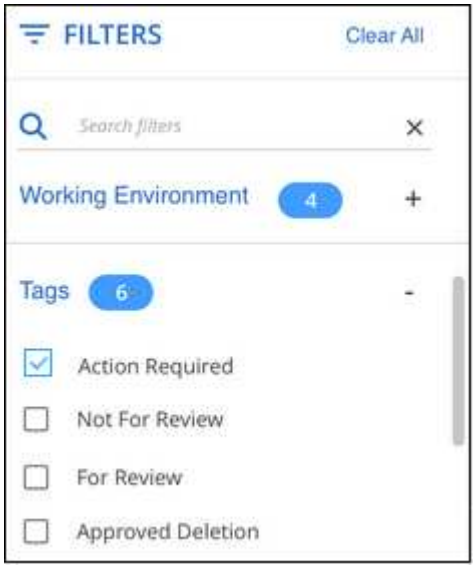
Tenere presente che il tag non viene aggiunto al file allo stesso modo in cui le etichette AIP fanno parte dei metadati del file. Il tag è appena visto dagli utenti di BlueXP che utilizzano la classificazione BlueXP in modo da poter vedere se un file deve essere cancellato o controllato per un certo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

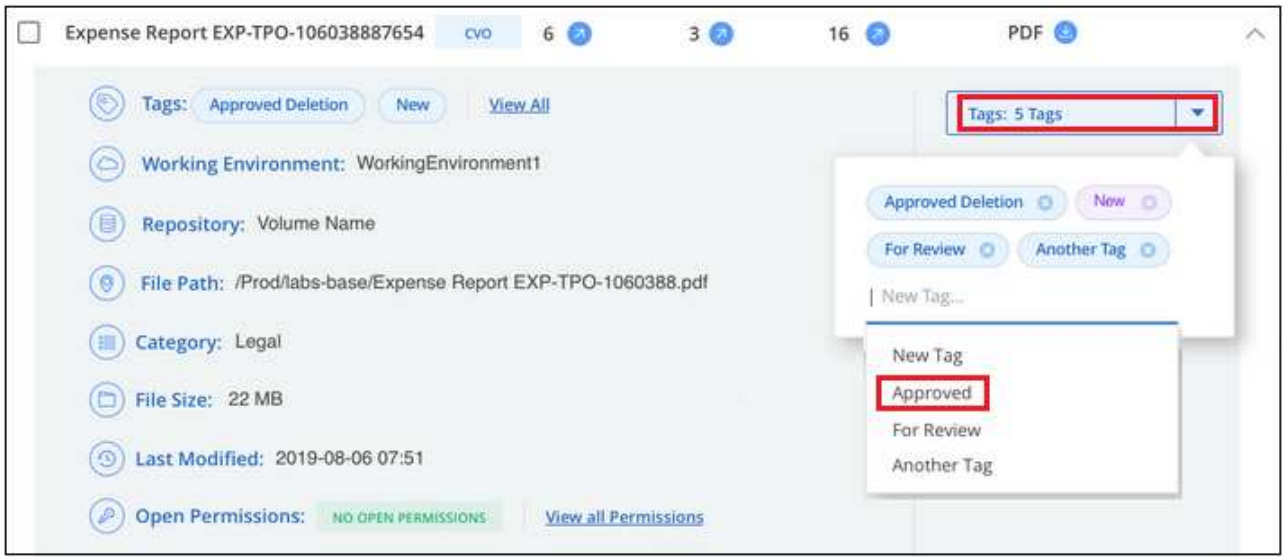
Per aggiungere un tag a un singolo file:

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

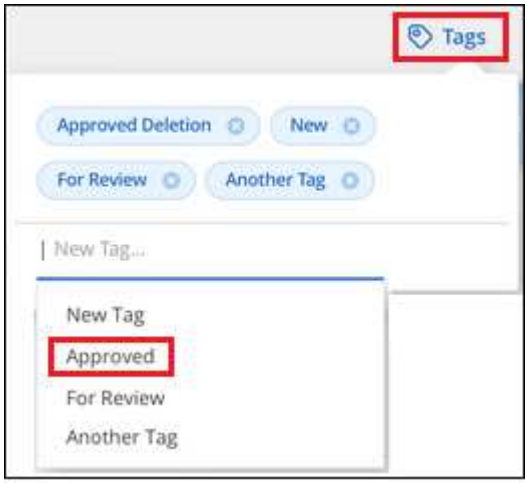
1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da contrassegnare.

   - 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).

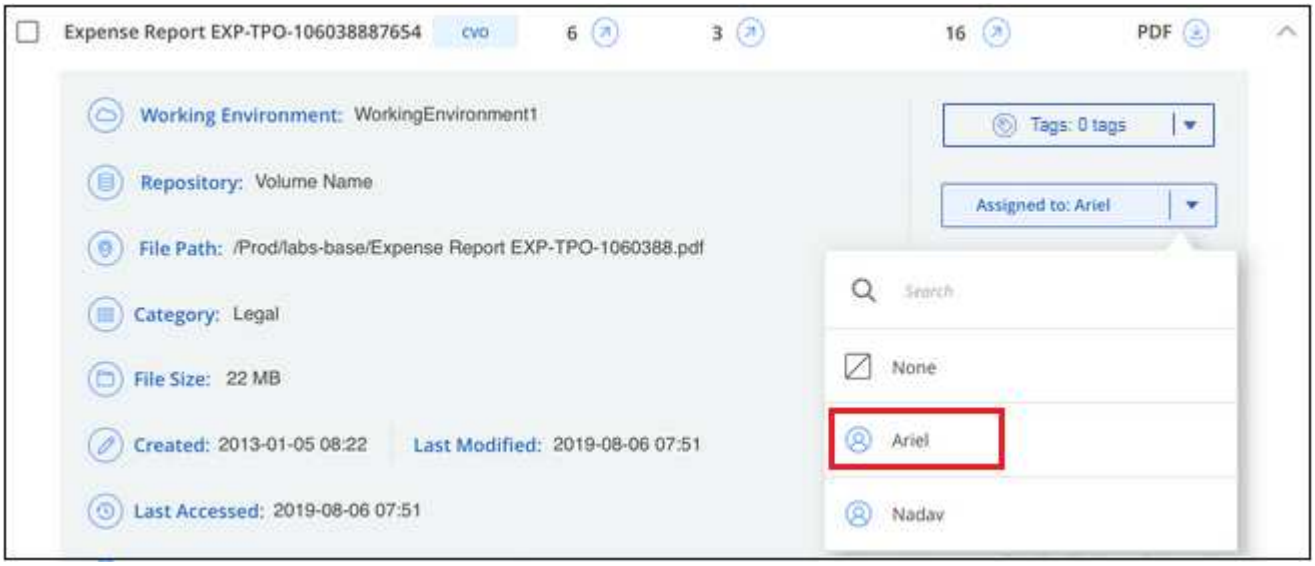
Si noti che il nome utente non viene aggiunto al file come parte dei metadati del file, ma viene visualizzato solo dagli utenti BlueXP quando si utilizza la classificazione BlueXP.

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.

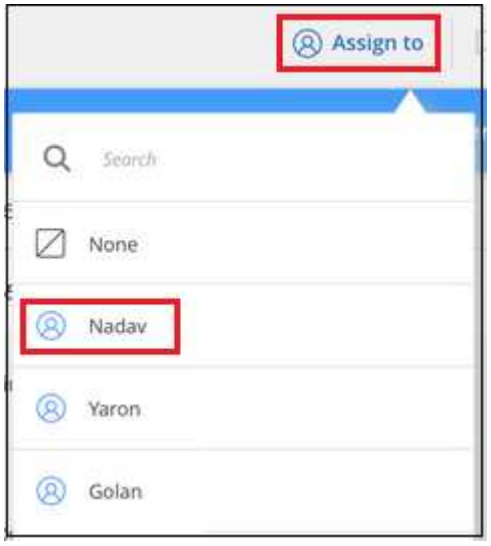
Per assegnare un utente a più file, procedere come segue. Nota: È possibile assegnare un utente a un massimo di 20 file alla volta (una pagina nell'interfaccia utente).

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.

Gestisci i tuoi dati privati con la classificazione BlueXP

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.

> Queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

- 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

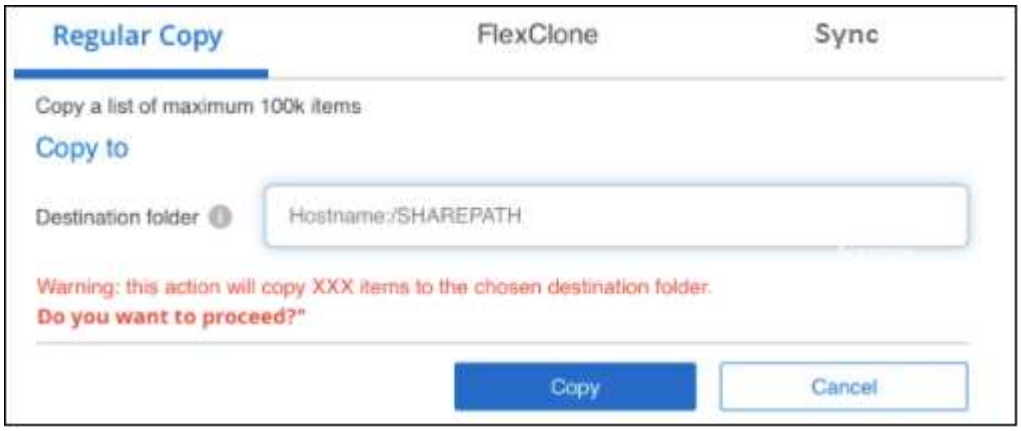
- Per copiare i file è necessario disporre delle autorizzazioni. "Informazioni sull'accesso degli utenti alle informazioni sulla conformità" .
- La copia dei file richiede che la condivisione NFS di destinazione consenta l'accesso dall'istanza di classificazione BlueXP.
- È possibile copiare da 1 a 100,000 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.

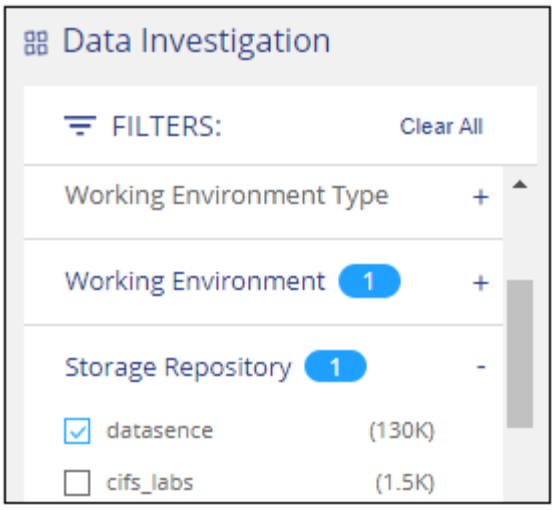
Nota: i volumi FlexGroup non possono essere clonati perché non sono supportati da FlexClone.

Requisiti

- Per copiare i file è necessario disporre delle autorizzazioni. "Informazioni sull'accesso degli utenti alle informazioni sulla conformità" .
- 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.

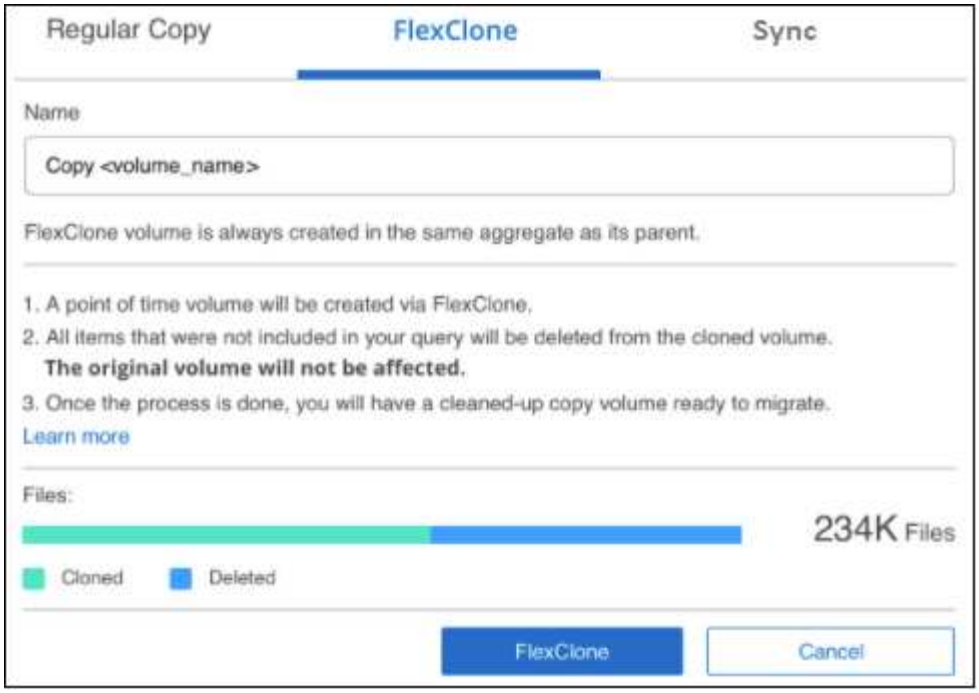


Applicare eventuali altri filtri in modo da visualizzare solo i file che si desidera clonare nel nuovo volume.

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 delle autorizzazioni. "Informazioni sull'accesso degli

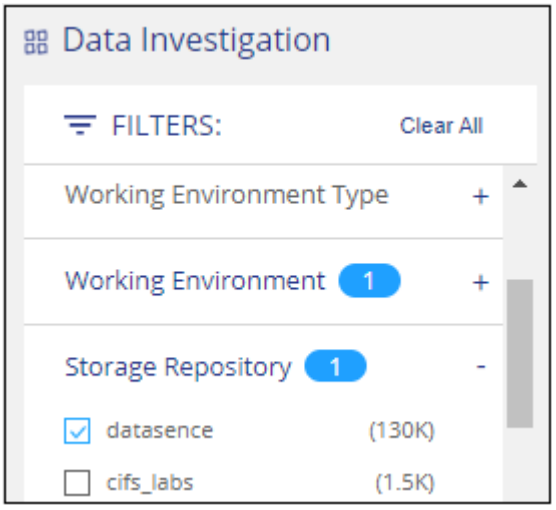
utenti alle informazioni sulla conformità" .

