Gestire la classificazione BlueXP

BlueXP classification

NetApp
April 03, 2024

Sommario

Gestire la classificazione BlueXP

Aggiungi identificatori di dati personali alle scansioni di classificazione BlueXP

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

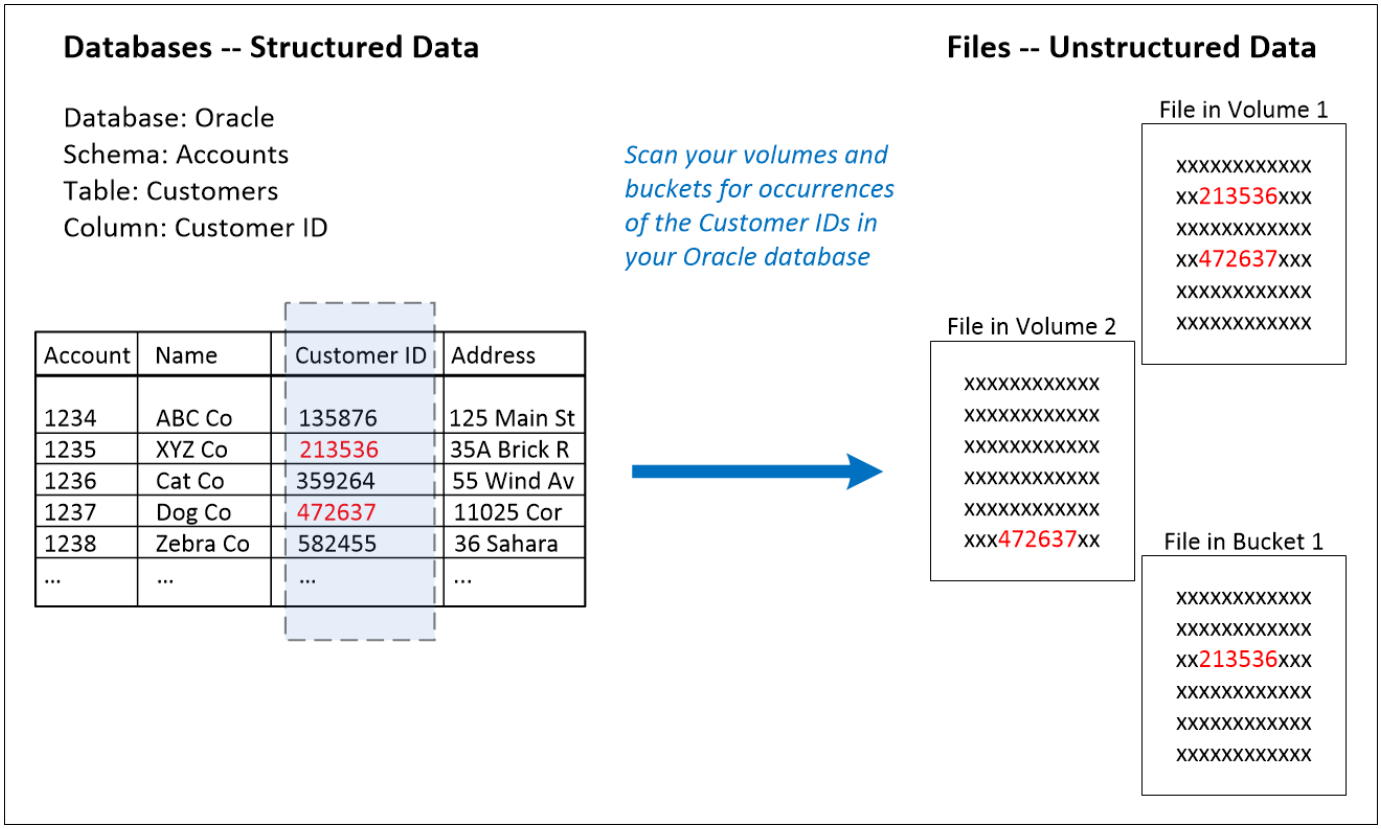
- È possibile aggiungere identificatori univoci in base a colonne specifiche nei database che si sta eseguendo la scansione.
- È possibile aggiungere parole chiave personalizzate da un file di testo — queste parole sono identificate all'interno dei dati.
- È possibile aggiungere un modello personale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

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

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

Aggiungere identificatori di dati personali personalizzati dai database

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



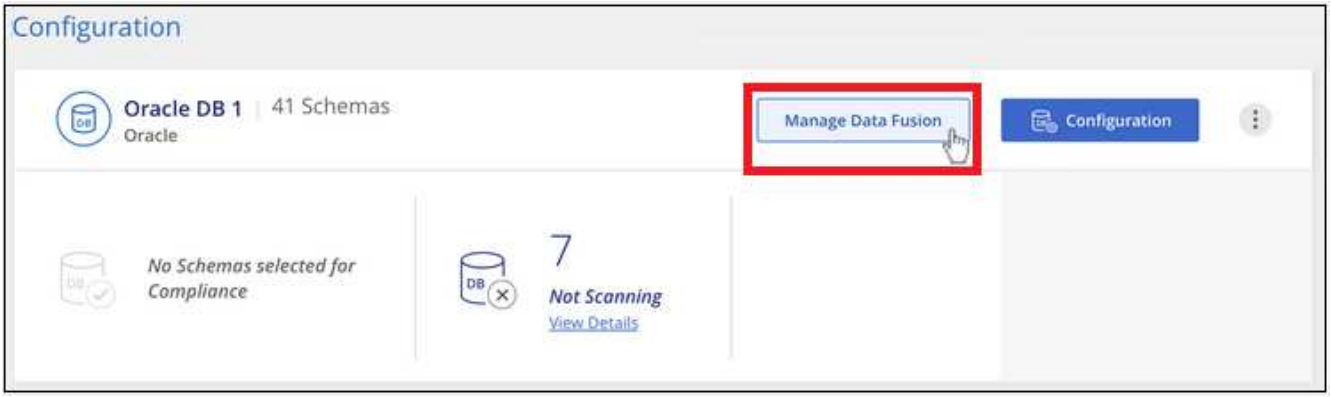
Come puoi vedere, sono stati trovati due ID cliente univoci in due volumi e in un bucket S3. Verranno identificate anche le corrispondenze presenti nelle tabelle del database.

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

Fasi

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

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



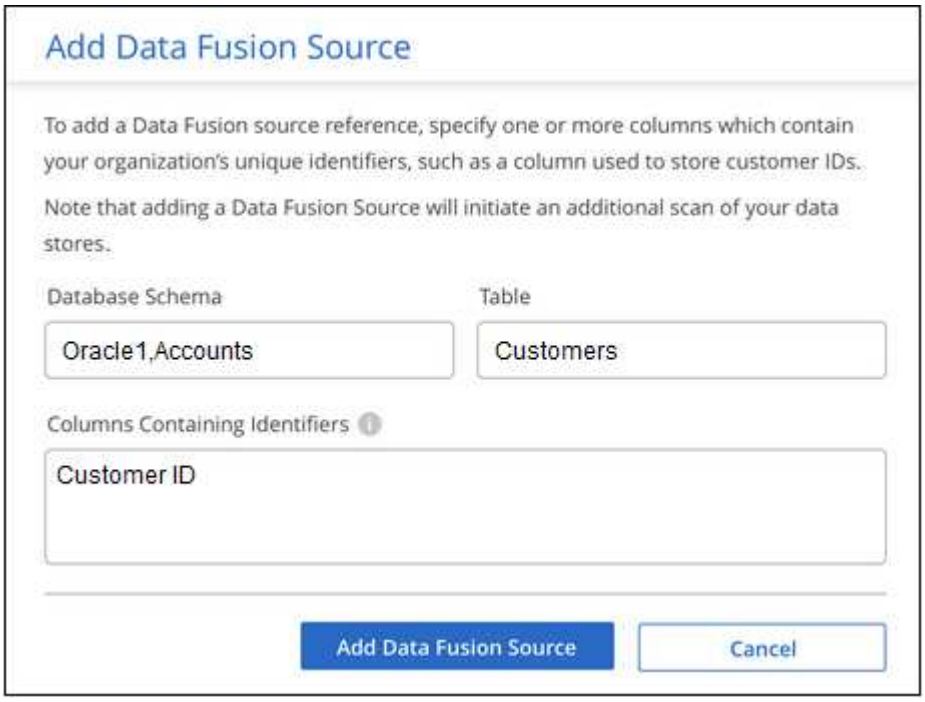
2. Fare clic su **Add Data Fusion source** (Aggiungi origine dati) nella pagina successiva.
3. Nella pagina *Aggiungi origine data Fusion*:

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

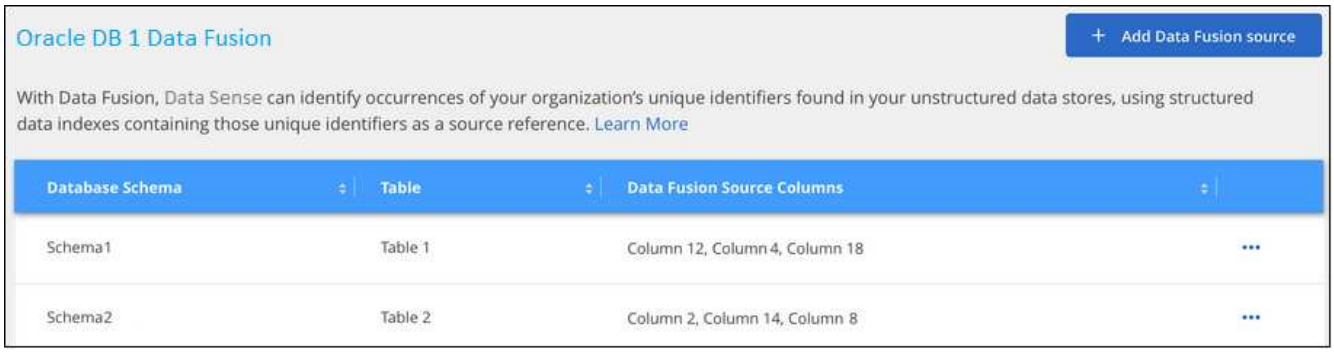
b. Inserire il nome della tabella nello schema.

c. Inserire la colonna o le colonne che contengono gli identificatori univoci che si desidera utilizzare.

