# Attivare la scansione sulle origini dati

BlueXP classification

NetApp
April 03, 2024

# Sommario

# Attivare la scansione sulle origini dati

## Introduzione alla classificazione BlueXP per Cloud Volumes ONTAP e on-premise ONTAP

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

### Avvio rapido

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

**1 Individuare le origini dati da sottoporre a scansione**

Prima di poter eseguire la scansione dei volumi, è necessario aggiungere i sistemi come ambienti di lavoro in BlueXP:

- Per i sistemi Cloud Volumes ONTAP, questi ambienti di lavoro dovrebbero essere già disponibili in BlueXP
- Per sistemi ONTAP on-premise, "BlueXP deve rilevare i cluster ONTAP"

**2 Distribuire l'istanza di classificazione BlueXP**

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

**3 Abilitare la classificazione BlueXP e selezionare i volumi da sottoporre a scansione**

Selezionare la scheda **Configuration** (Configurazione) e attivare le scansioni di compliance per i volumi in ambienti di lavoro specifici.

**4 Garantire l'accesso ai volumi**

Ora che la classificazione BlueXP è attivata, assicurarsi che sia in grado di accedere a tutti i volumi.

- L'istanza di classificazione BlueXP richiede una connessione di rete a ogni subnet Cloud Volumes ONTAP o sistema ONTAP on-premise.
- I gruppi di protezione per Cloud Volumes ONTAP devono consentire le connessioni in entrata dall'istanza di classificazione BlueXP.
- Assicurarsi che queste porte siano aperte per l'istanza di classificazione BlueXP:
  - Per NFS - porte 111 e 2049.
  - Per CIFS - porte 139 e 445.
- I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.
- La classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS.

Fare clic su **Compliance** > **Configuration** > **Edit CIFS Credentials** (Modifica credenziali CIFS) e fornire le credenziali.

**5** **Gestire i volumi che si desidera sottoporre a scansione**

Selezionare o deselezionare i volumi da sottoporre a scansione per avviare o interrompere la scansione della classificazione BlueXP.

## Rilevamento delle origini dati che si desidera acquisire

Se le origini dati che si desidera sottoporre a scansione non sono già presenti nell'ambiente BlueXP, è possibile aggiungerle all'area di lavoro.

I sistemi Cloud Volumes ONTAP dovrebbero essere già disponibili in Canvas in BlueXP. Per i sistemi ONTAP on-premise, è necessario disporre di "BlueXP Scopri questi cluster".

## Implementazione dell'istanza di classificazione BlueXP

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

Se si esegue la scansione di sistemi Cloud Volumes ONTAP e ONTAP on-premise accessibili tramite Internet, è possibile "Implementare la classificazione BlueXP nel cloud" oppure "in una sede on-premise con accesso a internet".

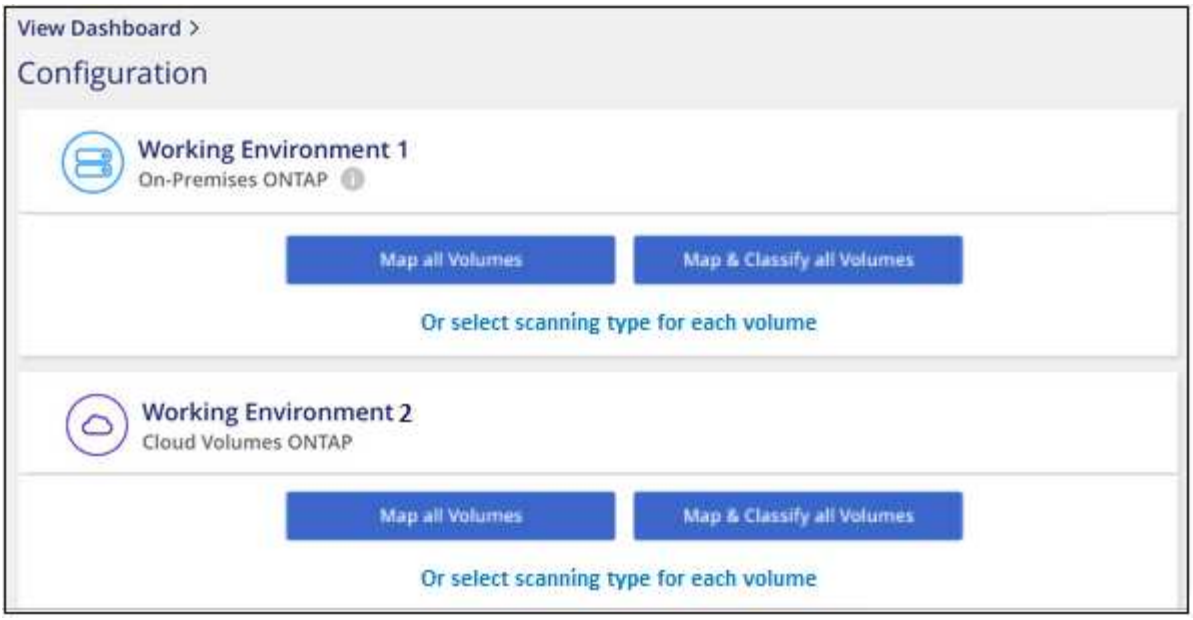
Se si esegue la scansione di sistemi ONTAP on-premise che sono stati installati in un sito buio e che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector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

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

## Abilitazione della classificazione BlueXP negli ambienti di lavoro

Puoi abilitare la classificazione BlueXP sui sistemi Cloud Volumes ONTAP in qualsiasi cloud provider supportato e sui cluster ONTAP on-premise.

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




2. Selezionare la modalità di scansione dei volumi in ciascun ambiente di lavoro. "Scopri le scansioni di mappatura e classificazione":
   - Per mappare tutti i volumi, fare clic su **Map All Volumes** (Mappa tutti i volumi).
   - Per mappare e classificare tutti i volumi, fare clic su **Map & Classify All Volumes** (Mappa e classificazione di tutti i volumi).
   - Per personalizzare la scansione per ciascun volume, fare clic su **o selezionare il tipo di scansione per ciascun volume**, quindi scegliere i volumi da mappare e/o classificare.

     Vedere Attivazione e disattivazione delle scansioni di compliance sui volumi per ulteriori informazioni.
3. Nella finestra di dialogo di conferma, fare clic su **approva** per avviare la scansione dei volumi con la classificazione BlueXP.

**Risultato**

La classificazione BlueXP avvia la scansione dei volumi selezionati nell'ambiente di lavoro. I risultati saranno disponibili nella dashboard Compliance non appena la classificazione BlueXP completa le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati, che potrebbe essere di pochi minuti o ore.

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

## Verificare che la classificazione BlueXP abbia accesso ai volumi

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

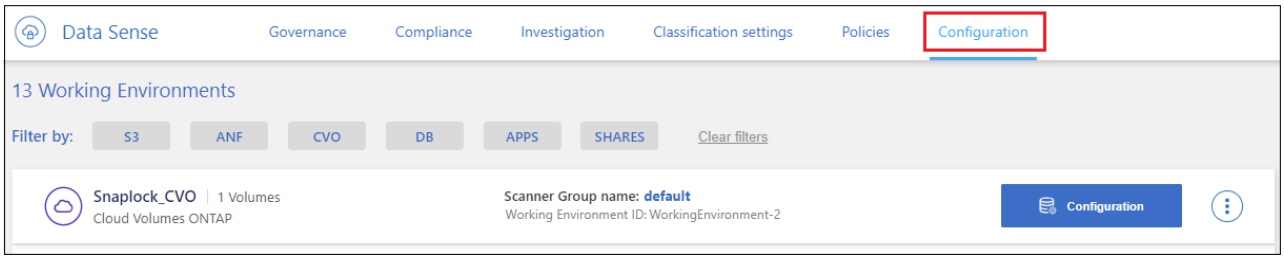
**Fasi**

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

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

3. Assicurarsi che le seguenti porte siano aperte per l'istanza di classificazione BlueXP:
   - Per NFS - porte 111 e 2049.
   - Per CIFS - porte 139 e 445.
4. Assicurarsi che i criteri di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza di classificazione BlueXP in modo che possa accedere ai dati di ciascun volume.
5. Se si utilizza CIFS, fornire la classificazione BlueXP con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.

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

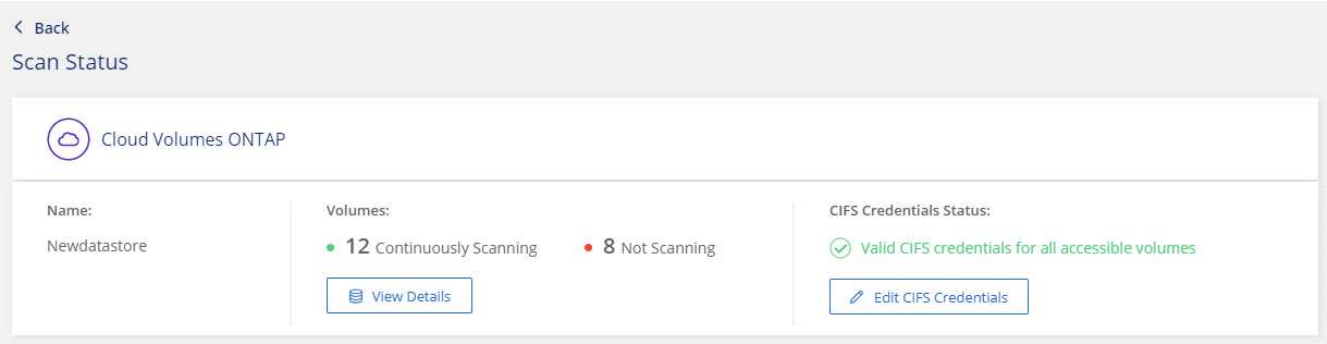
   
   

   b. Per ciascun ambiente di lavoro, fare clic su **Edit CIFS Credentials** (Modifica credenziali CIFS) e immettere il nome utente e la password necessari per la classificazione BlueXP per accedere ai volumi CIFS nel sistema.

