



# **Gestire la classificazione BlueXP**

## **BlueXP classification**

NetApp  
September 23, 2024

# Sommario

- Gestire la classificazione BlueXP ..... 1
  - Escludere directory specifiche dalle scansioni di classificazione BlueXP ..... 1
  - Definire altri ID di gruppo come aperti all'organizzazione ..... 4
  - Rimuovere le origini dati dalla classificazione BlueXP ..... 5
  - Disinstallazione della classificazione BlueXP ..... 7

# Gestire la classificazione BlueXP

## Escludere directory specifiche dalle scansioni di classificazione BlueXP

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

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

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

### Origini dati supportate

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

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

### Definire le directory da escludere dalla scansione

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



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

### Fasi

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

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

Non modificare altro contenuto in questo file.

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

```
update_data_providers_from_config_file.sh
```

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

## Risultato

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

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

## Esempi

### Configurazione 1:

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

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

### Risultati previsti per i percorsi che saranno esclusi:

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

### Esempi di percorsi che non verranno esclusi:

- /CVO1/\*cartella

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

### Configurazione 2:

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

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

### Risultati previsti per i percorsi che saranno esclusi:

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

### Esempi di percorsi che non verranno esclusi:

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

### Configurazione 3:

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

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

### Risultati previsti per i percorsi che saranno esclusi:

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

### Esempi di percorsi che non verranno esclusi:

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

## Escape di caratteri speciali nei nomi delle cartelle

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

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

Ad esempio:

Percorso in origine: `/project/*not_to_scan`

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

## Consente di visualizzare l'elenco di esclusione corrente

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

```
get_data_providers_configuration.sh
```

## Definire altri ID di gruppo come aperti all'organizzazione

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

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

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

## Aggiungere l'autorizzazione "Apri all'organizzazione" agli ID gruppo

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

### Fasi

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

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

Non modificare altro contenuto in questo file.

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

```
update_data_providers_from_config_file.sh
```

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

### Risultato

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

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

### Consente di visualizzare l'elenco corrente degli ID di gruppo

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

```
get_data_providers_configuration.sh
```

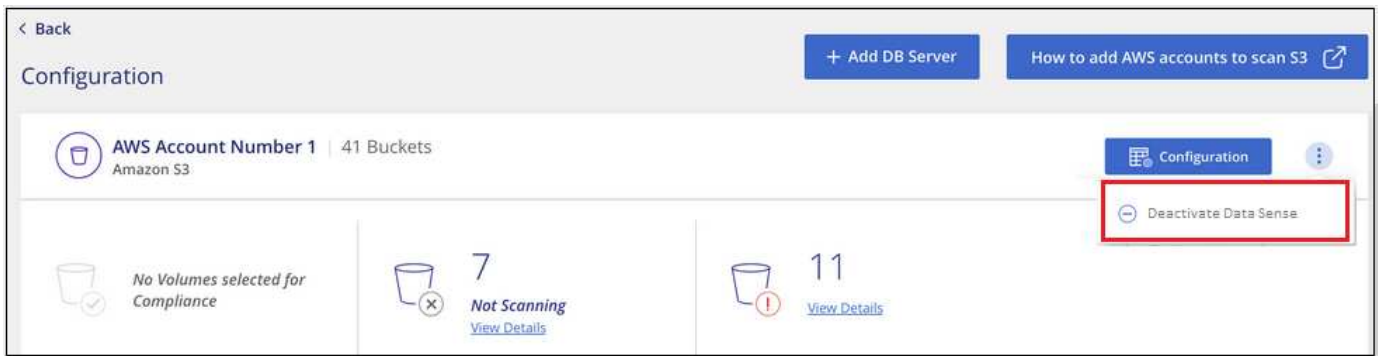
## Rimuovere le origini dati dalla classificazione BlueXP

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

### Disattivare le scansioni di conformità per un ambiente di lavoro

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


1. Dalla pagina *Configuration*, 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 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

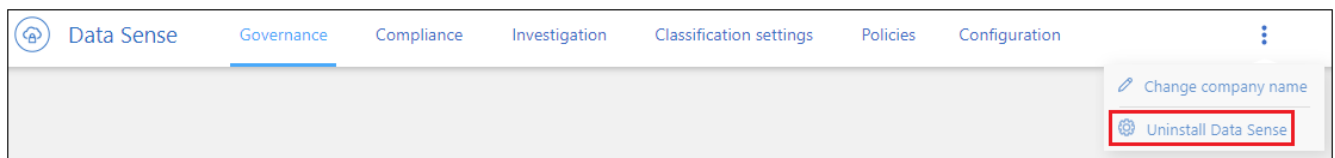
È possibile disinstallare il software di classificazione BlueXP per risolvere i problemi o per rimuovere in modo permanente il software dall'host. L'eliminazione dell'istanza comporta anche l'eliminazione dei dischi associati in cui risiedono i dati indicizzati. Tutte le informazioni sottoposte a scansione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



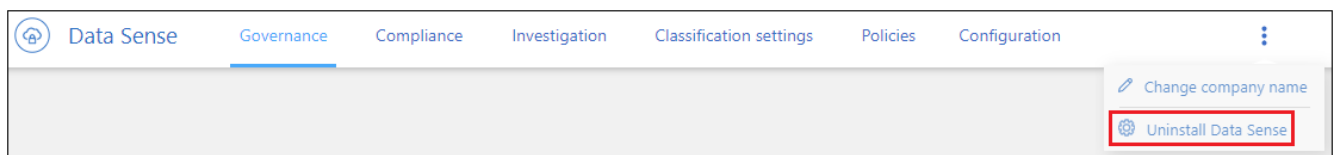
2. Nella finestra di dialogo *Uninstall Data Sense*, digitare **uninstall** per confermare che si desidera disconnettere l'istanza di classificazione BlueXP dal connettore BlueXP, quindi fare clic su **Uninstall** (Disinstalla).
3. Accedere alla console del provider di servizi cloud ed eliminare l'istanza 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"](#).

## Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.