- 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.

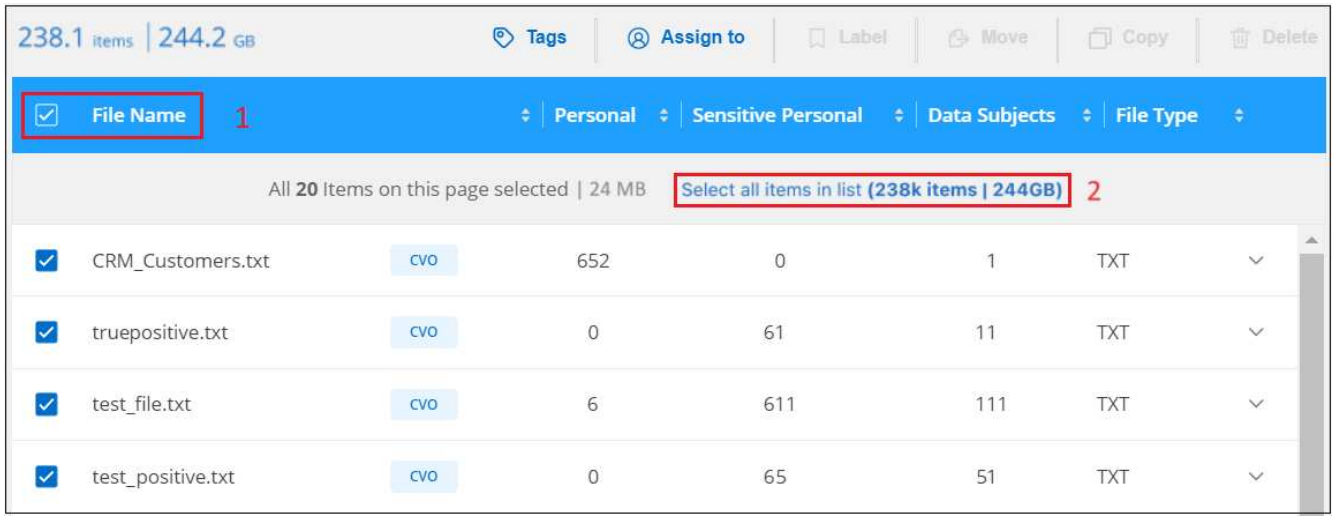


   Applicare eventuali altri filtri in modo da visualizzare solo i file che si desidera copiare e sincronizzare nel sistema di destinazione.

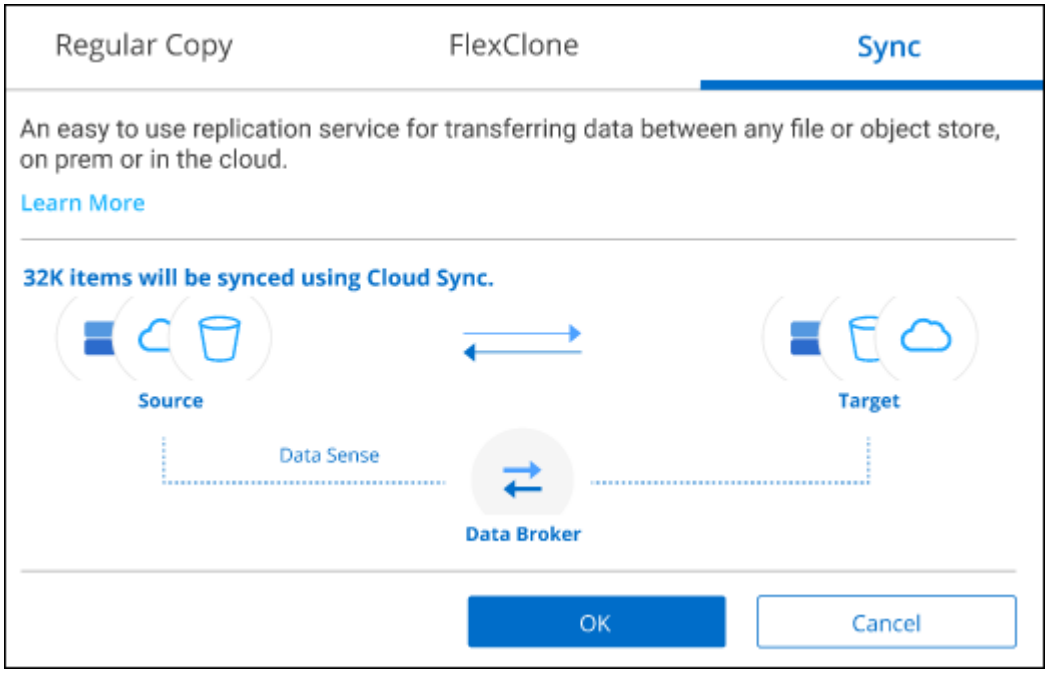
2. Nel riquadro dei risultati dell'analisi, selezionare tutti i file su tutte le pagine selezionando la casella nella riga del titolo (

), 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 delle autorizzazioni. "Informazioni sull'accesso degli utenti alle informazioni sulla conformità" .
- 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.

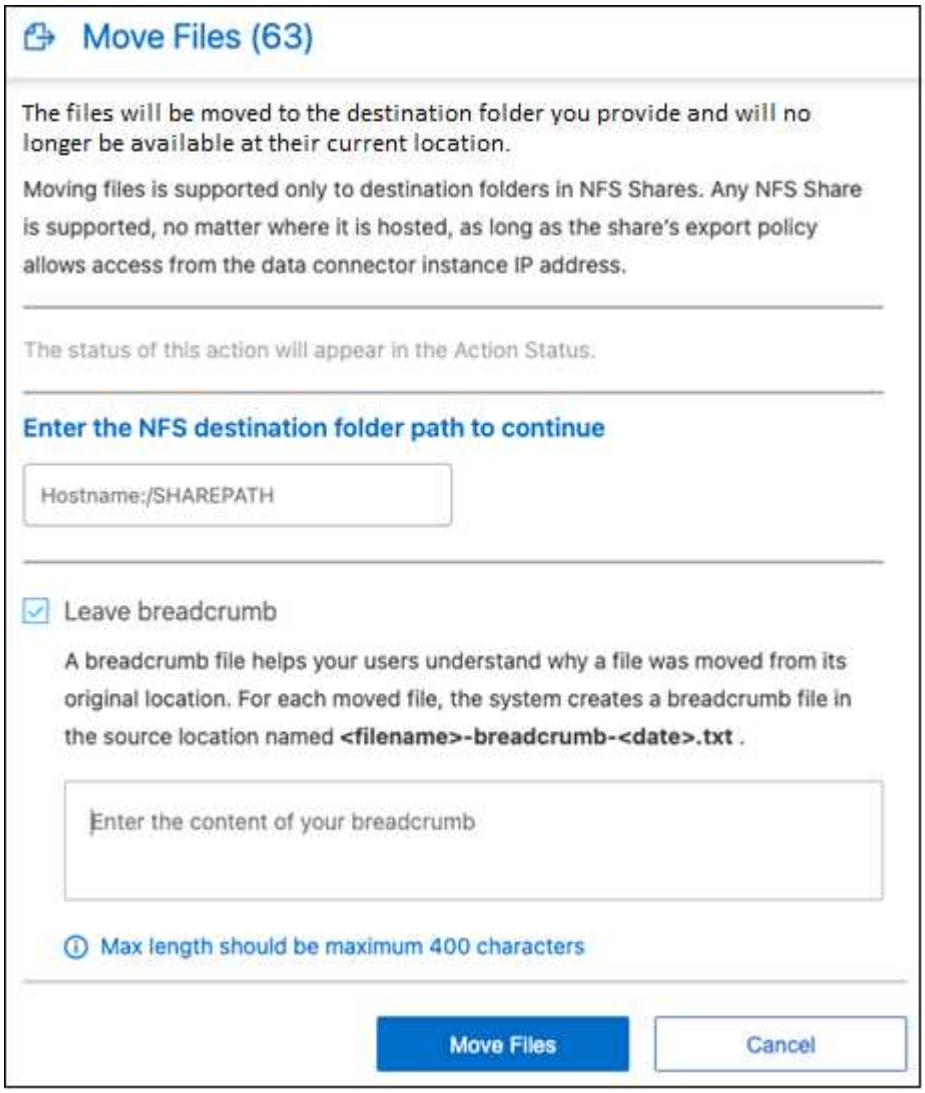
Fasi

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.

> 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 delle autorizzazioni. "Informazioni sull'accesso degli utenti alle informazioni sulla conformità" .
- 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).

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.

> Per creare una classificazione personalizzata nella versione 1,43 e successive, vedere Creare una classificazione personalizzata.

> Queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

- 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.

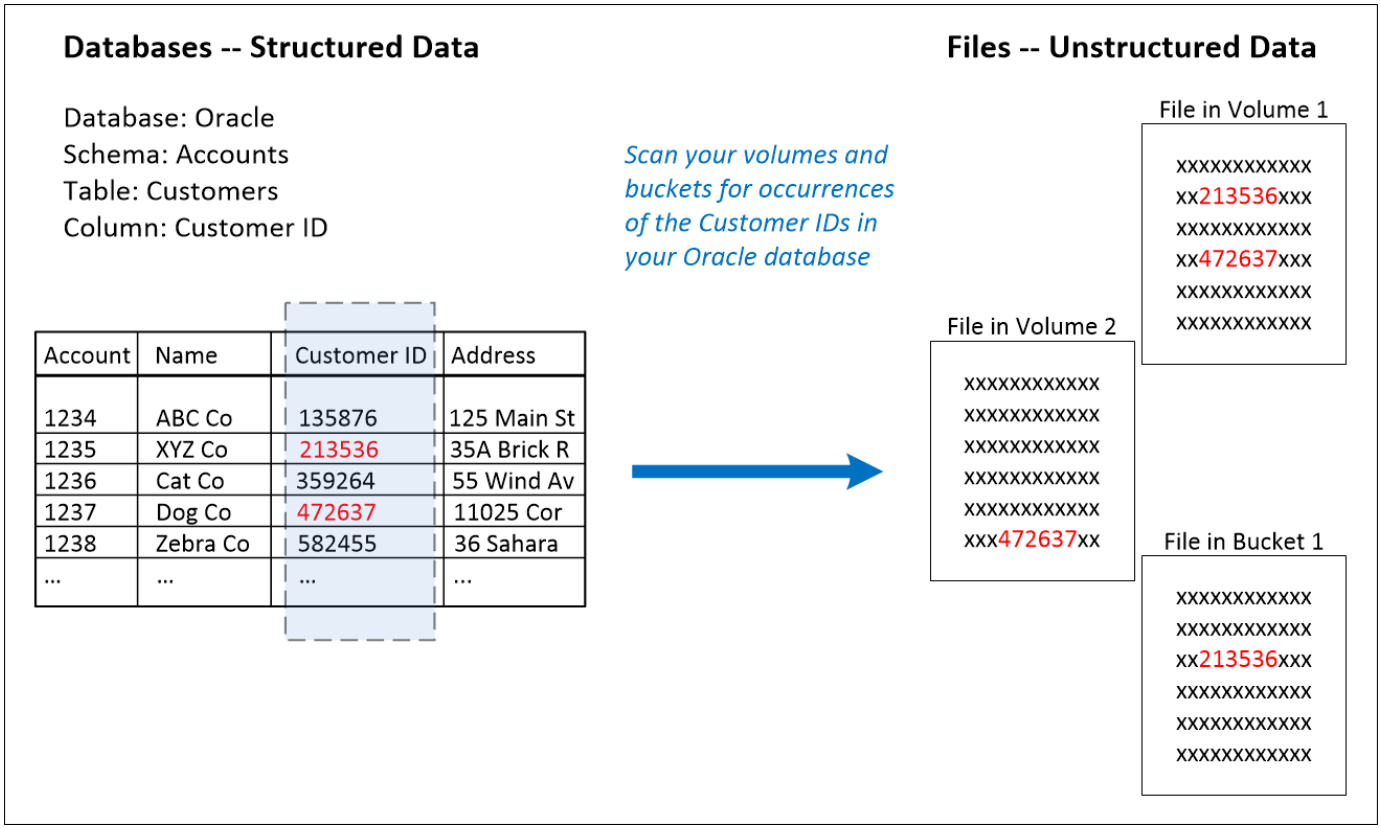
- È possibile aggiungere categorie personalizzate per identificare dove si trovano categorie specifiche di informazioni nei dati.

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

Data Fusion consente di eseguire la scansione dei dati dell'organizzazione 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 cercherà 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.



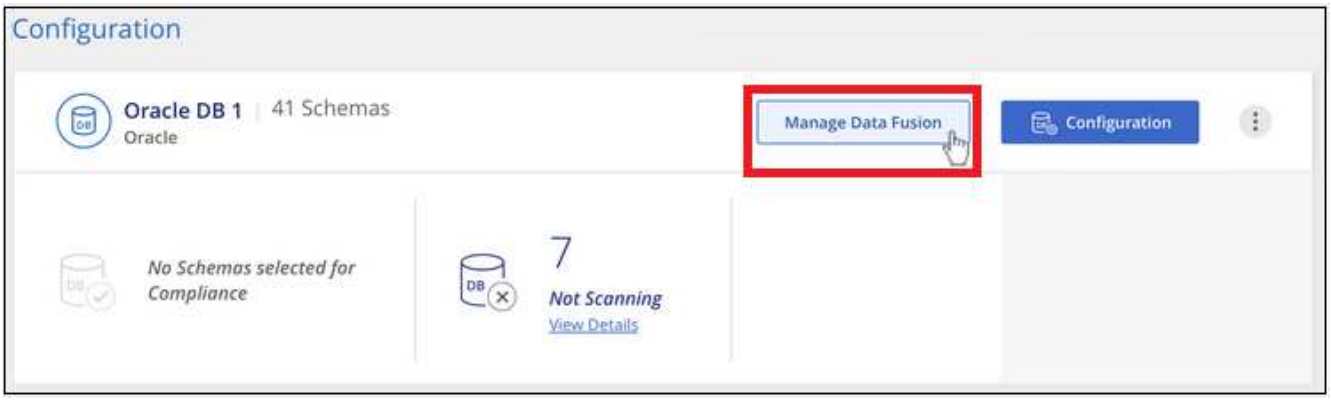
Come puoi vedere, sono stati trovati due ID cliente univoci in due volumi e in un bucket S3. Verranno identificate anche le corrispondenze presenti nelle tabelle del database.