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

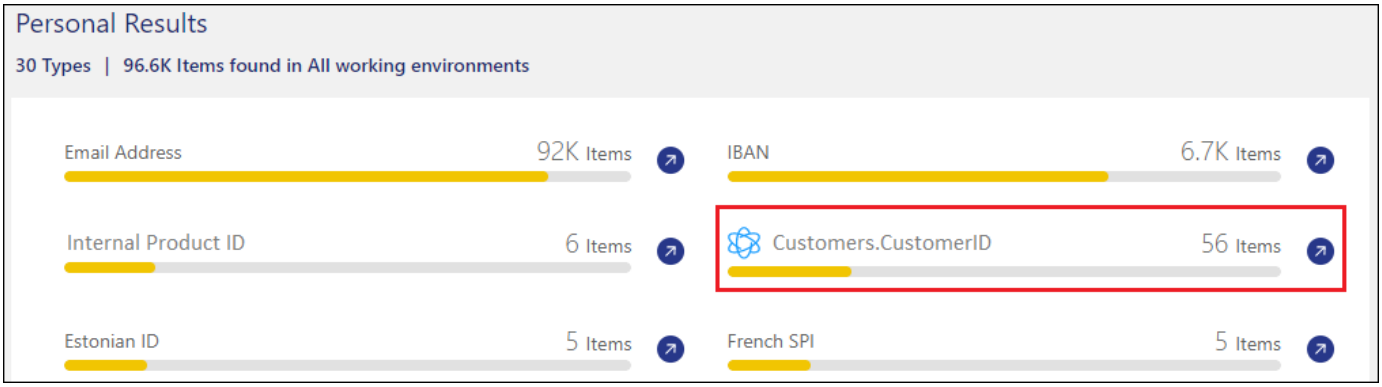


4. Fare clic su **Aggiungi origine Data Fusion**.



Risultati

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



Eliminare un'origine Data Fusion

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

Aggiungere parole chiave personalizzate da un elenco di parole

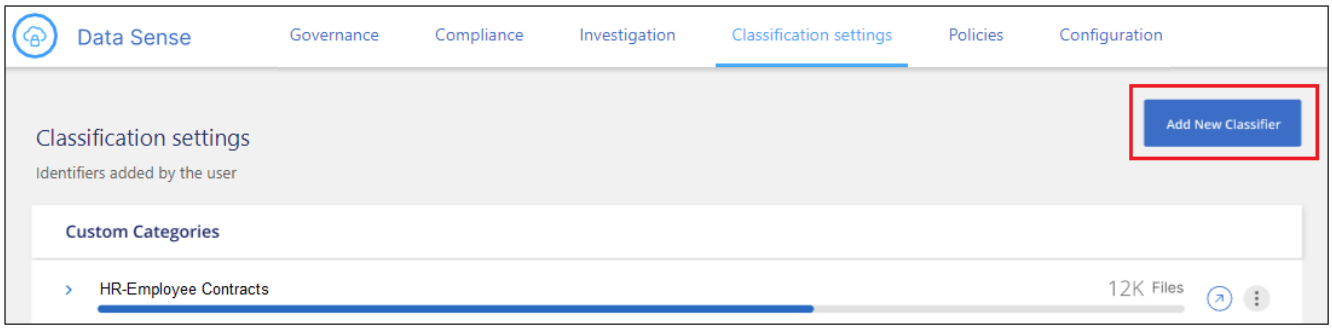
È possibile aggiungere parole chiave personalizzate alla classificazione BlueXP in modo che identifichi la posizione in cui tali informazioni sono contenute nei dati. È possibile aggiungere le parole chiave inserendo ciascuna parola che si desidera venga riconosciuta dalla classificazione BlueXP. Le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

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

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

Fasi

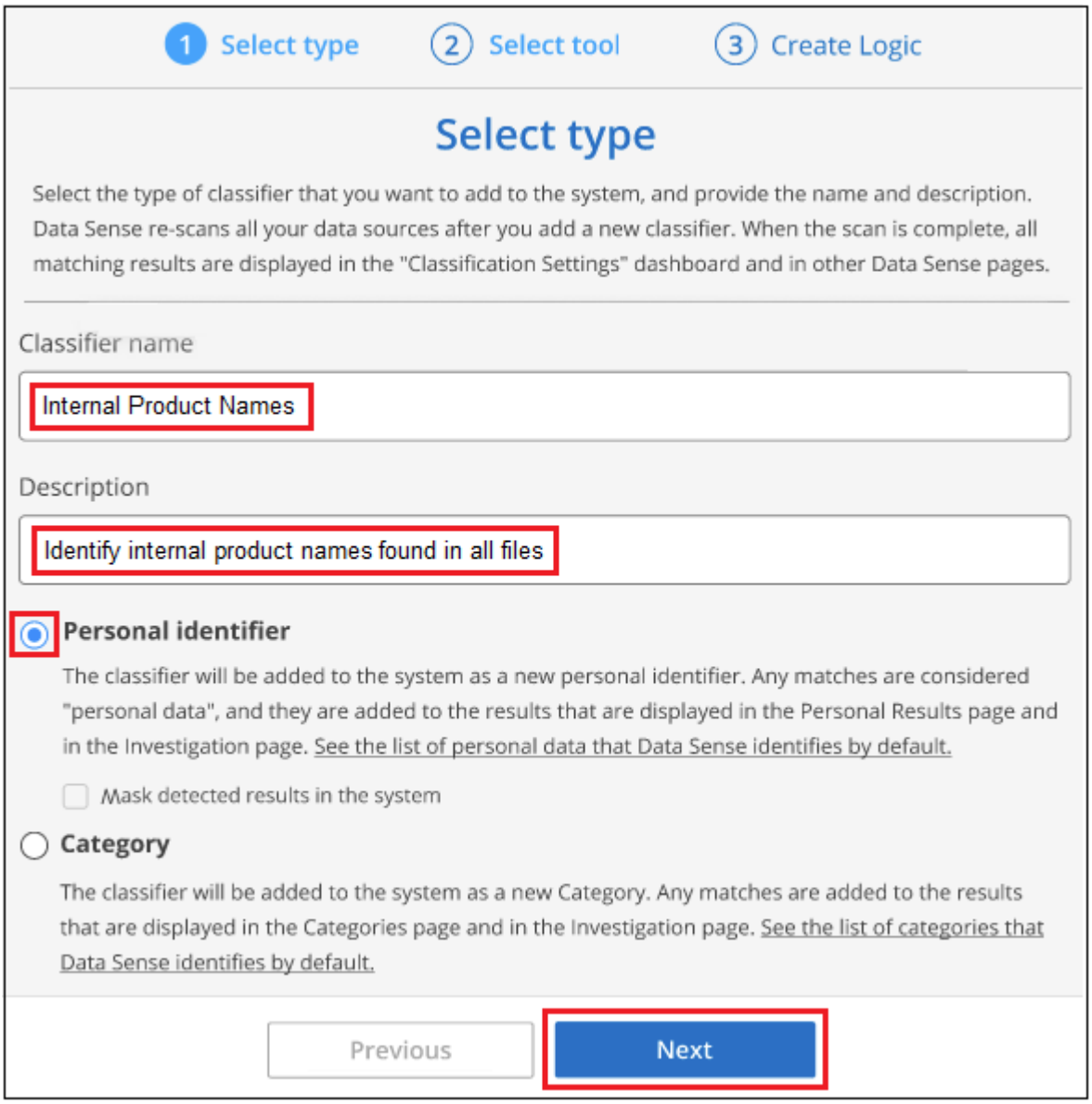
1. Dalla scheda *Impostazioni classificazione*, fare clic su **Aggiungi nuovo classificatore** per avviare la procedura guidata *Aggiungi classificatore personalizzato*.