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

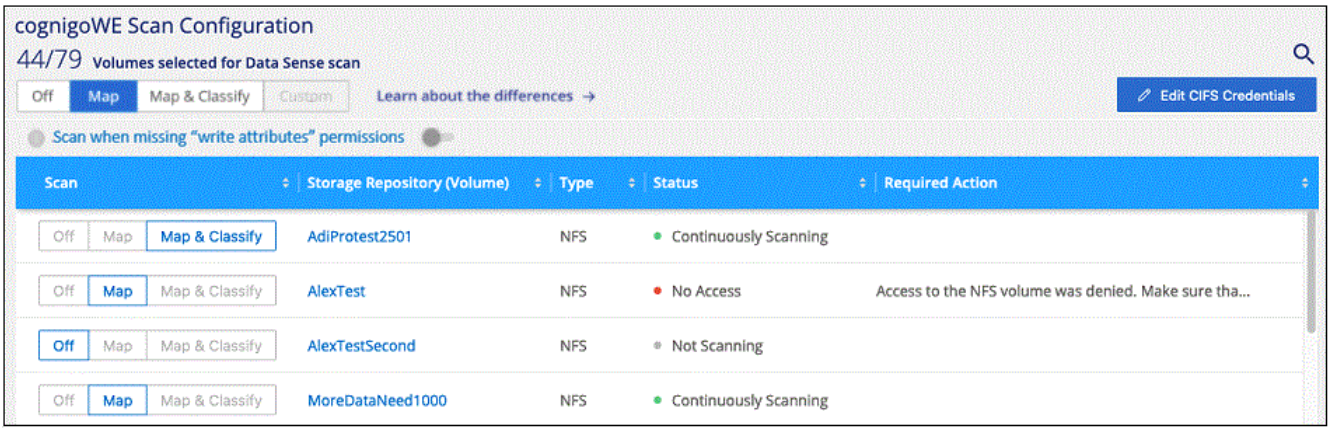
   Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory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

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




6. Nella pagina *Configuration*, fare clic su **View Details** (Visualizza dettagli) per esaminare lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

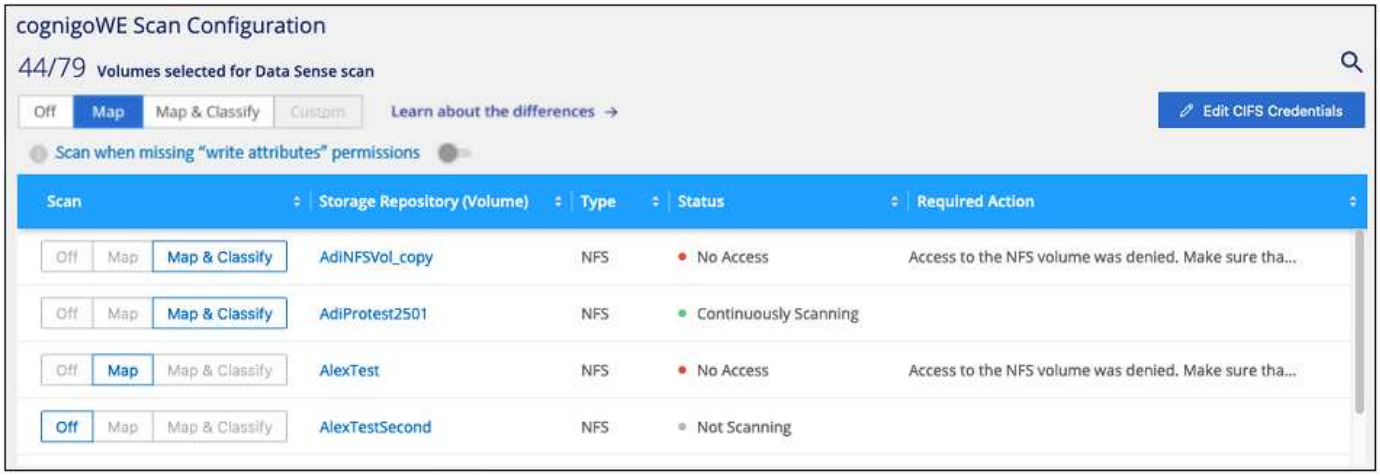
   Ad esempio, l'immagine seguente mostra quattro volumi, uno dei quali non è in grado di eseguire la scansione a causa di problemi di connettività di rete tra l'istanza di classificazione BlueXP e il volume.




## Attivazione e disattivazione delle scansioni di compliance sui volumi

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

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



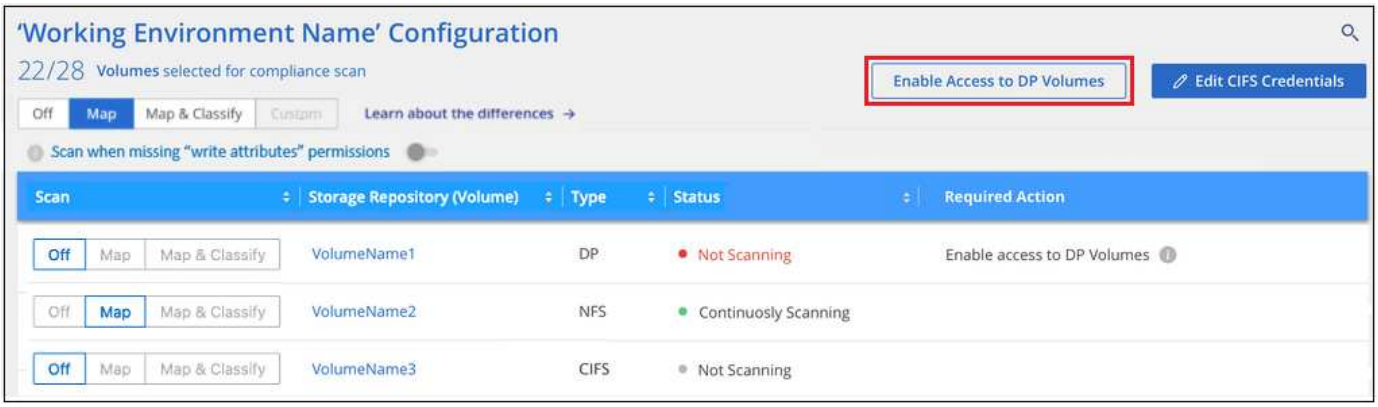

| A: | Eseguire questa operazione: |
|---|---|
| Abilitare le scansioni di sola mappatura su un volume | Nell'area del volume, fare clic su **Map** (Mappa) |
| Abilitare la scansione completa su un volume | Nell'area del volume, fare clic su **Map & Classify** (Mappa e classificazione) |
| Disattivare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

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

## Scansione dei volumi di protezione dei dati

Per impostazione predefinita, i volumi di protezione dei dati (DP) non vengono sottoposti a scansione perché non sono esposti esternamente e la classificazione BlueXP non può accedervi. Questi sono i volumi di destinazione per le operazioni SnapMirror da un sistema ONTAP on-premise o da un sistema Cloud Volumes ONTAP.

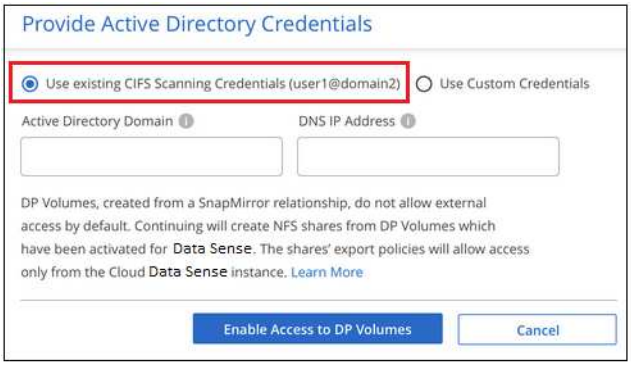
Inizialmente, l'elenco dei volumi identifica questi volumi come *Type* **DP** con *Status* **Not Scanning** e *Required Action* **Enable Access to DP Volumes**.

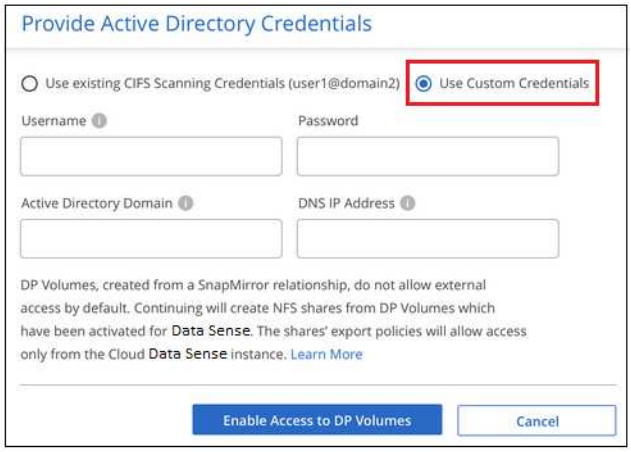



**Fasi**

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

1. Fare clic su **Enable Access to DP Volumes** (attiva accesso ai volumi DP) nella parte superiore della pagina.
2. Leggere il messaggio di conferma e fare nuovamente clic su **Enable Access to DP Volumes** (attiva accesso ai volumi DP).
   - I volumi creati inizialmente come volumi NFS nel sistema ONTAP di origine sono abilitati.
   - I volumi creati inizialmente come volumi CIFS nel sistema ONTAP di origine richiedono l'immissione delle credenziali CIFS per eseguire la scansione di tali volumi DP. Se sono già state immesse le credenziali Active Directory in modo che la classificazione BlueXP possa eseguire la scansione dei volumi CIFS, è possibile utilizzare tali credenziali oppure specificare un set diverso di credenziali Admin.




3. Attivare ciascun volume DP che si desidera sottoporre a scansione allo stesso modo in cui sono stati attivati altri volumi.

**Risultato**

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

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

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

# Introduzione alla classificazione BlueXP per Azure NetApp Files

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

## Avvio rapido

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

**1 Individuare i sistemi Azure NetApp Files che si desidera sottoporre a scansione**

Prima di eseguire la scansione dei volumi Azure NetApp Files, "BlueXP deve essere configurato per rilevare la configurazione".

**2 Distribuire l'istanza di classificazione BlueXP**

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

**3 Abilitare la classificazione BlueXP e selezionare i volumi da sottoporre a scansione**

Fare clic su **Compliance**, selezionare la scheda **Configuration** e attivare le scansioni di compliance per i volumi in ambienti di lavoro specifici.

**4 Garantire l'accesso ai volumi**

Ora che la classificazione BlueXP è attivata, assicurarsi che sia in grado di accedere a tutti i volumi.

- L'istanza di classificazione BlueXP richiede una connessione di rete a ciascuna subnet Azure NetApp Files.
- Assicurarsi che queste porte siano aperte per l'istanza di classificazione BlueXP:
  - Per NFS: Porte 111 e 2049.
  - Per CIFS – porte 139 e 445.
- I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.
- La classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS.

  Fare clic su **Compliance** > **Configuration** > **Edit CIFS Credentials** (Modifica credenziali CIFS) e fornire le credenziali.

**5** **Gestire i volumi che si desidera sottoporre a scansione**

Selezionare o deselezionare i volumi da sottoporre a scansione per avviare o interrompere la scansione della classificazione BlueXP.

