Funzioni obsolete

BlueXP classification

NetApp
August 06, 2025

This PDF was generated from https://docs.netapp.com/it-it/bluexp-classification/reference-free-paid.html on August 06, 2025. Always check docs.netapp.com for the latest.

Sommario

Funzioni obsolete . . . 1
Funzionalità obsolete di classificazione BlueXP . . . 1
Origini dati supportate . . . 1
Funzionalità di conformità . . . 1
Funzioni per la gestione dei dati . . . 2
Implementa le deprecazioni di classificazione BlueXP . . . 3
Installare la classificazione BlueXP su host multipli per configurazioni di grandi dimensioni senza accesso a Internet . . . 3
Deprecazioni dei dati di scansione . . . 4
Esegui la scansione dei bucket Amazon S3 con classificazione BlueXP . . . 4
Eseguire la scansione degli account OneDrive con classificazione BlueXP . . . 12
Eseguire la scansione degli account SharePoint con la classificazione BlueXP . . . 15
Eseguire la scansione degli account Google Drive con classificazione BlueXP . . . 20
Eseguire la scansione dei dati StorageGRID con classificazione BlueXP . . . 22
Gestire le deprecazioni dei dati . . . 26
Visualizza i dettagli di governance dei tuoi dati utilizzando il dashboard di governance della classificazione BlueXP . . . 26
Organizza i tuoi dati privati con la classificazione BlueXP . . . 27
Gestisci i tuoi dati privati con la classificazione BlueXP . . . 36
Aggiungi identificatori di dati personali alle scansioni di classificazione BlueXP . . . 47
Visualizzare lo stato delle azioni di conformità nella classificazione BlueXP . . . 63
Controllare la cronologia delle azioni di classificazione di BlueXP . . . 64
Riduzione della velocità di scansione della classificazione BlueXP . . . 65
Rimuovere un account OneDrive, SharePoint o Google Drive dalla classificazione BlueXP . . . 66

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.

1 Imposta i requisiti S3 nel tuo ambiente cloud

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

2 Distribuire l'istanza di classificazione BlueXP

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

3 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.

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.

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.

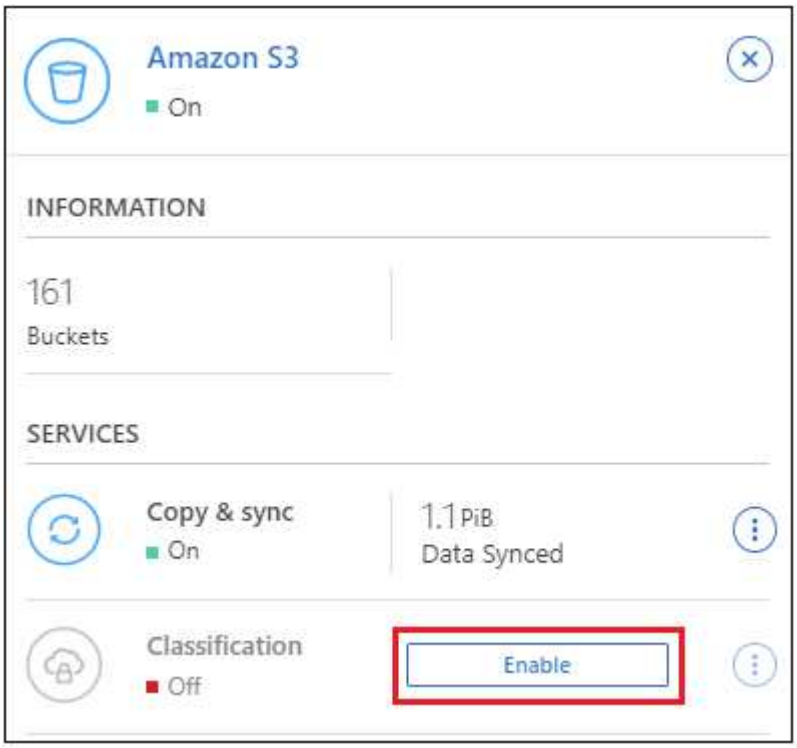
Attivazione della classificazione BlueXP nell'ambiente di lavoro S3

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

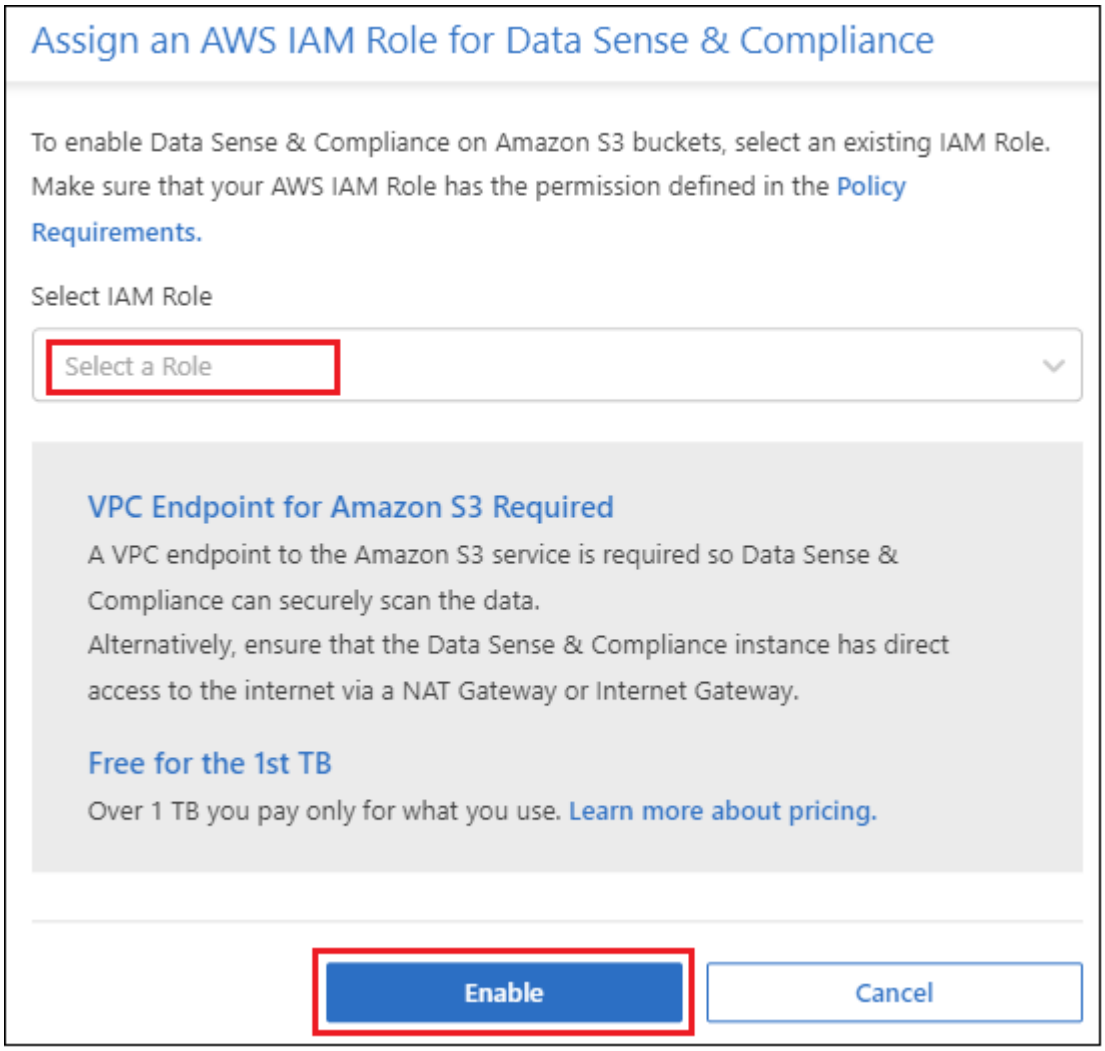
Fasi

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.

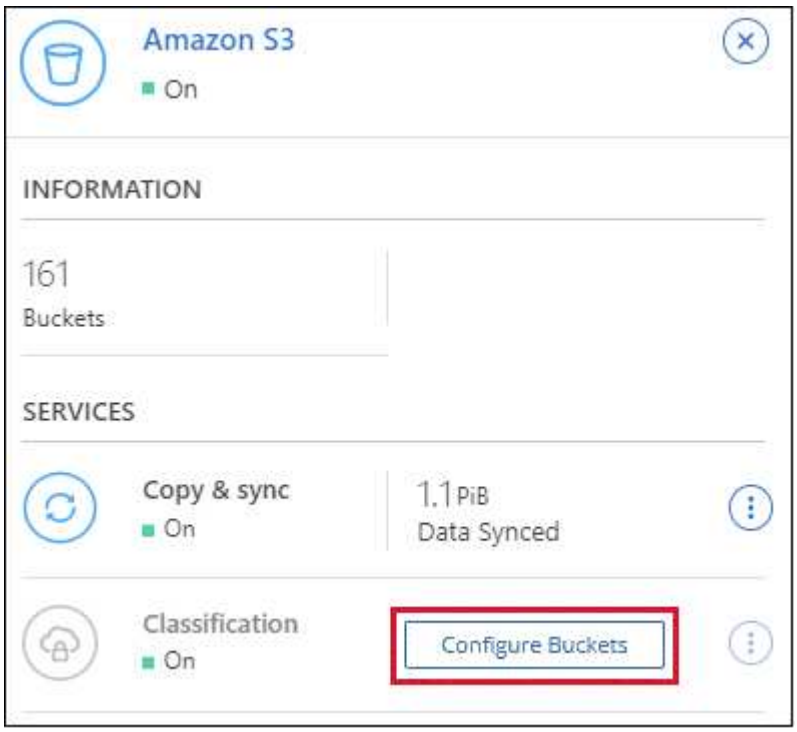
Quando BlueXP viene eseguito nell'account AWS che dispone dei bucket S3 che si desidera sottoporre a scansione, rileva tali bucket e li visualizza in un ambiente di lavoro Amazon S3.

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

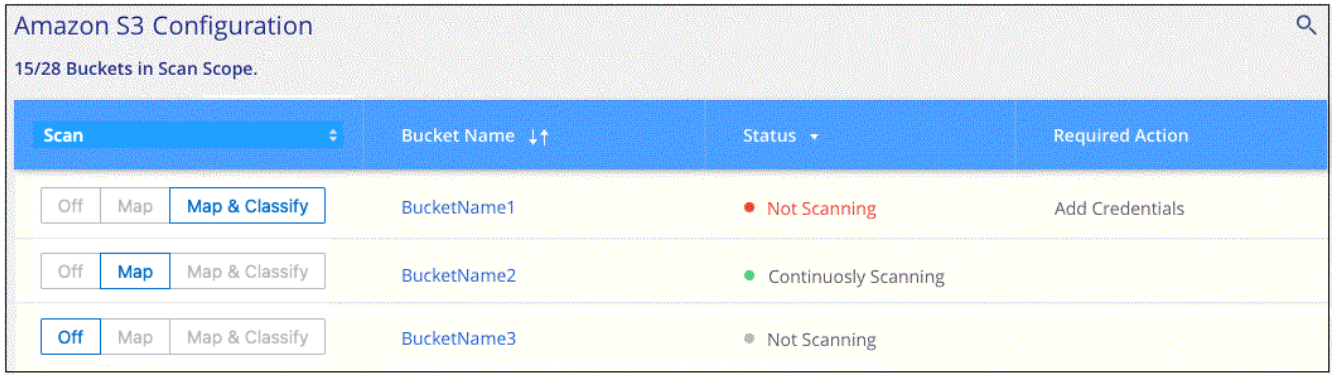
Fasi

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.

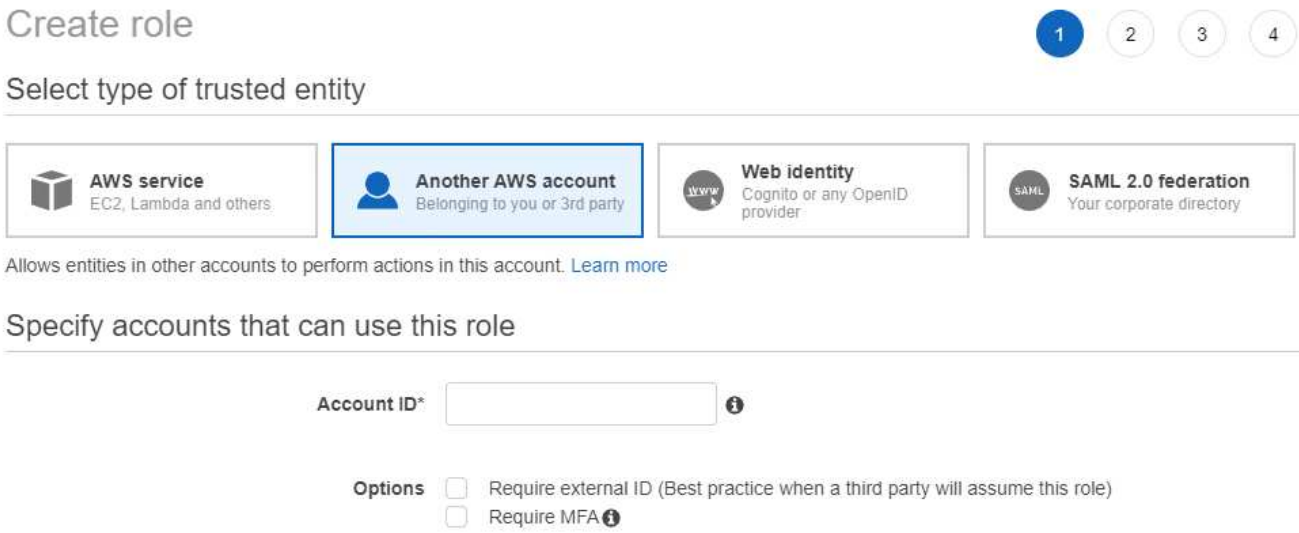
Scansione dei bucket da account AWS aggiuntivi

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.

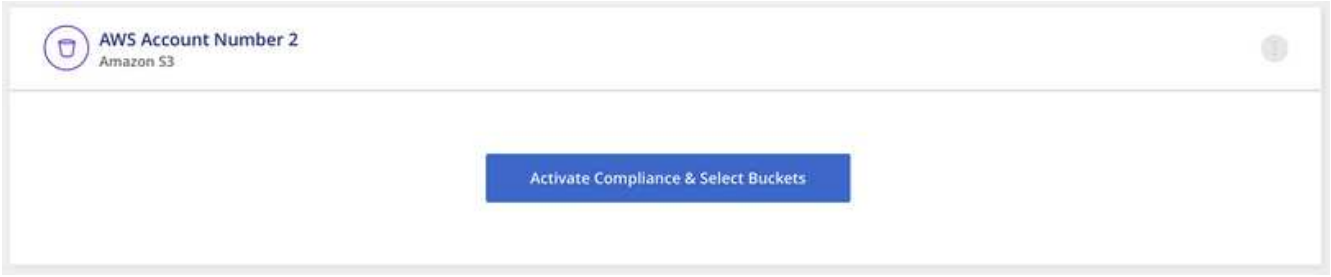
b. Selezionare **Allega criteri**, quindi **Crea criterio**.

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.

Verifica dei prerequisiti di OneDrive

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

Distribuire l'istanza di classificazione BlueXP

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

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.

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

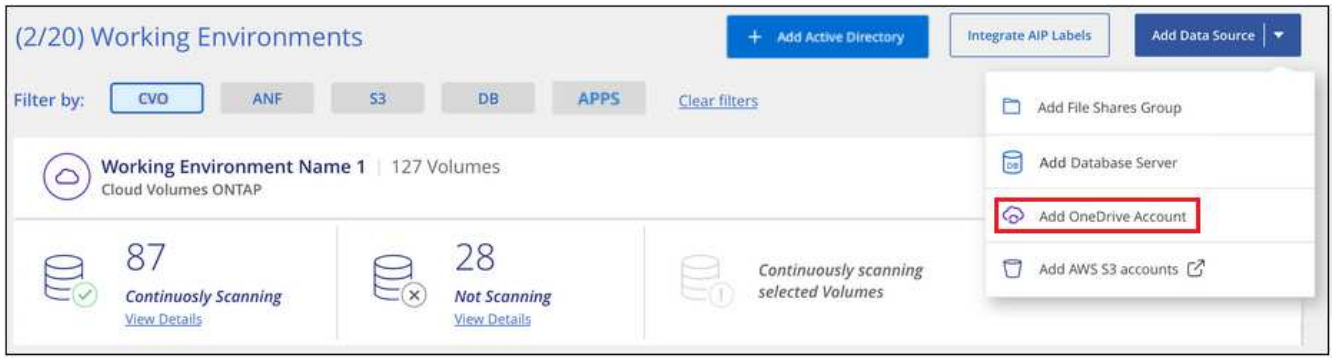
connettività Internet.

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.

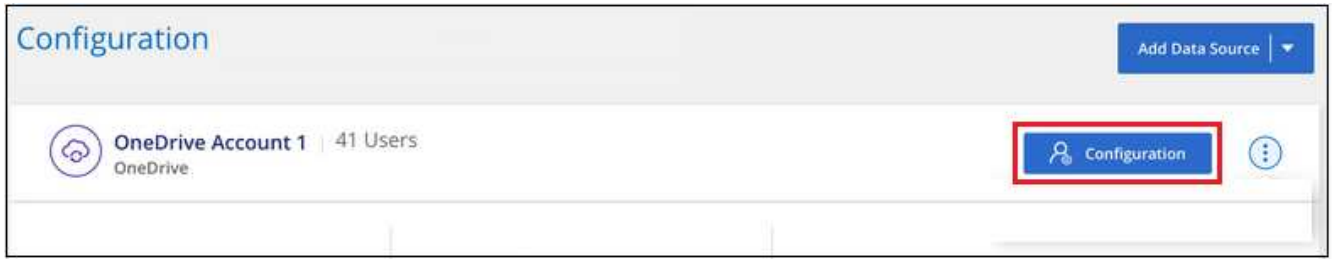
L'account OneDrive viene aggiunto all'elenco degli ambienti di lavoro.