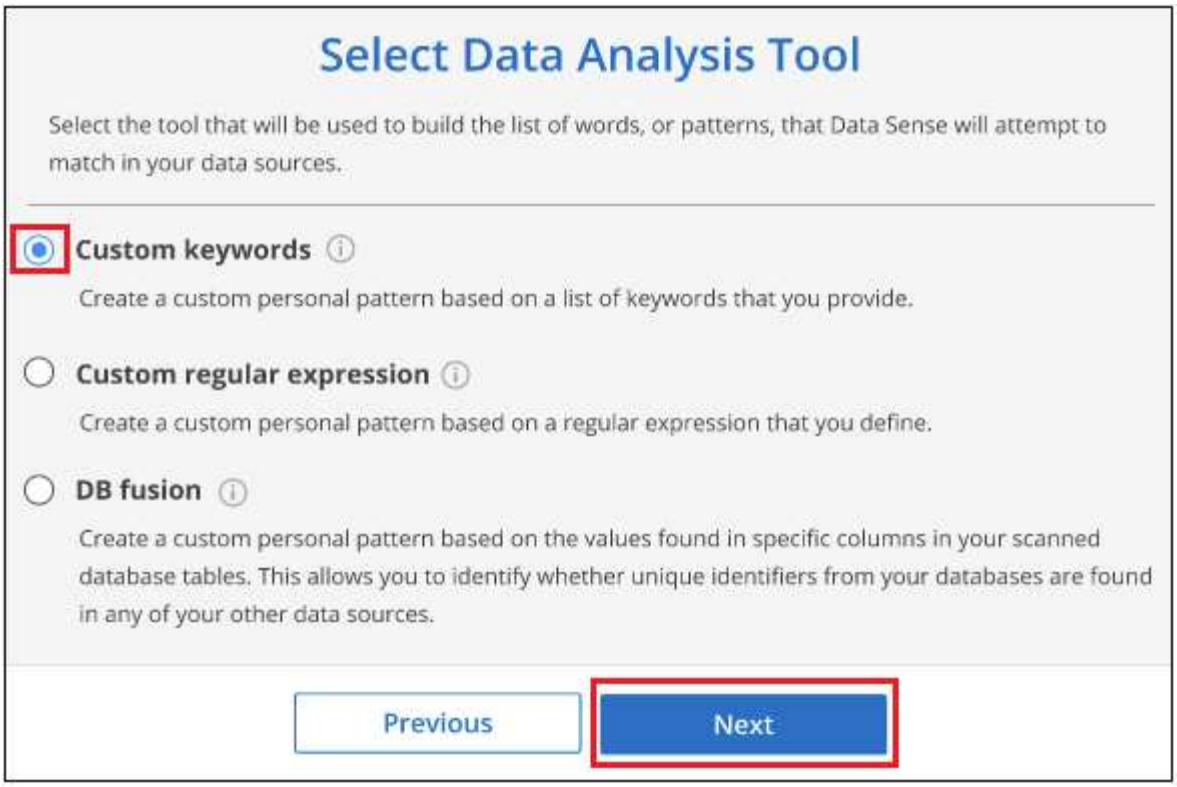
2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Personal identifier**, quindi fare clic su **Next**.

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

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

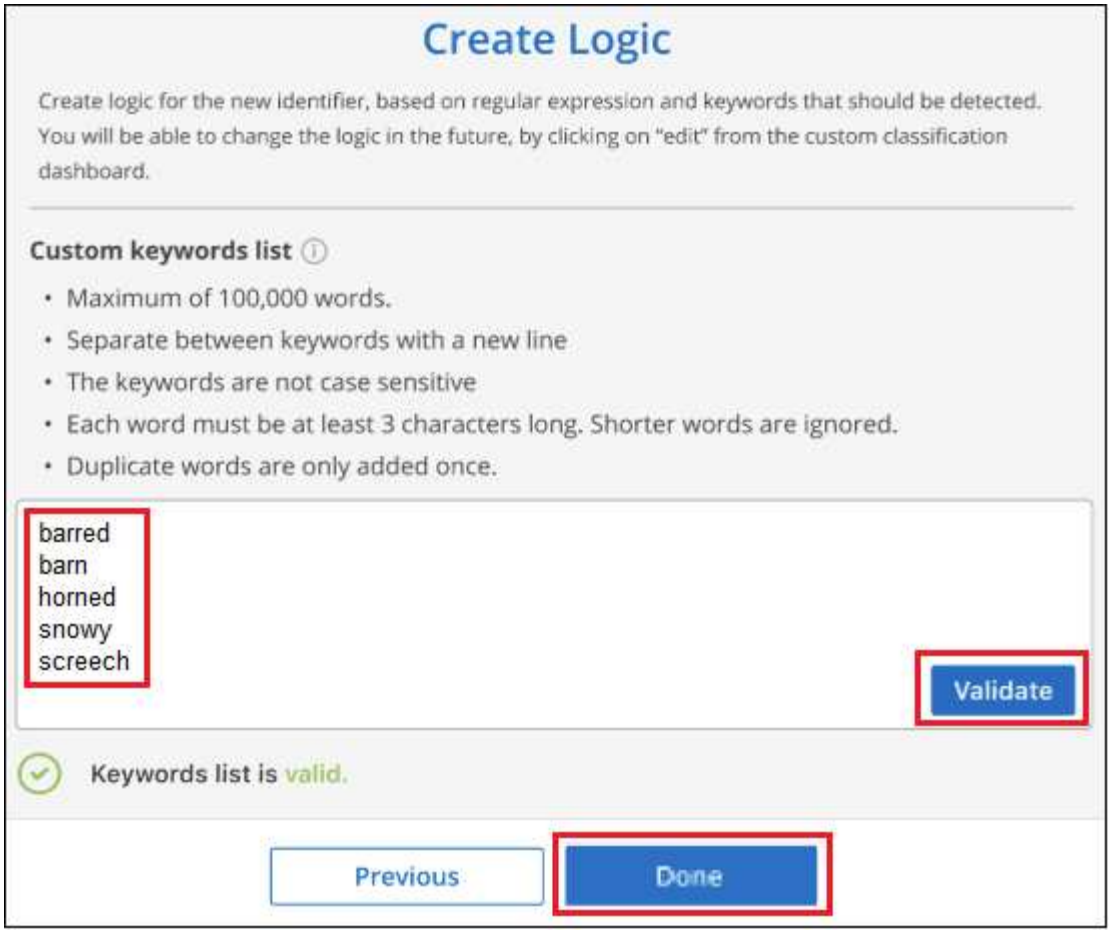


3. Nella pagina *Select Data Analysis Tool*, selezionare **Custom Keywords** come metodo da utilizzare per definire il classificatore, quindi fare clic su **Next**.



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

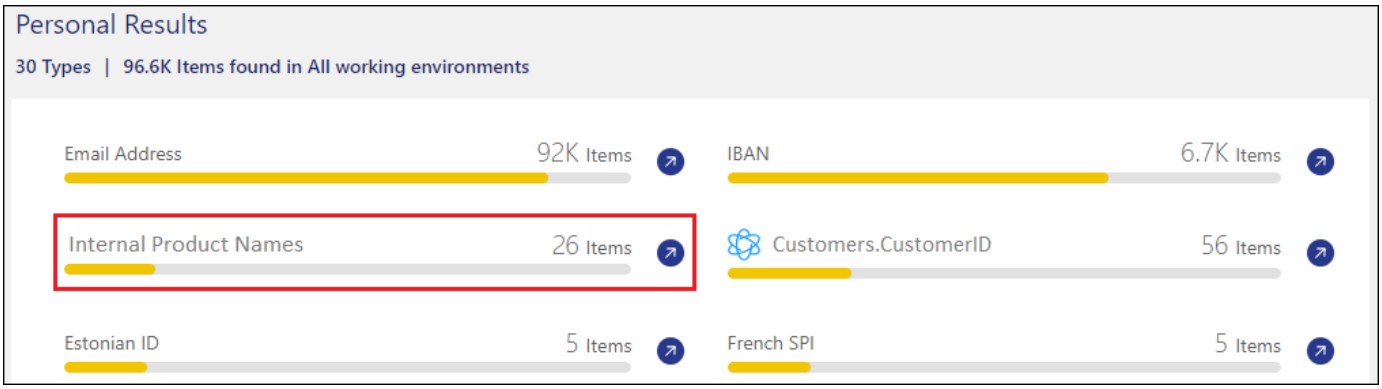
   La schermata seguente mostra i nomi dei prodotti interni (diversi tipi di gufi). La ricerca della classificazione BlueXP per questi elementi non fa distinzione tra maiuscole e minuscole.