## Rilevamento del sistema Azure NetApp Files che si desidera sottoporre a scansione

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

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

## Implementazione dell'istanza di classificazione BlueXP

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

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

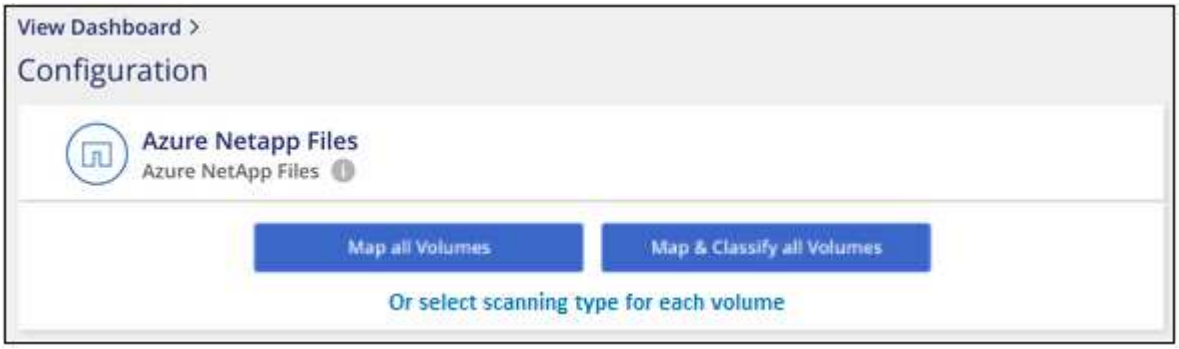
**Nota:** l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei volumi Azure NetApp Files.

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

## Abilitazione della classificazione BlueXP negli ambienti di lavoro

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

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




2. Selezionare la modalità di scansione dei volumi in ciascun ambiente di lavoro. "Scopri le scansioni di mappatura e classificazione":
   - Per mappare tutti i volumi, fare clic su **Map All Volumes** (Mappa tutti i volumi).
   - Per mappare e classificare tutti i volumi, fare clic su **Map & Classify All Volumes** (Mappa e classificazione di tutti i volumi).
   - Per personalizzare la scansione per ciascun volume, fare clic su **o selezionare il tipo di scansione per ciascun volume**, quindi scegliere i volumi da mappare e/o classificare.

Vedere Attivazione e disattivazione delle scansioni di compliance sui volumi per ulteriori informazioni.

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

**Risultato**

La classificazione BlueXP avvia la scansione dei volumi selezionati nell'ambiente di lavoro. I risultati saranno disponibili nella dashboard Compliance non appena la classificazione BlueXP completa le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati, che potrebbe essere di pochi minuti o ore.

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

## Verificare che la classificazione BlueXP abbia accesso ai volumi

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

**Fasi**

1. Assicurarsi che sia presente una connessione di rete tra l'istanza di classificazione BlueXP e ciascuna rete che include volumi per Azure NetApp Files.

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

2. Assicurarsi che le seguenti porte siano aperte per l'istanza di classificazione BlueXP:
   - Per NFS: Porte 111 e 2049.
   - Per CIFS – porte 139 e 445.
3. Assicurarsi che i criteri di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza di classificazione BlueXP in modo che possa accedere ai dati di ciascun volume.
4. Se si utilizza CIFS, fornire la classificazione BlueXP con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.

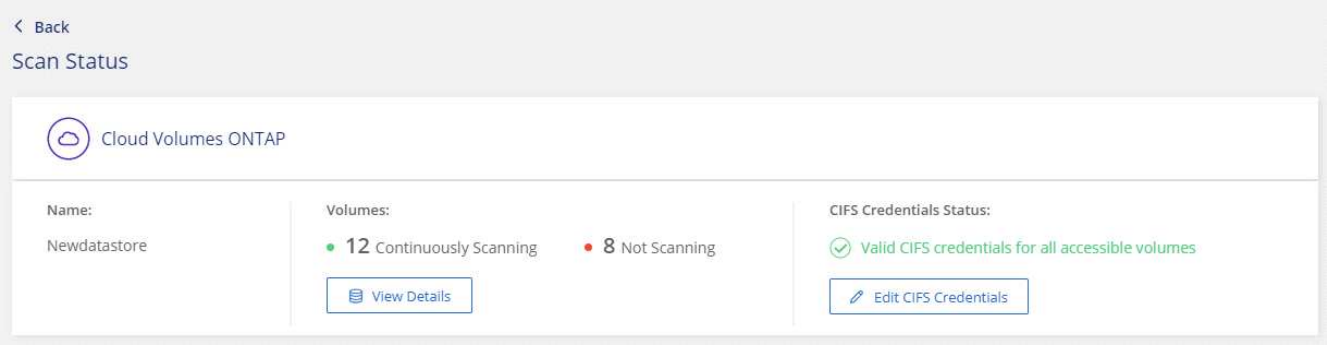
   a. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification** (Governance > classificazione), quindi selezionare la scheda **Configuration** (Configurazione).


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

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

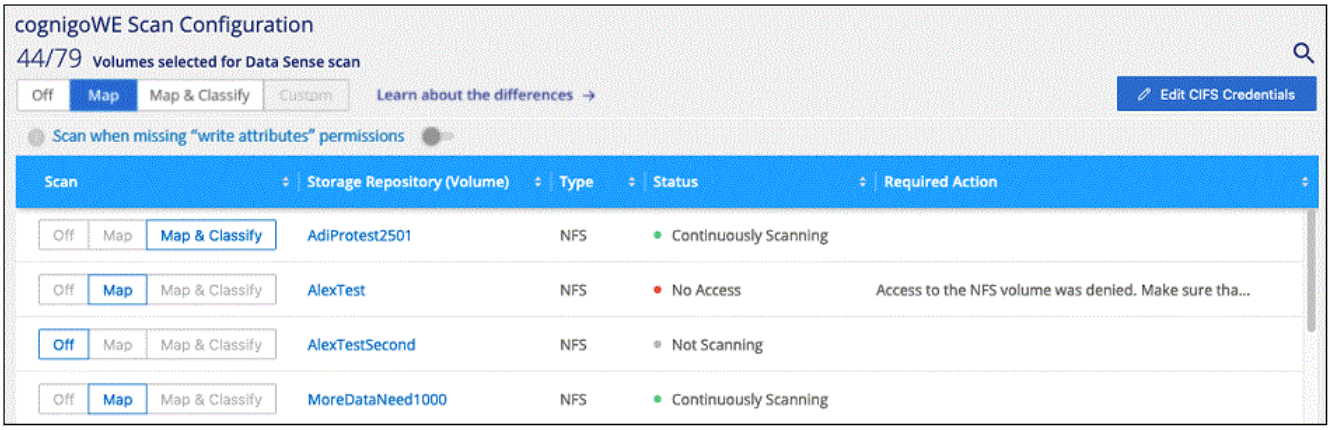
   Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory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

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




5. Nella pagina *Configuration*, fare clic su **View Details** (Visualizza dettagli) per esaminare lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

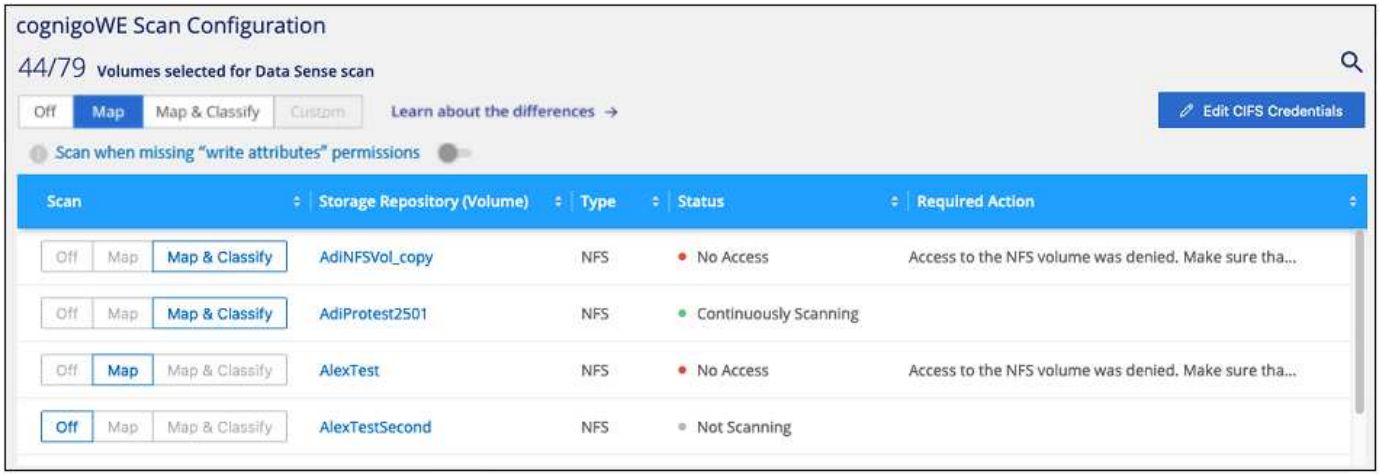
   Ad esempio, l'immagine seguente mostra quattro volumi, uno dei quali non è in grado di eseguire la scansione a causa di problemi di connettività di rete tra l'istanza di classificazione BlueXP e il volume.



## Attivazione e disattivazione delle scansioni di compliance sui volumi

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

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




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

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

# Inizia a utilizzare la classificazione BlueXP per Amazon FSX per ONTAP

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

## Prima di iniziare

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

  "Gruppi di sicurezza AWS per istanze Linux"

  "Gruppi di sicurezza AWS per le istanze di Windows"

  "AWS Elastic Network Interface (ENI)"

## Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso per ottenere informazioni dettagliate.

1 **Scopri il file system FSX per ONTAP che desideri sottoporre a scansione**

Prima di eseguire la scansione di FSX per i volumi ONTAP, "È necessario disporre di un ambiente di lavoro FSX con volumi configurati".

2 **Distribuire l'istanza di classificazione BlueXP**

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

3 **Abilitare la classificazione BlueXP e selezionare i volumi da sottoporre a scansione**

Selezionare la scheda **Configuration** (Configurazione) e attivare le scansioni di compliance per i volumi in ambienti di lavoro specifici.

4 **Garantire l'accesso ai volumi**

Ora che la classificazione BlueXP è attivata, assicurarsi che sia in grado di accedere a tutti i volumi.

- L'istanza di classificazione BlueXP richiede una connessione di rete a ciascuna subnet FSX per ONTAP.
- Assicurarsi che le seguenti porte siano aperte per l'istanza di classificazione BlueXP:
  - Per NFS: Porte 111 e 2049.
  - Per CIFS – porte 139 e 445.
- I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.

- La classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS. + fare clic su **Compliance** > **Configuration** > **Edit CIFS Credentials** (Modifica credenziali CIFS) e fornire le credenziali.

**5** **Gestire i volumi che si desidera sottoporre a scansione**

Selezionare o deselezionare i volumi da sottoporre a scansione per avviare o interrompere la scansione della classificazione BlueXP.