Aggiunta di utenti OneDrive alle scansioni di conformità

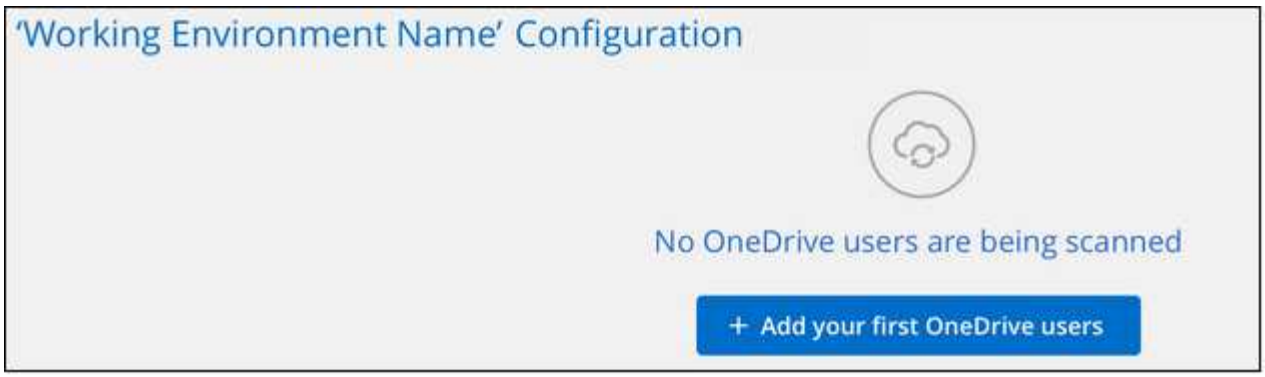
Puoi aggiungere singoli utenti OneDrive o tutti gli utenti OneDrive, in modo che i loro file vengano sottoposti a scansione in base alla classificazione BlueXP.

Fasi

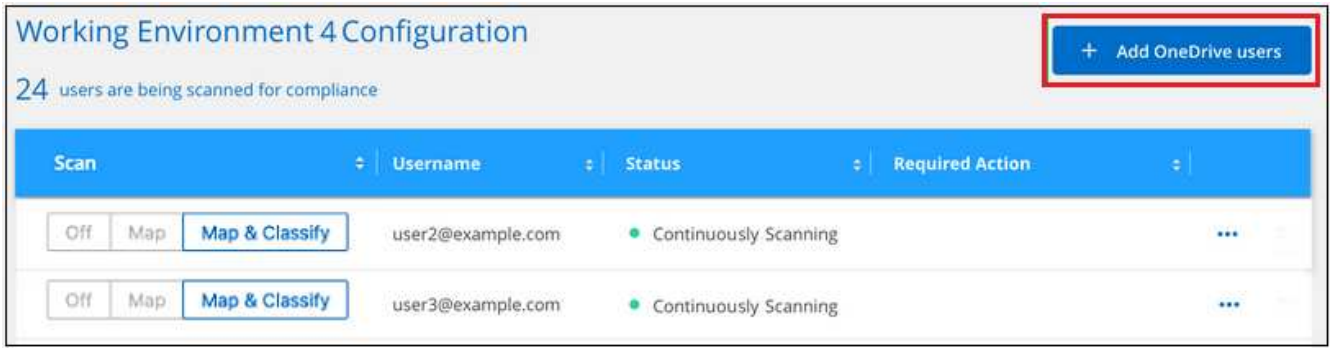
1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** dell'account OneDrive.



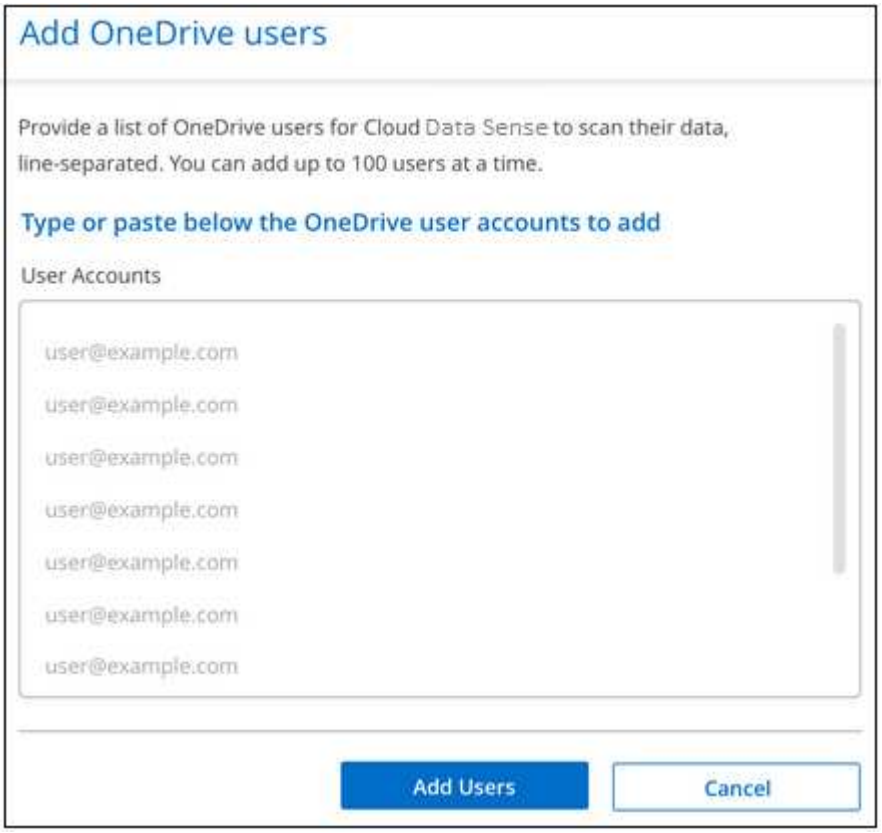
2. Se è la prima volta che si aggiungono utenti per questo account OneDrive, fare clic su **Aggiungi i primi utenti OneDrive**.



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.

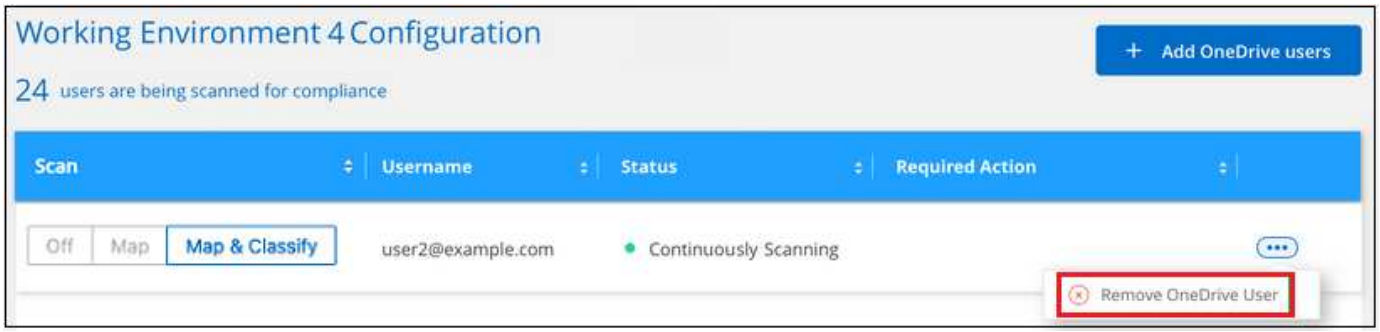
A:	Eseguire questa operazione:
Attiva scansioni solo mappatura sui file utente	Fare clic su **Map** (Mappa)
Attiva scansioni complete sui file utente	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione dei file utente	Fare clic su **Off**

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".

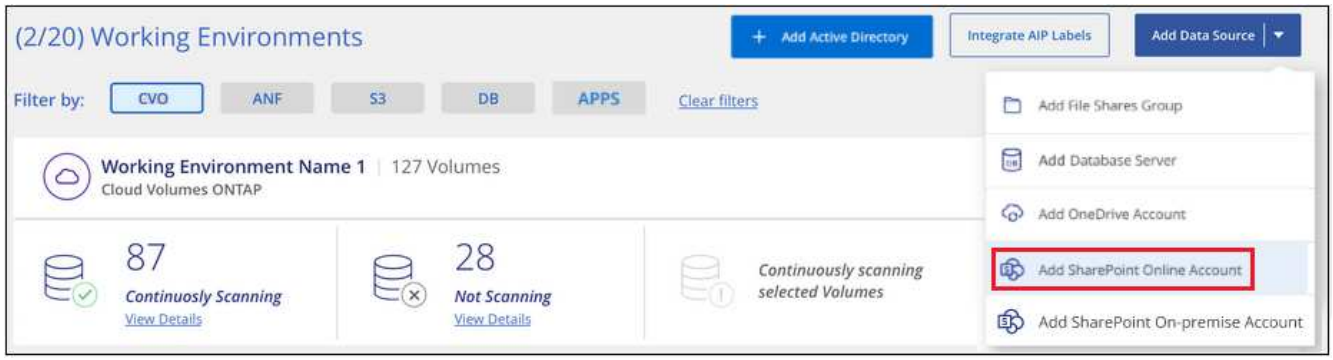
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

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.

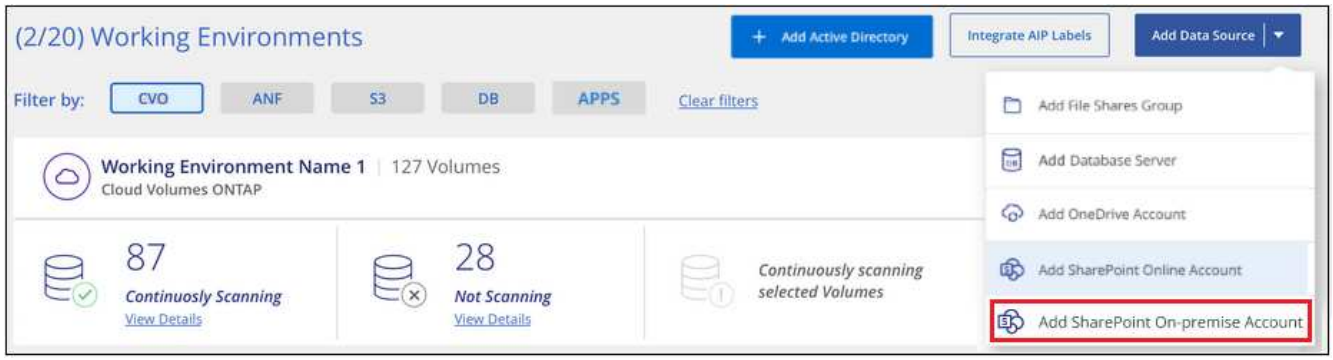
Aggiungere un account SharePoint in sede

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

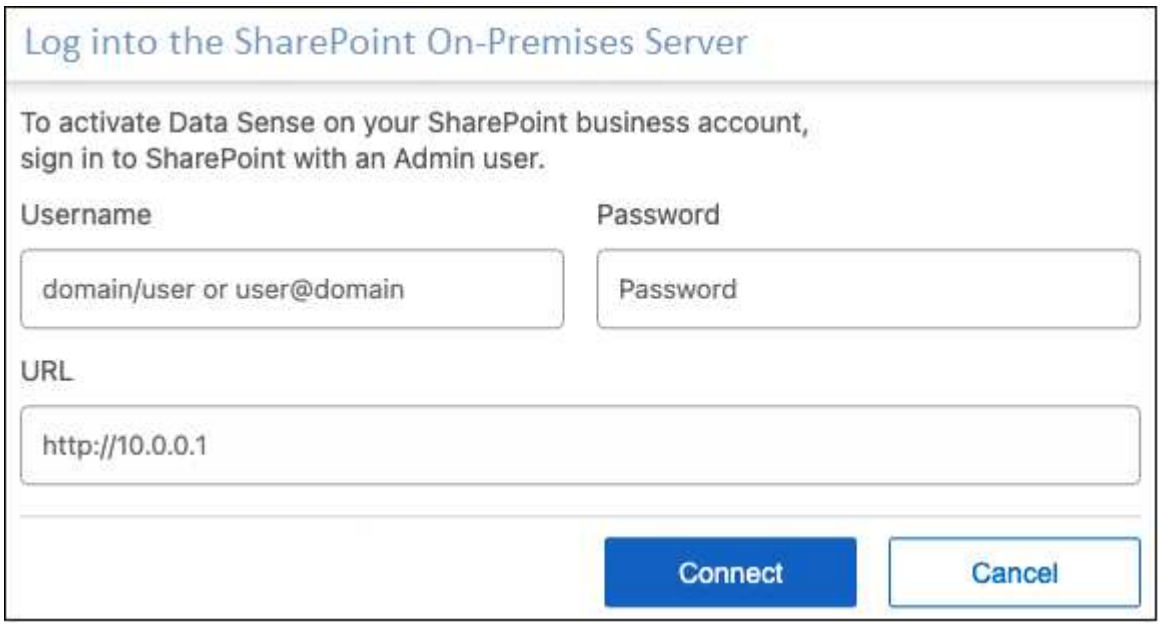
Fasi

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.

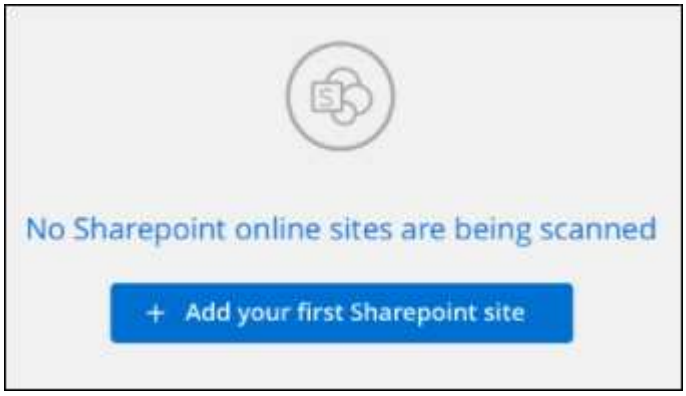
Aggiungere i siti SharePoint alle scansioni di conformità

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

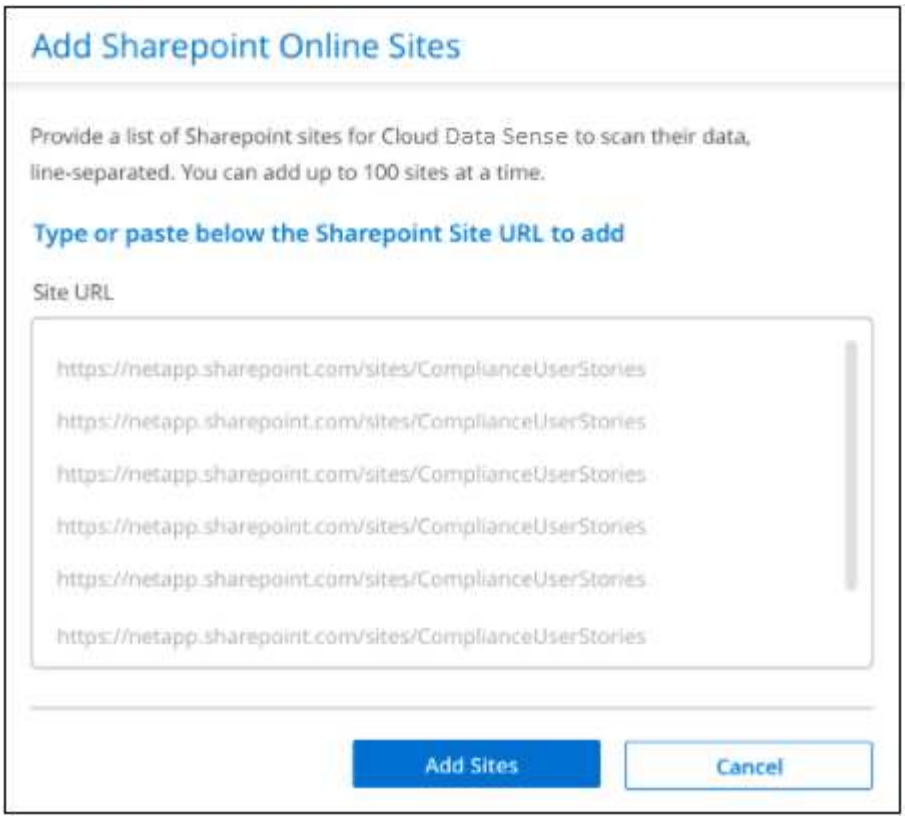
1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** dell'account SharePoint.

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.