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

Risultati

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



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

Aggiungere identificatori di dati personali personalizzati utilizzando un regex

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

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

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

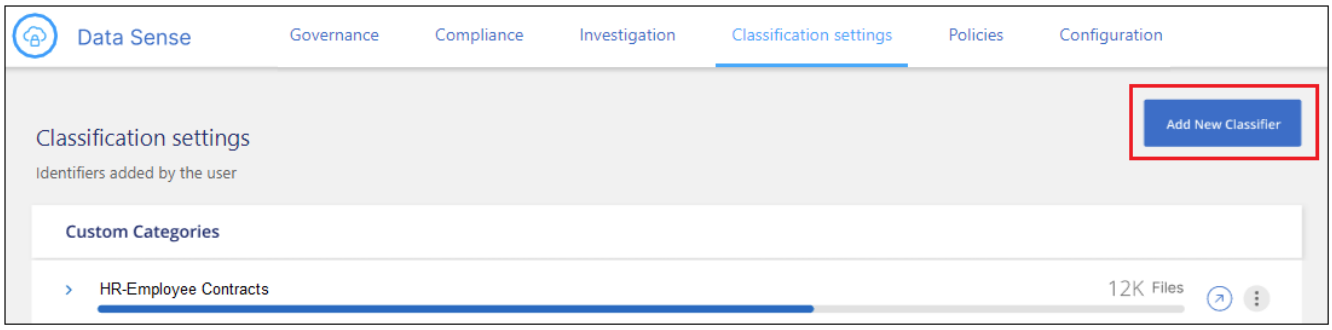
Dopo aver aggiunto il regex, la classificazione BlueXP riavvia la scansione di tutte le origini dati. Una volta completata la scansione, i nuovi risultati verranno visualizzati nella dashboard di conformità della classificazione BlueXP nella sezione "risultati personali" e nella pagina delle indagini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

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

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

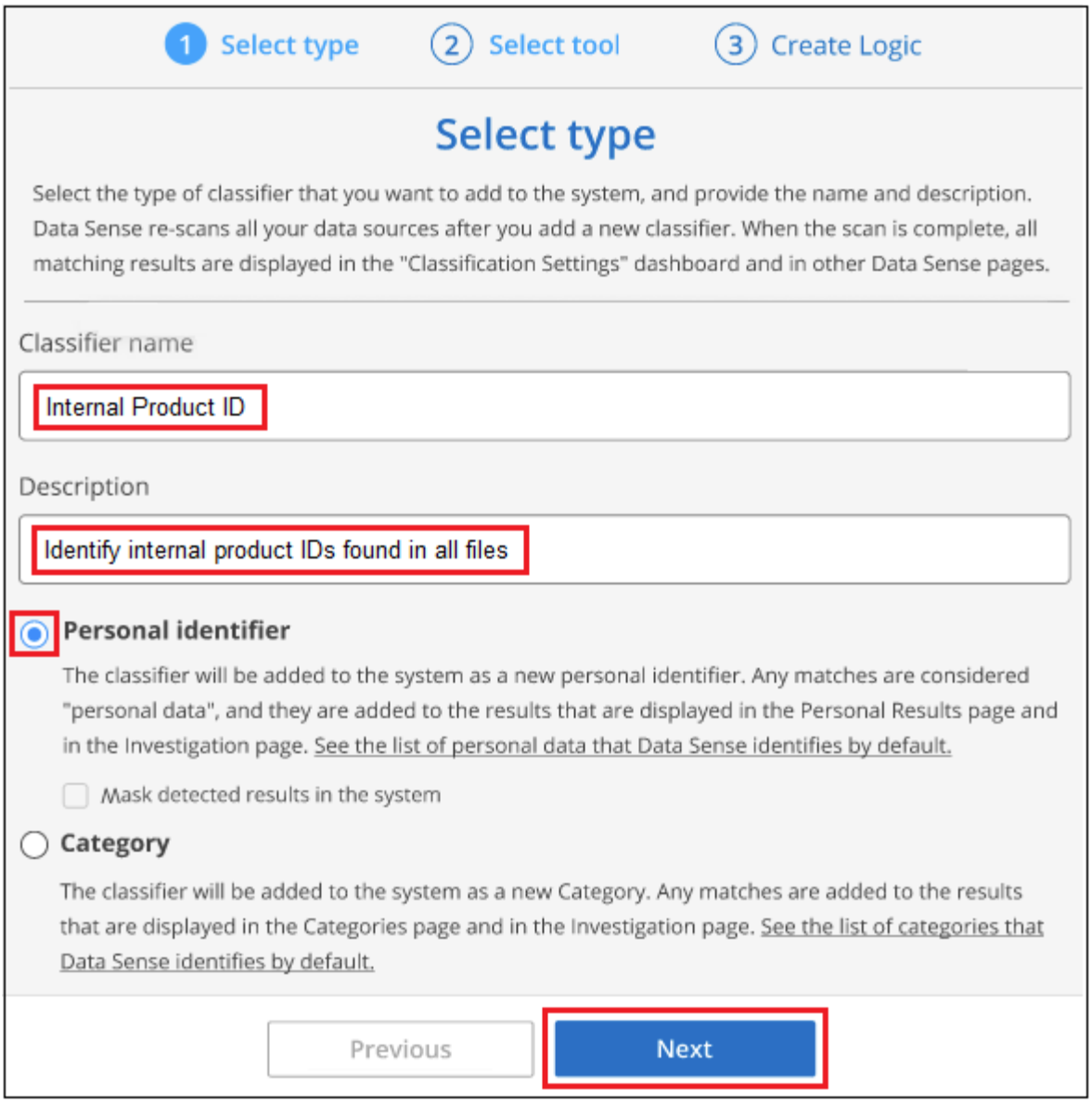
Fasi

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

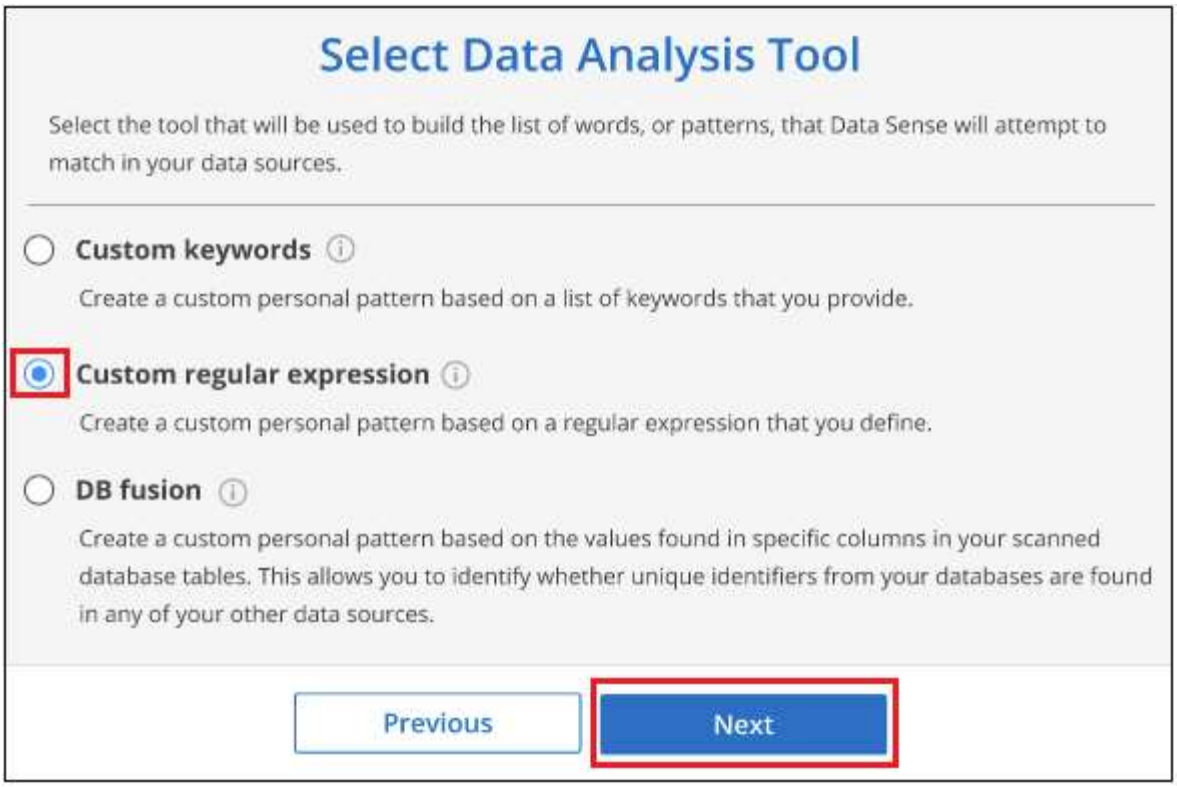


2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Personal identifier**, quindi fare clic su **Next**.