## Rilevamento del file system FSX per ONTAP che si desidera sottoporre a scansione

Se il file system FSX per ONTAP che si desidera sottoporre a scansione non è già in BlueXP come ambiente di lavoro, è possibile aggiungerlo all'area di lavoro in questo momento.

"Scopri come individuare o creare il file system FSX per ONTAP in BlueXP".

## Implementazione dell'istanza di classificazione BlueXP

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

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

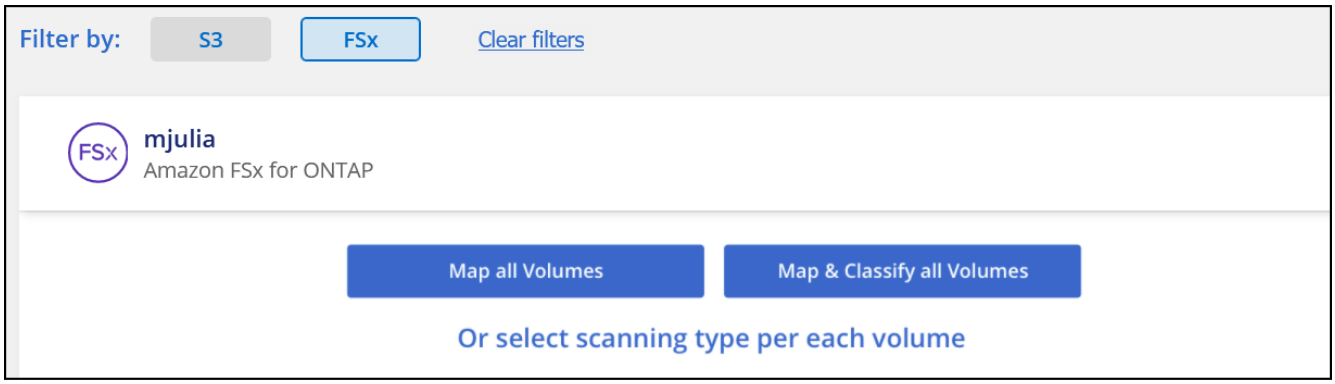
**Nota:** l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei volumi FSX.

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

## Abilitazione della classificazione BlueXP negli ambienti di lavoro

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

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




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

classificazione di tutti i volumi).

- Per personalizzare la scansione per ciascun volume, fare clic su **o selezionare il tipo di scansione per ciascun volume**, quindi scegliere i volumi da mappare e/o classificare.

  Vedere Attivazione e disattivazione delle scansioni di compliance sui volumi per ulteriori informazioni.

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

**Risultato**

La classificazione BlueXP avvia la scansione dei volumi selezionati nell'ambiente di lavoro. I risultati saranno disponibili nella dashboard Compliance non appena la classificazione BlueXP completa le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati, che potrebbe essere di pochi minuti o ore.

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

## Verificare che la classificazione BlueXP abbia accesso ai volumi

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

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

**Fasi**

1. Nella pagina *Configuration*, fare clic su **View Details** (Visualizza dettagli) per esaminare lo stato e correggere eventuali errori.

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

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

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

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

3. Assicurarsi che le seguenti porte siano aperte per l'istanza di classificazione BlueXP.
    - Per NFS: Porte 111 e 2049.
    - Per CIFS – porte 139 e 445.
4. Assicurarsi che i criteri di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza di classificazione BlueXP in modo che possa accedere ai dati di ciascun volume.
5. Se si utilizza CIFS, fornire la classificazione BlueXP con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.

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

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

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

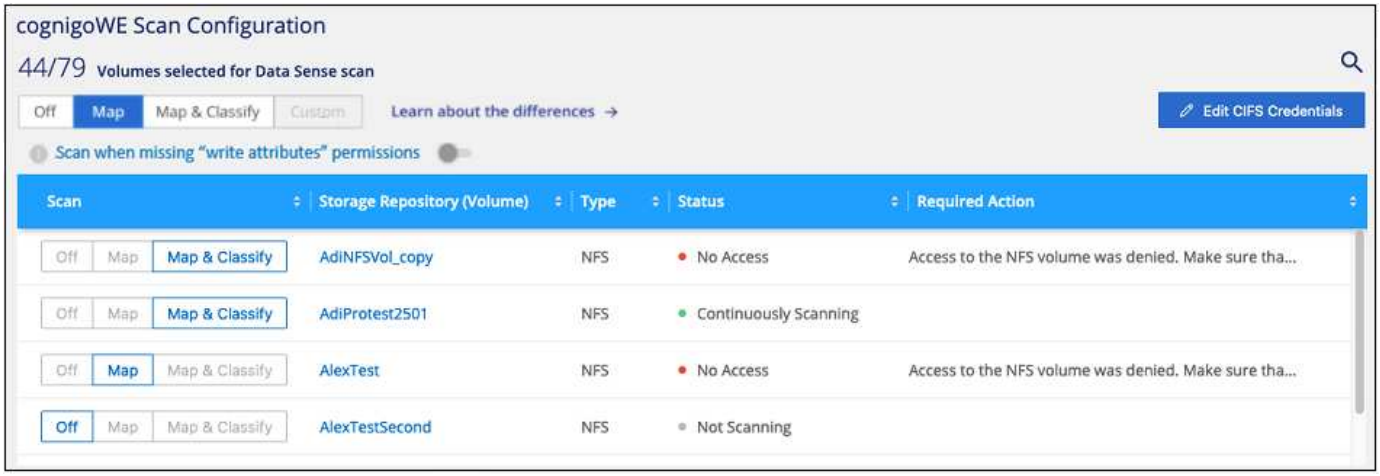
    Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory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

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

## Attivazione e disattivazione delle scansioni di compliance sui volumi

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

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



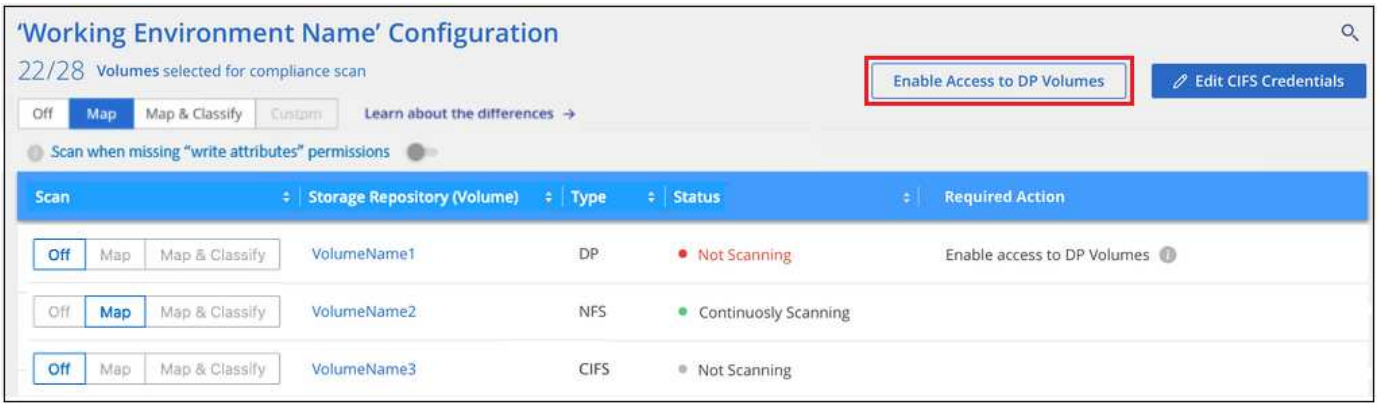

| A: | Eseguire questa operazione: |
|---|---|
| Abilitare le scansioni di sola mappatura su un volume | Nell'area del volume, fare clic su **Map** (Mappa) |
| Abilitare la scansione completa su un volume | Nell'area del volume, fare clic su **Map & Classify** (Mappa e classificazione) |
| Disattivare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

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

## Scansione dei volumi di protezione dei dati

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

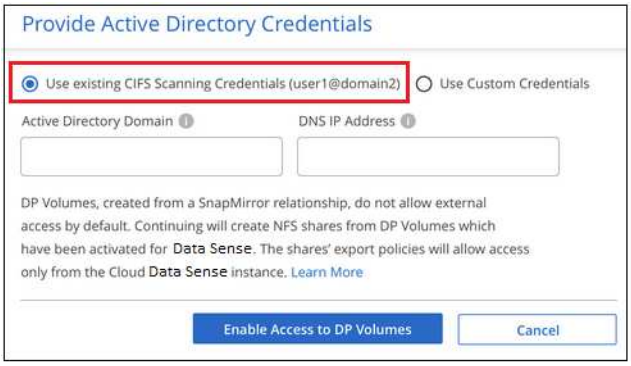
Inizialmente, l'elenco dei volumi identifica questi volumi come *Type* **DP** con *Status* **Not Scanning** e *Required Action* **Enable Access to DP Volumes**.

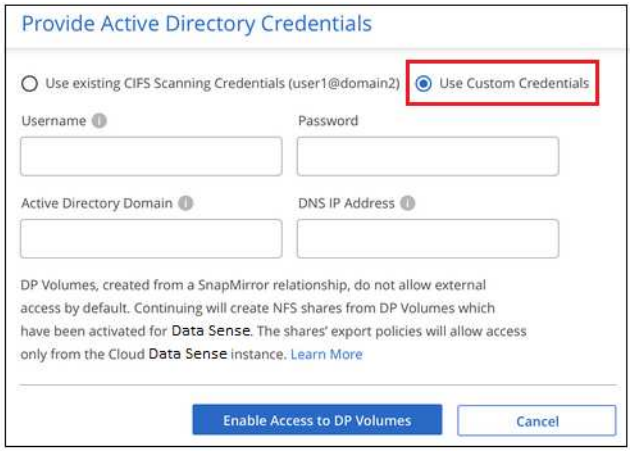



**Fasi**

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

1. Fare clic su **Enable Access to DP Volumes** (attiva accesso ai volumi DP) nella parte superiore della pagina.
2. Leggere il messaggio di conferma e fare nuovamente clic su **Enable Access to DP Volumes** (attiva accesso ai volumi DP).
   - I volumi creati inizialmente come volumi NFS nel file system FSX di origine per ONTAP sono abilitati.
   - I volumi creati inizialmente come volumi CIFS nel file system FSX di origine per ONTAP richiedono l'immissione delle credenziali CIFS per eseguire la scansione di tali volumi DP. Se sono già state immesse le credenziali Active Directory in modo che la classificazione BlueXP possa eseguire la scansione dei volumi CIFS, è possibile utilizzare tali credenziali oppure specificare un set diverso di credenziali Admin.




3. Attivare ciascun volume DP che si desidera sottoporre a scansione allo stesso modo in cui sono stati attivati altri volumi.