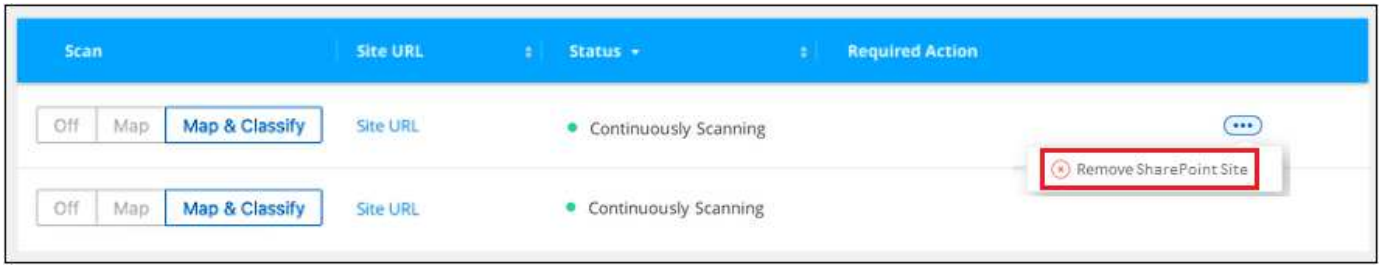
A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura sui file	Fare clic su **Map** (Mappa)
Attivare scansioni complete sui file	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione dei file	Fare clic su **Off**

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".

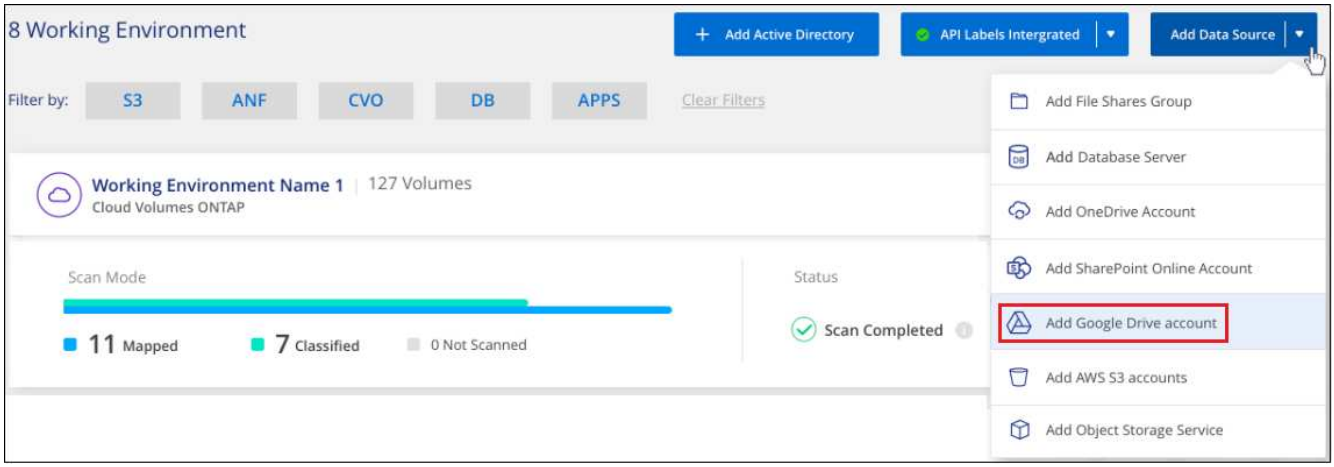
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

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.

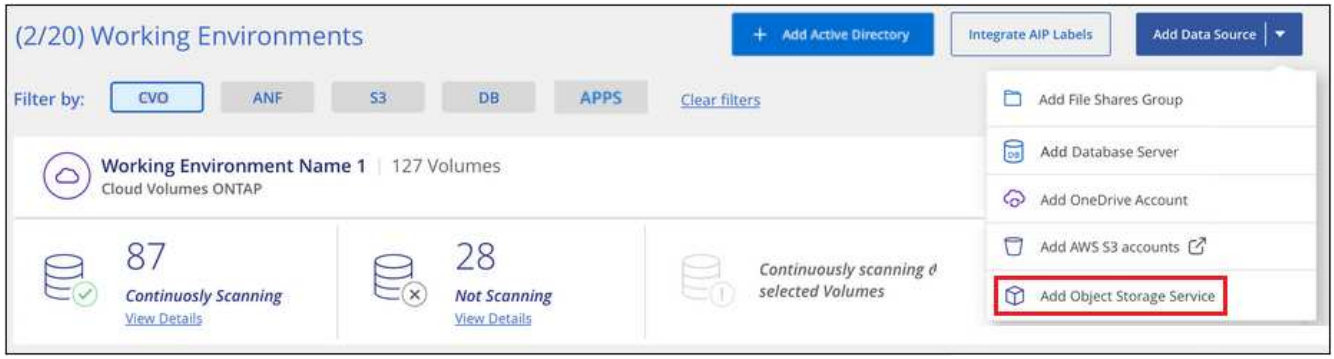
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Aggiunta del servizio di storage a oggetti alla classificazione BlueXP

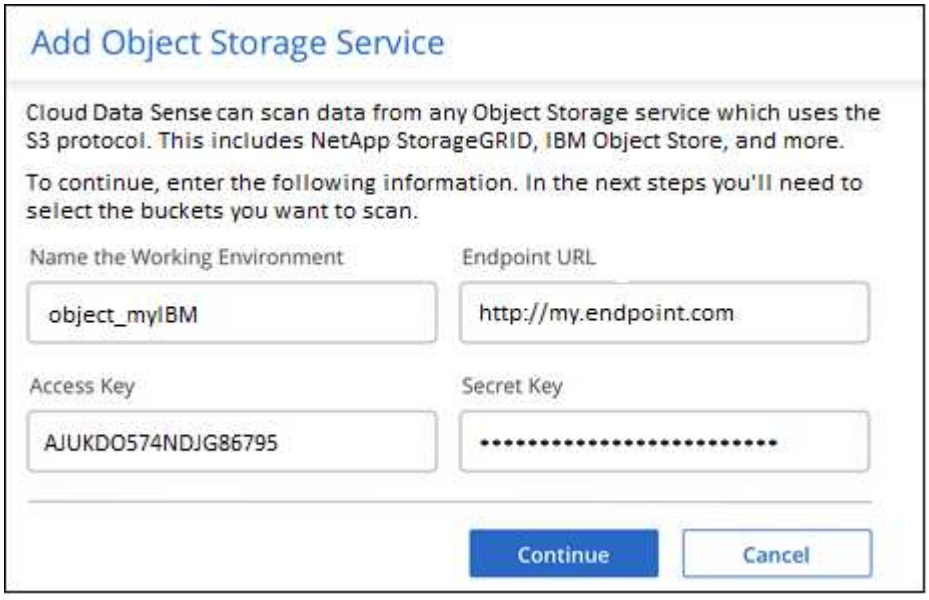
Aggiungere il servizio di storage a oggetti.

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

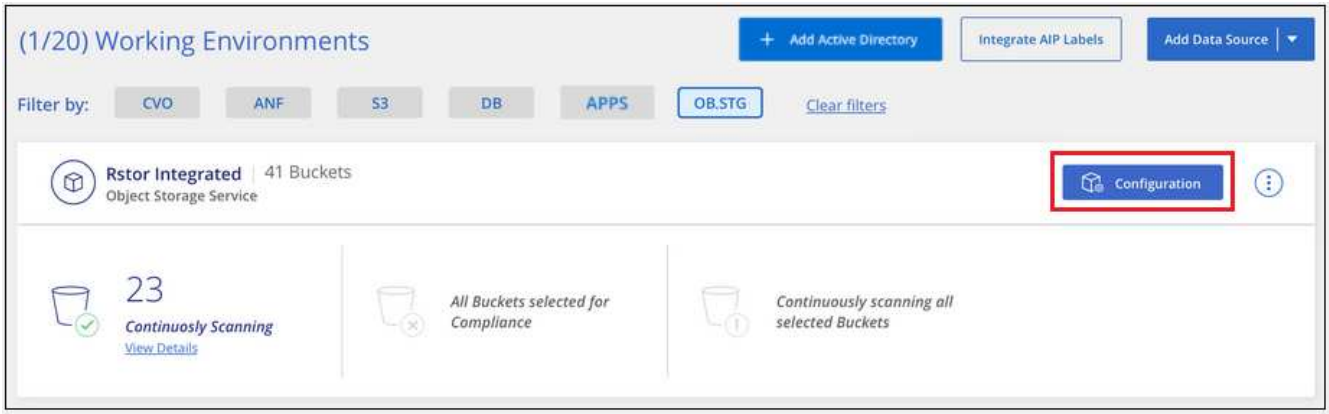
Il nuovo servizio di storage a oggetti viene aggiunto all'elenco degli ambienti di lavoro.

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

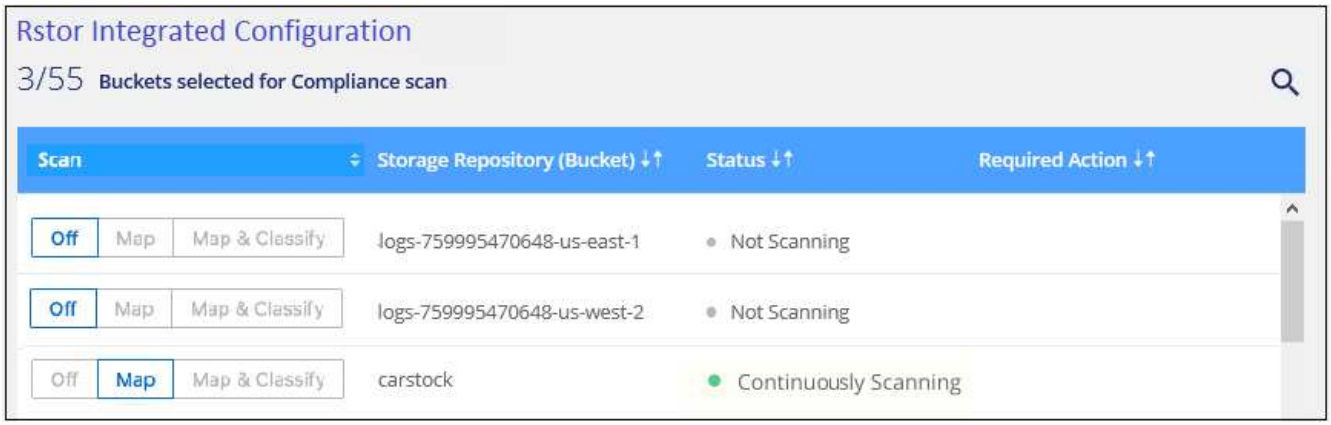
Dopo aver attivato la classificazione BlueXP sul servizio di storage a oggetti, il passaggio successivo consiste nel configurare i bucket che si desidera sottoporre a scansione. La classificazione BlueXP rileva tali bucket e li visualizza nell'ambiente di lavoro creato.

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.

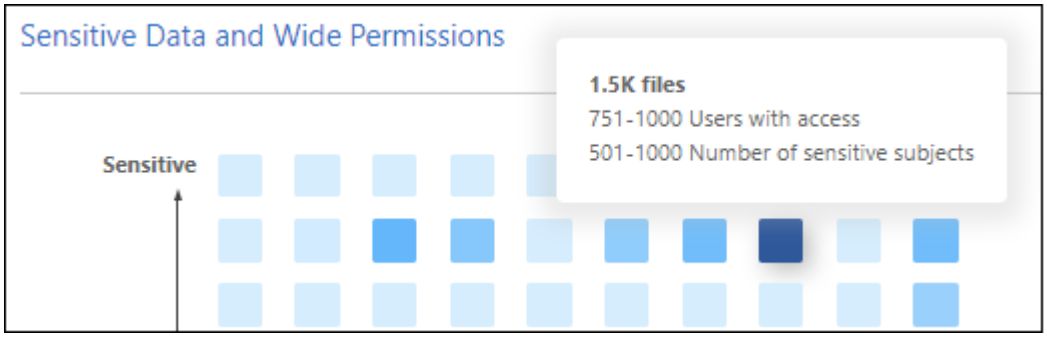
NOTA queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

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 .

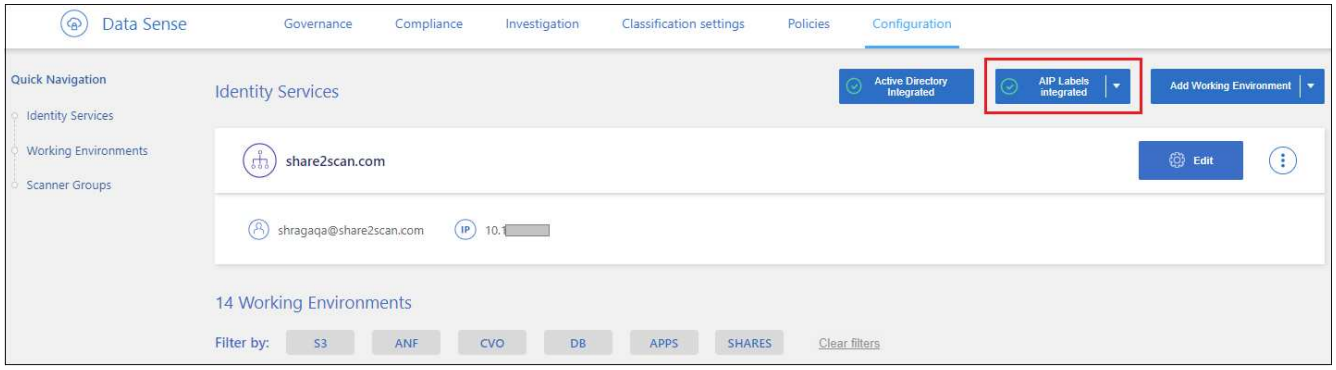
Requisiti

- 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.

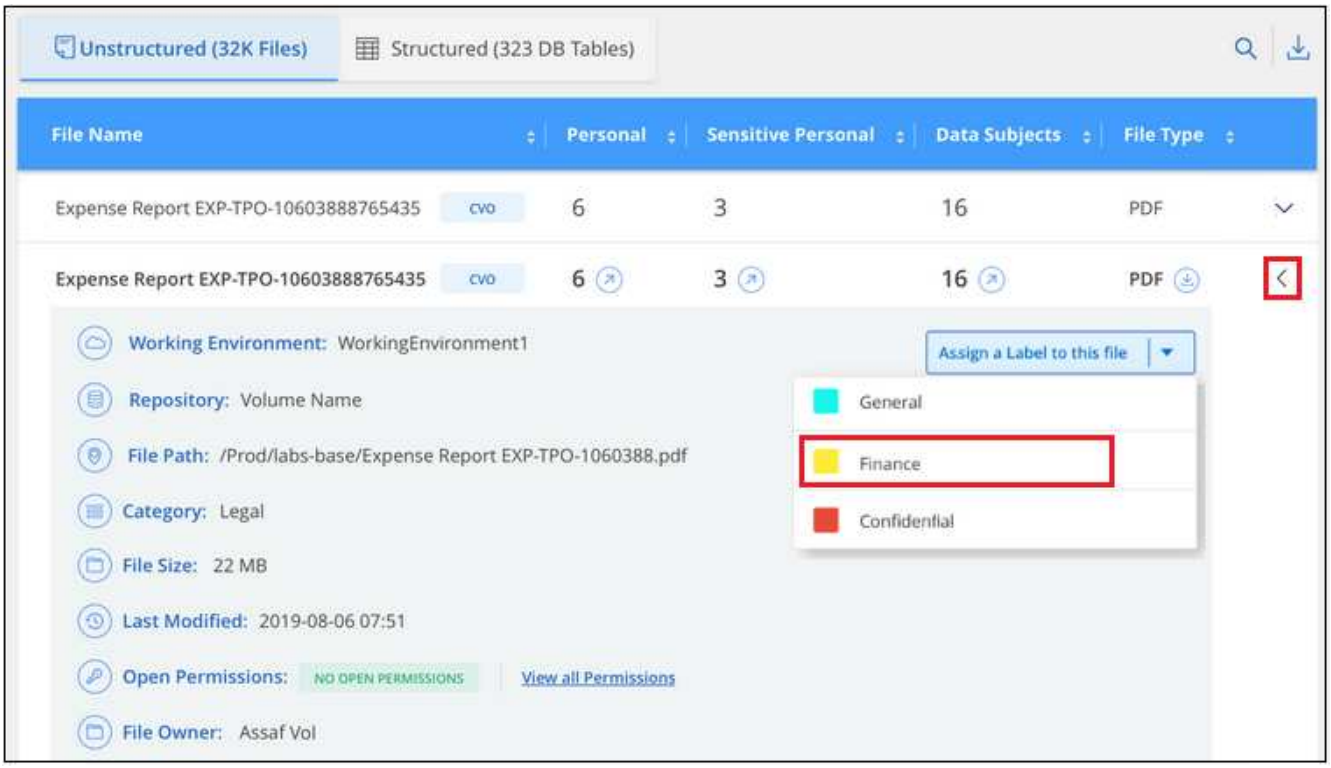
Assegnare manualmente le etichette AIP

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.

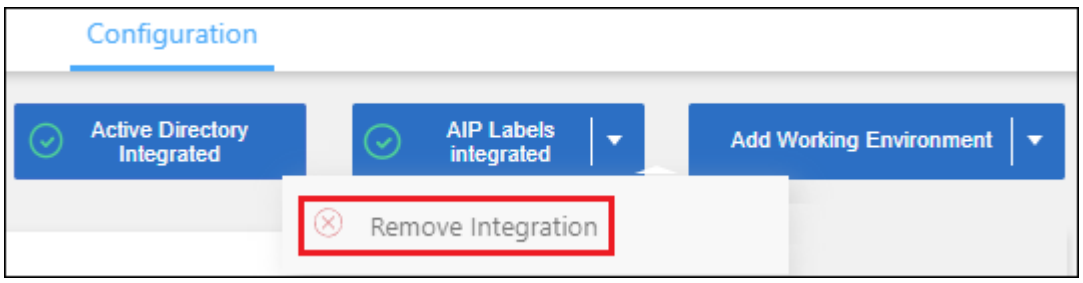
Rimuovere l'integrazione AIP

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.