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.



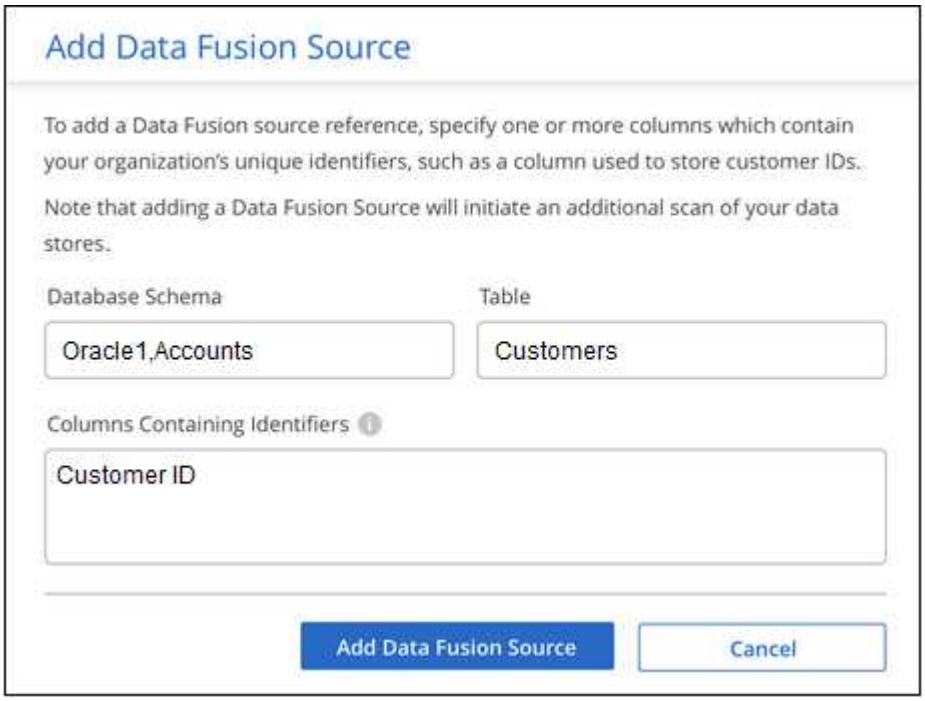
2. Fare clic su **Add Data Fusion source** (Aggiungi origine dati) nella pagina successiva.
3. Nella pagina *Aggiungi origine data Fusion*:

   a. Selezionare lo schema del database dal menu a discesa.

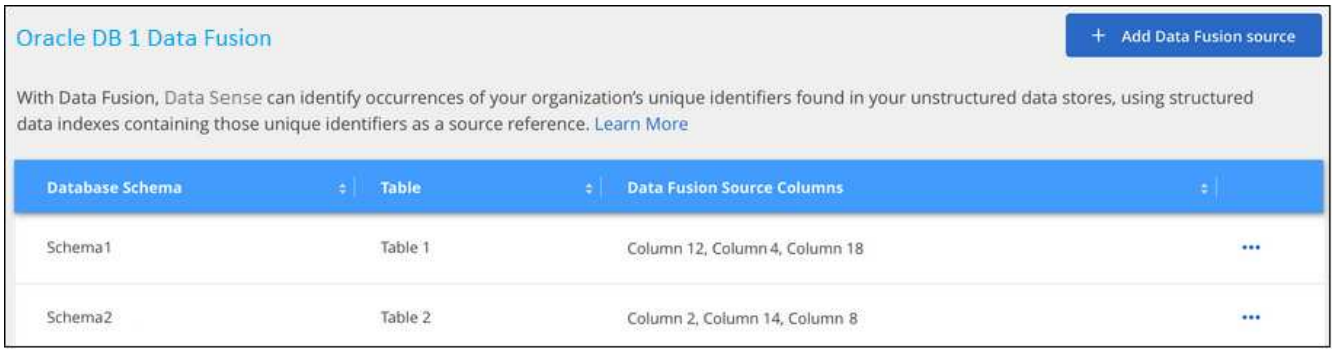
   b. Inserire il nome della tabella nello schema.

   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.

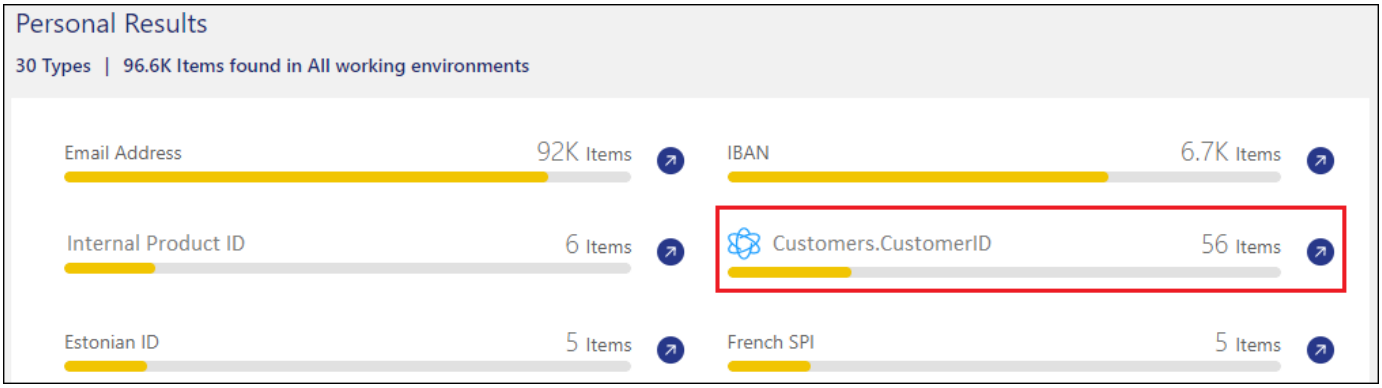


4. Fare clic su **Aggiungi origine Data Fusion**.



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.

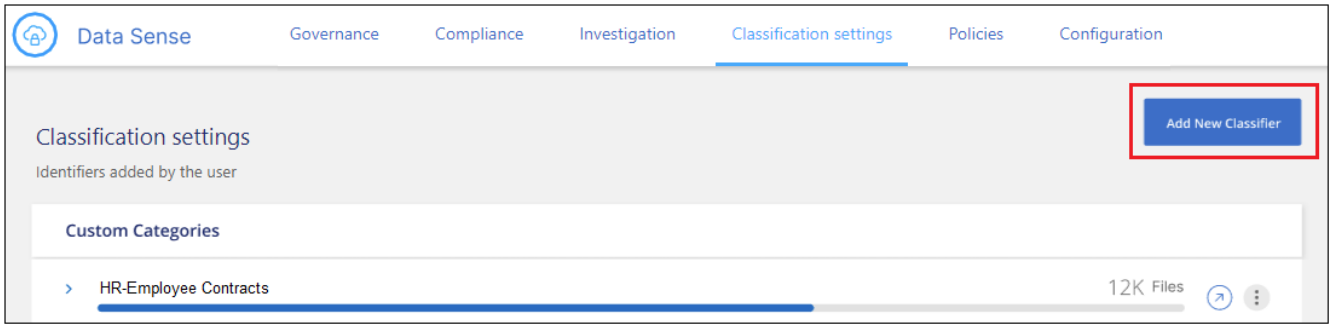
Ad esempio, è possibile visualizzare i nomi dei prodotti interni in tutti i file per assicurarsi che non siano accessibili in posizioni non sicure.

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

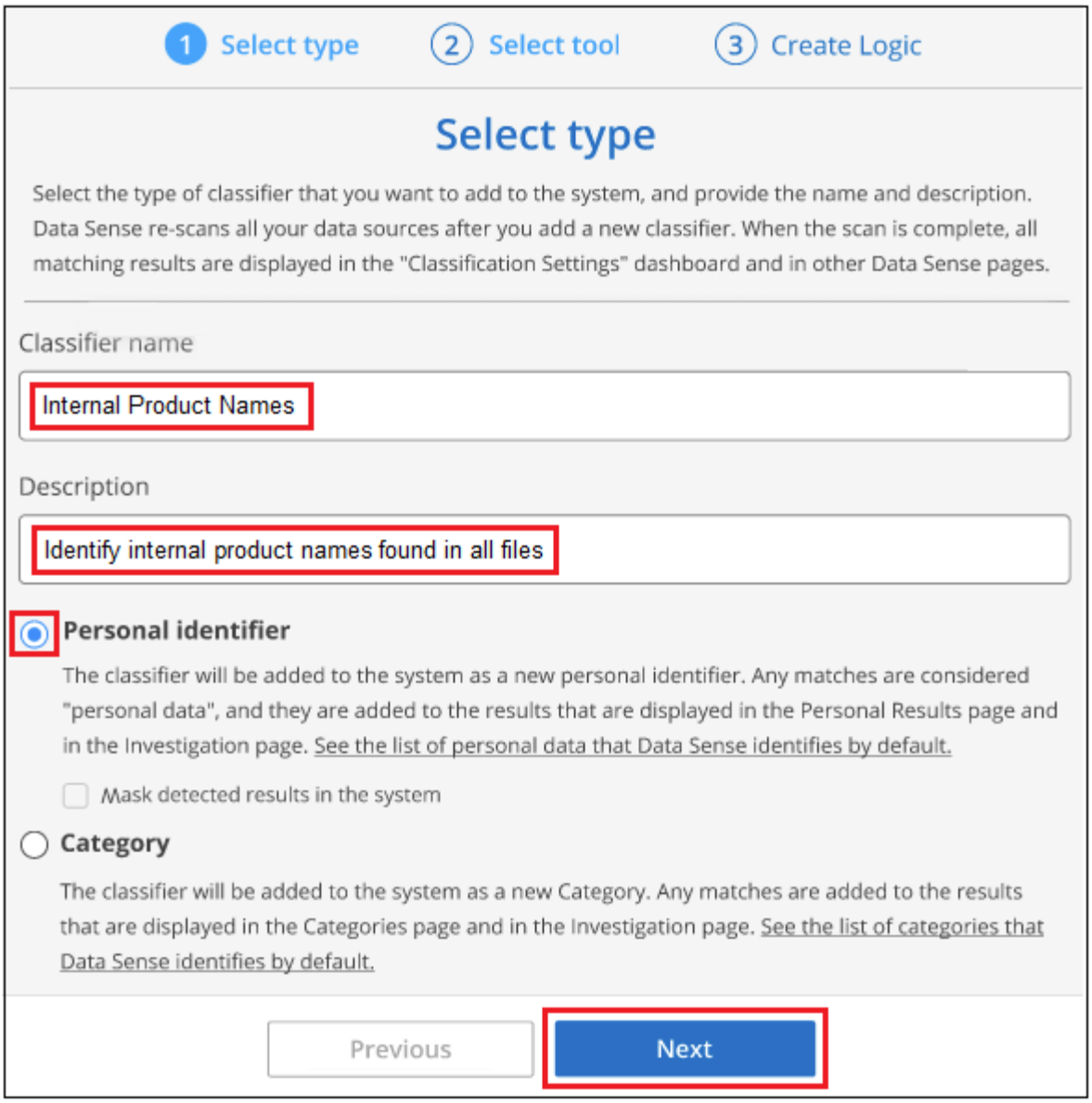
1. Dalla scheda *Impostazioni classificazione*, fare clic su **Aggiungi nuovo classificatore** per avviare la procedura guidata *Aggiungi classificatore personalizzato*.



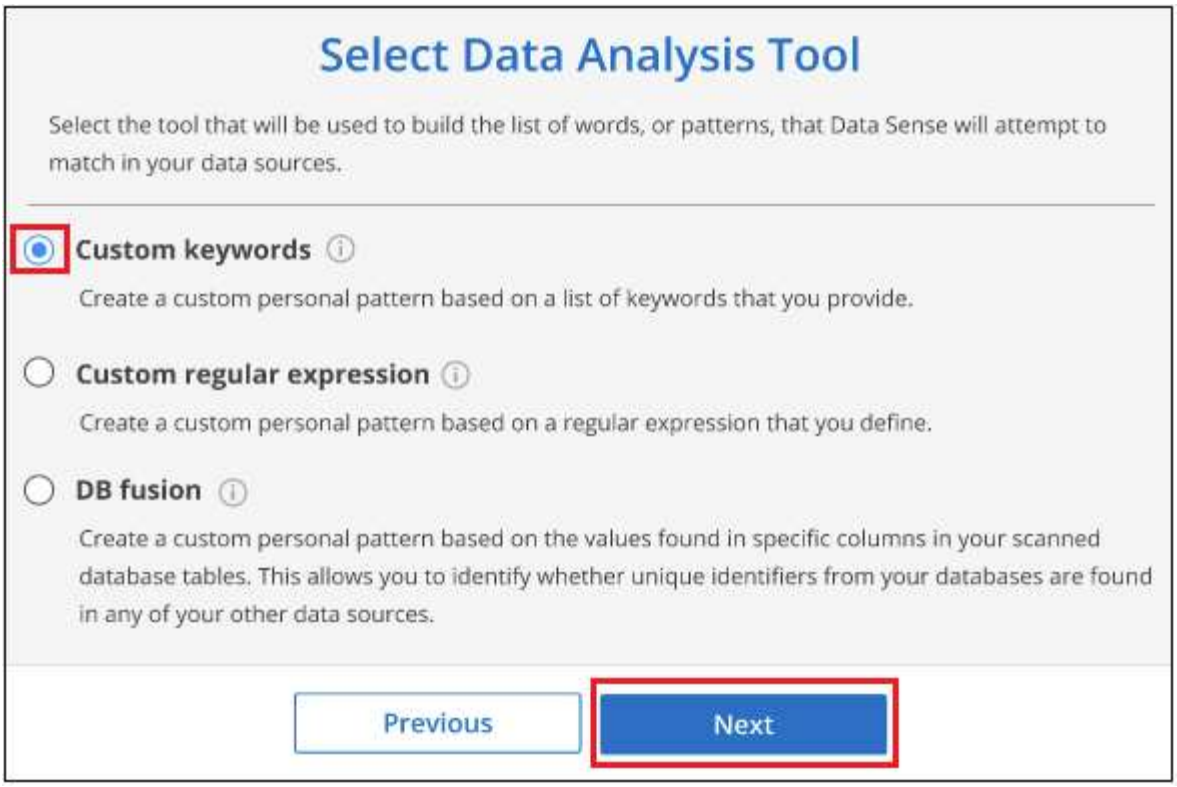
2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Personal identifier**, quindi fare clic su **Next**.