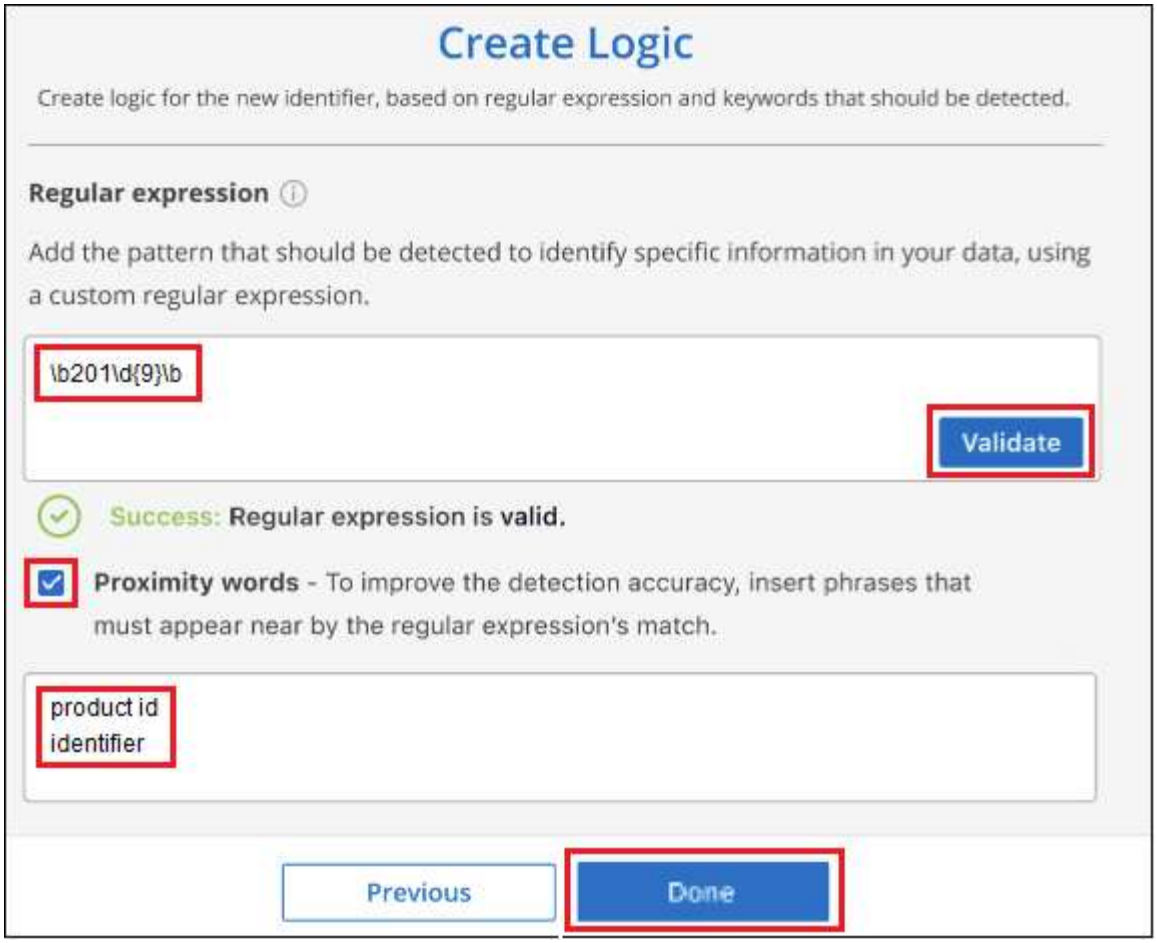
   Il nome immesso viene visualizzato nell'interfaccia utente di classificazione BlueXP come intestazione per i file sottoposti a scansione che corrispondono ai requisiti del classificatore e come nome del filtro nella pagina di analisi. Puoi anche selezionare la casella "Mask Detected Results in the system"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



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

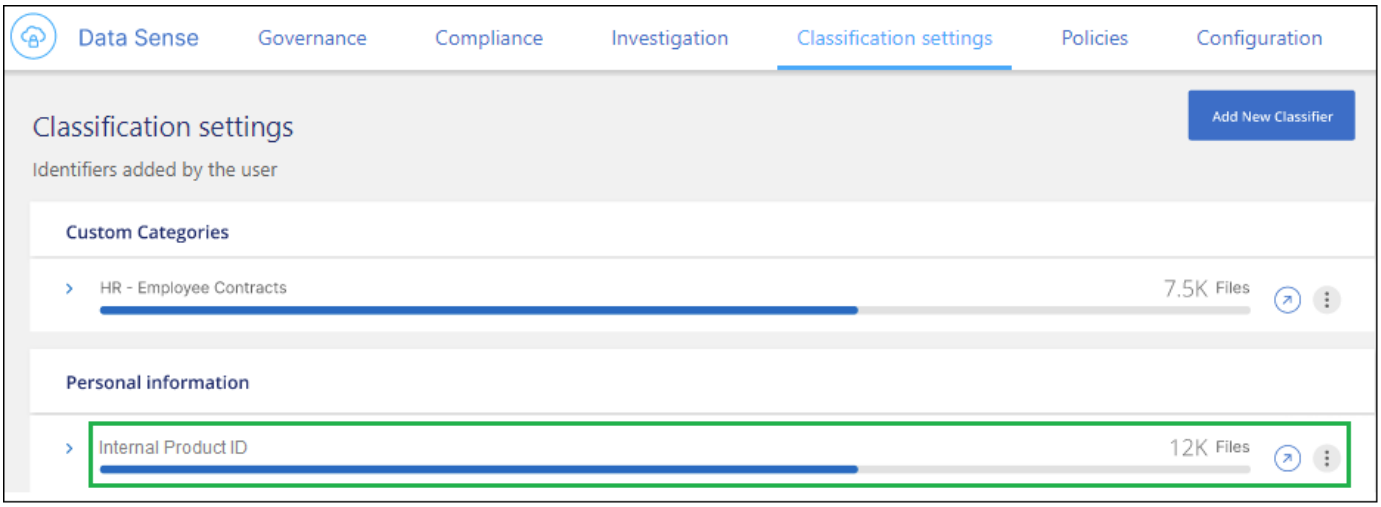


4. Nella pagina *Create Logic*, immettere l'espressione regolare e le parole di prossimità, quindi fare clic su **Done**.
   a. È possibile immettere qualsiasi espressione regolare legale. Fare clic sul pulsante **Validate** (convalida) per verificare che la classificazione BlueXP sia valida e che non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



Risultati

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



Aggiungere categorie personalizzate

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

l'elenco delle categorie predefinite".

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

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

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

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

Di cosa hai bisogno

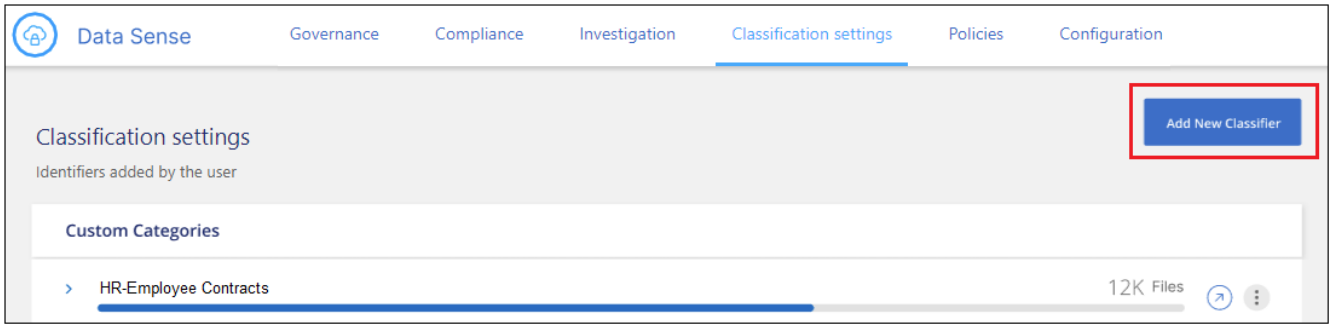
È necessario creare un minimo di 25 file di training contenenti esempi delle categorie di dati che si desidera vengano riconosciute dalla classificazione BlueXP. Sono supportati i seguenti tipi di file:

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

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

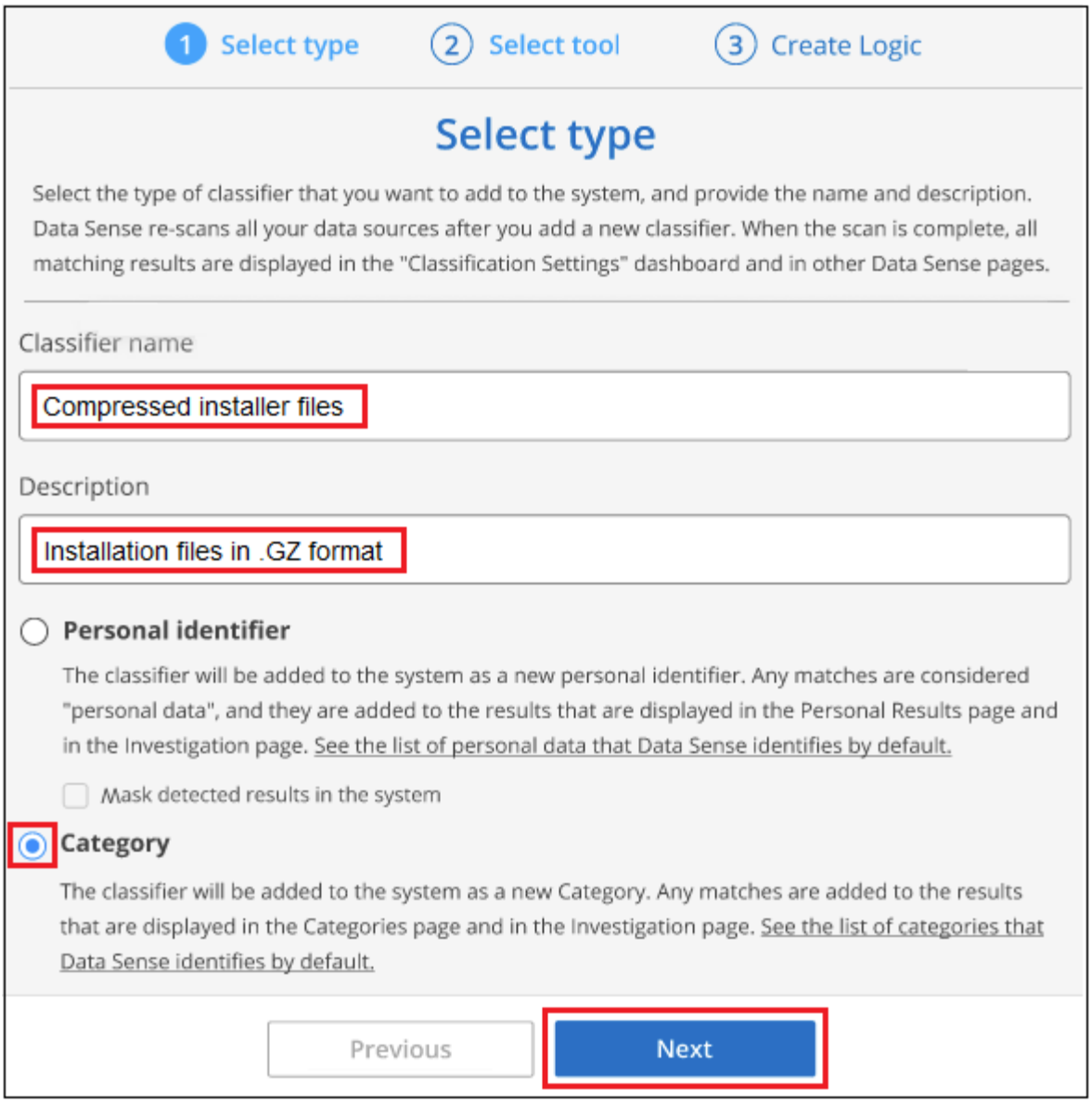
Fasi

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

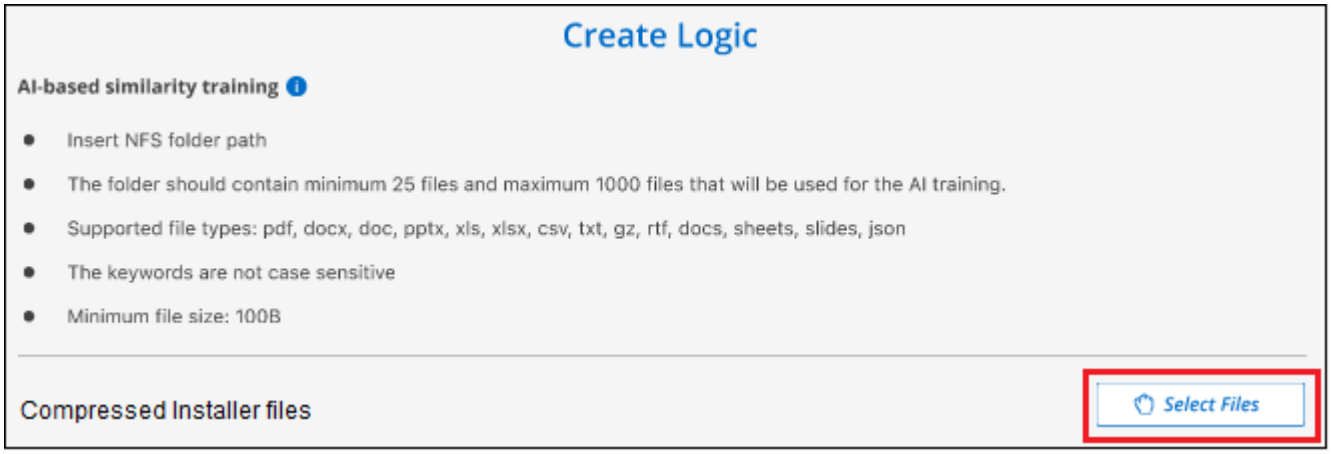


2. Nella pagina *Select type*, inserire il nome del classificatore, fornire una breve descrizione, selezionare **Category**, quindi fare clic su **Next**.

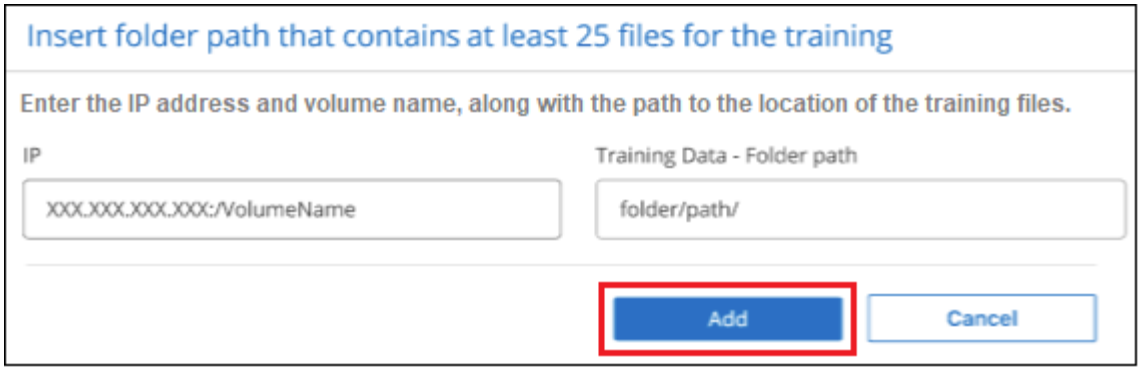
   Il nome immesso viene visualizzato nell'interfaccia utente di classificazione BlueXP come intestazione per i file sottoposti a scansione che corrispondono alla categoria di dati che si sta definendo e come nome del filtro nella pagina di analisi.



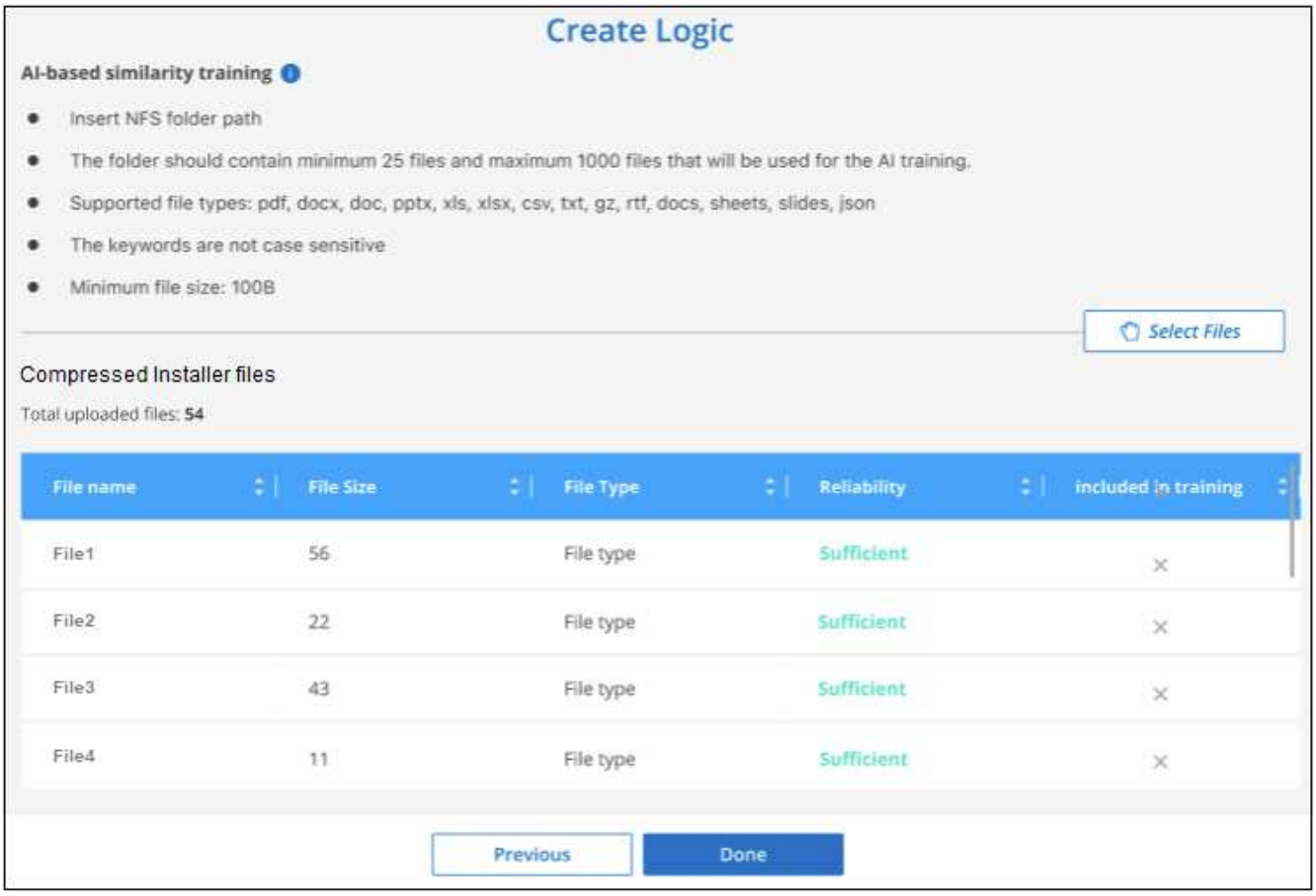
3. Nella pagina *Create Logic*, assicurarsi di aver preparato i file di apprendimento, quindi fare clic su **Select Files** (Seleziona file).