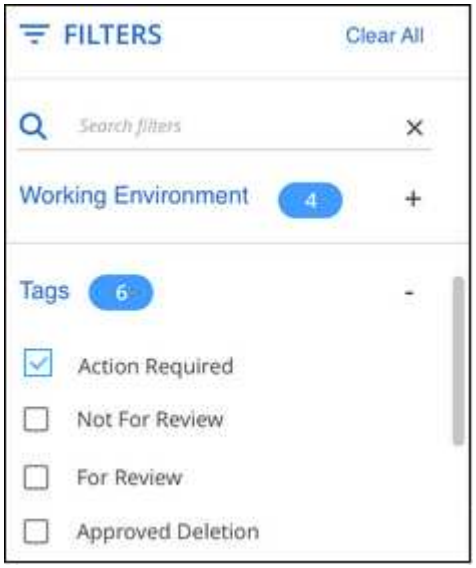
Tenere presente che il tag non viene aggiunto al file allo stesso modo in cui le etichette AIP fanno parte dei metadati del file. Il tag è appena visto dagli utenti di BlueXP che utilizzano la classificazione BlueXP in modo da poter vedere se un file deve essere cancellato o controllato per un certo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

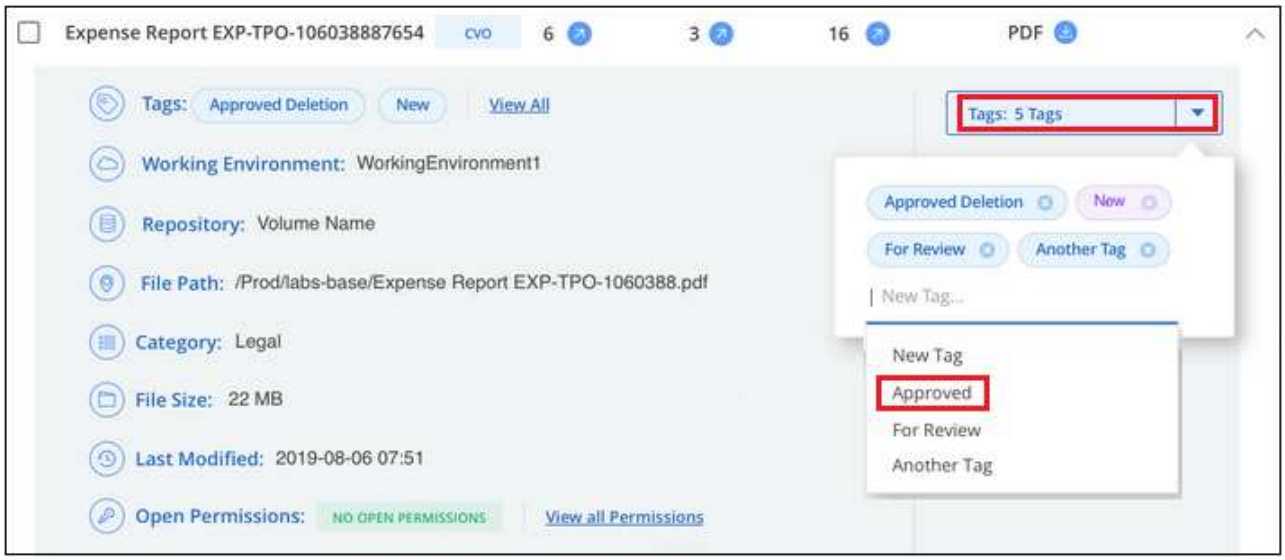
Per aggiungere un tag a un singolo file:

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

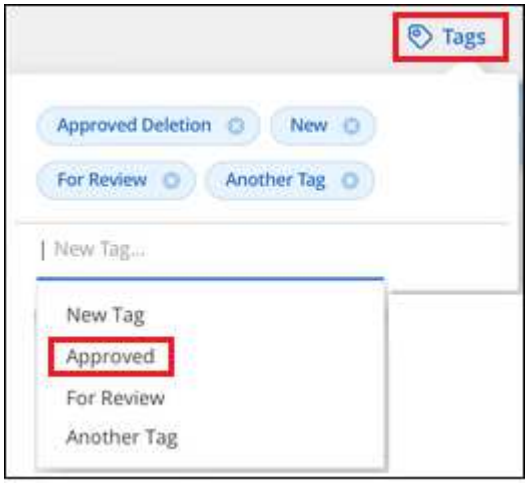
1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da contrassegnare.

   - 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).

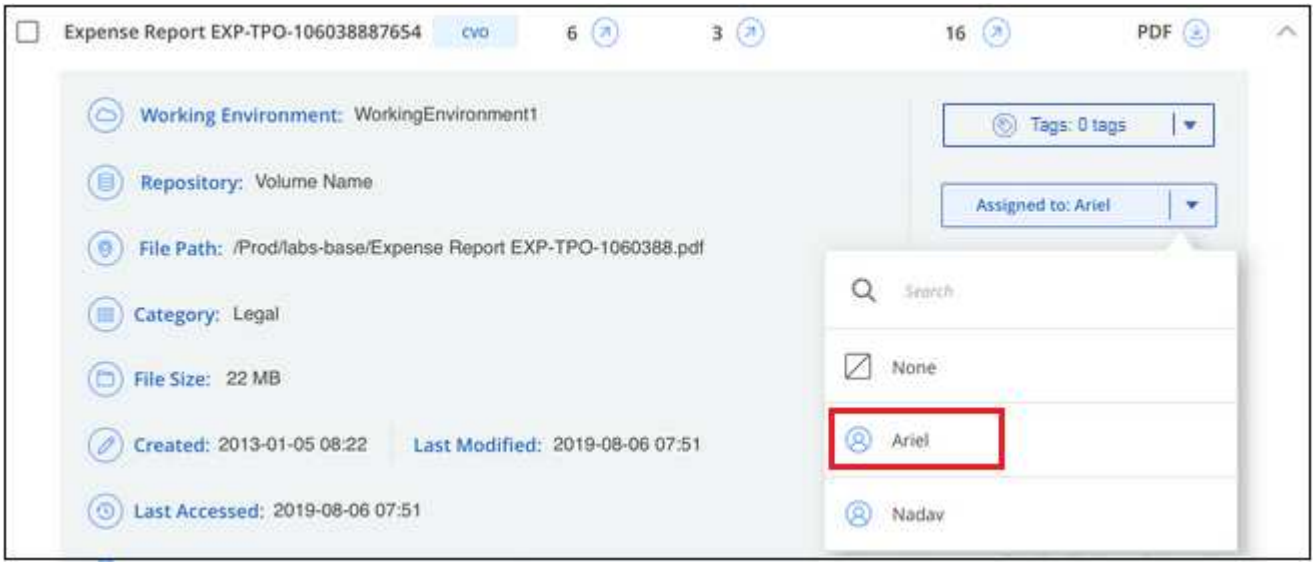
Si noti che il nome utente non viene aggiunto al file come parte dei metadati del file, ma viene visualizzato solo dagli utenti BlueXP quando si utilizza la classificazione BlueXP.

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.

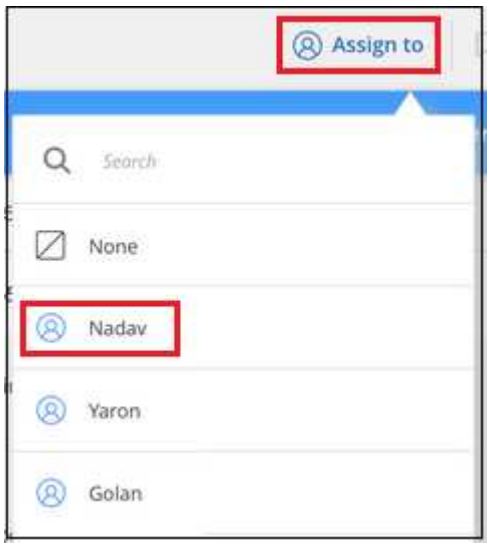
Per assegnare un utente a più file, procedere come segue. Nota: È possibile assegnare un utente a un massimo di 20 file alla volta (una pagina nell'interfaccia utente).

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

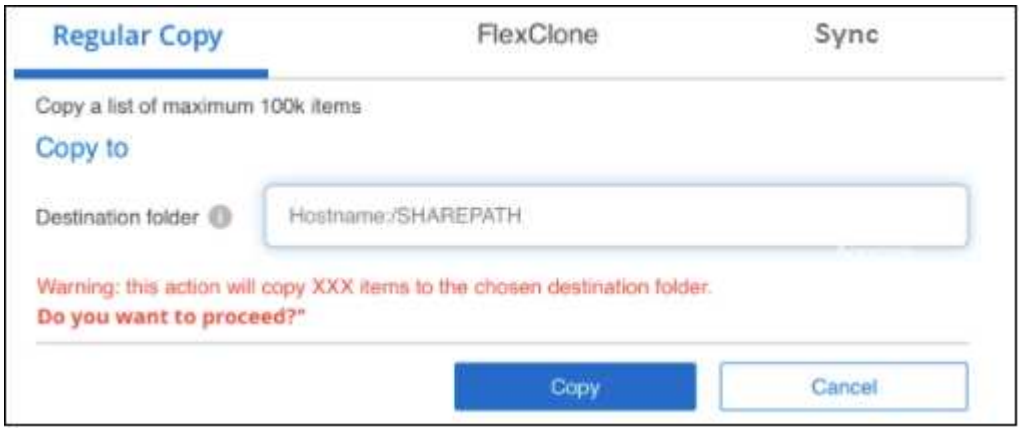
- Per copiare i file è necessario disporre delle autorizzazioni. "Informazioni sull'accesso degli utenti alle informazioni sulla conformità" .
- La copia dei file richiede che la condivisione NFS di destinazione consenta l'accesso dall'istanza di classificazione BlueXP.
- È possibile copiare da 1 a 100,000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

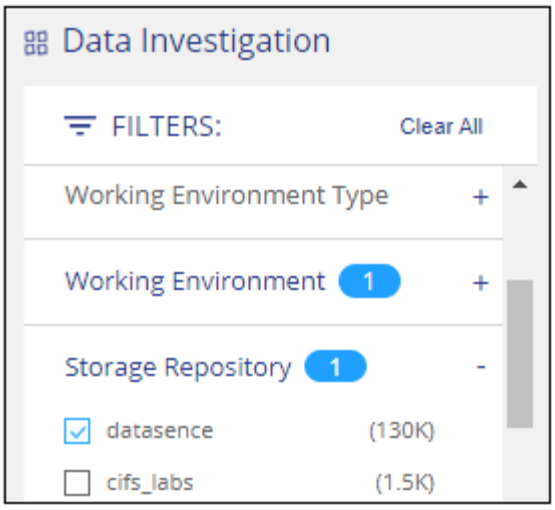
Nota: i volumi FlexGroup non possono essere clonati perché non sono supportati da FlexClone.

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.

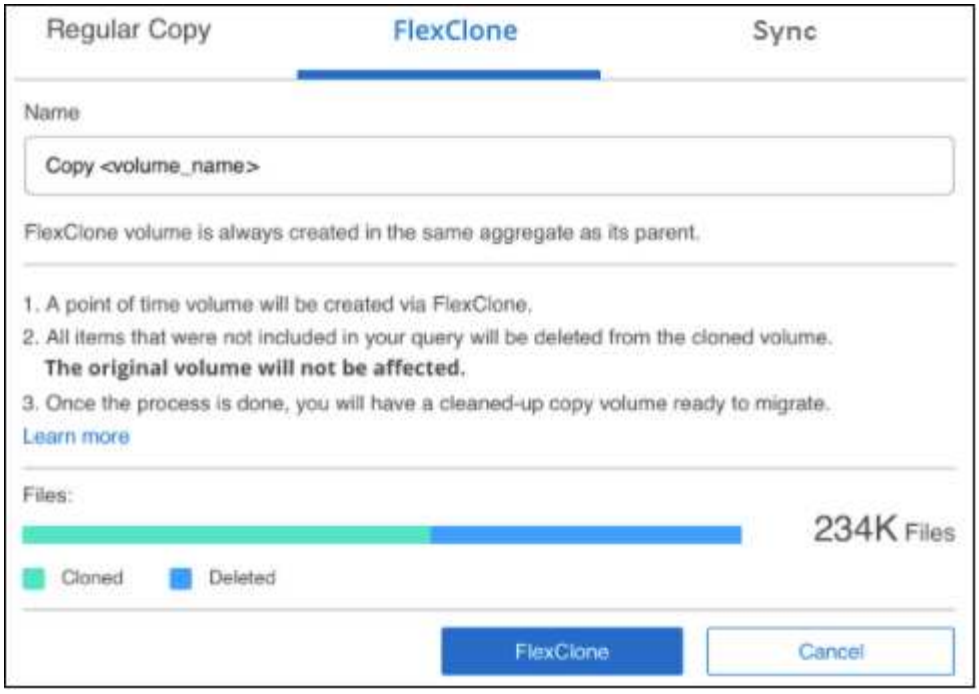


Applicare eventuali altri filtri in modo da visualizzare solo i file che si desidera clonare nel nuovo volume.

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

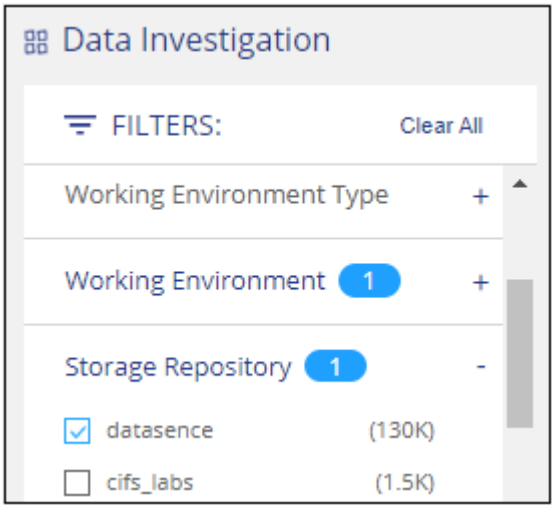
utenti alle informazioni sulla conformità" .

- 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.

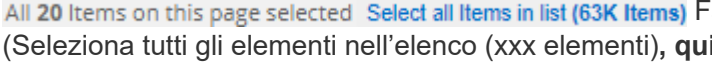
Fasi

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.

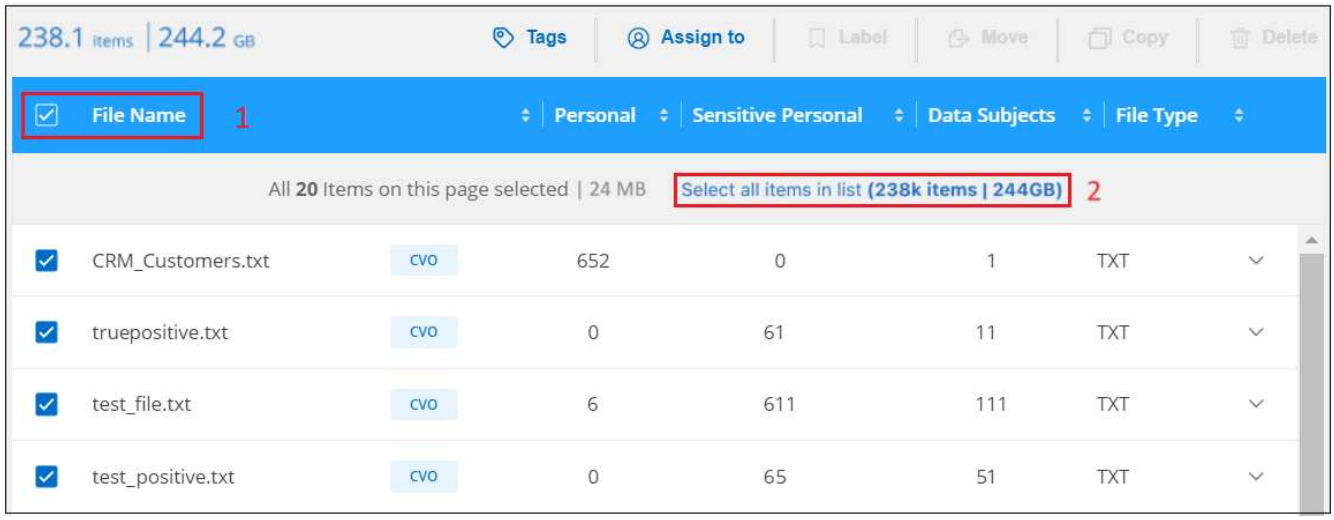


   Applicare eventuali altri filtri in modo da visualizzare solo i file che si desidera copiare e sincronizzare nel sistema di destinazione.