   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).

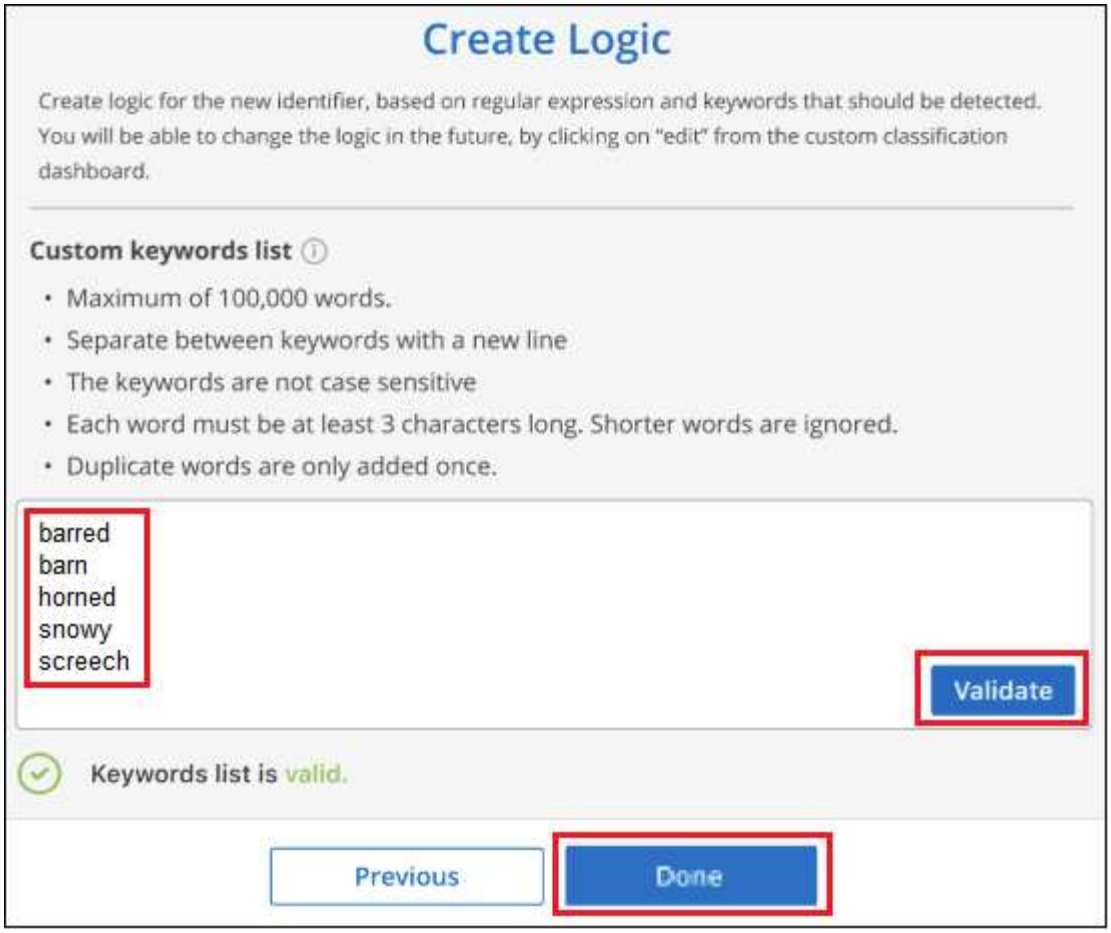


3. Nella pagina *Select Data Analysis Tool*, selezionare **Custom Keywords** come metodo da utilizzare per definire il classificatore, quindi fare clic su **Next**.



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

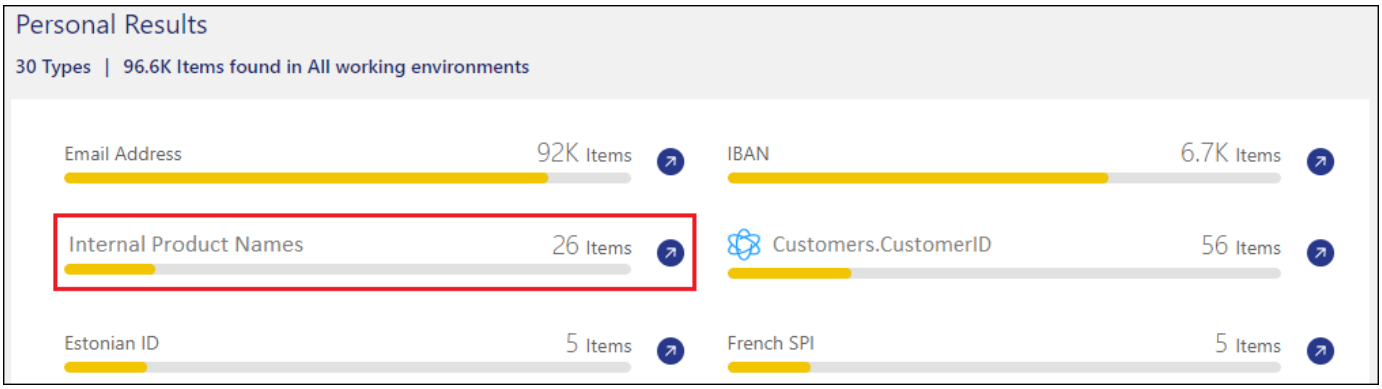
   La schermata seguente mostra i nomi dei prodotti interni (diversi tipi di gufi). La ricerca della classificazione BlueXP per questi elementi non fa distinzione tra maiuscole e minuscole.



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**.

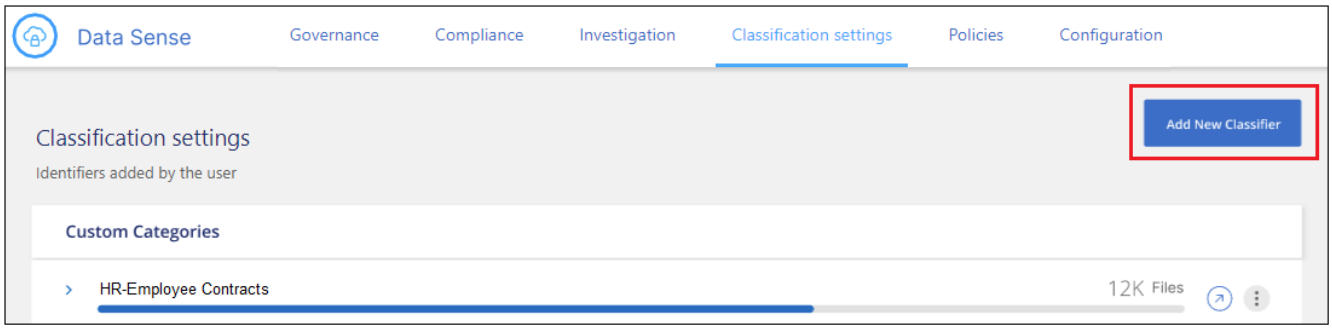
Dopo aver aggiunto il regex, la classificazione BlueXP riavvia la scansione di tutte le origini dati. Una volta completata la scansione, i nuovi risultati verranno visualizzati nella dashboard di conformità della classificazione BlueXP nella sezione "risultati personali" e nella pagina delle indagini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

> La classificazione BlueXP non supporta i flag di pattern quando si crea un regex. Ciò significa che non si dovrebbe utilizzare "/".

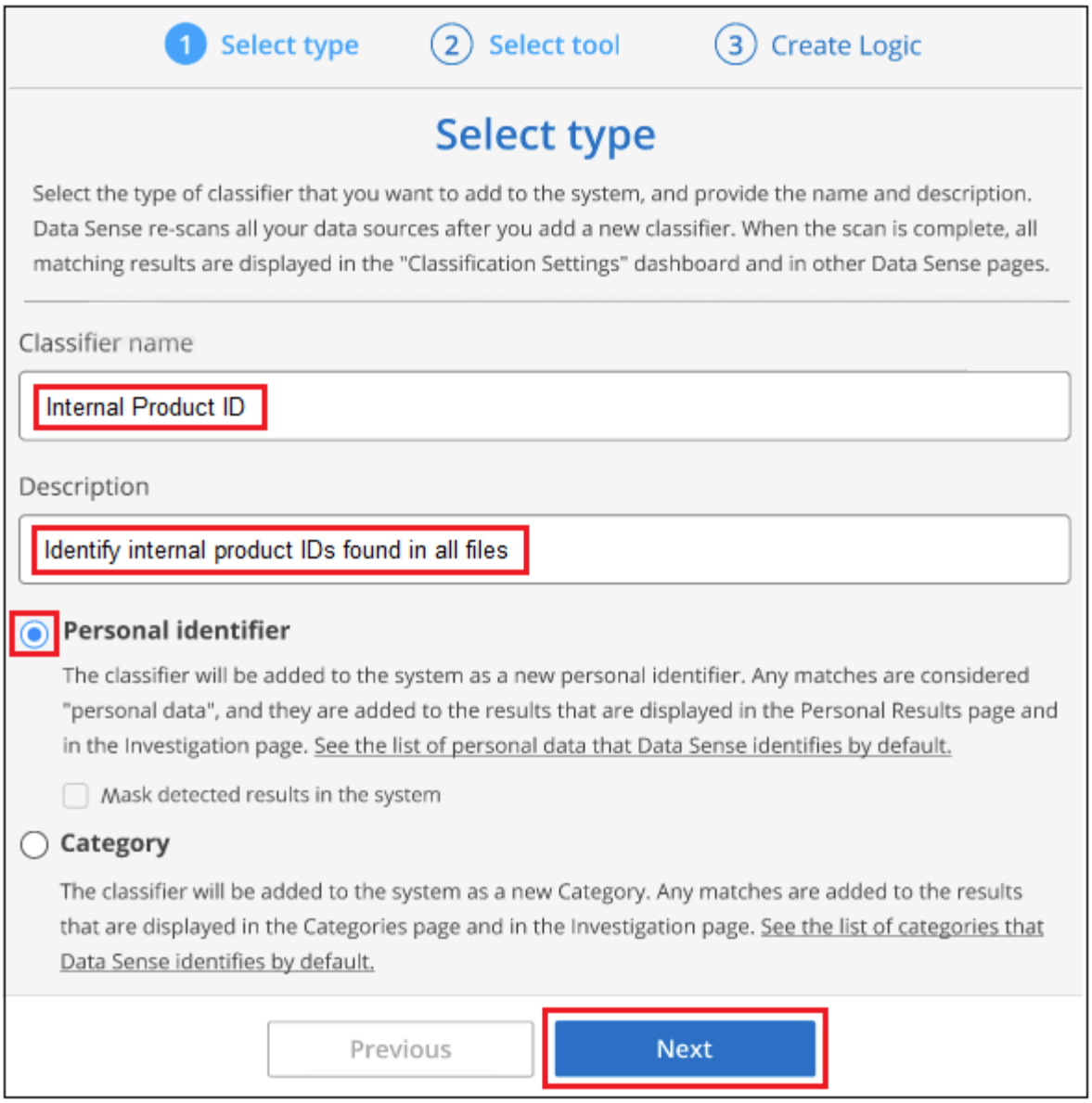
Fasi

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

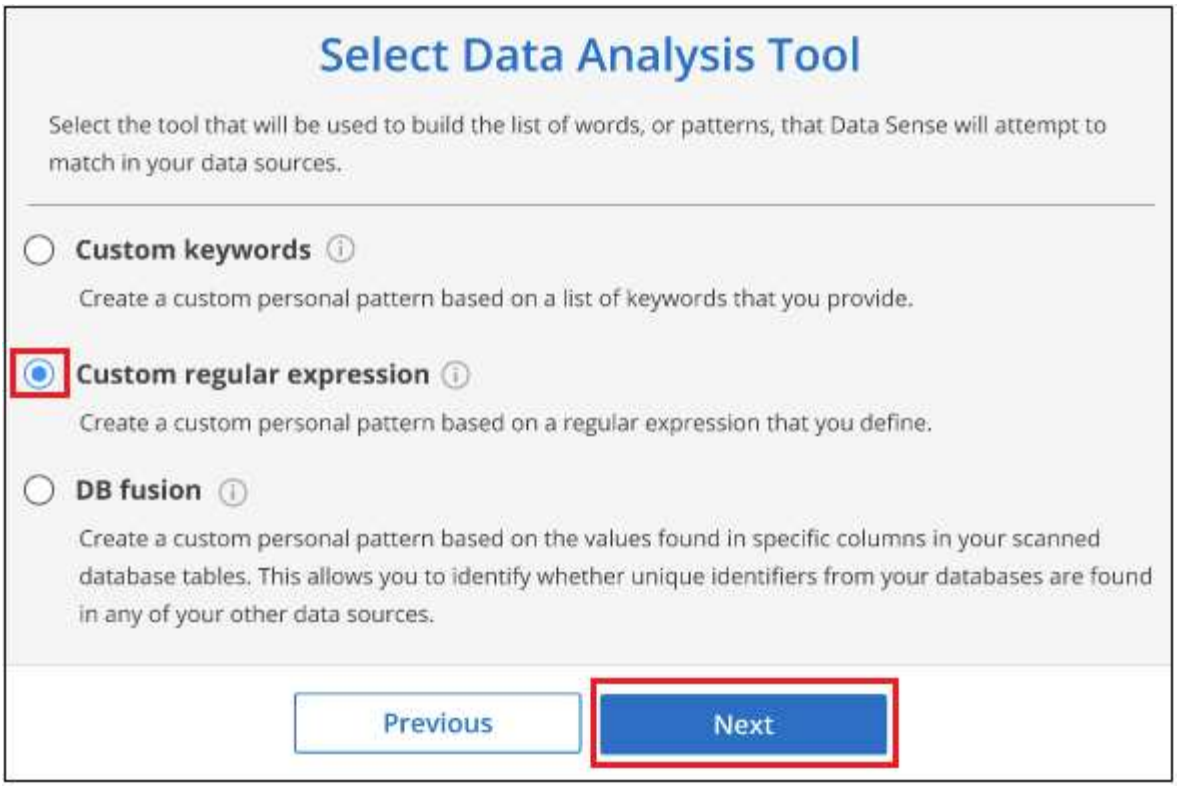


2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Personal identifier**, quindi fare clic su **Next**.