**Risultato**

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

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

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

# Introduzione alla classificazione BlueXP per Amazon S3

La classificazione BlueXP consente di eseguire la scansione dei bucket Amazon S3 per identificare i dati personali e sensibili presenti nello storage a oggetti S3. La classificazione BlueXP può eseguire la scansione di qualsiasi bucket dell'account, indipendentemente dal fatto che sia stato creato per una soluzione NetApp.

## Avvio rapido

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

1. **Imposta i requisiti S3 nel tuo ambiente cloud**

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

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 sono automatizzati finché l'istanza dispone di connettività Internet.

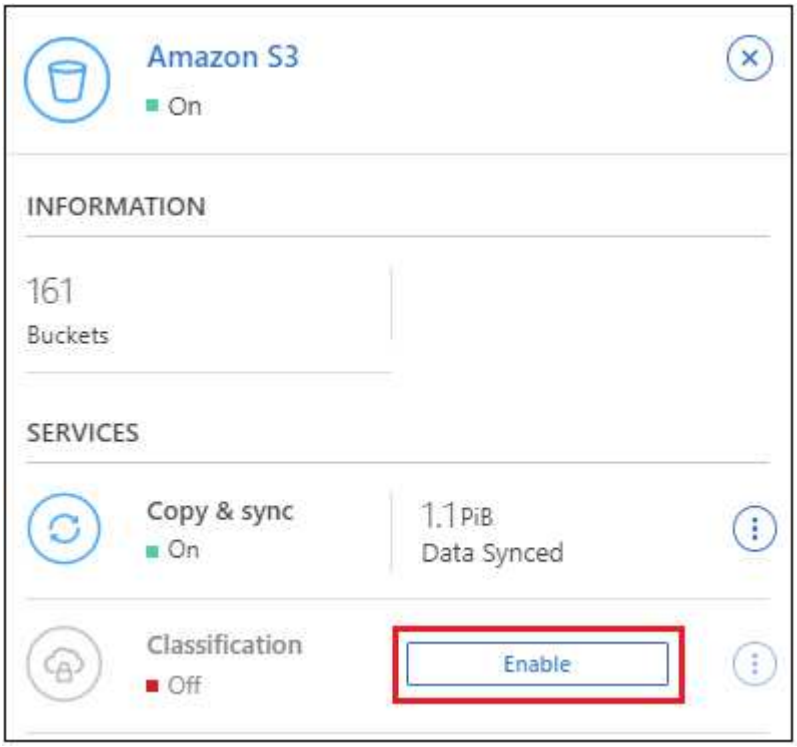
## Attivazione della classificazione BlueXP nell'ambiente di lavoro S3

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

**Fasi**

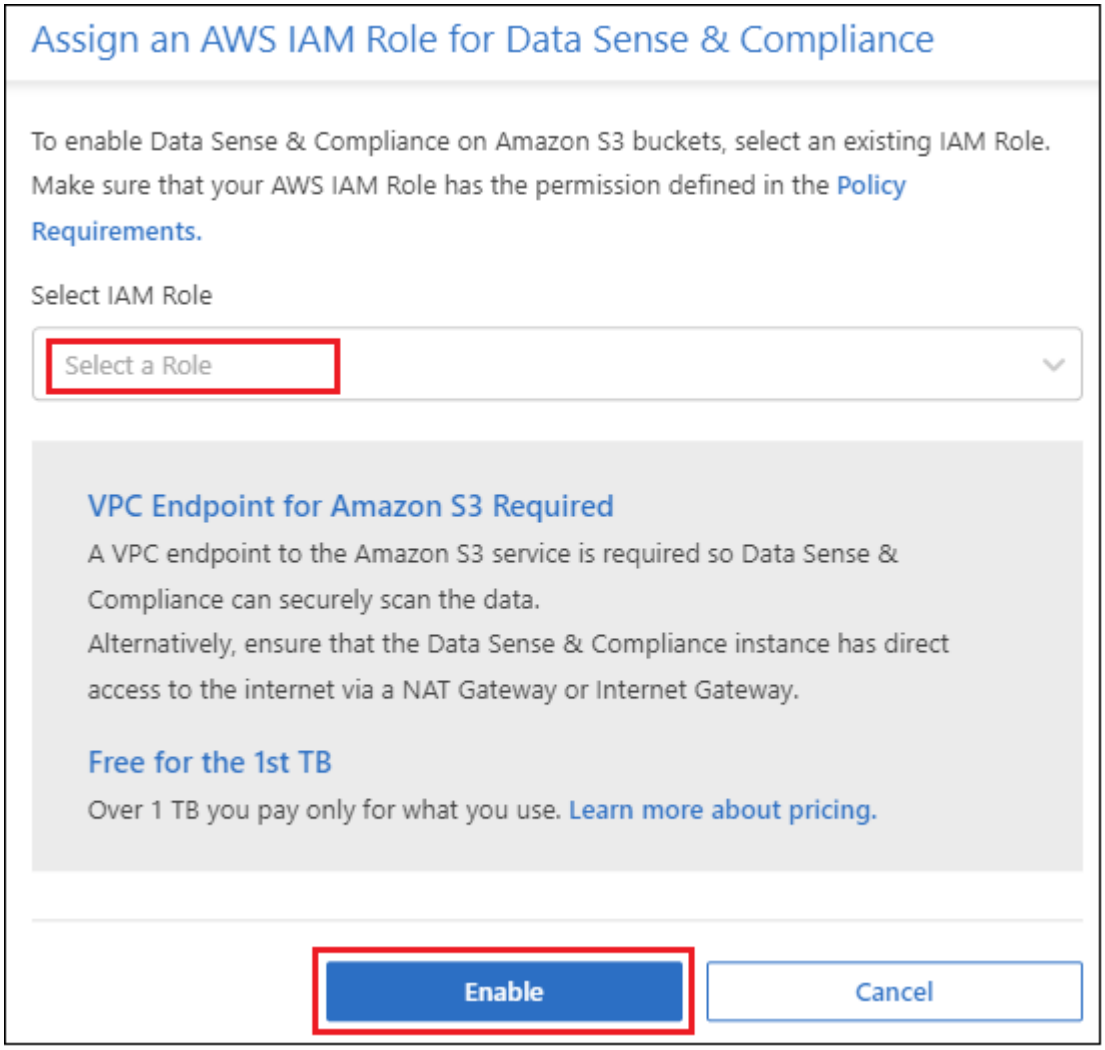
1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Storage > Canvas**.
2. Selezionare l'ambiente di lavoro Amazon S3.


3. Nel riquadro servizi a destra, fare clic su **Enable** (attiva) accanto a **Classification** (classificazione).




4. Quando richiesto, assegnare un ruolo IAM all'istanza di classificazione BlueXP che ha le autorizzazioni

richieste.




5. Fare clic su **Enable** (attiva).

È inoltre possibile attivare le scansioni di conformità per un ambiente di lavoro dalla pagina di configurazione facendo clic su ⋮ E selezionando **Activate BlueXP classification** (attiva classificazione BlueXP).

**Risultato**

BlueXP assegna il ruolo IAM all'istanza.

## Attivazione e disattivazione delle scansioni di compliance sui bucket S3

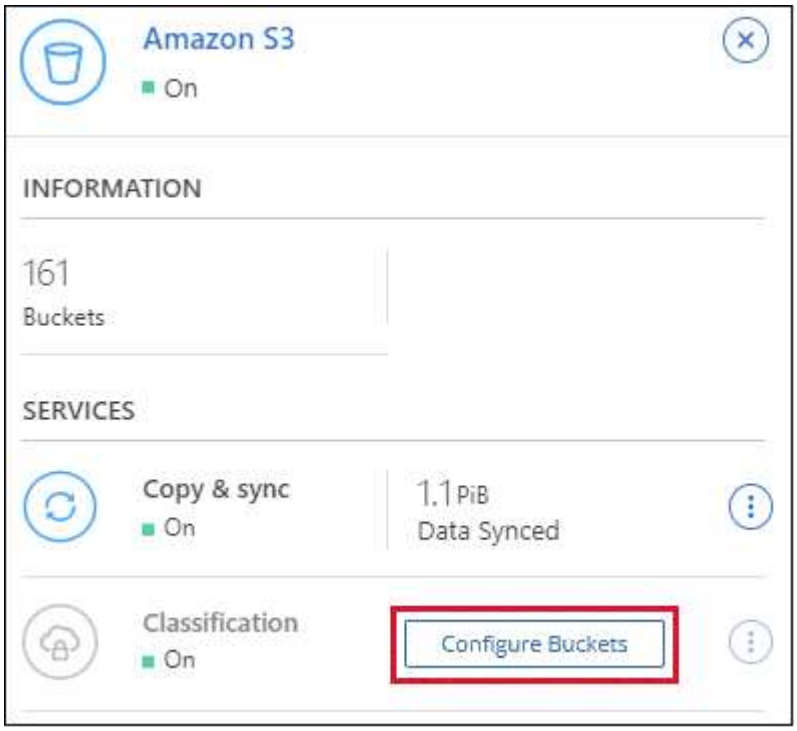
Dopo che BlueXP ha attivato la classificazione BlueXP su Amazon S3, il passaggio successivo consiste nella configurazione dei bucket che si desidera sottoporre a scansione.

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

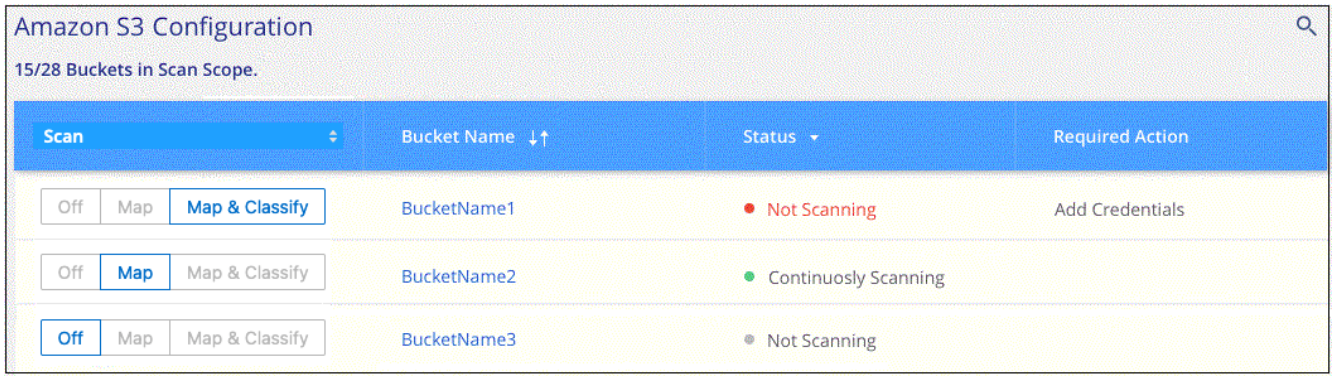
La classificazione BlueXP può anche Eseguire la scansione dei bucket S3 che si trovano in diversi account AWS.