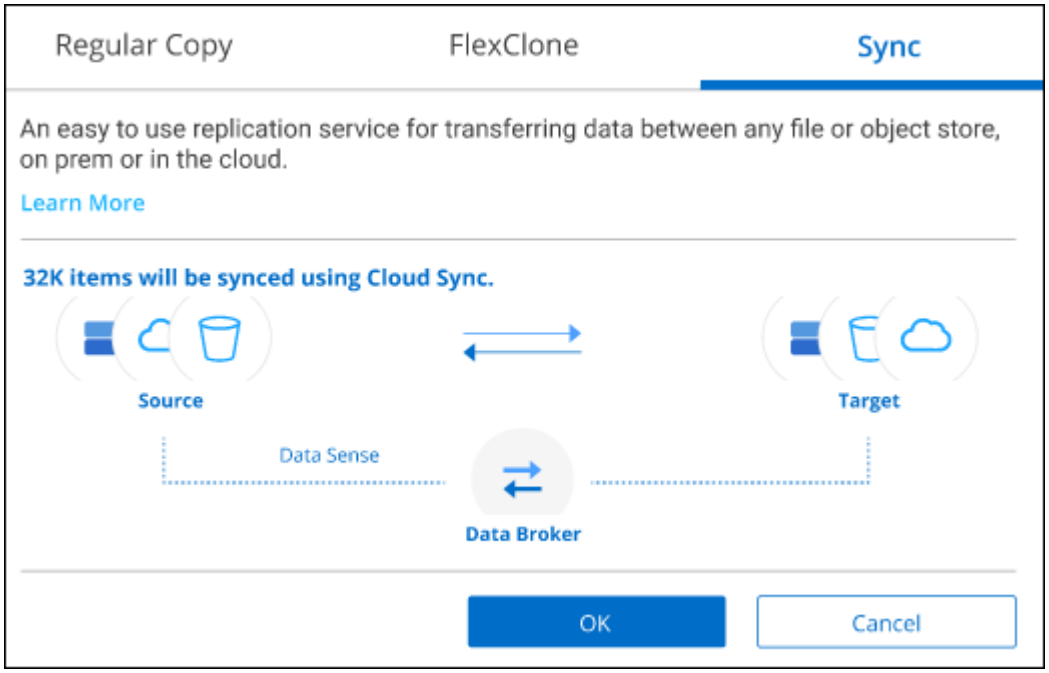
2. Nel riquadro dei risultati dell'analisi, selezionare tutti i file su tutte le pagine selezionando la casella nella riga del titolo (

), 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.

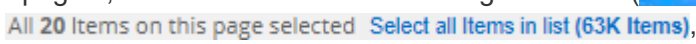
Fasi

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).

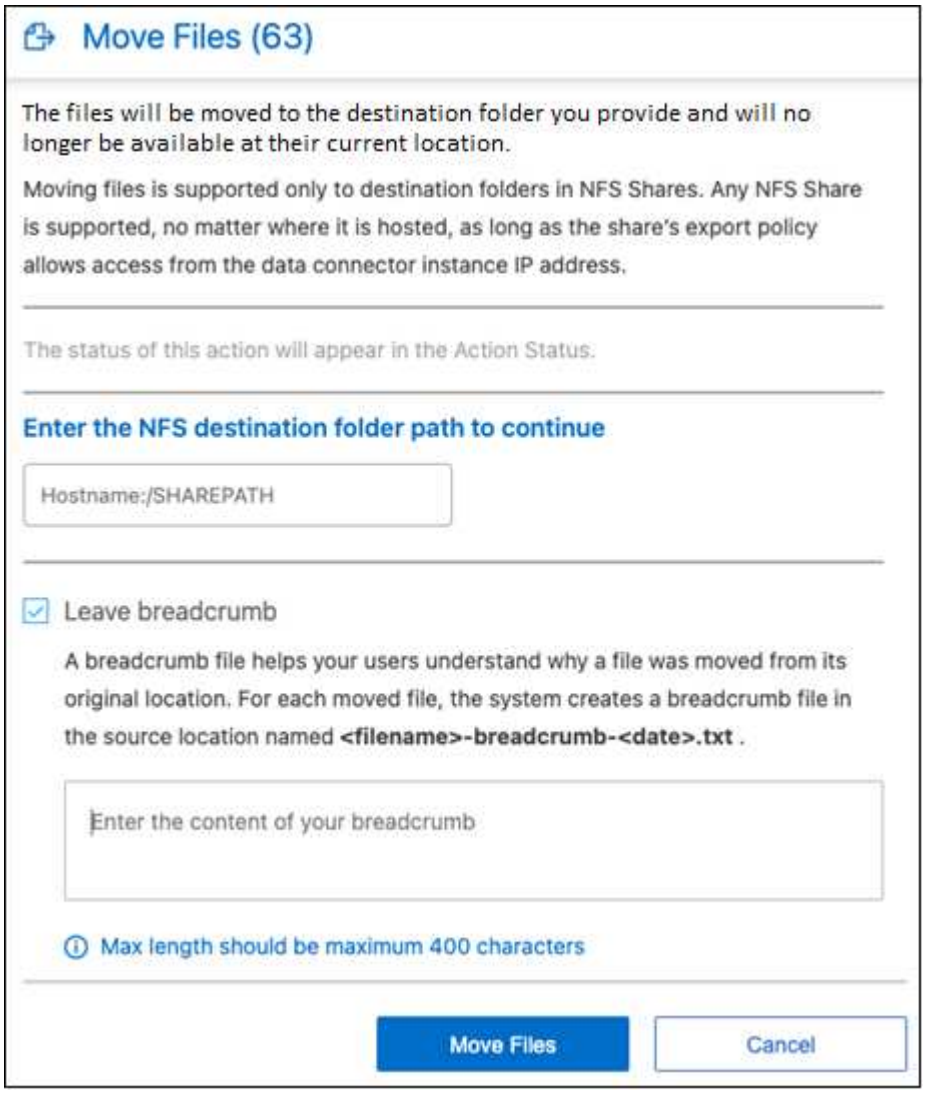
- Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (

).
- Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (

), quindi nel messaggio a comparsa 

, 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.

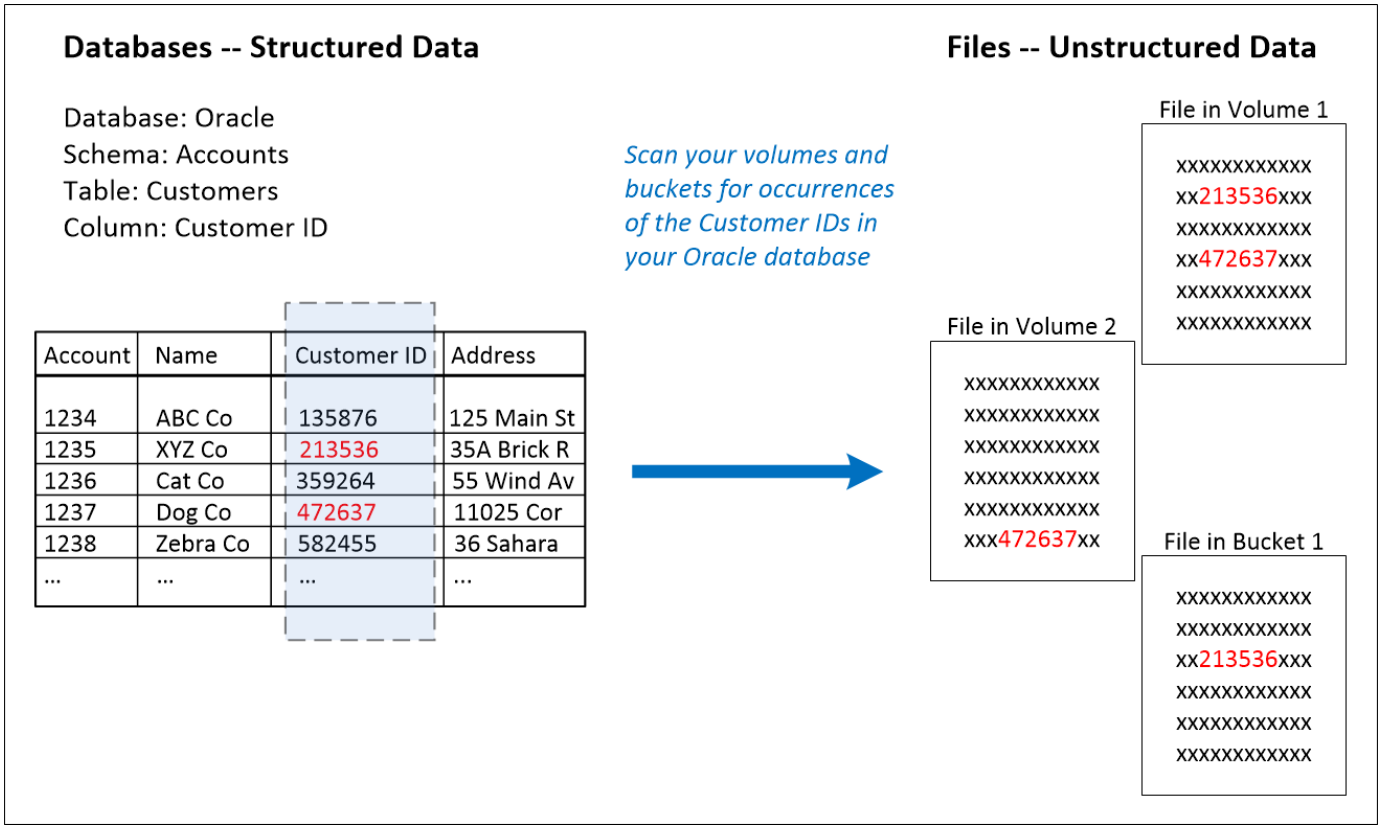
- È possibile aggiungere categorie personalizzate per identificare dove si trovano categorie specifiche di informazioni nei dati.

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.



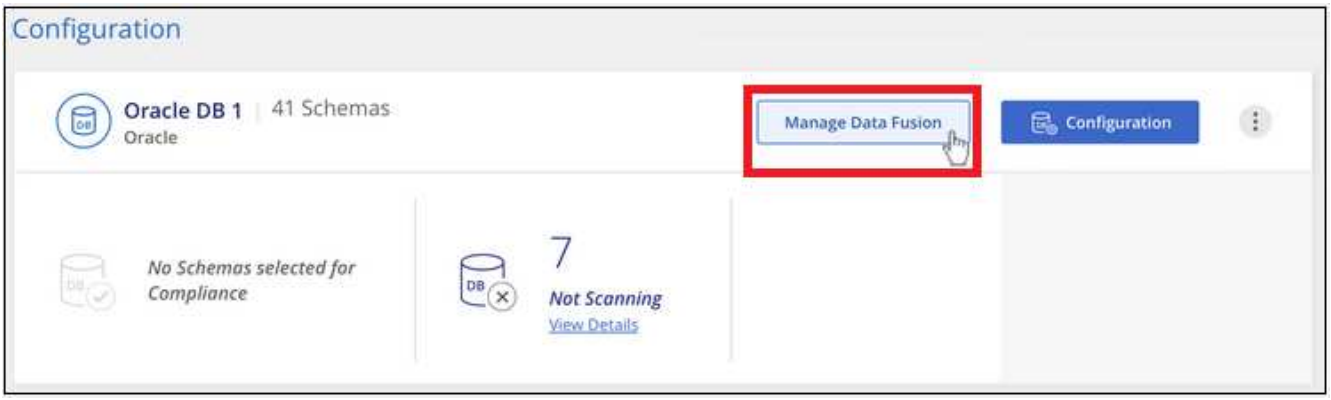
Come puoi vedere, sono stati trovati due ID cliente univoci in due volumi e in un bucket S3. Verranno identificate anche le corrispondenze presenti nelle tabelle del database.

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.



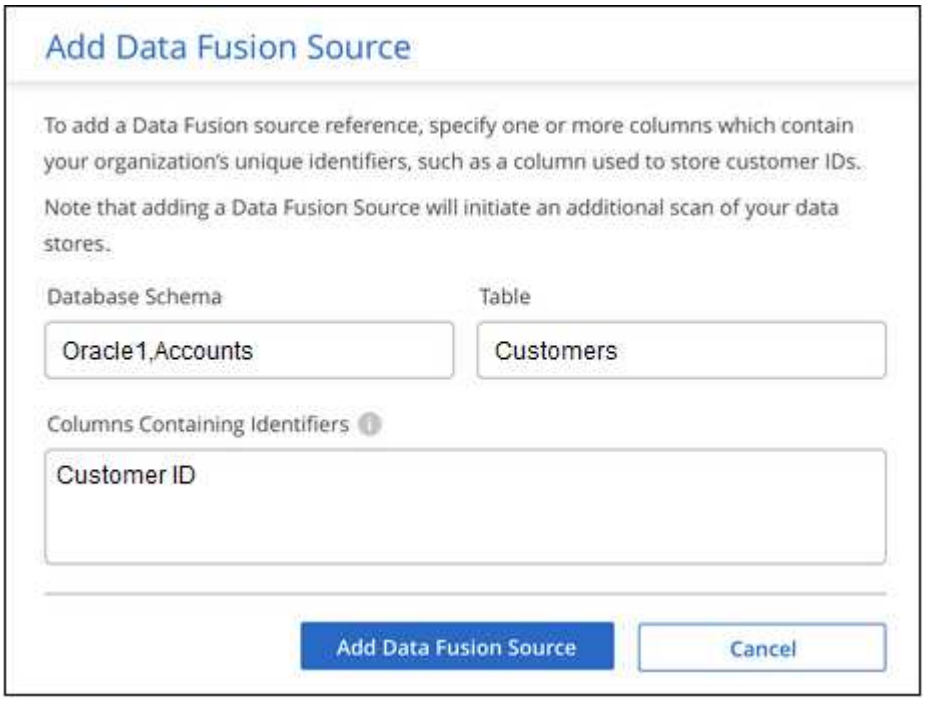
2. Fare clic su **Add Data Fusion source** (Aggiungi origine dati) nella pagina successiva.
3. Nella pagina *Aggiungi origine data Fusion*:

   a. Selezionare lo schema del database dal menu a discesa.

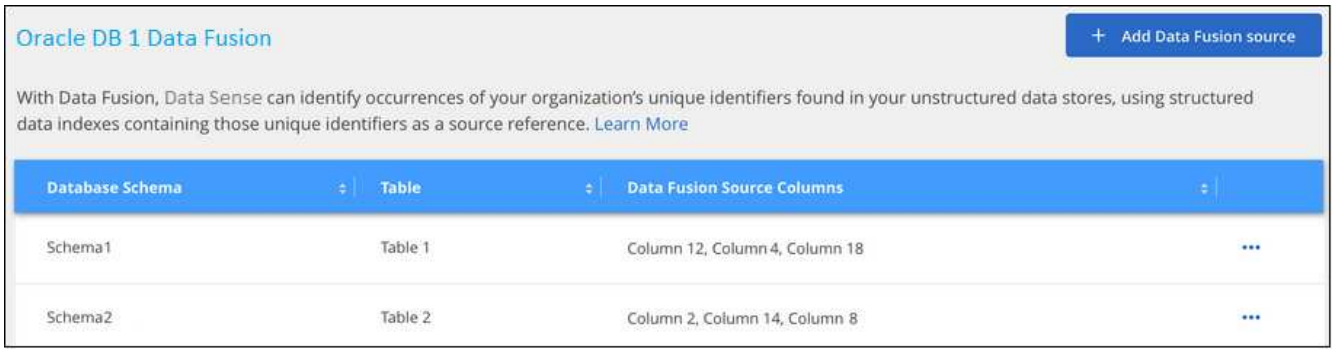
   b. Inserire il nome della tabella nello schema.

   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.

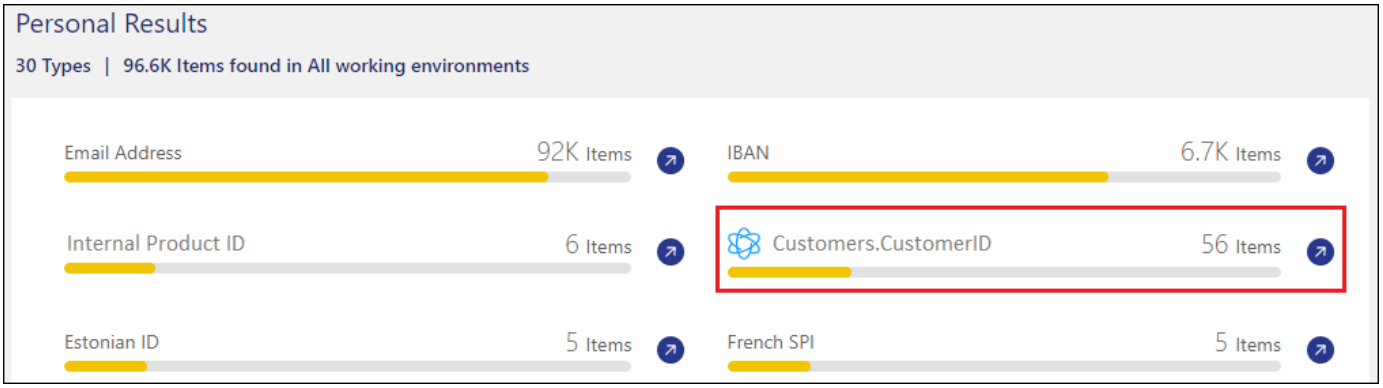


4. Fare clic su **Aggiungi origine Data Fusion**.



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.

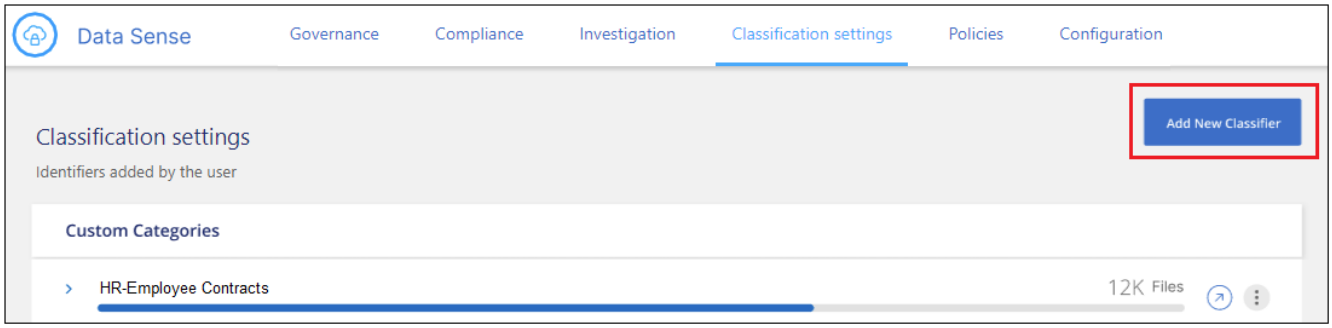
Ad esempio, è possibile visualizzare i nomi dei prodotti interni in tutti i file per assicurarsi che non siano accessibili in posizioni non sicure.