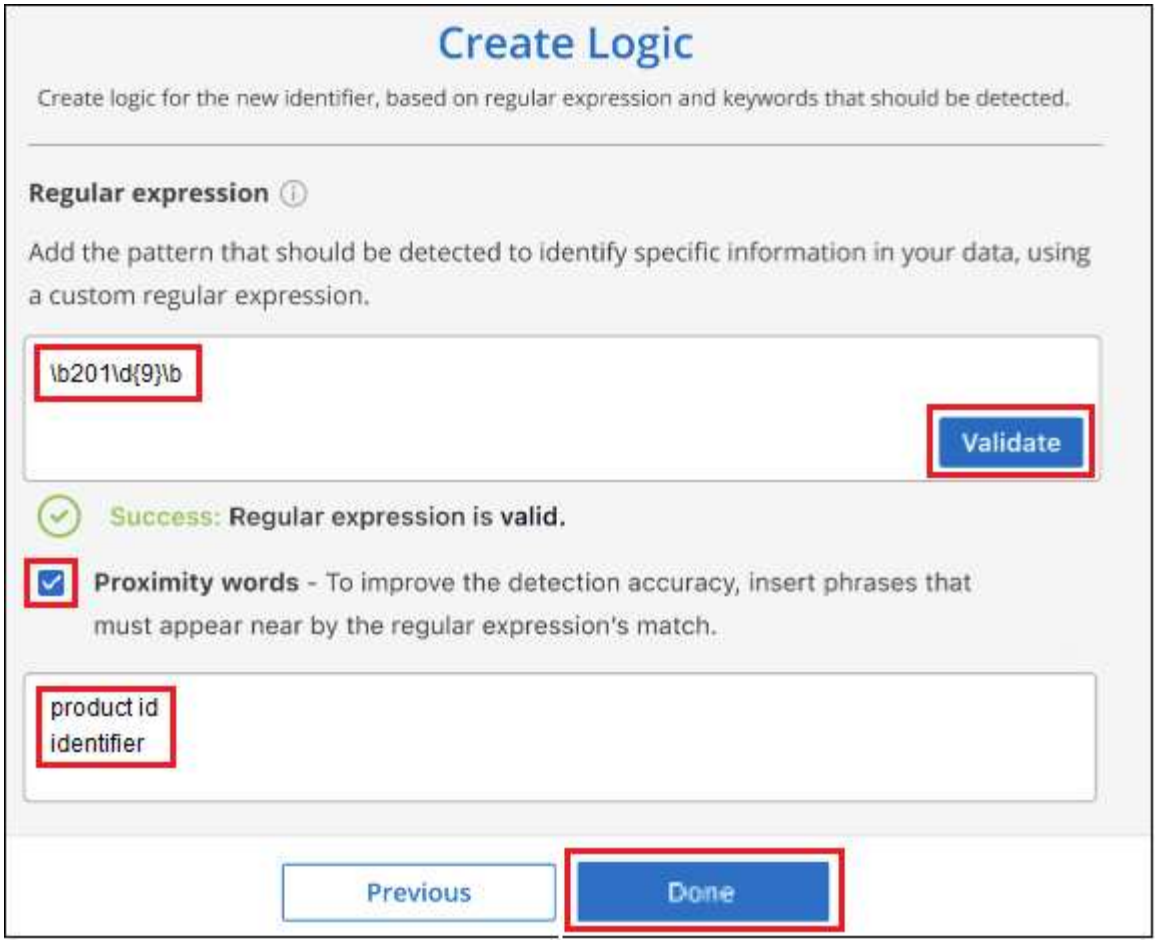
   Il nome immesso viene visualizzato nell'interfaccia utente di classificazione BlueXP come intestazione per i file sottoposti a scansione che corrispondono ai requisiti del classificatore e come nome del filtro nella pagina di analisi. Puoi anche selezionare la casella "Mask Detected Results in the system" (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**.

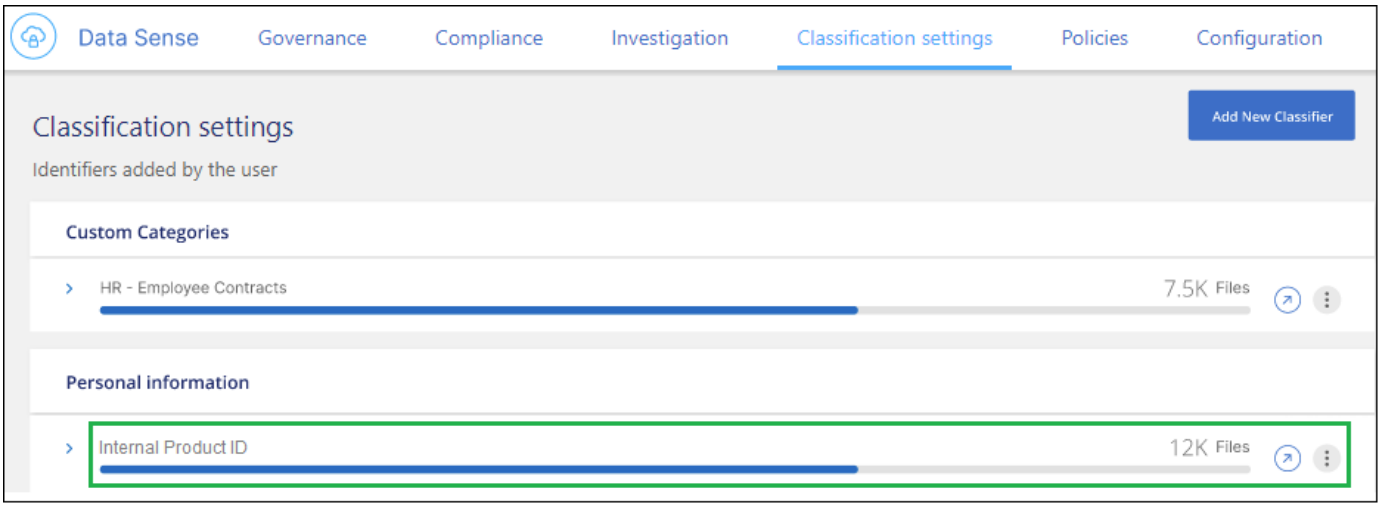


4. Nella pagina *Create Logic*, immettere l'espressione regolare e le parole di prossimità, quindi fare clic su **Done**.
   a. È possibile immettere qualsiasi espressione regolare legale. Fare clic sul pulsante **Validate** (convalida) per verificare che la classificazione BlueXP sia valida e che non 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".