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



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



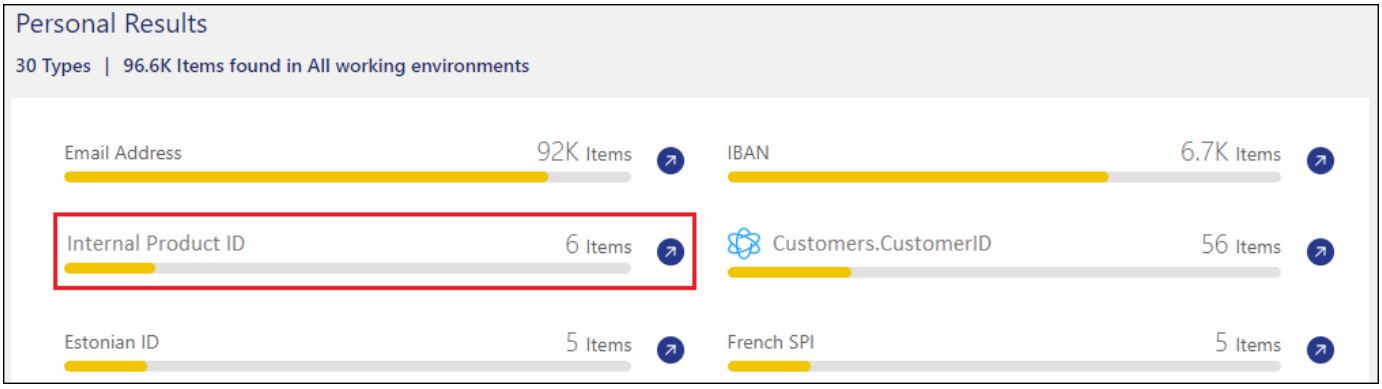
Risultati

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

Visualizzare i risultati dei classificatori personalizzati

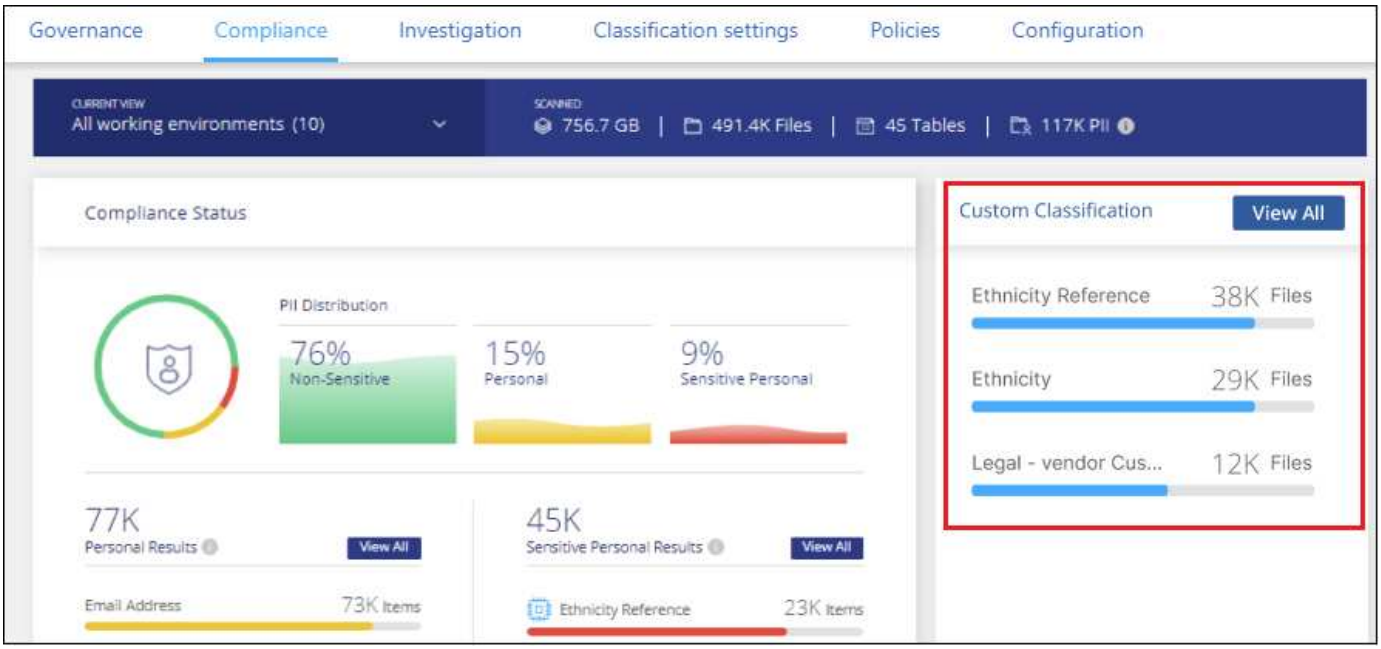
È possibile visualizzare i risultati da qualsiasi classificatore personalizzato nella dashboard di conformità e nella pagina di analisi. Ad esempio, questa schermata mostra le informazioni corrispondenti nella dashboard di

conformità nella sezione "risultati personali".



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

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

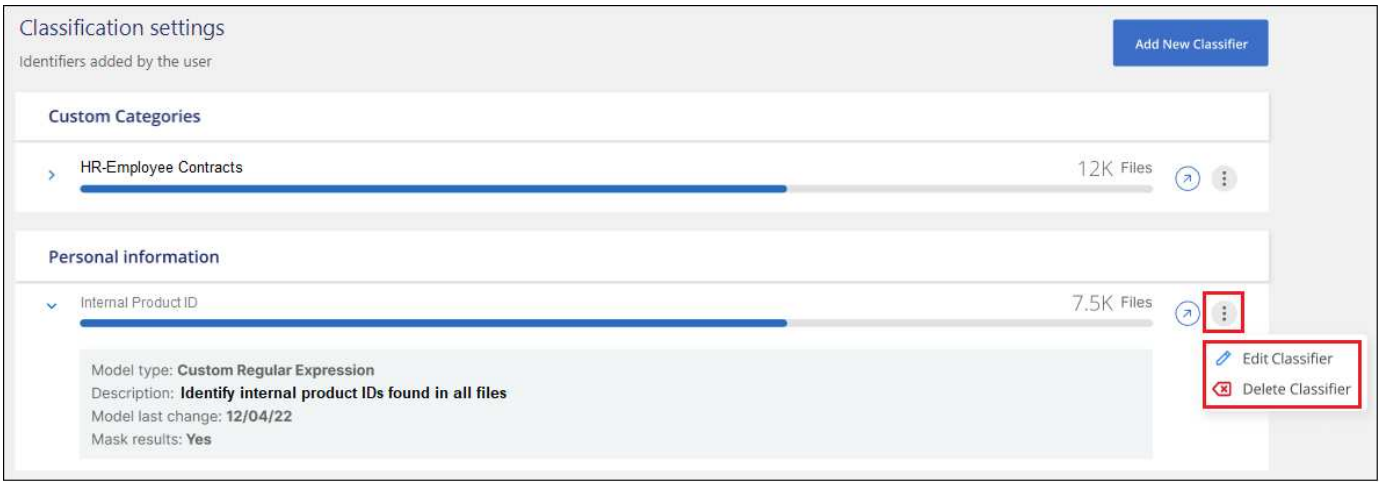


Gestire classificatori personalizzati

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

Al momento non è possibile modificare i classificatori Data Fusion.

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



Escludere directory specifiche dalle scansioni di classificazione BlueXP

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

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

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

Origini dati supportate

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

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

Definire le directory da escludere dalla scansione

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

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

Fasi

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

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

   Non modificare altro contenuto in questo file.

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

   ```
   update_data_providers_from_config_file.sh
   ```

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

Risultato

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

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

Esempi

Configurazione 1:

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

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

Risultati previsti per i percorsi che saranno esclusi:

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

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

Esempi di percorsi che non verranno esclusi:

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

Configurazione 2:

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

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

Risultati previsti per i percorsi che saranno esclusi:

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

Esempi di percorsi che non verranno esclusi:

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

Configurazione 3:

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

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

Risultati previsti per i percorsi che saranno esclusi:

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

Esempi di percorsi che non verranno esclusi:

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

Escape di caratteri speciali nei nomi delle cartelle

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

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

Percorso in origine: `/project/*not_to_scan`

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

Consente di visualizzare l'elenco di esclusione corrente

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

```
get_data_providers_configuration.sh
```

Visualizzazione dello stato delle azioni di compliance

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

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

Lo stato può essere:

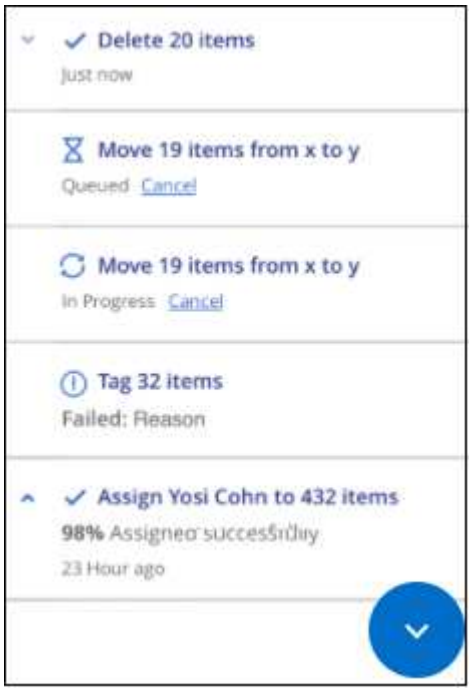
- Operazione riuscita - un'azione di classificazione BlueXP è terminata e tutti gli elementi sono riusciti.
- Successo parziale - Un'azione di classificazione BlueXP è terminata e alcuni elementi non sono riusciti e altri sono riusciti.
- In corso - l'azione è ancora in corso.
- Accodato - l'azione non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

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

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

Fasi

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



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

Definire altri ID di gruppo come aperti all'organizzazione

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

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

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

stata distribuita nel cloud.