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

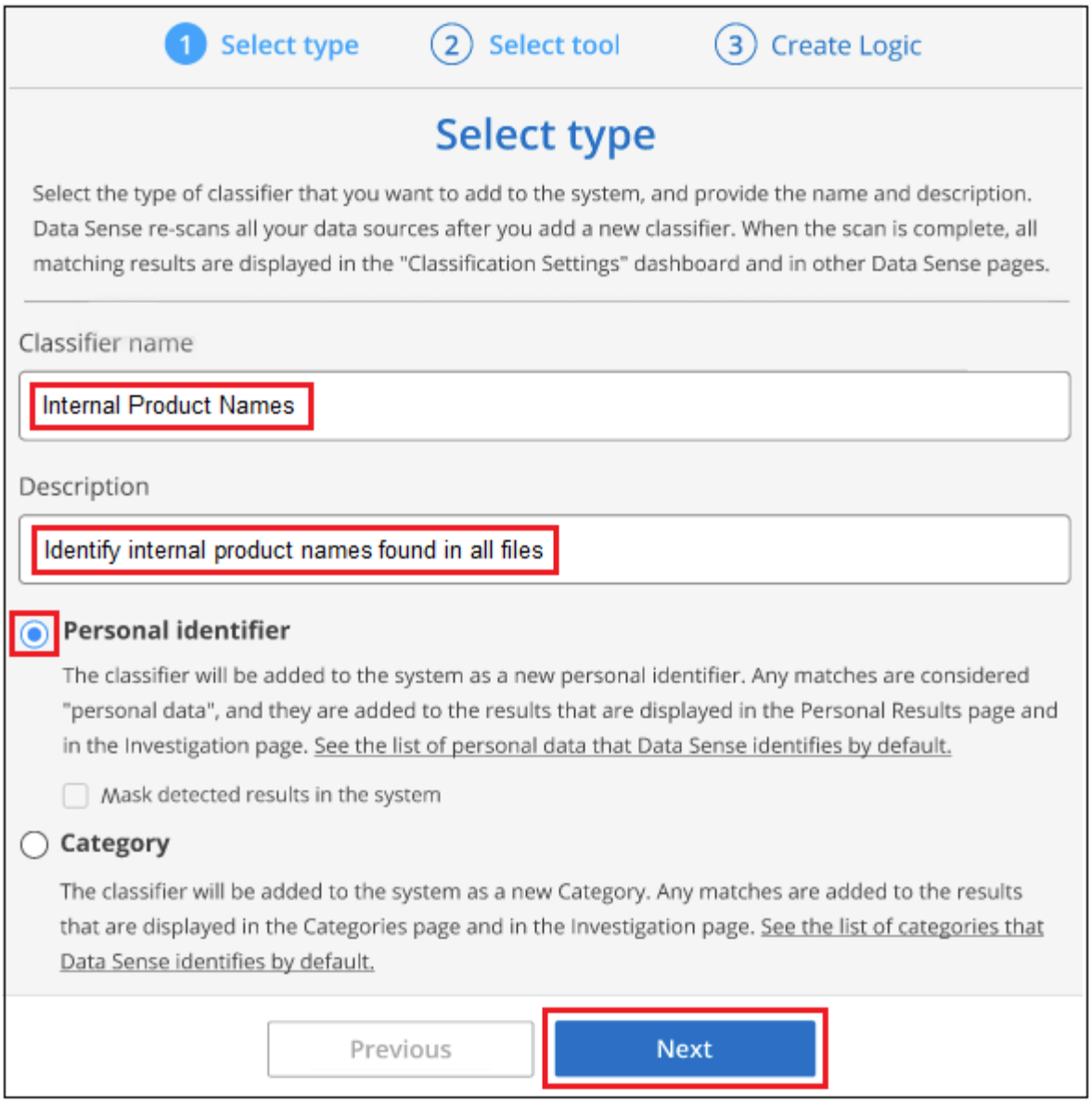
1. Dalla scheda *Impostazioni classificazione*, fare clic su **Aggiungi nuovo classificatore** per avviare la procedura guidata *Aggiungi classificatore personalizzato*.



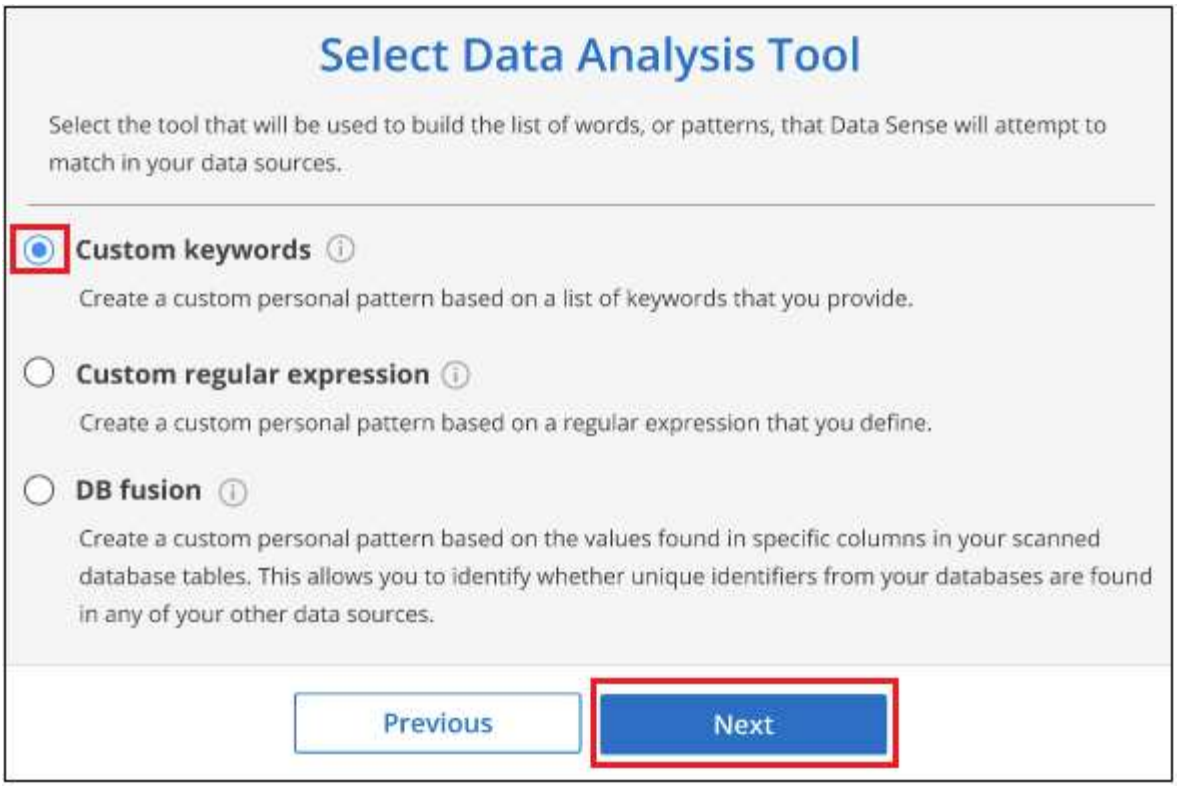
2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Personal identifier**, quindi fare clic su **Next**.

   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).

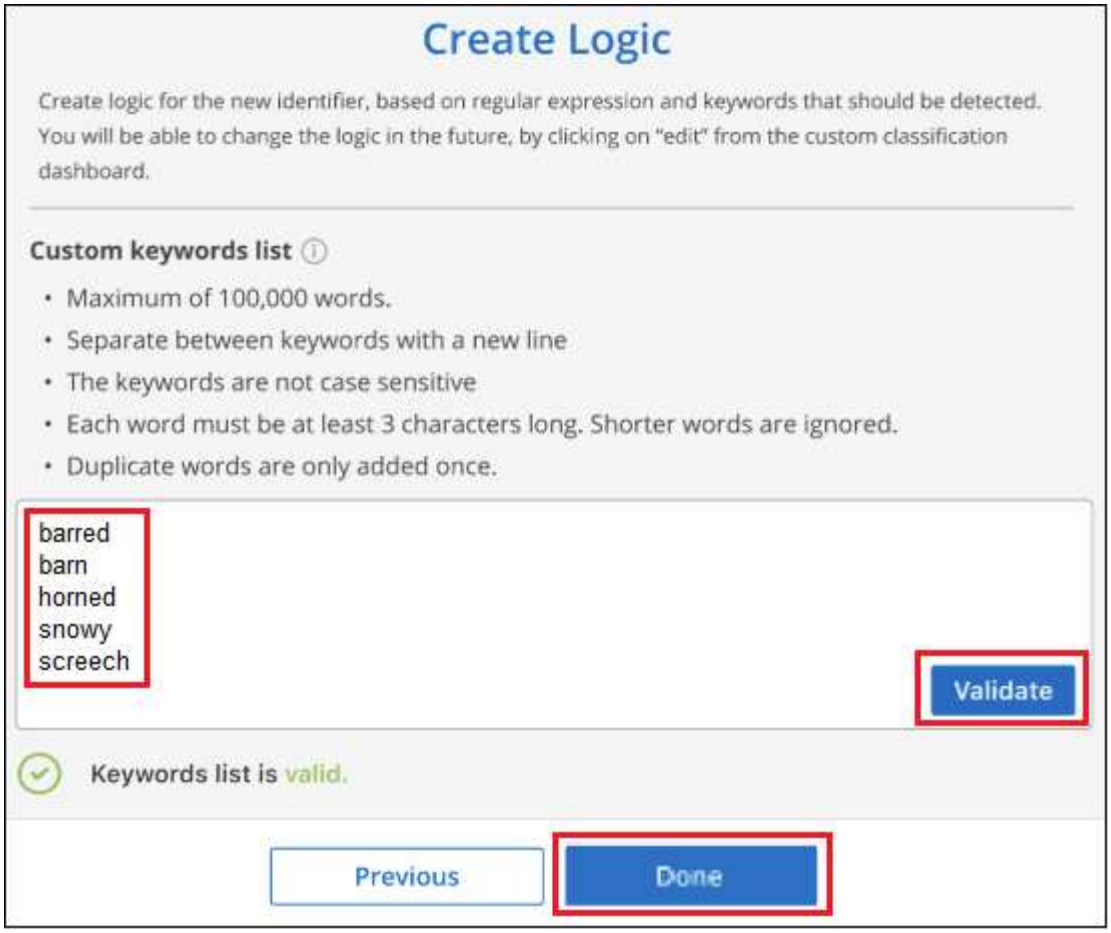


3. Nella pagina *Select Data Analysis Tool*, selezionare **Custom Keywords** come metodo da utilizzare per definire il classificatore, quindi fare clic su **Next**.



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

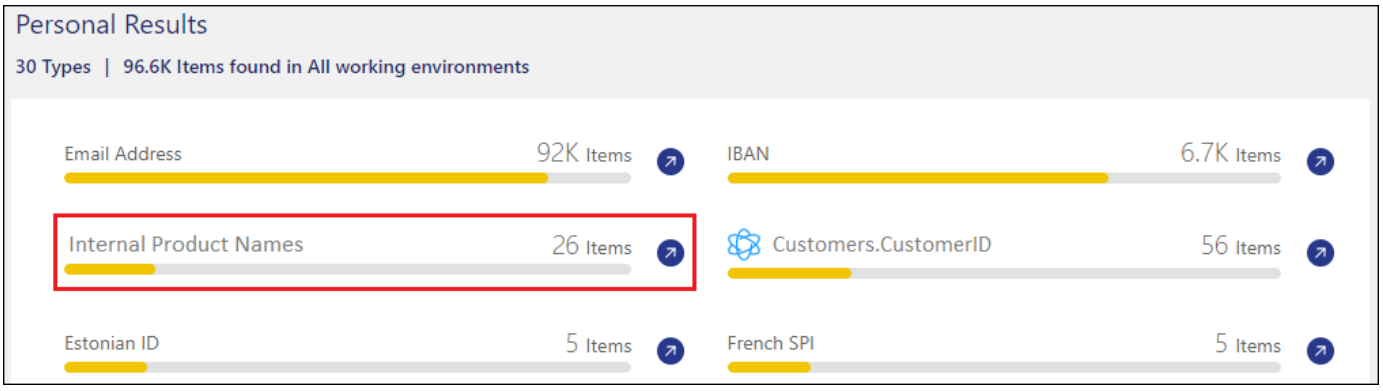
   La schermata seguente mostra i nomi dei prodotti interni (diversi tipi di gufi). La ricerca della classificazione BlueXP per questi elementi non fa distinzione tra maiuscole e minuscole.



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**.

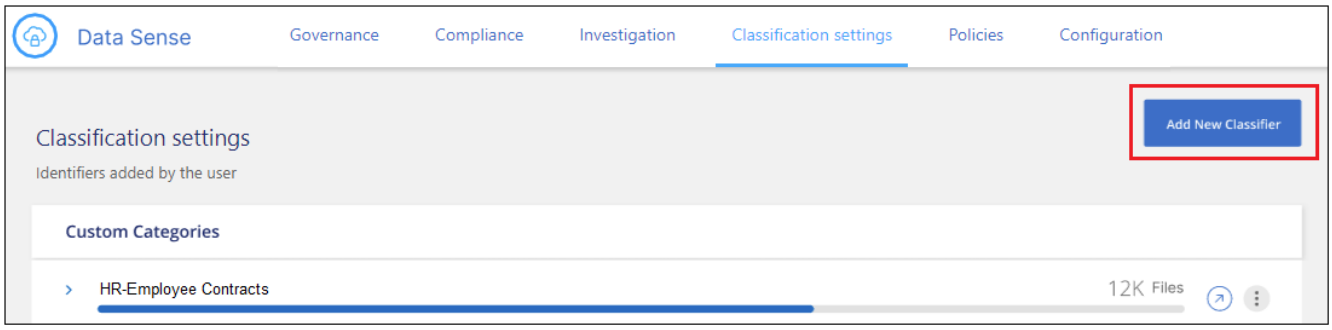
Dopo aver aggiunto il regex, la classificazione BlueXP riavvia la scansione di tutte le origini dati. Una volta completata la scansione, i nuovi risultati verranno visualizzati nella dashboard di conformità della classificazione BlueXP nella sezione "risultati personali" e nella pagina delle indagini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