Prima di iniziare

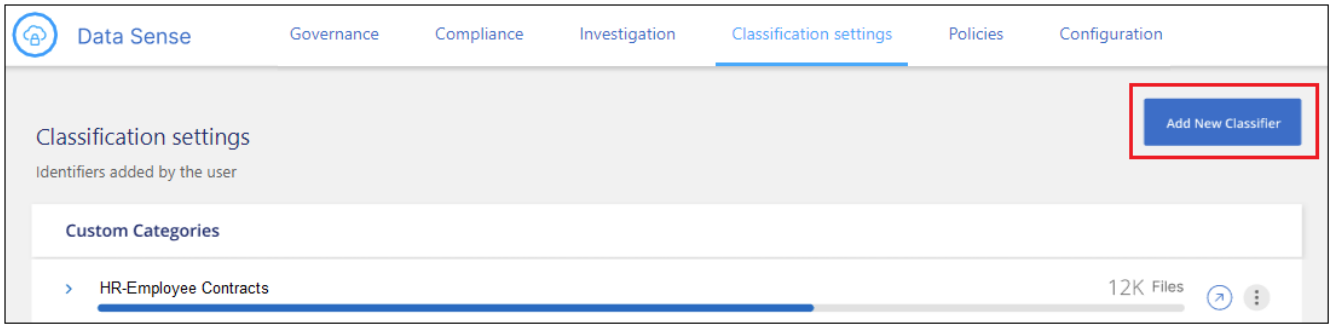
È necessario creare un minimo di 25 file di training contenenti esempi delle categorie di dati che si desidera vengano riconosciute dalla classificazione BlueXP. Sono supportati i seguenti tipi di file:

```
.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.

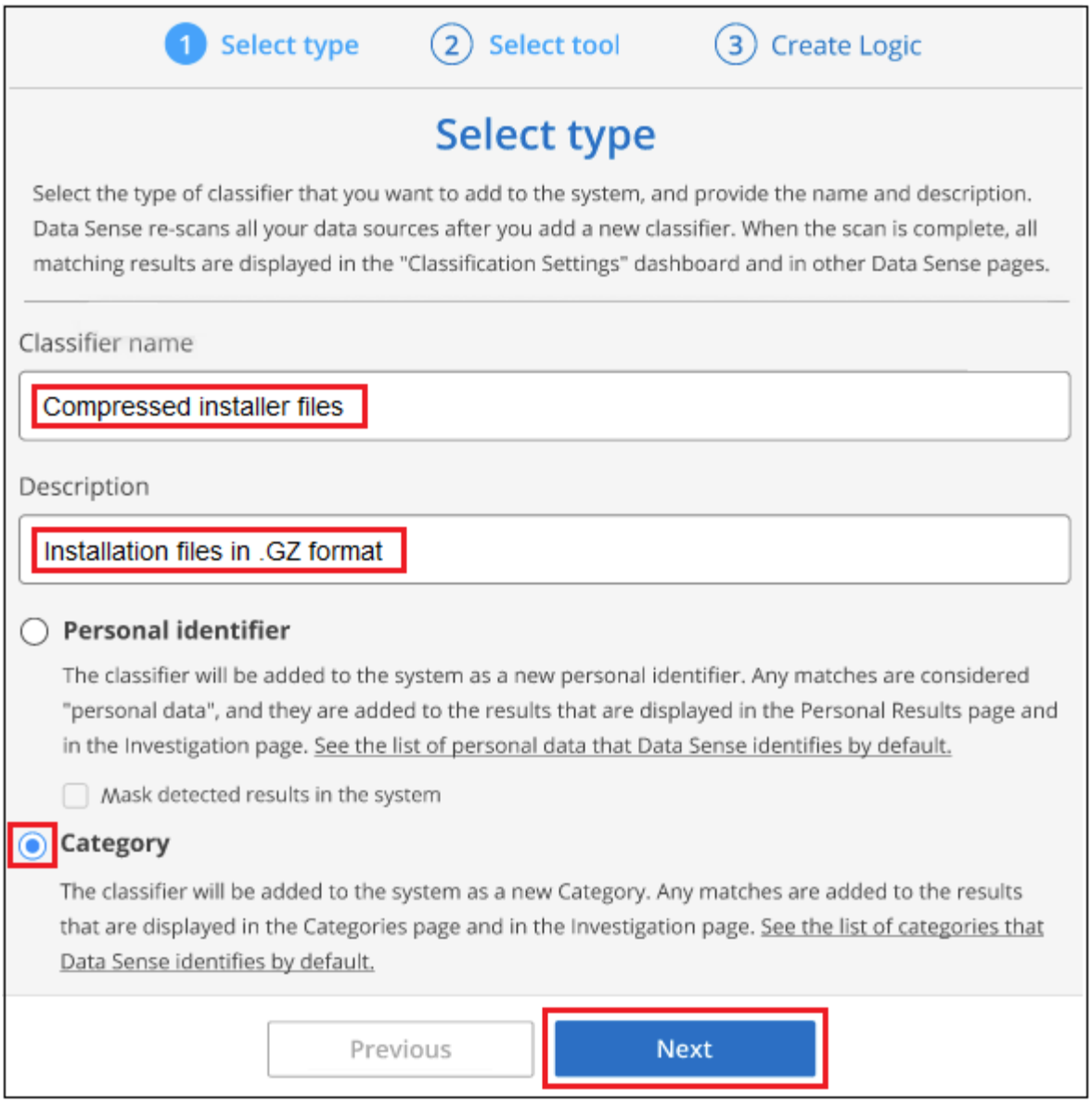
Fasi

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

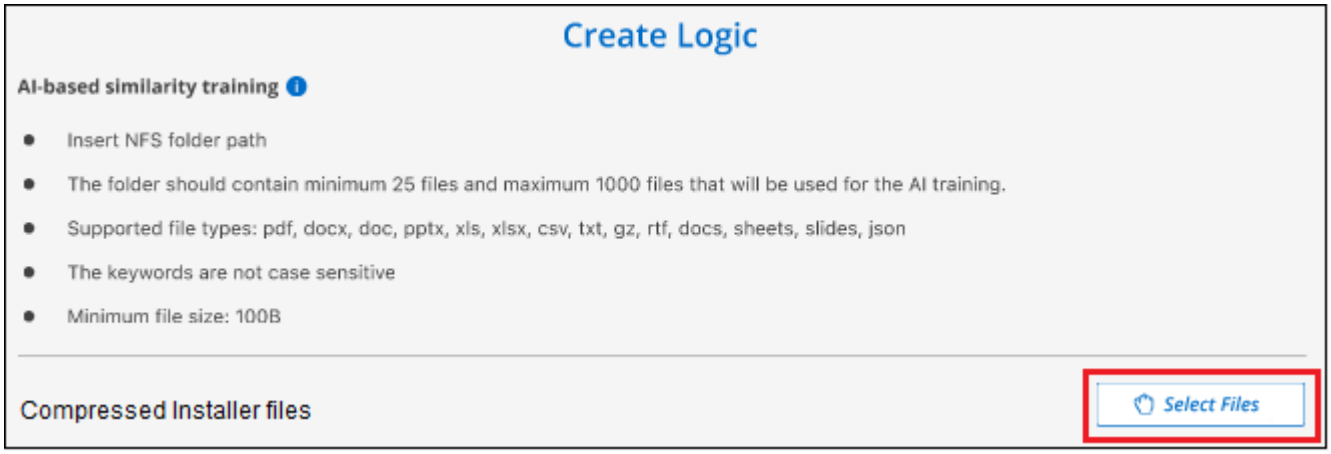


2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Category**, quindi fare clic su **Next**.

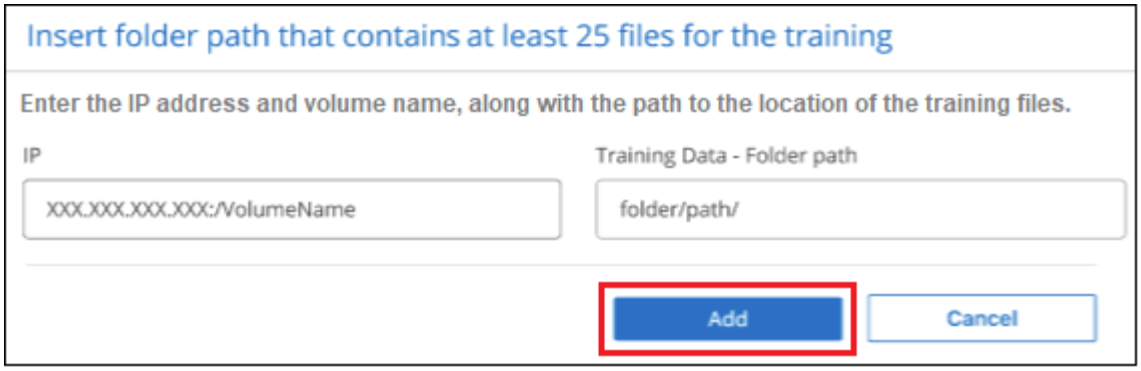
   Il nome immesso viene visualizzato nell'interfaccia utente di classificazione BlueXP come intestazione per i file sottoposti a scansione che corrispondono alla categoria di dati che si sta definendo e come nome del filtro nella pagina di analisi.



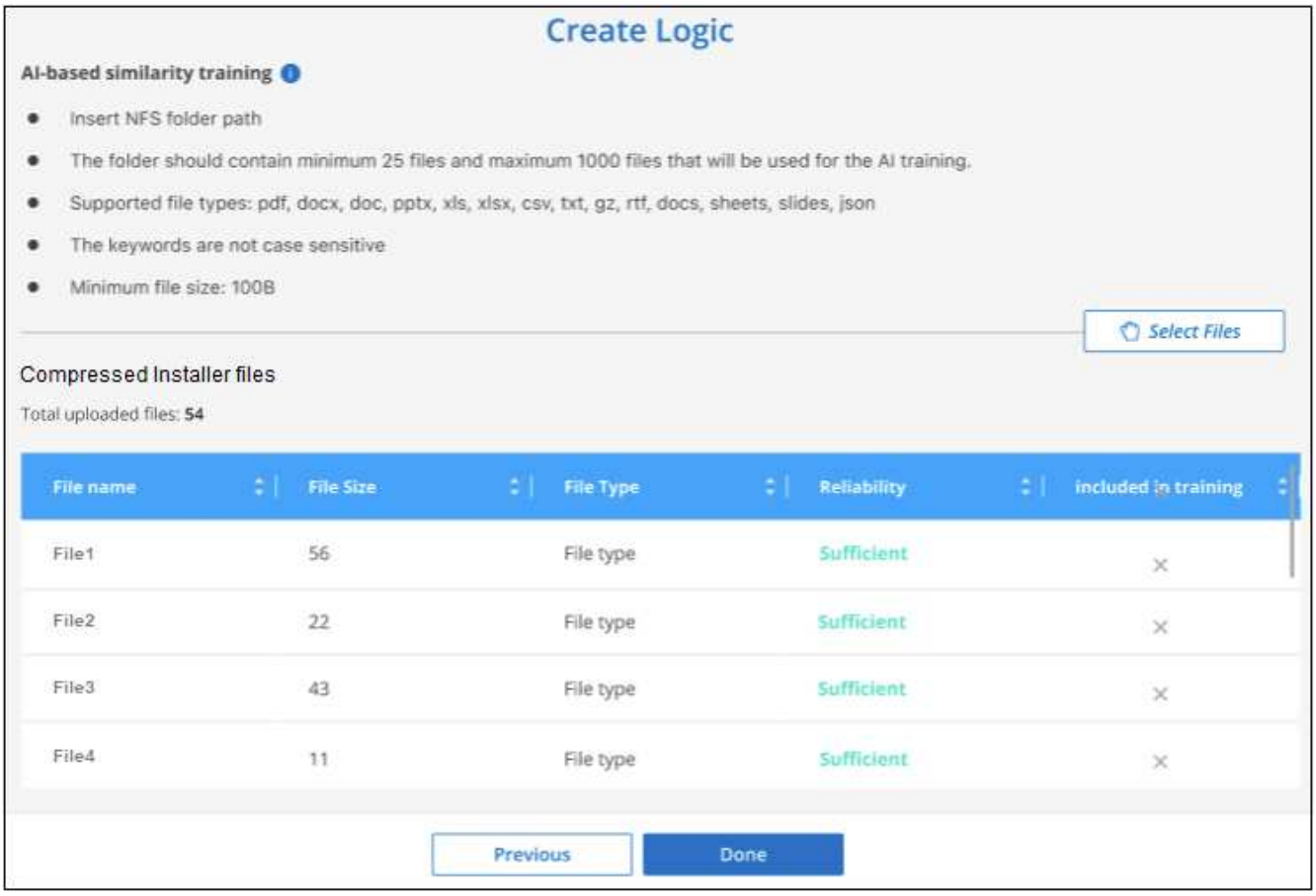
3. Nella pagina *Create Logic*, assicurarsi di aver preparato i file di apprendimento, quindi fare clic su **Select Files** (Seleziona file).



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**.



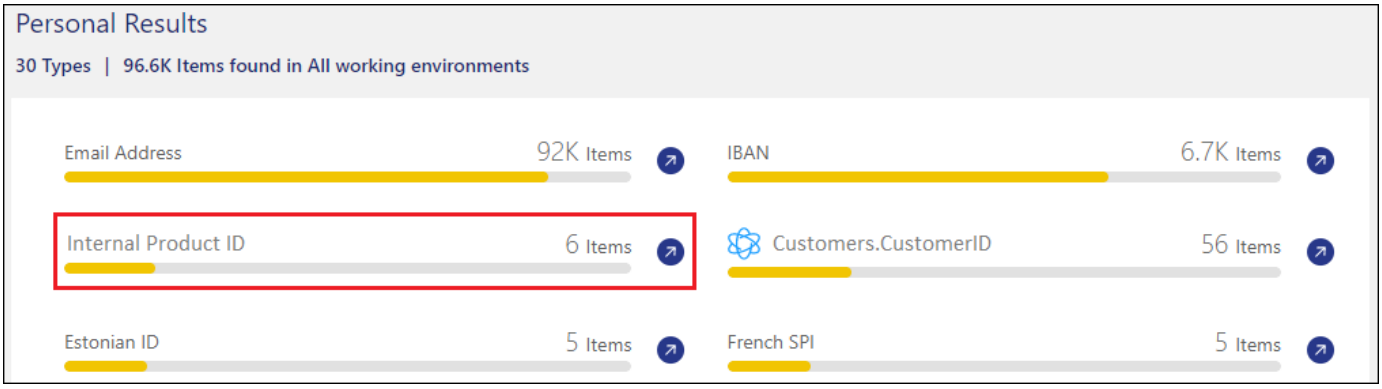
Risultati

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

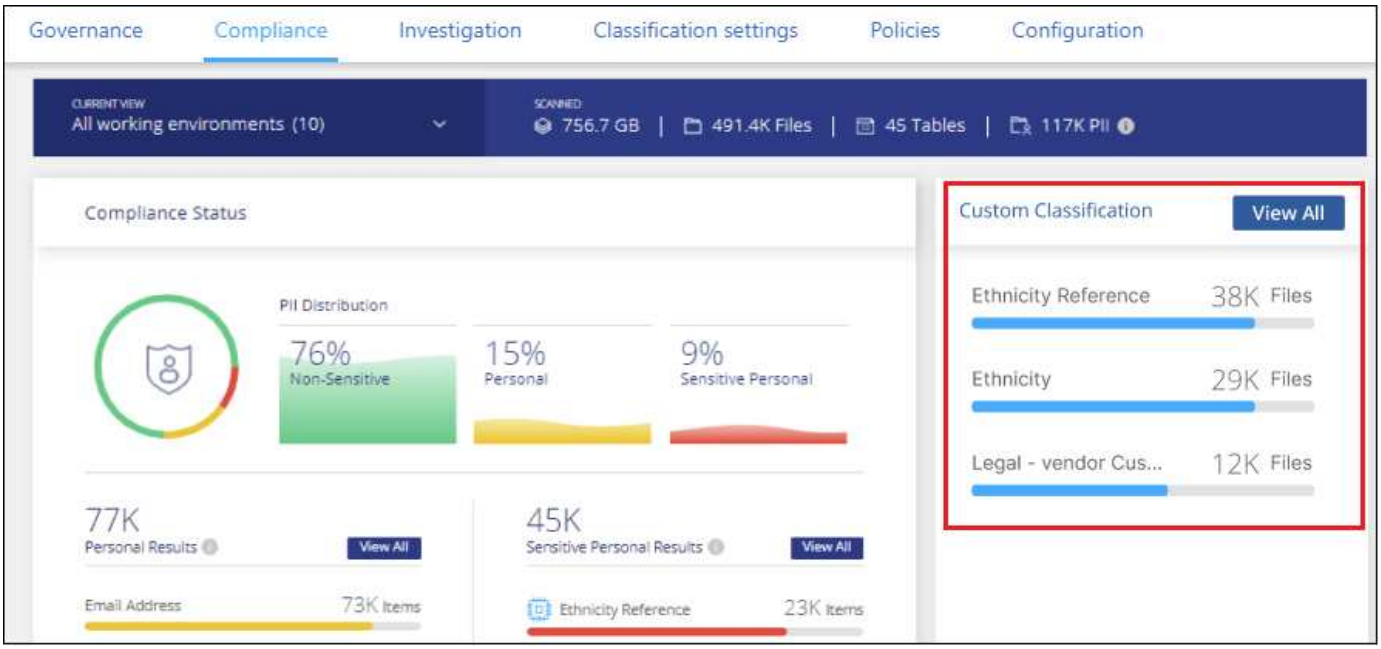
È possibile visualizzare i risultati da qualsiasi classificatore personalizzato nella dashboard di conformità e nella pagina di analisi. Ad esempio, questa schermata mostra le informazioni corrispondenti nella dashboard di

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.

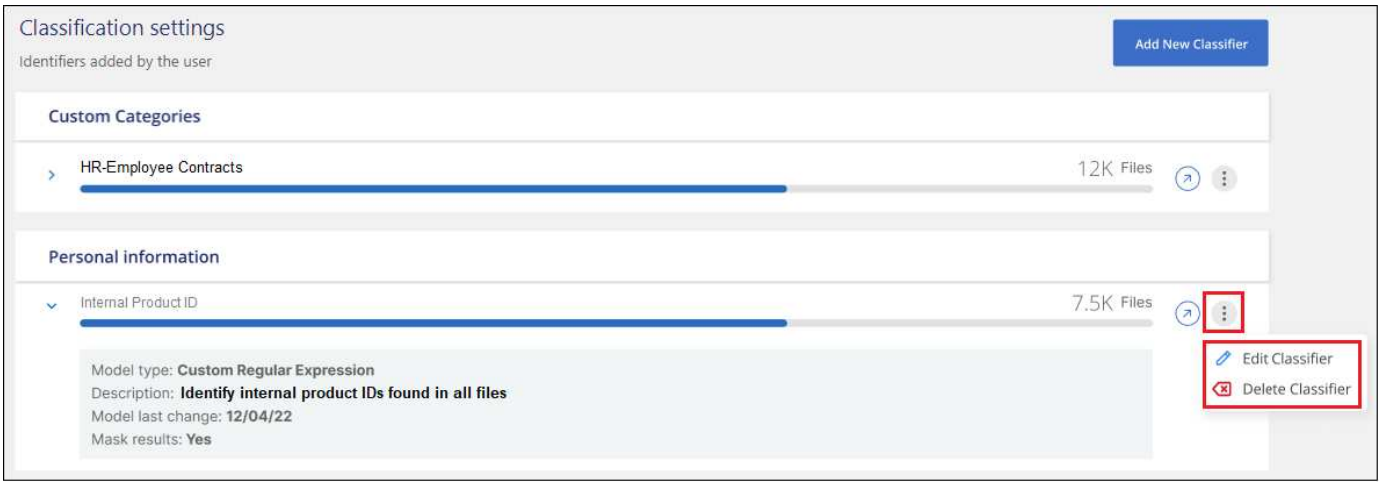


Gestire classificatori personalizzati

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.



Visualizzare lo stato delle azioni di conformità nella classificazione BlueXP

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.

> Queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

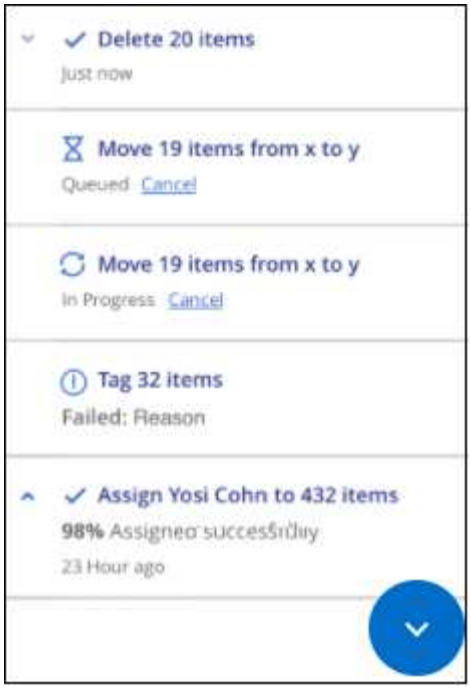
Lo stato può essere:

- 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.

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.

> Queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

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 (eliminazione, copia, spostamento, creazione di una ricerca salvata, aggiornamento della ricerca salvata, nuova scansione dei file, download del 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 ricerca salvato
  - 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".

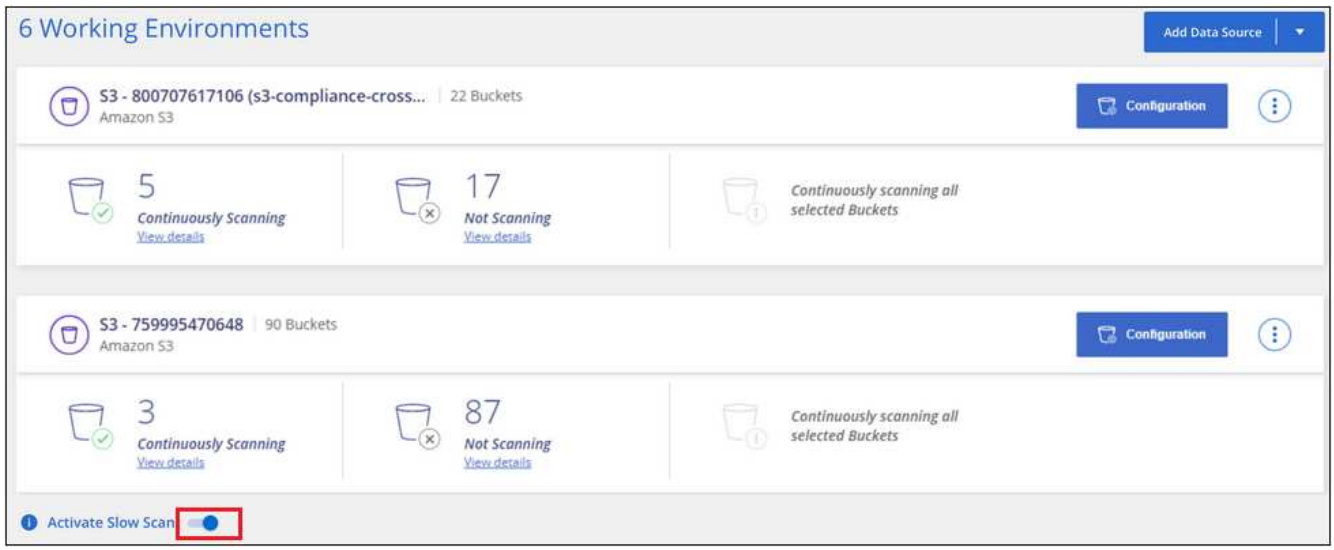
Se attivata, la scansione lenta viene utilizzata su tutte le origini dati, non è possibile configurare la scansione lenta per un singolo ambiente di lavoro o un'origine dati.

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

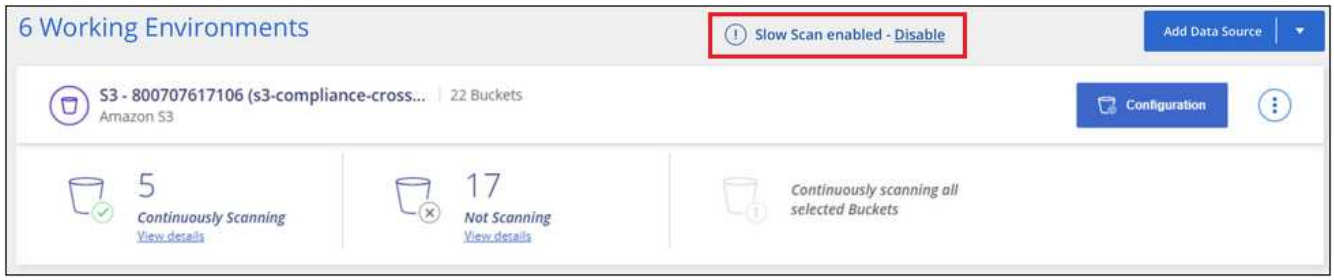
Queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

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.

Rimuovere 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*, selezionare il pulsante nella riga per l'account OneDrive, SharePoint o Google Drive, quindi selezionare **Remove OneDrive account**, **Remove SharePoint account** o **Remove Google Drive account**.

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

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 dei dati nella classificazione BlueXP

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)

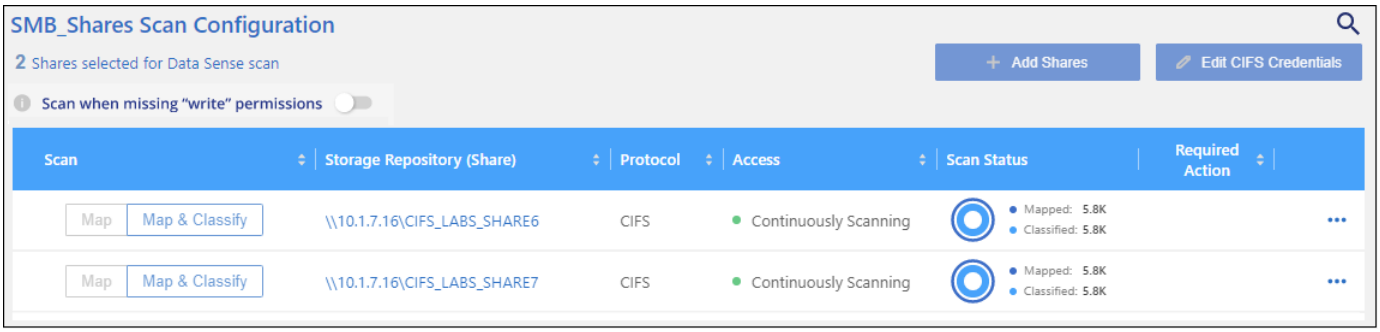
- La classificazione BlueXP non estrae l'ora dell'ultimo accesso dalle origini dei dati del database.
- Le versioni precedenti del sistema operativo Windows (ad esempio, Windows 7 e Windows 8) disattivano per impostazione predefinita la raccolta dell'attributo "ultimo tempo di accesso" perché può influire 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

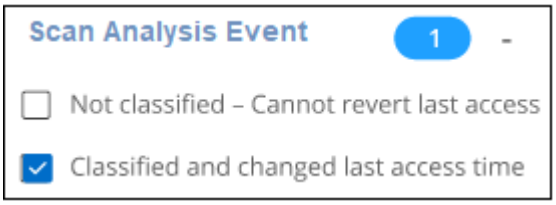
configurati con SnapLock dispongono di autorizzazioni di sola lettura e non possono riportare l'ultimo orario di accesso all'indicatore data e ora originale.

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 ai sistemi ONTAP on-premise, Cloud Volumes ONTAP, Azure NetApp Files, FSX per ONTAP e alle condivisioni di file di terze parti.

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
  - 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 al supporto BlueXP

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"
- "Google Cloud NetApp Volumes"

Panoramica sulla registrazione del supporto

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

- Registrazione del numero di serie dell'account BlueXP (il numero di serie 960xxxxxxxxx a 20 cifre si trova nella pagina risorse di supporto 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 BlueXP per ricevere assistenza NetApp