**Fasi**

1. Selezionare l'ambiente di lavoro Amazon S3.
2. Nel riquadro servizi a destra, fare clic su **Configura bucket**.




3. Abilita scansioni di sola mappatura o scansioni di mappatura e classificazione sui bucket.




| A: | Eseguire questa operazione: |
|---|---|
| Attivare scansioni solo mappatura su un bucket | Fare clic su **Map** (Mappa) |
| Abilitare scansioni complete su un bucket | Fare clic su **Map & Classify** (Mappa e classificazione) |
| Disattivare la scansione su un bucket | Fare clic su **Off** |

**Risultato**

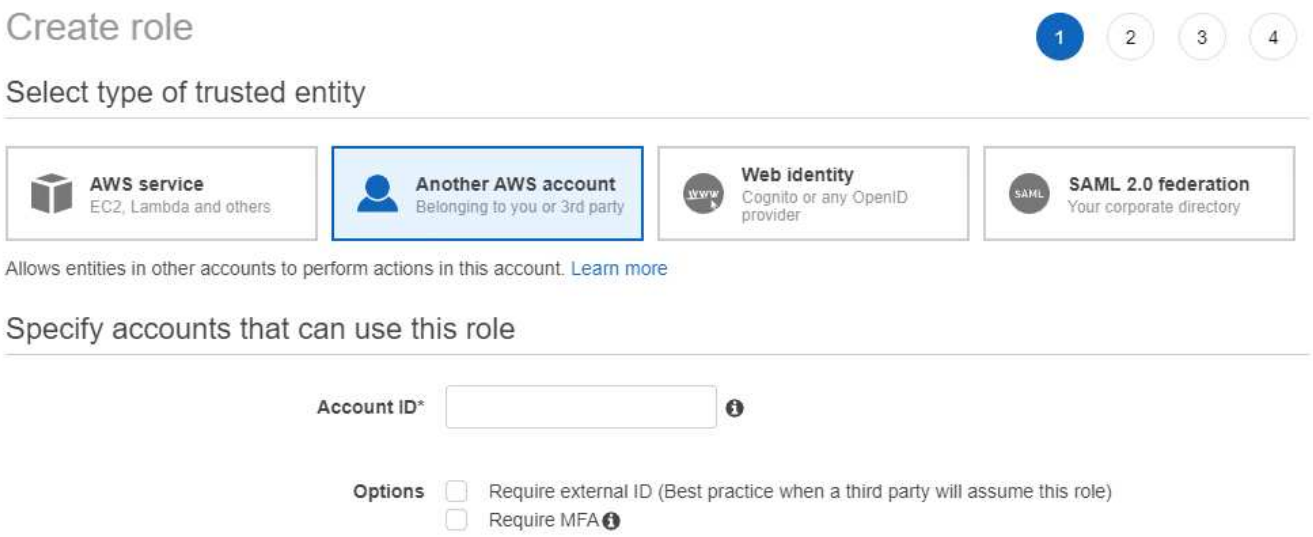
La classificazione BlueXP avvia la scansione dei bucket S3 abilitati. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

## Scansione dei bucket da account AWS aggiuntivi

È possibile eseguire la scansione dei bucket S3 che si trovano sotto un account AWS diverso assegnando un ruolo da tale account per accedere all'istanza di classificazione BlueXP esistente.

**Fasi**

1. Accedere all'account AWS di destinazione in cui si desidera eseguire la scansione dei bucket S3 e creare un ruolo IAM selezionando **un altro account AWS**.




   Assicurarsi di effettuare le seguenti operazioni:

   - Inserire l'ID dell'account in cui risiede l'istanza di classificazione BlueXP.
   - Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.
   - Allegare il criterio IAM di classificazione BlueXP. Assicurarsi che disponga delle autorizzazioni necessarie.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Accedere all'account AWS di origine in cui risiede l'istanza di classificazione BlueXP e selezionare il ruolo

IAM associato all'istanza.

a. Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.

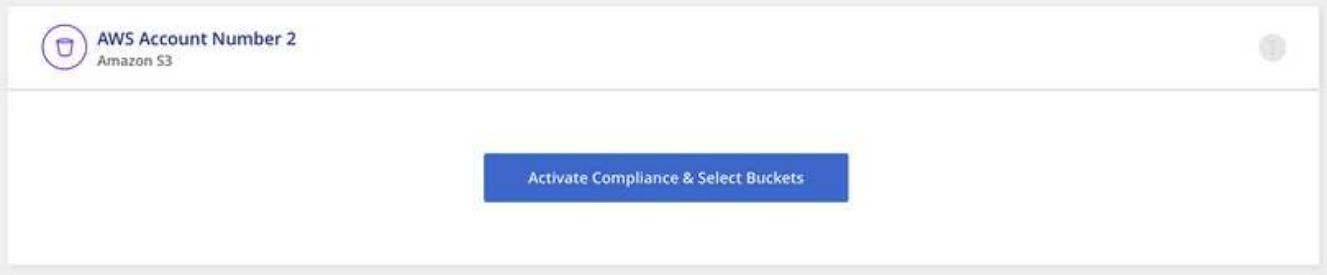
b. Fare clic su **Allega policy**, quindi su **Crea policy**.

c. Creare un criterio che includa l'azione "sts:AssumeRole" e specificare l'ARN del ruolo creato nell'account di destinazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

L'account del profilo dell'istanza di classificazione BlueXP ora ha accesso all'account AWS aggiuntivo.

3. Accedere alla pagina **Amazon S3 Configuration** (Configurazione Amazon S3) per visualizzare il nuovo account AWS. Nota: La sincronizzazione dell'ambiente di lavoro del nuovo account e la visualizzazione di queste informazioni possono richiedere alcuni minuti prima che la classificazione BlueXP venga eseguita.




4. Fare clic su **Activate BlueXP classification & Select Bucket** (attiva classificazione BlueXP e seleziona bucket) e selezionare i bucket da sottoporre a scansione.

#### Risultato

La classificazione BlueXP avvia la scansione dei nuovi bucket S3 abilitati.

# Scansione degli schemi del database

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

Dopo aver abilitato la scansione del database, è possibile aggiungere identificatori univoci che la classificazione BlueXP identificherà in tutte le origini dati in base a colonne specifiche dei database. Questa funzione è denominata *Data Fusion*. "Scopri come aggiungere identificatori di dati personali personalizzati dai tuoi database".

## Avvio rapido

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

1. **Esaminare i prerequisiti del database**

Assicurarsi che il database sia supportato e di disporre delle informazioni necessarie per la connessione al database.

2. **Distribuire l'istanza di classificazione BlueXP**

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

3. **Aggiungere il server database**

Aggiungere il server database a cui si desidera accedere.

4. **Selezionare gli schemi**

Selezionare gli schemi da sottoporre a scansione.

## Esaminare i prerequisiti

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

#### Database supportati

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

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

- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

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

**Requisiti del database**

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

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

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

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

## Distribuire l'istanza di classificazione BlueXP

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

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

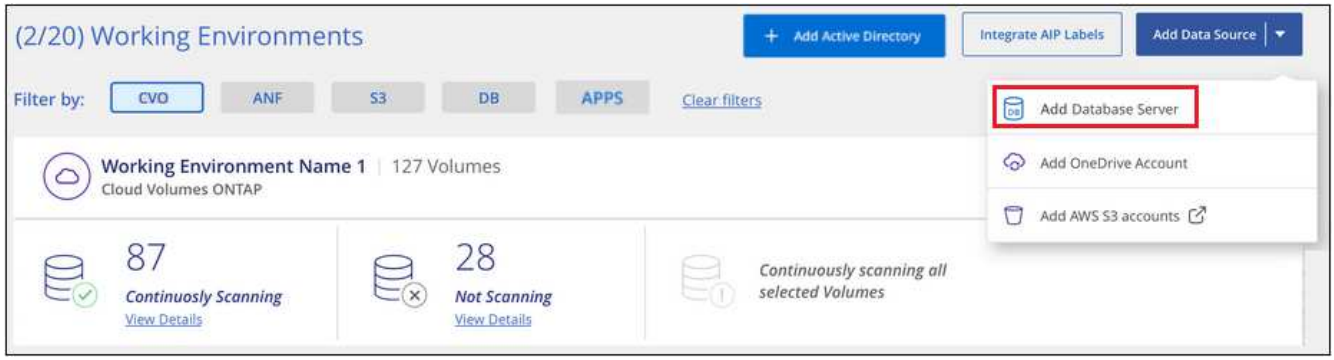
Se si eseguono scansioni di schemi di database installati in un sito buio che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella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

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

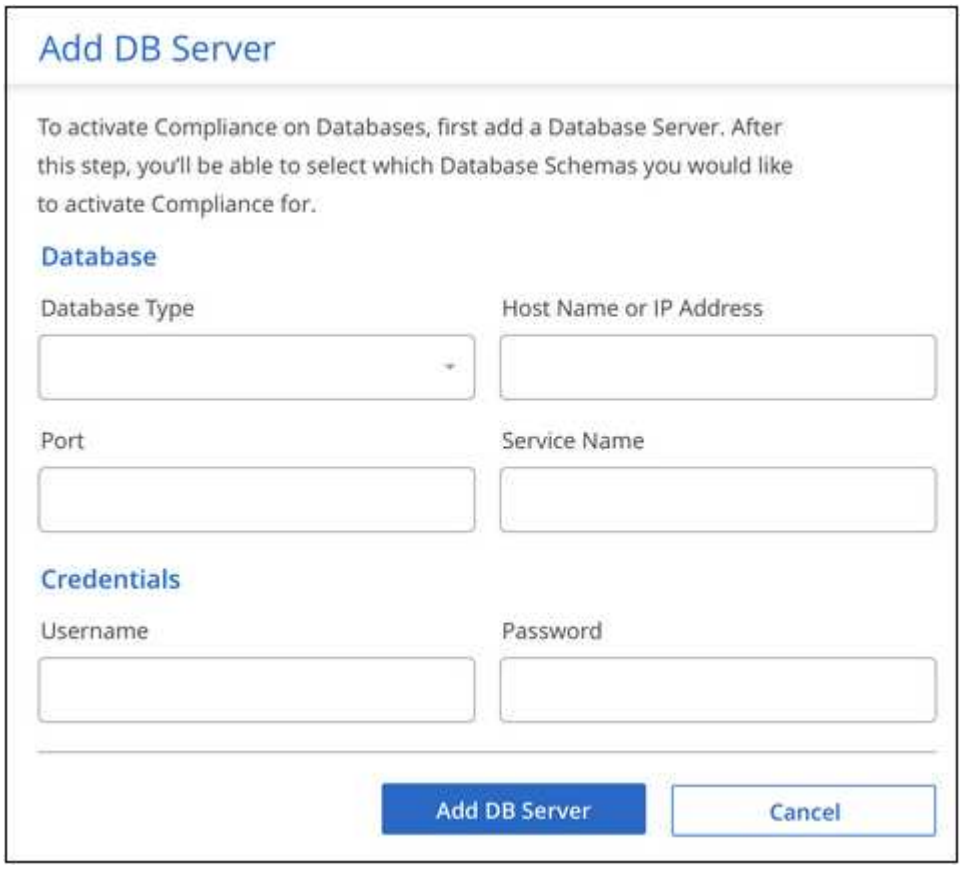
## Aggiungere il server database

Aggiungere il server di database in cui risiedono gli schemi.