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

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

Fasi

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

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

   Non modificare altro contenuto in questo file.

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

   ```
   update_data_providers_from_config_file.sh
   ```

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

Risultato

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

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

Consente di visualizzare l’elenco corrente degli ID di gruppo

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

```
get_data_providers_configuration.sh
```

Controllare la cronologia delle azioni di classificazione di BlueXP

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

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

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

Contenuto del file di log

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

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

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

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

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

Posizioni dei file di registro

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

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

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

Accedere ai file di registro

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

Riduzione della velocità di scansione della classificazione BlueXP

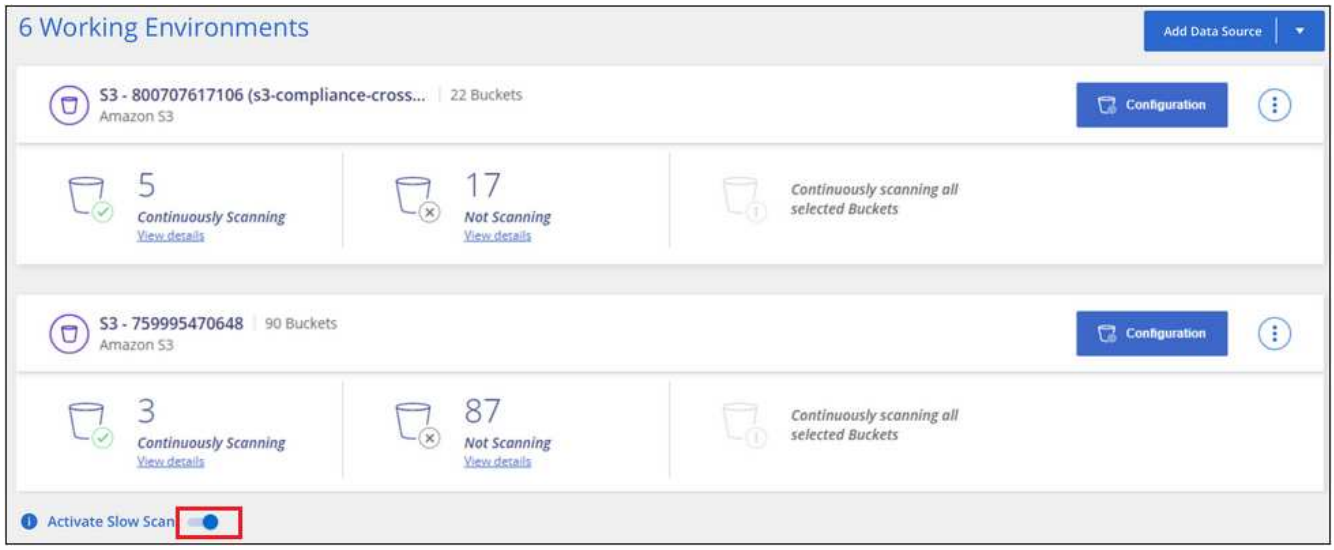
Le scansioni dei dati hanno un impatto trascurabile sui sistemi storage e sui dati. Tuttavia, se si è preoccupati anche di un impatto molto ridotto, è possibile configurare la classificazione BlueXP per eseguire scansioni "lente".

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

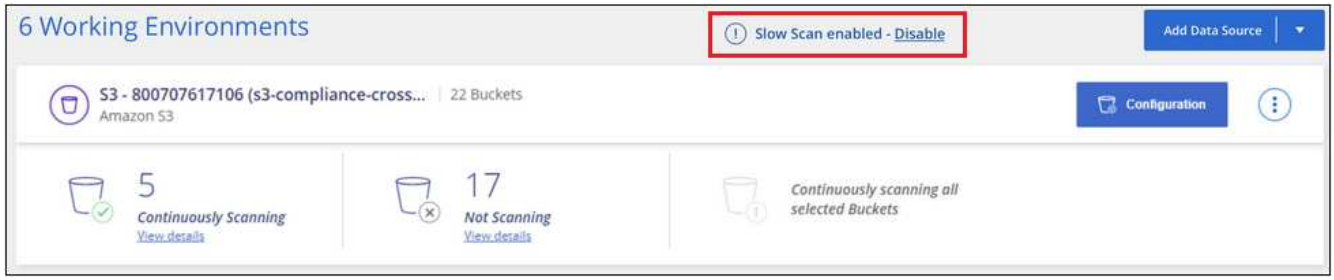
La velocità di scansione non può essere ridotta durante la scansione dei database.

Fasi

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



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



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

Rimozione delle origini dati dalla classificazione BlueXP

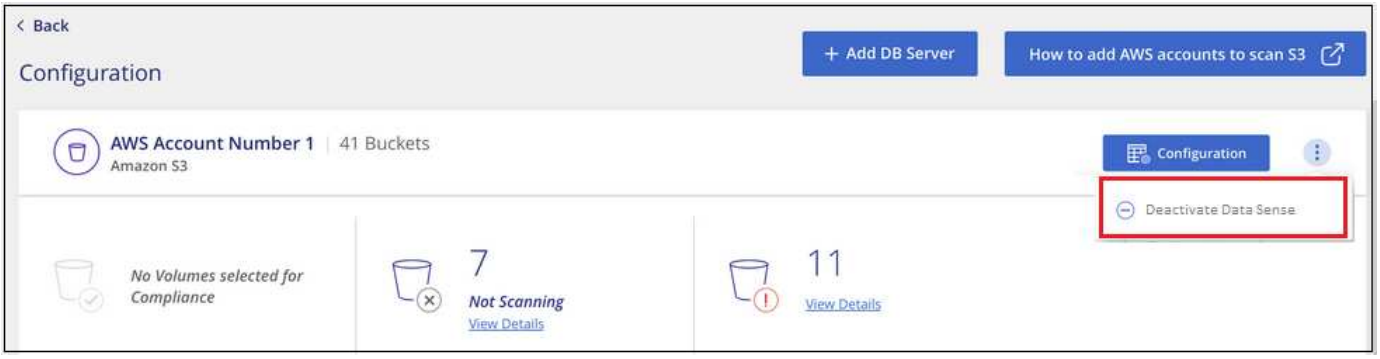
Se necessario, è possibile impedire alla classificazione BlueXP di eseguire la scansione di uno o più ambienti di lavoro, database, gruppi di condivisione file, account OneDrive, account Google Drive, O SharePoint.

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

Disattivazione delle scansioni di compliance per un ambiente di lavoro

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

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



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

Rimozione di un database dalla classificazione BlueXP

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

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

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

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

Fasi

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

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

Rimozione di un gruppo di condivisioni di file dalla classificazione BlueXP

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

Fasi

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

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

Disinstallazione della classificazione BlueXP

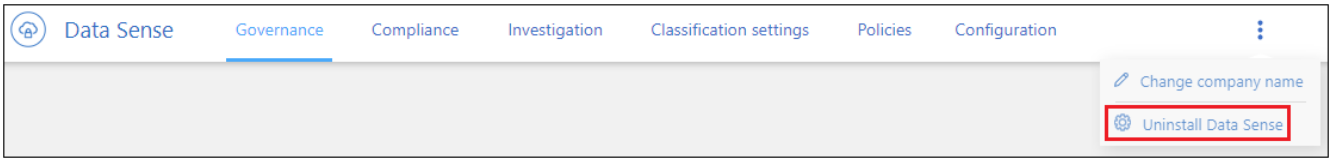
È possibile disinstallare il software di classificazione BlueXP per risolvere i problemi o per rimuovere in modo permanente il software dall'host. L'eliminazione dell'istanza comporta anche l'eliminazione dei dischi associati in cui risiedono i dati indicizzati. Tutte le informazioni sottoposte a scansione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

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

Disinstallare la classificazione BlueXP da un'implementazione cloud

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

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



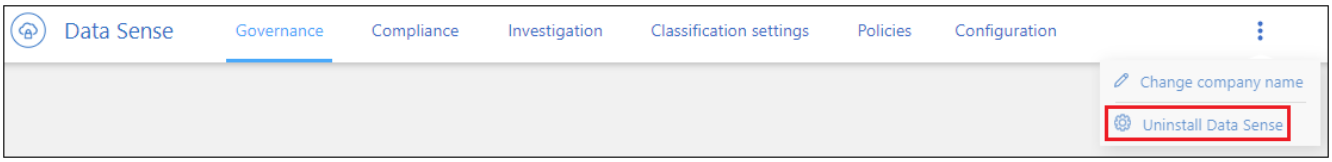
2. Nella finestra di dialogo *Uninstall Data Sense*, digitare **uninstall** per confermare che si desidera disconnettere l'istanza di classificazione BlueXP dal connettore BlueXP, quindi fare clic su **Uninstall** (Disinstalla).
3. Accedere alla console del provider di servizi cloud ed eliminare l'istanza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

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

Disinstallare la classificazione BlueXP da un'implementazione on-premise

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

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



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

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

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

```
cleanup.sh
```

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