Per registrarsi per ricevere assistenza e attivare i diritti di supporto, un utente dell'organizzazione (o account) BlueXP deve associare un account del sito di supporto NetApp al proprio login 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

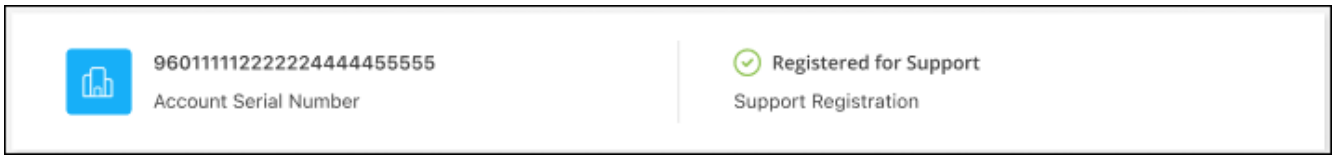
Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite BlueXP.

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 l'organizzazione BlueXP è registrata 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 la tua organizzazione BlueXP non sia registrata per il supporto. Finché un utente dell'organizzazione ha seguito questi passaggi, l'organizzazione è stata registrata.

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

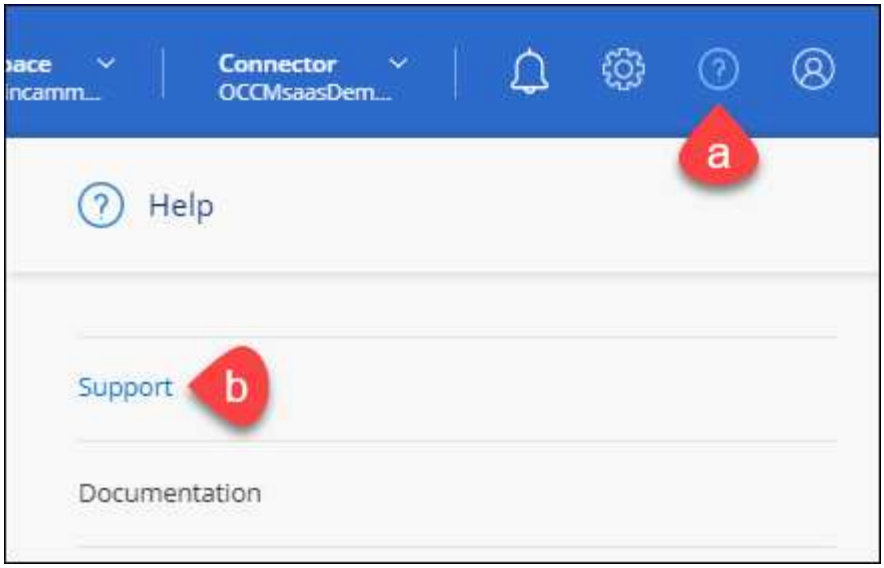
1. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account BlueXP (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

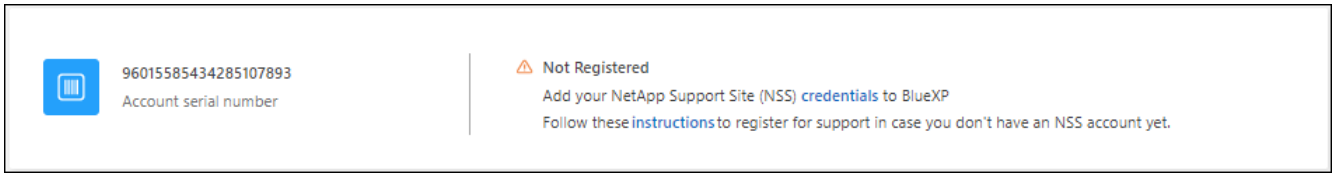
Se sei nuovo di NetApp e non disponi di un account NSS, segui i passaggi riportati di seguito.

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. Ciò velocizzerà l'elaborazione.

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

È necessario associare le credenziali del sito di supporto NetApp alla propria organizzazione BlueXP per abilitare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP:

- 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

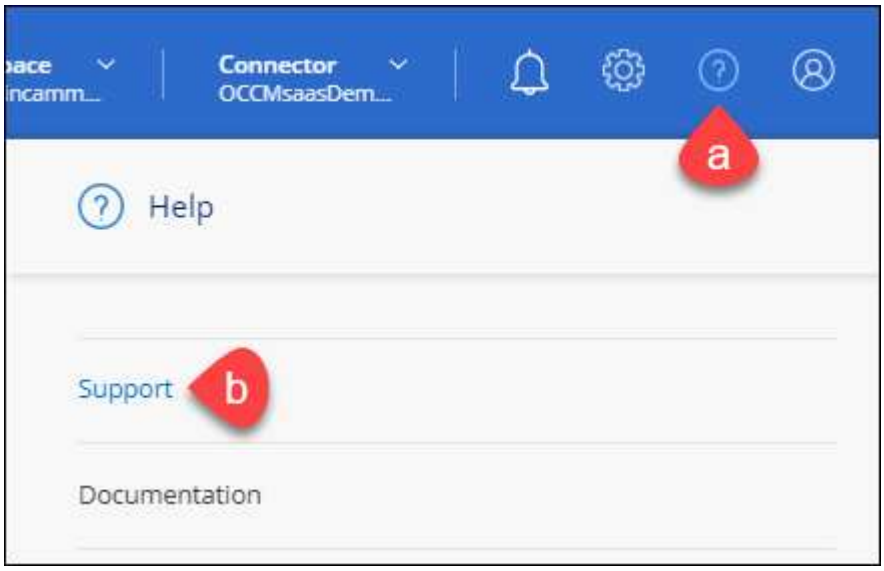
L'associazione delle credenziali NSS all'organizzazione BlueXP è diversa dall'account NSS associato a un accesso utente BlueXP .

Queste credenziali NSS sono associate all'ID organizzazione BlueXP specifico dell'utente. Gli utenti che appartengono all'organizzazione BlueXP possono accedere a queste credenziali da **supporto > Gestione NSS**.

- 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.

Assistenza per la classificazione BlueXP

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

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"
- "Google Cloud NetApp Volumes"

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'organizzazione (o account), del progetto (o dell'area di lavoro) BlueXP e del connettore selezionato nell'intestazione superiore del servizio.

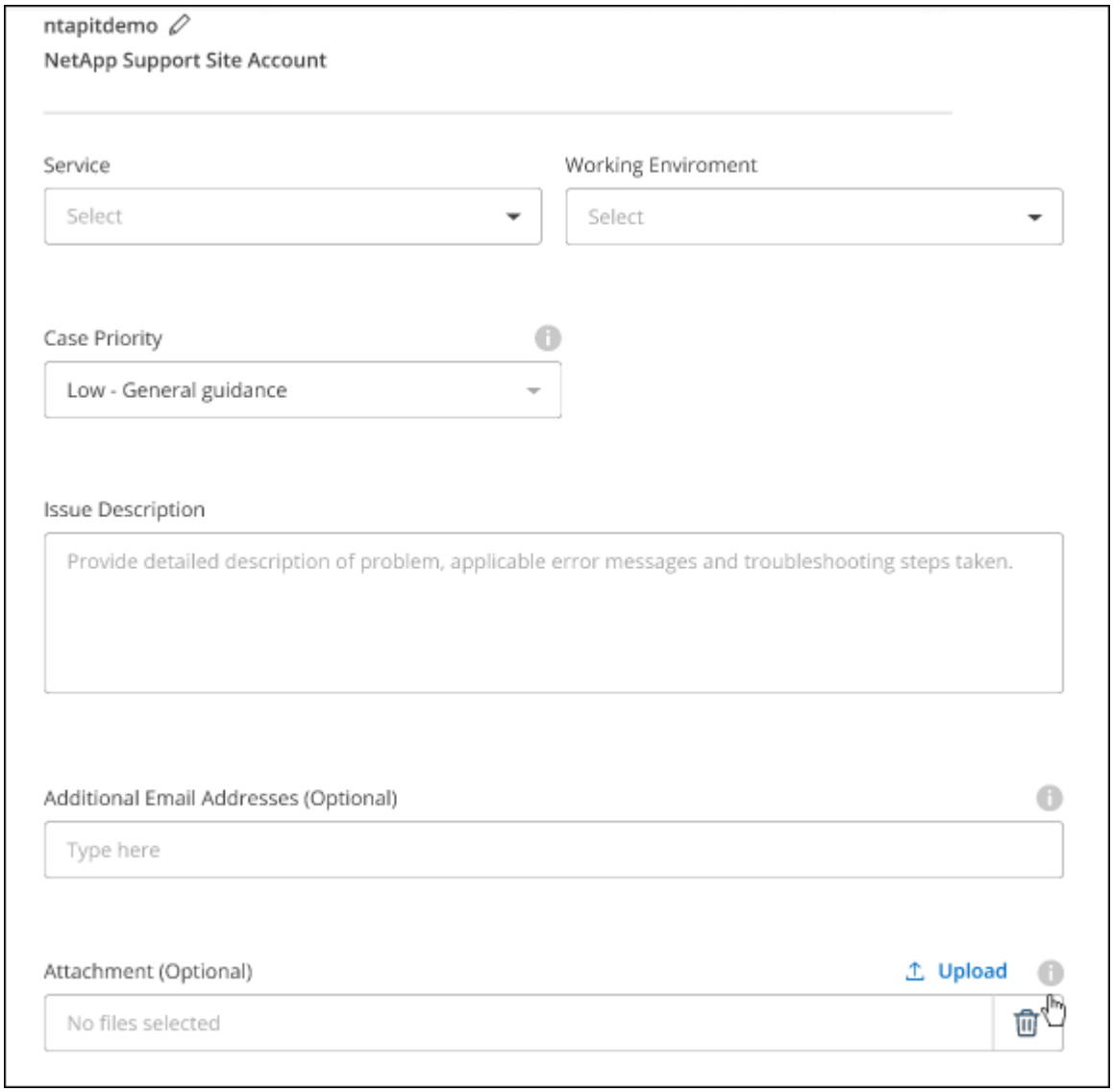
      - **Priorità caso**: Scegliere la priorità per il caso, che può essere bassa, Media, alta o critica.

        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.

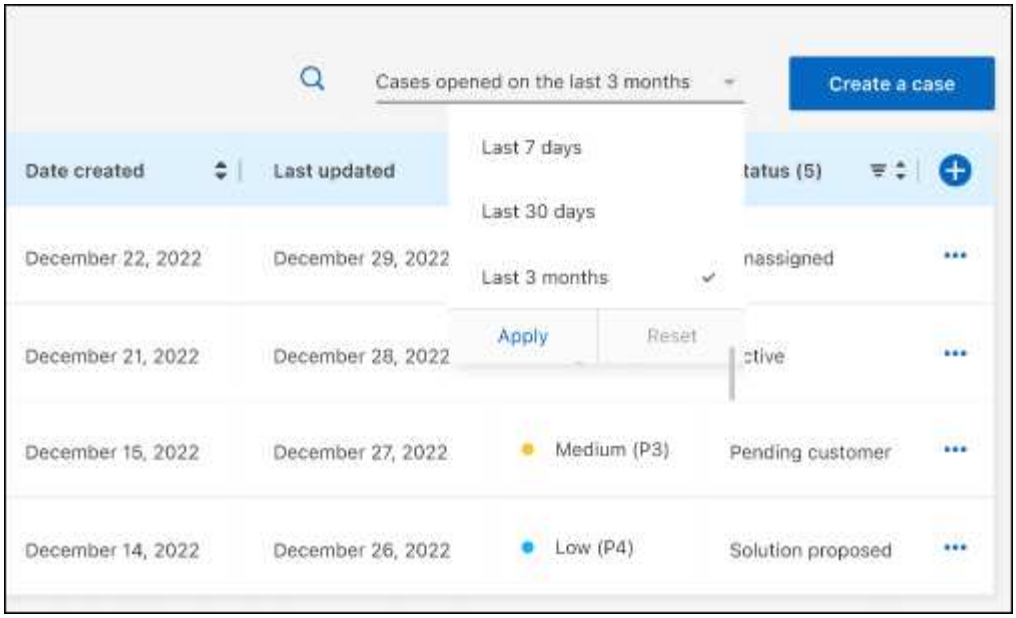
  I risultati della tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come priorità e Stato. Altre colonne offrono funzionalità di ordinamento.

  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.

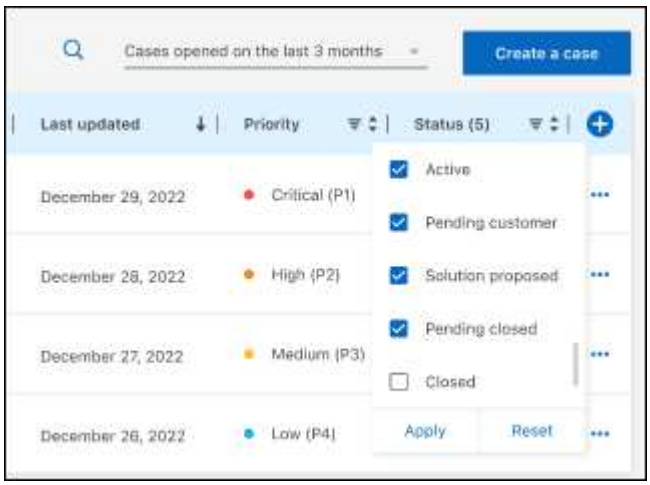
Fasi

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

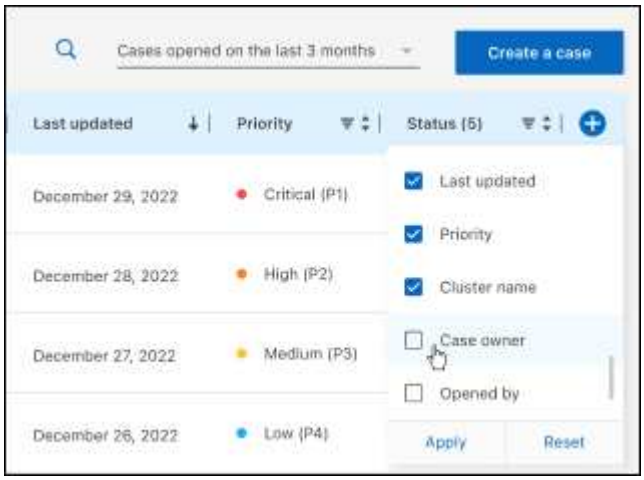
   La pagina **Gestione del caso** mostra i casi aperti relativi all'account NSS associato all'account utente BlueXP. Si tratta dello stesso account NSS visualizzato nella parte superiore della pagina **gestione NSS**.
3. Se si desidera, modificare le informazioni visualizzate nella tabella:
   - In **Organization's 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.

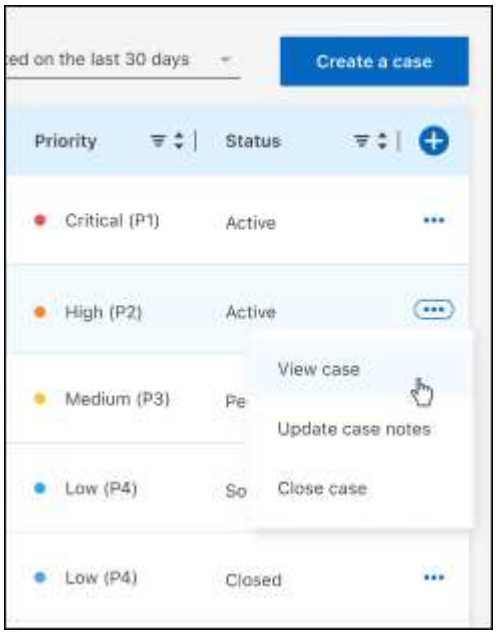


4. Gestire un caso esistente selezionando ••• e selezionando una delle opzioni disponibili:

   - **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**.



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.

Come funziona la classificazione BlueXP?

La classificazione BlueXP implementa un altro layer di ai insieme al tuo 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".

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

Sì, la classificazione BlueXP dispone di un'API REST per le funzionalità supportate nella versione di classificazione BlueXP che fa parte della piattaforma BlueXP core. Vedere "Documentazione API".

La classificazione BlueXP è disponibile attraverso i marketplace del cloud?

La classificazione BlueXP fa parte delle funzionalità principali di BlueXP , pertanto non è necessario utilizzare i mercati per questo servizio .

Analisi e scansione della classificazione BlueXP

Le seguenti domande si riferiscono alle prestazioni di scansione della classificazione BlueXP e all'analisi.

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".

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

Le scansioni dei dati hanno un impatto trascurabile sui sistemi storage e sui dati.