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add Database Server** (Aggiungi server database).




2. Inserire le informazioni richieste per identificare il server di database.
   a. Selezionare il tipo di database.
   b. Immettere la porta e il nome host o l'indirizzo IP per la connessione al database.
   c. Per i database Oracle, immettere il nome del servizio.
   d. Inserire le credenziali in modo che la classificazione BlueXP possa accedere al server.
   e. Fare clic su **Add DB Server** (Aggiungi server DB).




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

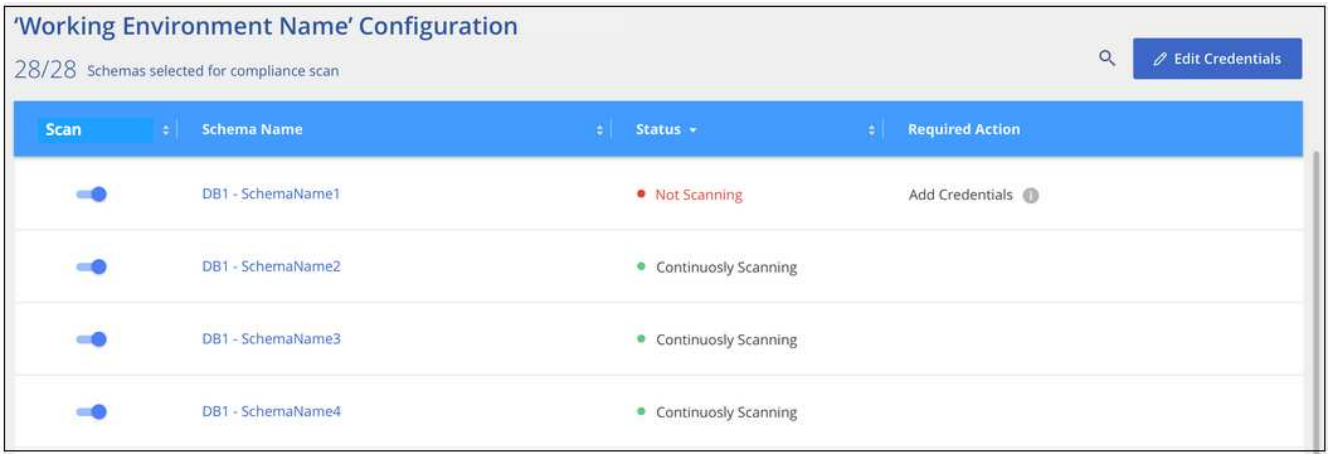
## Abilitare e disabilitare le scansioni di conformità sugli schemi di database

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

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

1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** del database che si desidera configurare.


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




**Risultato**

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

Si noti che la classificazione BlueXP esegue la scansione dei database una volta al giorno, poiché i database non vengono sottoposti a scansione continua come altre origini dati.

# Scansione degli account OneDrive

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

## Avvio rapido

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

1 **Verifica dei prerequisiti di OneDrive**

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

**2 Distribuire l'istanza di classificazione BlueXP**

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

**3 Aggiungere l'account OneDrive**

Utilizzando le credenziali dell'utente Admin, accedere all'account OneDrive a cui si desidera accedere in modo che venga aggiunto come nuovo ambiente di lavoro.

**4 Aggiungere gli utenti e selezionare il tipo di scansione**

Aggiungere l'elenco degli utenti dall'account OneDrive che si desidera sottoporre a scansione e selezionare il tipo di scansione. È possibile aggiungere fino a 100 utenti alla volta.

## Verifica dei requisiti di OneDrive

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

- È necessario disporre delle credenziali di accesso Admin per l'account OneDrive for Business che fornisce l'accesso in lettura ai file dell'utente.
- Avrai bisogno di un elenco degli indirizzi e-mail separato da righe per tutti gli utenti di cui desideri eseguire la scansione delle cartelle di OneDrive.

## Implementazione dell'istanza di classificazione BlueXP

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

La classificazione BlueXP può essere "implementato nel cloud" oppure "in una sede on-premise con accesso a internet".

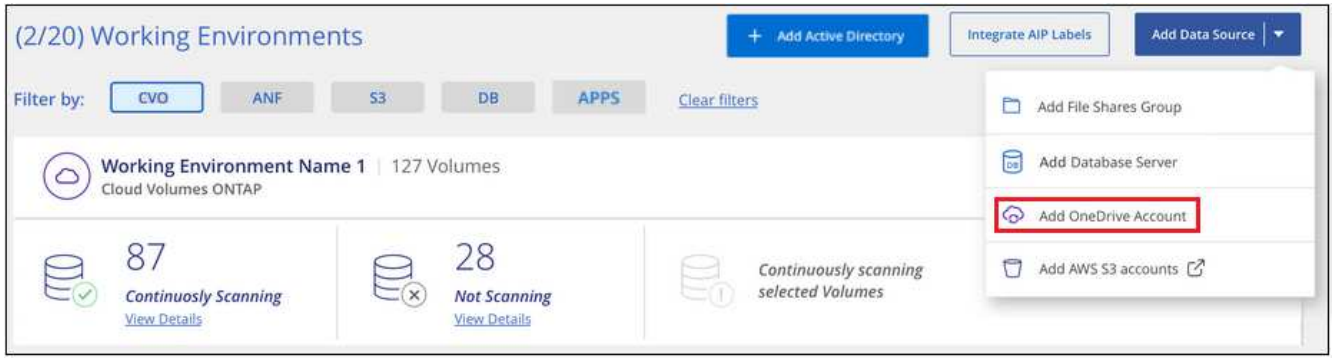
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

## Aggiunta dell'account OneDrive

Aggiungere l'account OneDrive in cui risiedono i file utente.

**Fasi**

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add OneDrive account** (Aggiungi account OneDrive).




2. Nella finestra di dialogo Aggiungi un account OneDrive, fai clic su **Accedi a OneDrive**.
3. Nella pagina Microsoft che viene visualizzata, selezionare l'account OneDrive e immettere l'utente e la password di amministratore richiesti, quindi fare clic su **Accept** per consentire alla classificazione BlueXP di leggere i dati da questo account.

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

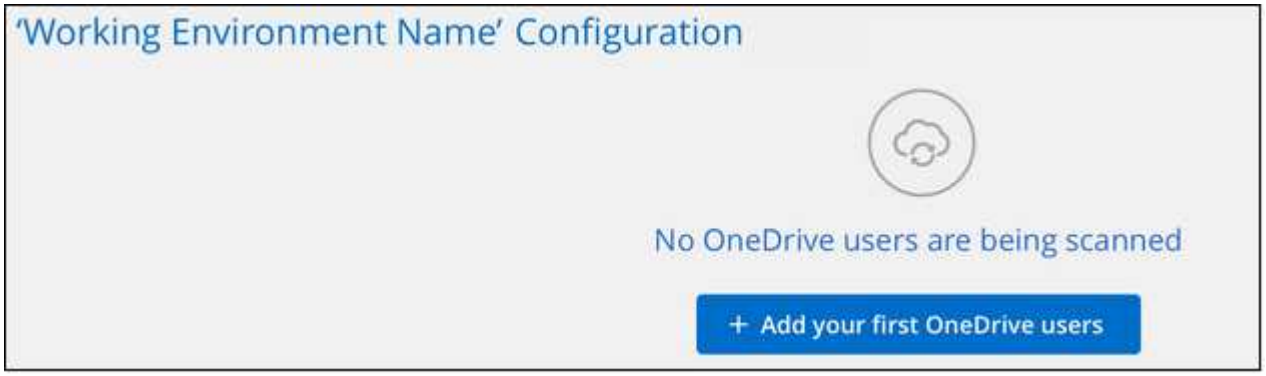
## Aggiunta di utenti OneDrive alle scansioni di conformità

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

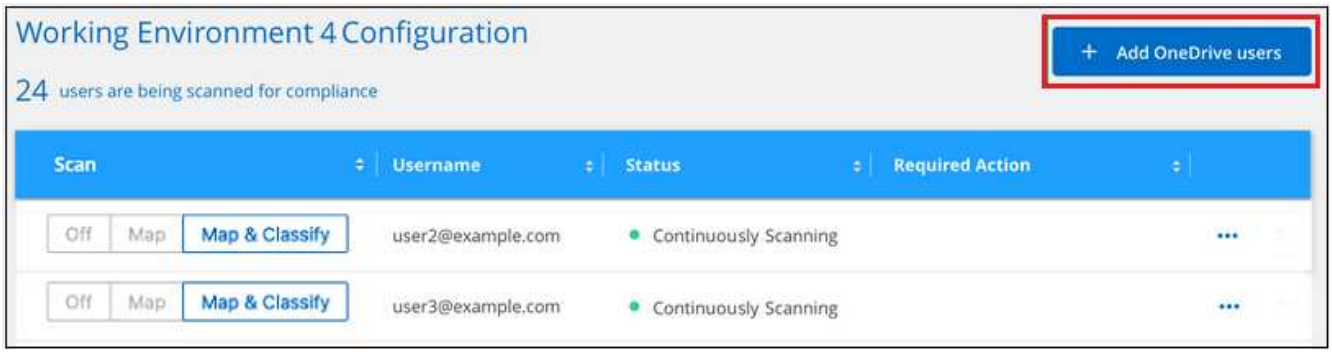
**Fasi**

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

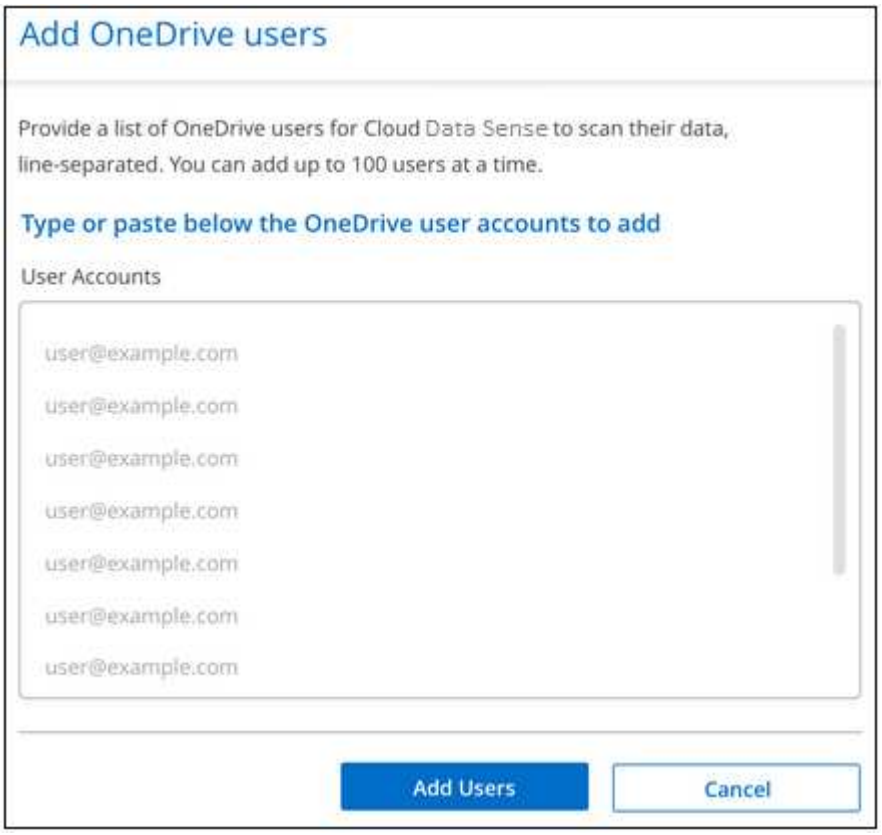

2. Se è la prima volta che si aggiungono utenti per questo account OneDrive, fare clic su **Aggiungi i primi utenti OneDrive**.