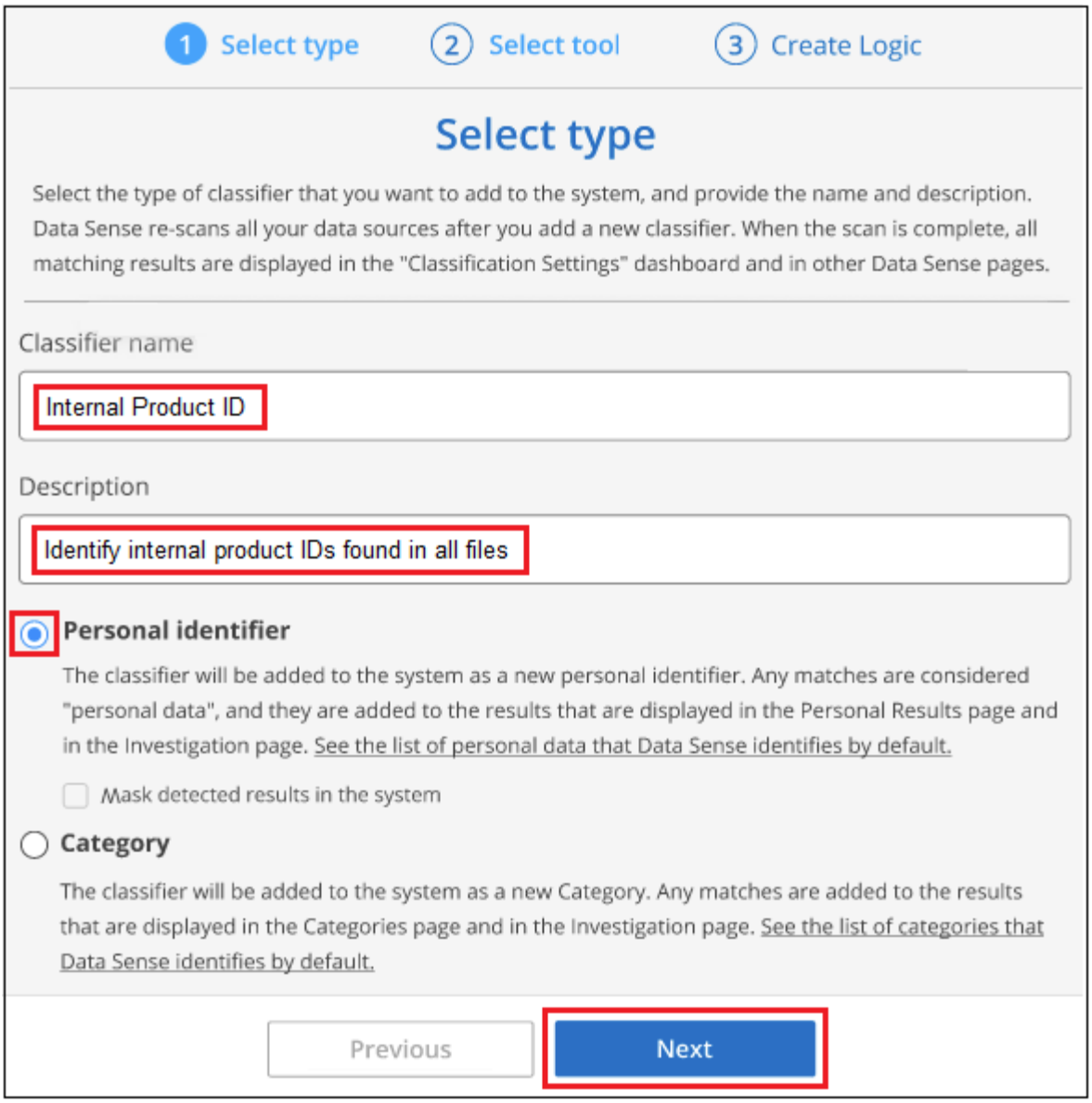
Fasi

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

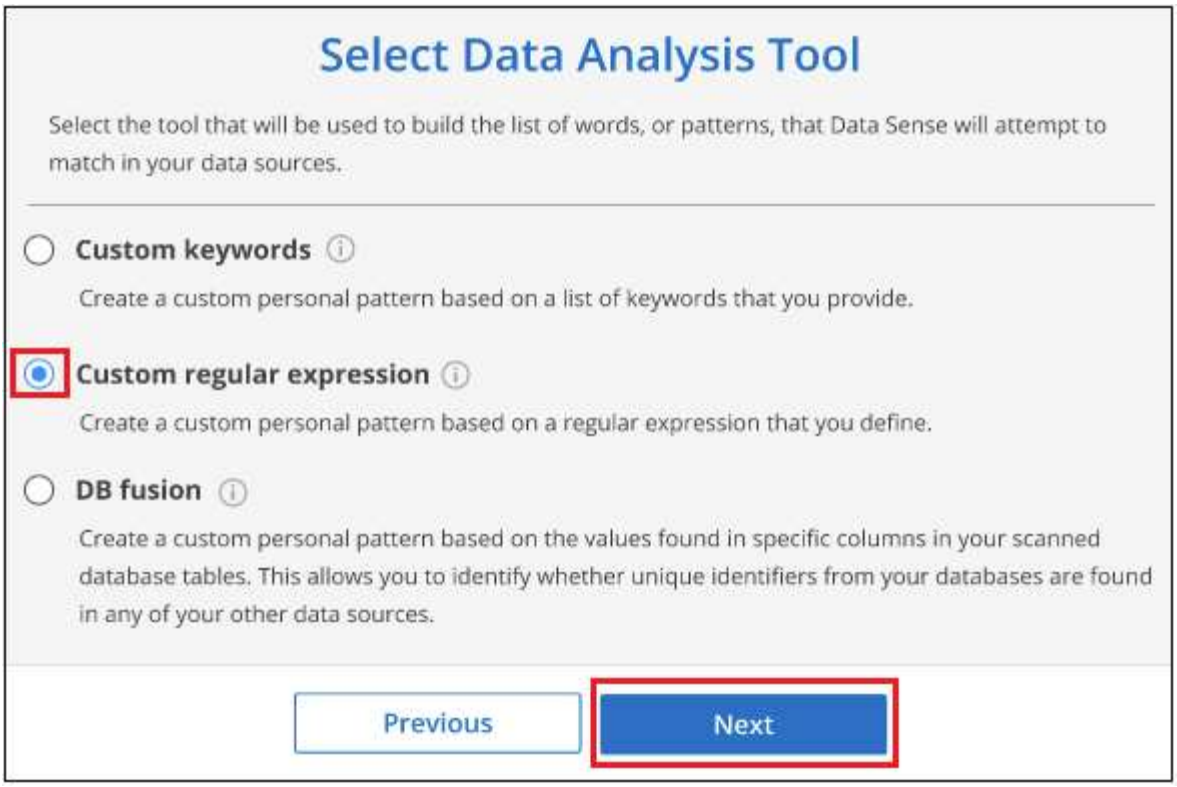


2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Personal identifier**, quindi fare clic su **Next**.

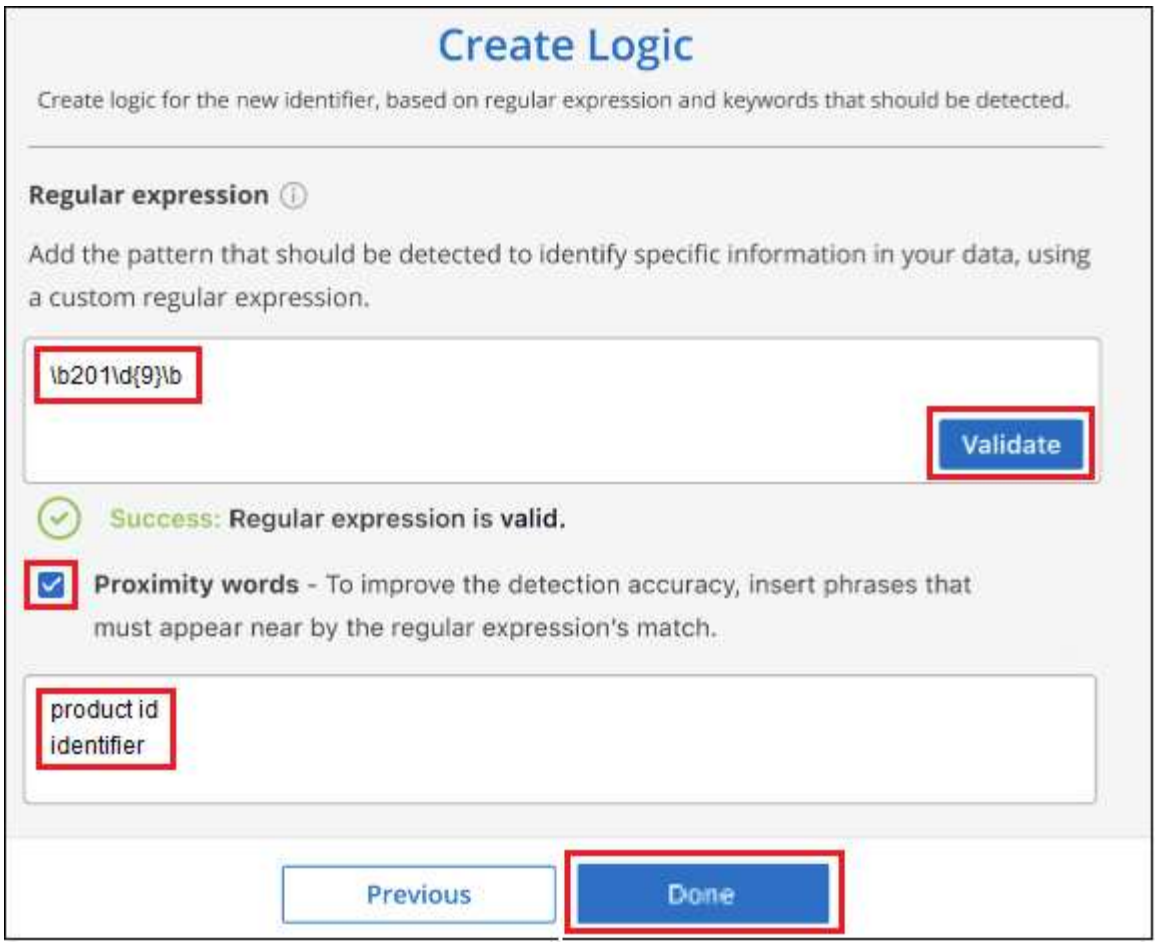
   Il nome immesso viene visualizzato nell'interfaccia utente di classificazione BlueXP come intestazione per i file sottoposti a scansione che corrispondono ai requisiti del classificatore e come nome del filtro nella pagina di analisi. Puoi anche selezionare la casella "Mask Detected Results in the system" (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**.

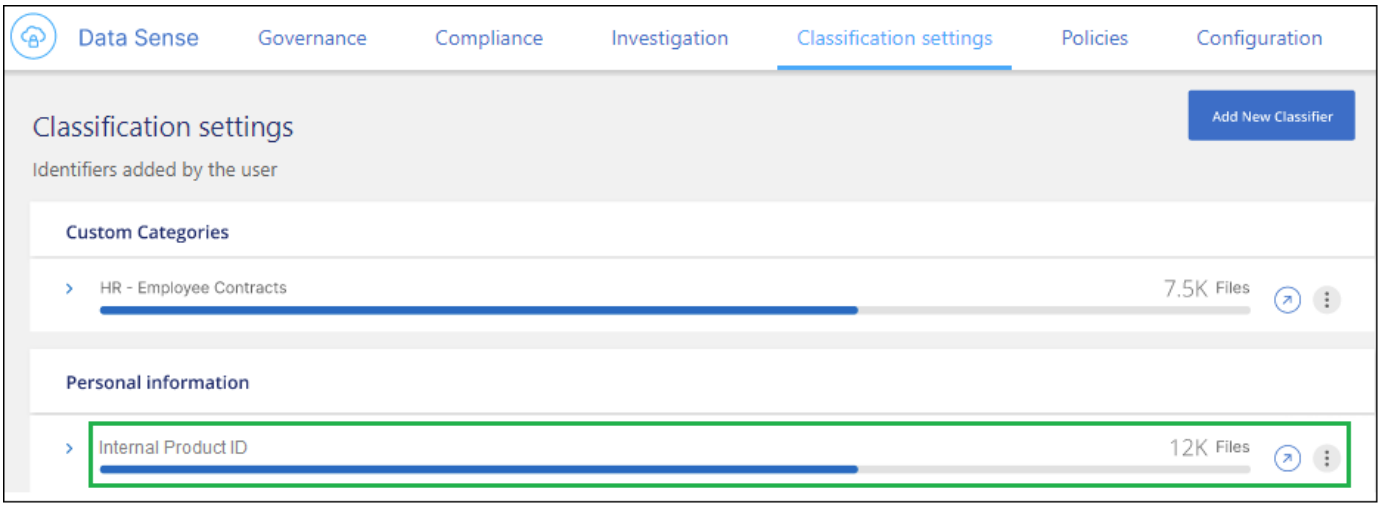


4. Nella pagina *Create Logic*, immettere l'espressione regolare e le parole di prossimità, quindi fare clic su **Done**.
   a. È possibile immettere qualsiasi espressione regolare legale. Fare clic sul pulsante **Validate** (convalida) per verificare che la classificazione BlueXP sia valida e che non 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

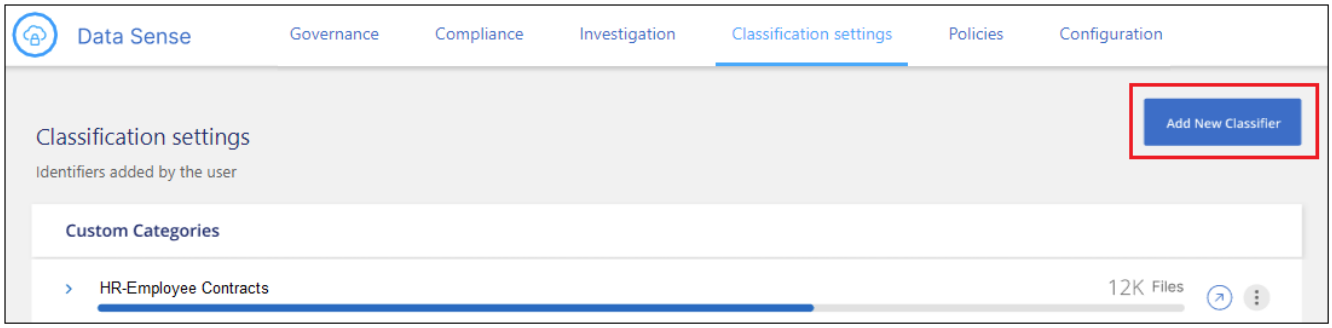
È necessario creare un minimo di 25 file di training contenenti esempi delle categorie di dati che si desidera vengano riconosciute dalla classificazione BlueXP. Sono supportati i seguenti tipi di file:

`.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.

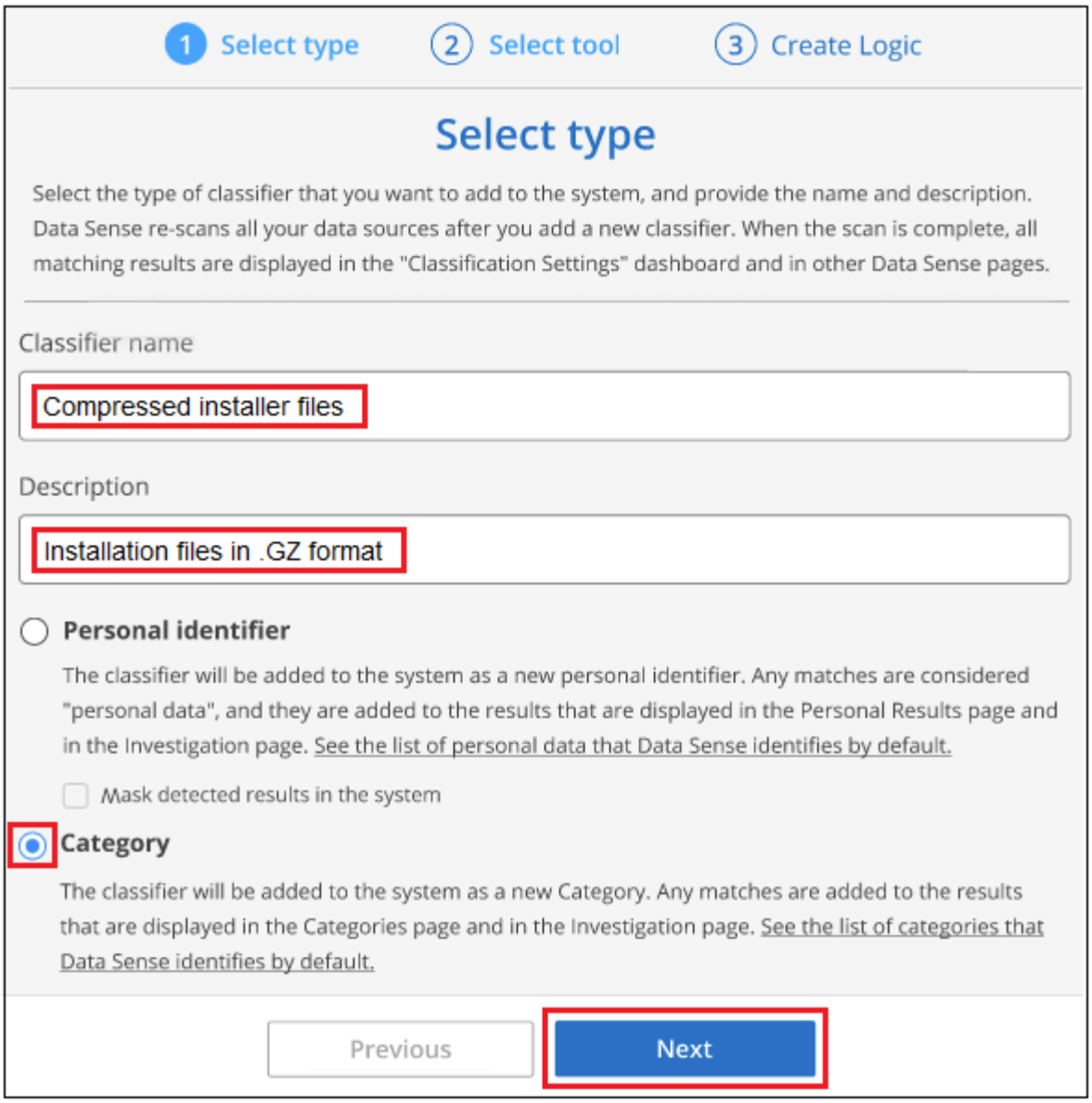
Fasi

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

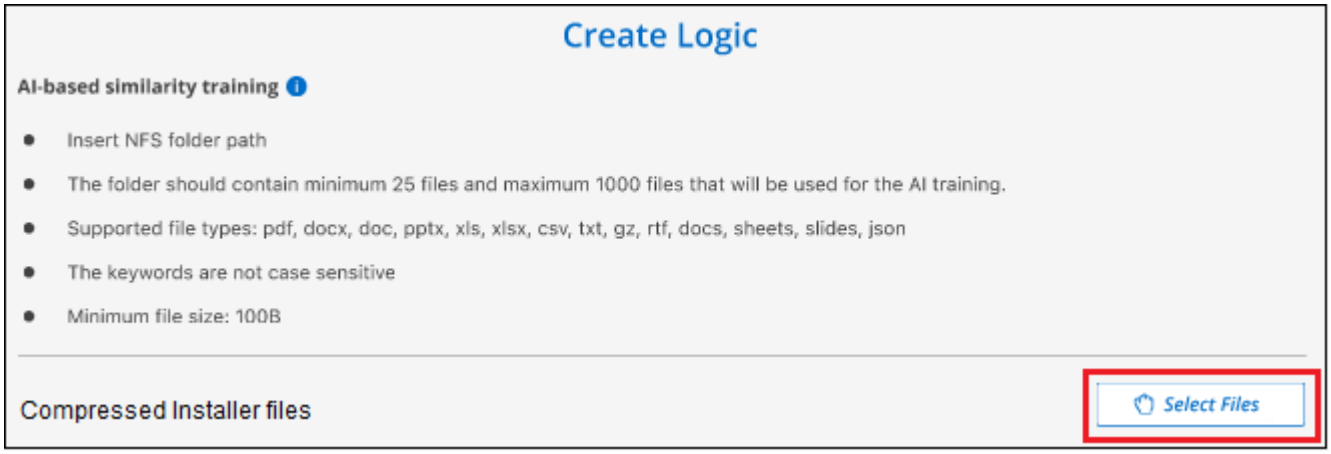


2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Category**, quindi fare clic su **Next**.