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). Per ulteriori informazioni, vedere "L'istanza di classificazione BlueXP" e. "Implementazione della classificazione BlueXP"

Quando si aggiungono inizialmente nuove origini dati, è anche possibile scegliere di eseguire solo una scansione di "mappatura" (solo mappatura) invece di una scansione di "classificazione" completa (mappa e classificazione). 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".

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 role-based access control (RBAC) per consentire lo spostamento o l'eliminazione dei file, se sono presenti le autorizzazioni giuste. Se non sono presenti le autorizzazioni corrette, è possibile assegnare le attività a un utente dell'organizzazione che dispone delle autorizzazioni appropriate.

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 o disattiva 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.

Puoi disattivare la classificazione BlueXP dall'eseguire la scansione di un singolo ambiente di lavoro, database o gruppo di condivisioni di file dalla pagina di configurazione della classificazione BlueXP. Vedere "Rimuovere le origini dati dalla classificazione BlueXP".

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.

Il servizio può 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".

Le snapshot che risiedono su volumi ONTAP vengono sottoposte a scansione?

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 livello nell'archiviazione a oggetti utilizzando solo la mappatura, esegue la scansione di tutti i dati presenti sui dischi locali e dei dati cold a livello nell'archiviazione a oggetti. Ciò vale anche per i prodotti non NetApp che implementano il tiering.

La scansione solo mappatura non riscalda i dati freddi: Rimane fredda e rimane nello storage a oggetti. D'altra parte, se si esegue la scansione Map & Classify, alcune configurazioni potrebbero riscaldare i dati cold.

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.

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".

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
- Storage a oggetti che utilizza il protocollo S3 (Simple Storage Service)

Vedere "Ambienti di lavoro e origini dati supportati".

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, .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 mappatura dati (solo scansione mappatura)**: 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.

- **Classificazione dei dati scansione profonda (scansione mappa e classificazione)**: Scansioni di classificazione BlueXP 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 Data Investigatcdion Details e nei Data Investigatcdion Reports.

La classificazione BlueXP è in grado di identificare molti tipi di dati privati, come le informazioni personali (PII) e le informazioni personali sensibili (SPII). Per ulteriori informazioni sui dati privati, fare riferimento alla sezione "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 BlueXP possono visualizzare solo le informazioni relative agli ambienti di lavoro che possono visualizzare in base alle loro autorizzazioni.

Inoltre, se si desidera consentire a determinati utenti di visualizzare solo i risultati della scansione di classificazione BlueXP senza la possibilità di gestire le impostazioni di classificazione BlueXP , è possibile assegnare a tali utenti il ruolo **visualizzatore di classificazione** (quando si utilizza BlueXP in modalità standard) o il ruolo **Visualizzatore di conformità** (quando si utilizza BlueXP in modalità limitata). "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

La seguente domanda riguarda le licenze e i costi per l'utilizzo della classificazione BlueXP.

Quanto costa la classificazione BlueXP?

La classificazione BlueXP è una funzionalità chiave di BlueXP e non è addebitata

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?

Durante la scansione dei dati, il connettore BlueXP deve essere installato nelle seguenti posizioni:

- Per Cloud Volumes ONTAP in AWS o Amazon FSX per ONTAP: Connector è in AWS.
- Per Cloud Volumes ONTAP in Azure o in Azure NetApp Files: Il connettore si trova in Azure.
- Per Cloud Volumes ONTAP in GCP: Il connettore è in GCP.
- Per i sistemi ONTAP on-premise: Il connettore è on-premise.

Se si dispone di dati in 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.

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

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

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.

"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.

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"

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.