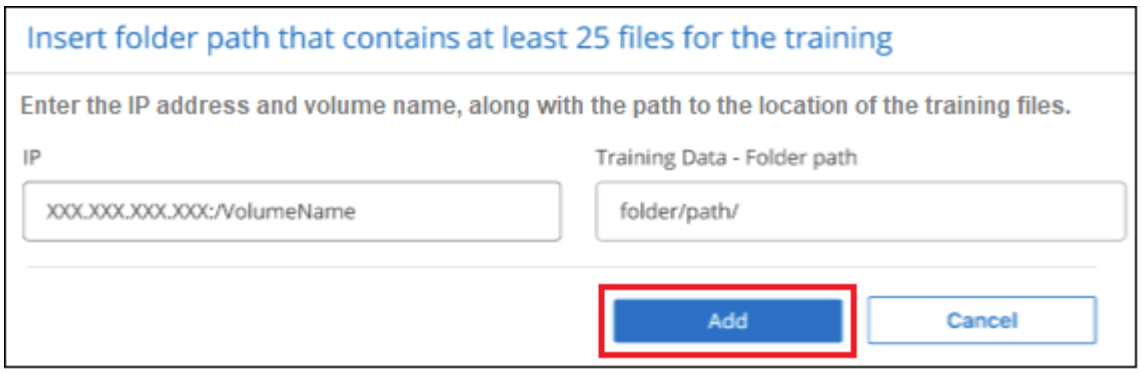
   Il nome immesso viene visualizzato nell'interfaccia utente di classificazione BlueXP come intestazione per i file sottoposti a scansione che corrispondono alla categoria di dati che si sta definendo e come nome del filtro nella pagina di analisi.



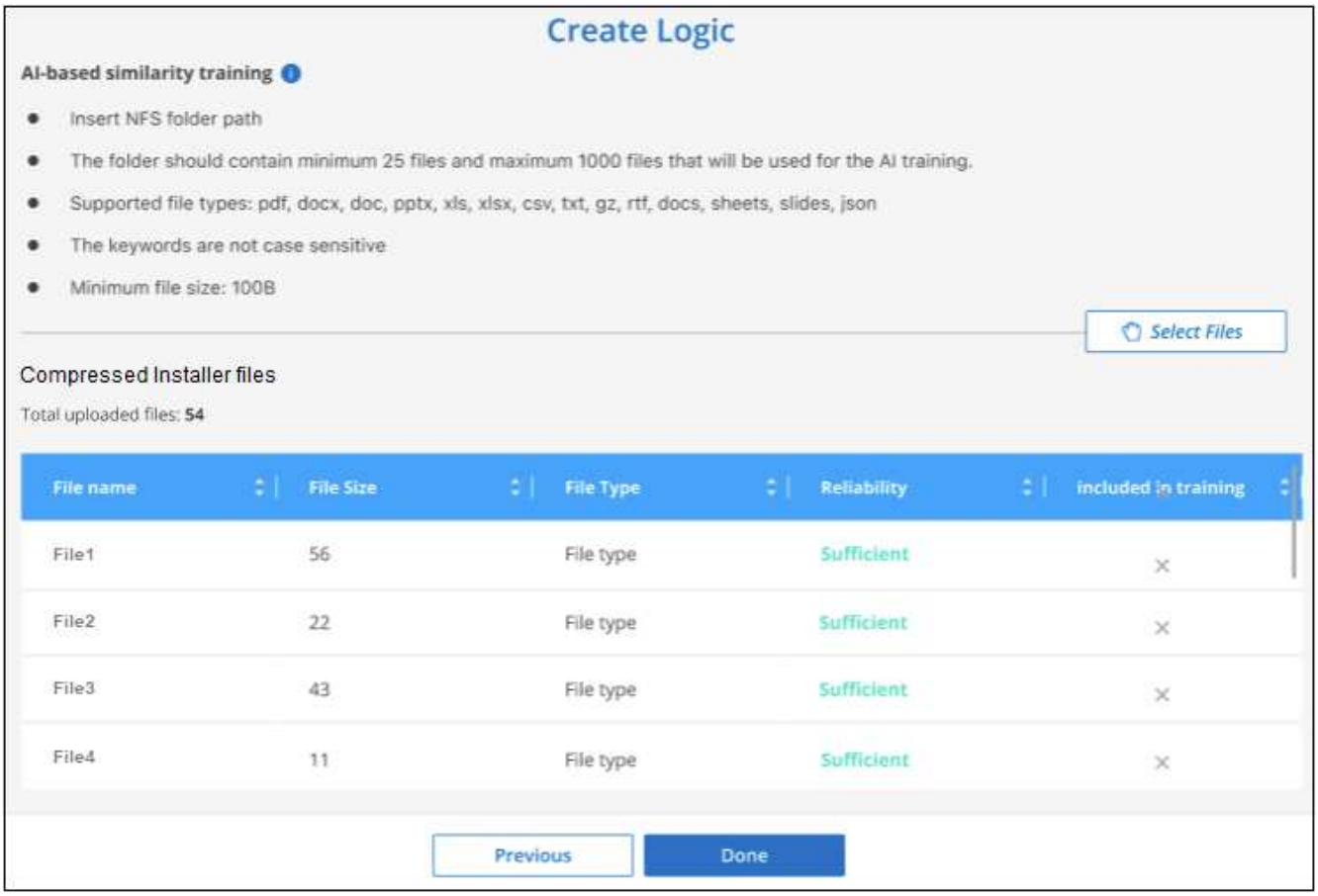
3. Nella pagina *Create Logic*, assicurarsi di aver preparato i file di apprendimento, quindi fare clic su **Select Files** (Seleziona file).



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**.



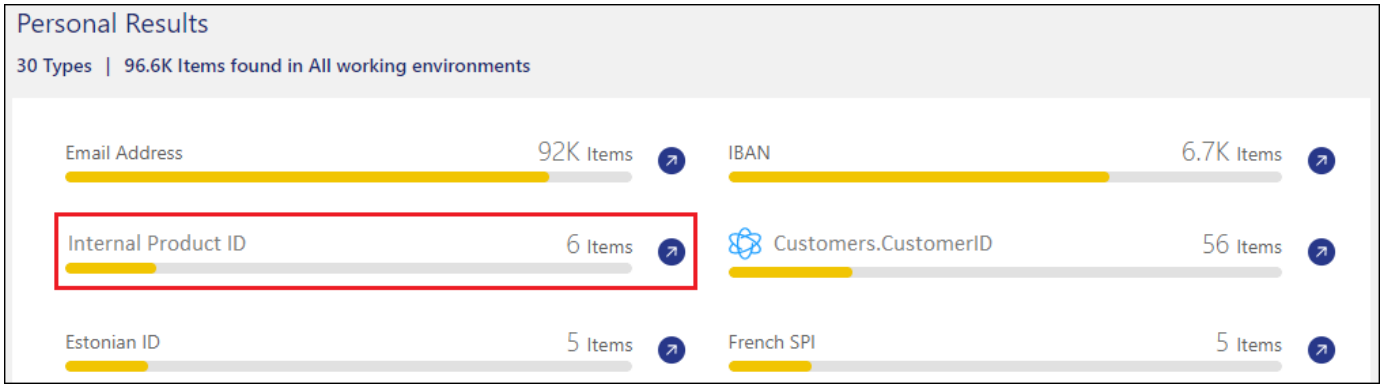
Risultati

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

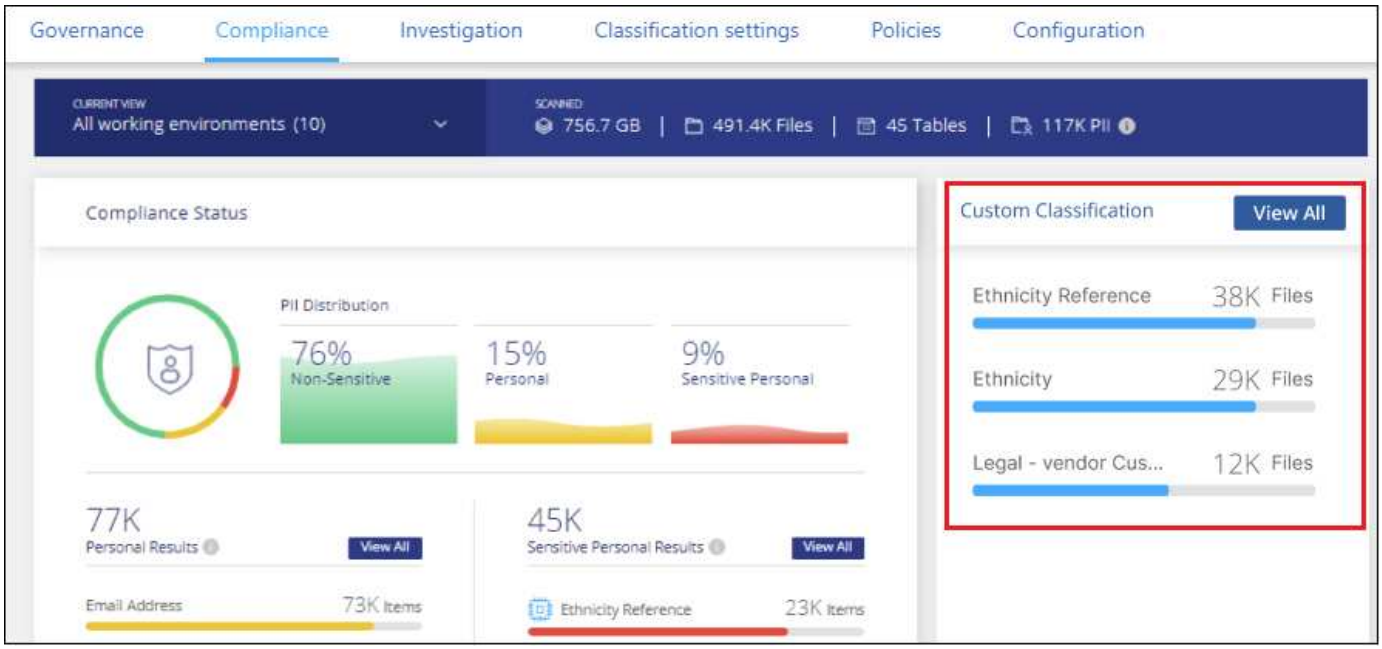
È possibile visualizzare i risultati da qualsiasi classificatore personalizzato nella dashboard di conformità e nella pagina di analisi. Ad esempio, questa schermata mostra le informazioni corrispondenti nella dashboard di

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.

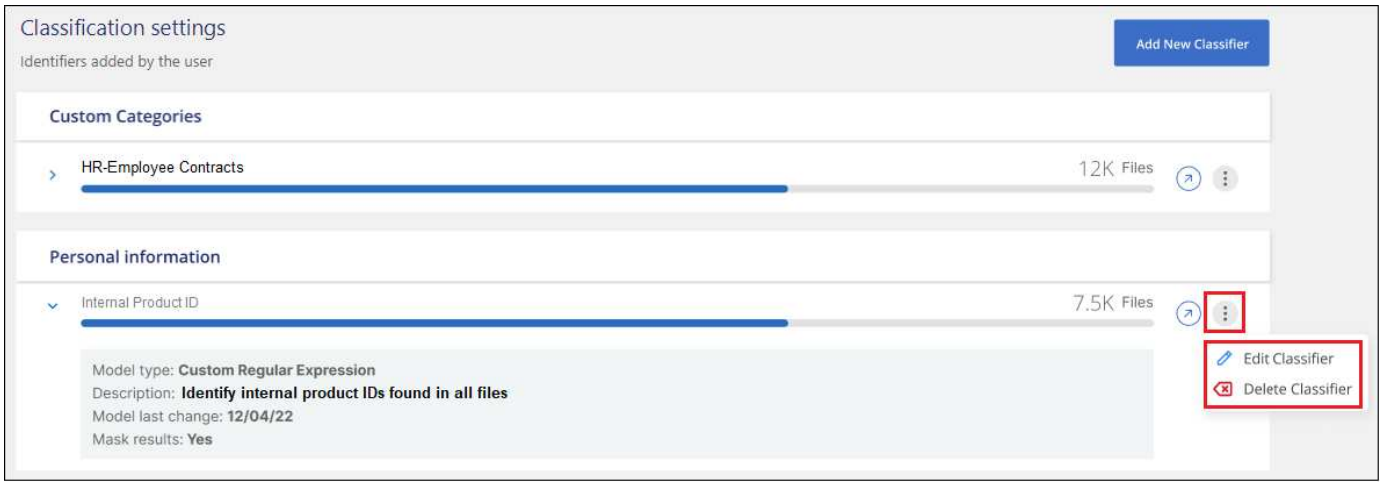


Gestire classificatori personalizzati

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.

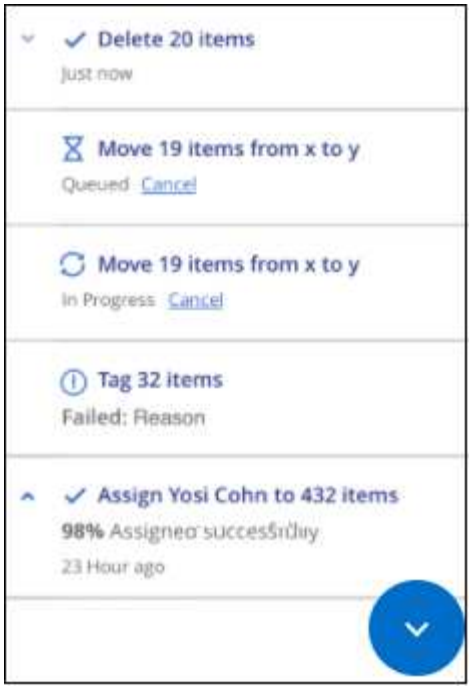
Lo stato può essere:

- 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".

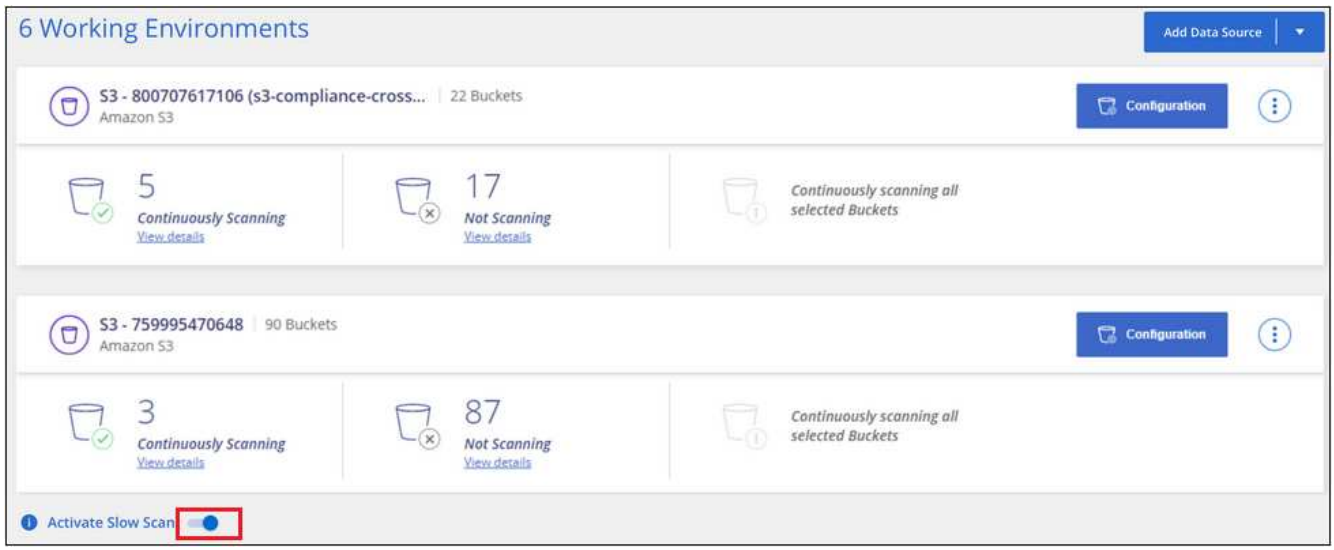
Se attivata, la scansione lenta viene utilizzata su tutte le origini dati, non è possibile configurare la scansione lenta per un singolo ambiente di lavoro o un'origine dati.

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

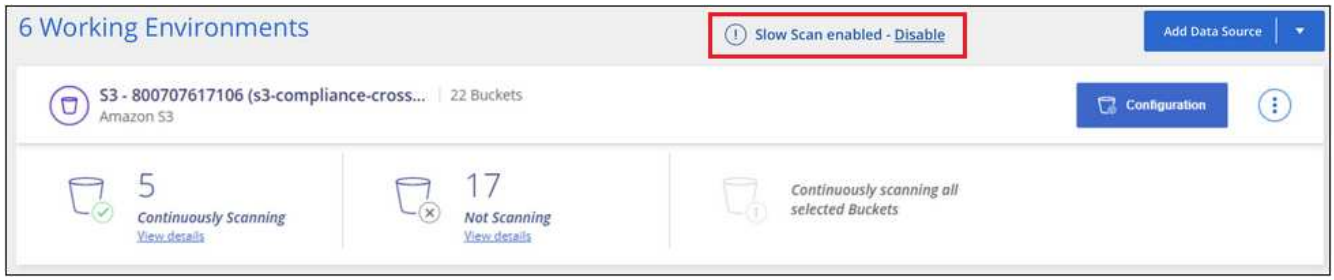
Queste informazioni sono rilevanti solo per le versioni precedenti della classificazione BlueXP 1,30 e precedenti.

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.

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.