Se si aggiungono altri utenti da un account OneDrive, fare clic su **Aggiungi utenti OneDrive**.




3. Aggiungere gli indirizzi e-mail degli utenti di cui si desidera eseguire la scansione - un indirizzo e-mail per riga (fino a 100 per sessione) - e fare clic su **Aggiungi utenti**.




Una finestra di dialogo di conferma visualizza il numero di utenti aggiunti.

Se la finestra di dialogo elenca gli utenti che non possono essere aggiunti, acquisire queste informazioni in modo da poter risolvere il problema. In alcuni casi è possibile aggiungere nuovamente l'utente con un indirizzo e-mail corretto.

4. Attivare scansioni di sola mappatura o scansioni di mappatura e classificazione sui file utente.

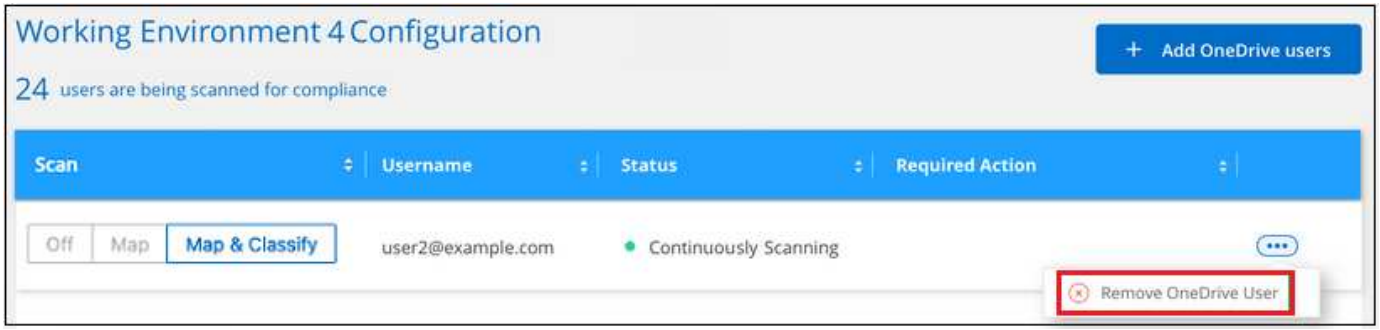
| A: | Eseguire questa operazione: |
|---|---|
| Attiva scansioni solo mappatura sui file utente | Fare clic su **Map** (Mappa) |
| Attiva scansioni complete sui file utente | Fare clic su **Map & Classify** (Mappa e classificazione) |
| Disattivare la scansione dei file utente | Fare clic su **Off**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

**Risultato**

La classificazione BlueXP avvia la scansione dei file per gli utenti aggiunti e i risultati vengono visualizzati nella dashboard e in altre posizioni.

### Rimozione di un utente OneDrive dalle scansioni di conformità

Se gli utenti lasciano l'azienda o se il loro indirizzo e-mail cambia, puoi rimuovere singoli utenti di OneDrive dall'eseguire la scansione dei loro file in qualsiasi momento. Fare clic su **Remove OneDrive User** (Rimuovi utente OneDrive) dalla pagina di configurazione.




Nota: È possibile "Elimina l'intero account OneDrive dalla classificazione BlueXP" Se non si desidera più eseguire la scansione dei dati utente dall'account OneDrive.

## Scansione degli account SharePoint

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

### Avvio rapido

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

1. **Esaminare i prerequisiti di SharePoint**

Assicurarsi di disporre di credenziali qualificate per accedere all'account SharePoint e di disporre degli URL dei siti SharePoint che si desidera sottoporre a scansione.

2. **Distribuire l'istanza di classificazione BlueXP**

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

3. **Accedere all'account SharePoint**

Utilizzando credenziali utente qualificate, accedere all'account SharePoint a cui si desidera accedere in modo che venga aggiunto come nuova origine dati/ambiente di lavoro.

4. **Aggiungere gli URL del sito SharePoint da sottoporre a scansione**

Aggiungere l'elenco degli URL del sito SharePoint che si desidera sottoporre a scansione nell'account SharePoint e selezionare il tipo di scansione. È possibile aggiungere fino a 100 URL alla volta e fino a 1,000 siti in totale per ciascun account.

## Analisi dei requisiti di SharePoint

Esaminare i seguenti prerequisiti per assicurarsi di essere pronti per attivare la classificazione BlueXP su un account SharePoint.

- È necessario disporre delle credenziali di accesso dell'utente Admin per l'account SharePoint che fornisce l'accesso in lettura a tutti i siti SharePoint.
  - Per SharePoint Online è possibile utilizzare un account non Admin, ma tale utente deve disporre dell'autorizzazione per accedere a tutti i siti SharePoint che si desidera sottoporre a scansione.
- Per SharePoint on-premise, è necessario anche l'URL di SharePoint Server.
- Per tutti i dati che si desidera sottoporre a scansione, è necessario disporre di un elenco degli URL del sito SharePoint separato da righe.

## Implementazione dell'istanza di classificazione BlueXP

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

- Per SharePoint Online, la classificazione BlueXP può essere "implementato nel cloud".
- Per SharePoint on-premise, è possibile installare la classificazione BlueXP "in una sede on-premise con accesso a internet" oppure "in una sede on-premise che non dispone di accesso a internet".

Quando la classificazione BlueXP viene installata in un sito senza accesso a Internet, BlueXP Connector deve essere installato nello stesso sito senza accesso a Internet. "Scopri di più".

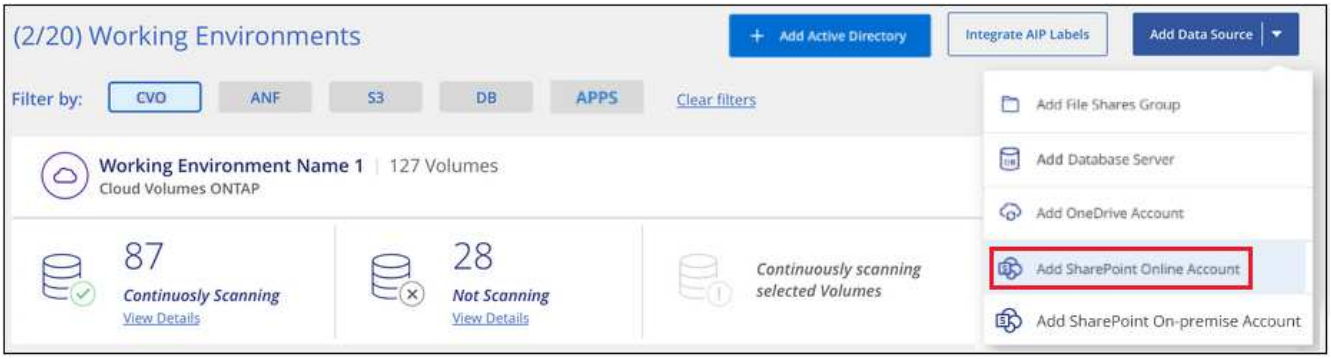
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

## Aggiunta di un account SharePoint Online

Aggiungere l'account SharePoint Online in cui risiedono i file utente.

### Fasi

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add SharePoint Online account** (Aggiungi account online SharePoint).



2. Nella finestra di dialogo Aggiungi un account online SharePoint, fare clic su **Accedi a SharePoint**.
3. Nella pagina Microsoft visualizzata, selezionare l'account SharePoint e immettere l'utente e la password (utente amministratore o altro utente con accesso ai siti SharePoint), quindi fare clic su **Accetta** per consentire alla classificazione BlueXP di leggere i dati da questo account.

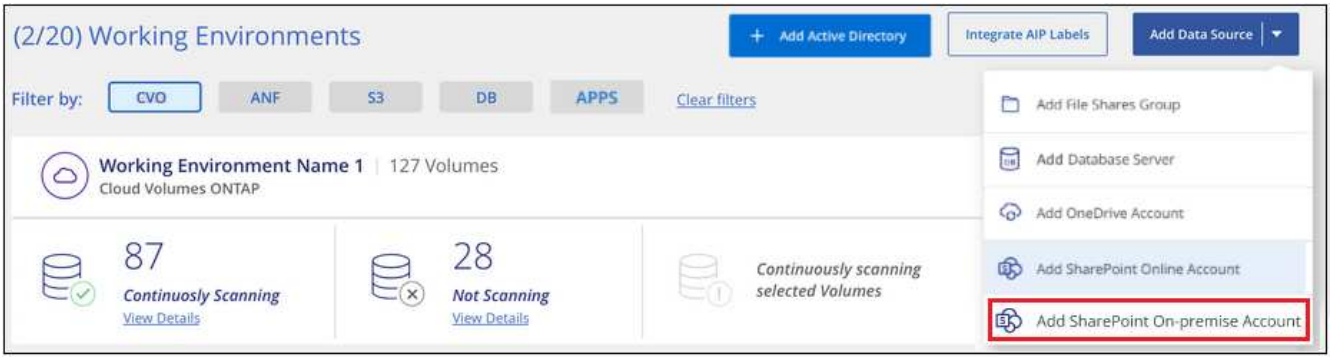
L'account SharePoint Online viene aggiunto all'elenco degli ambienti di lavoro.

## Aggiunta di un account SharePoint on-premise

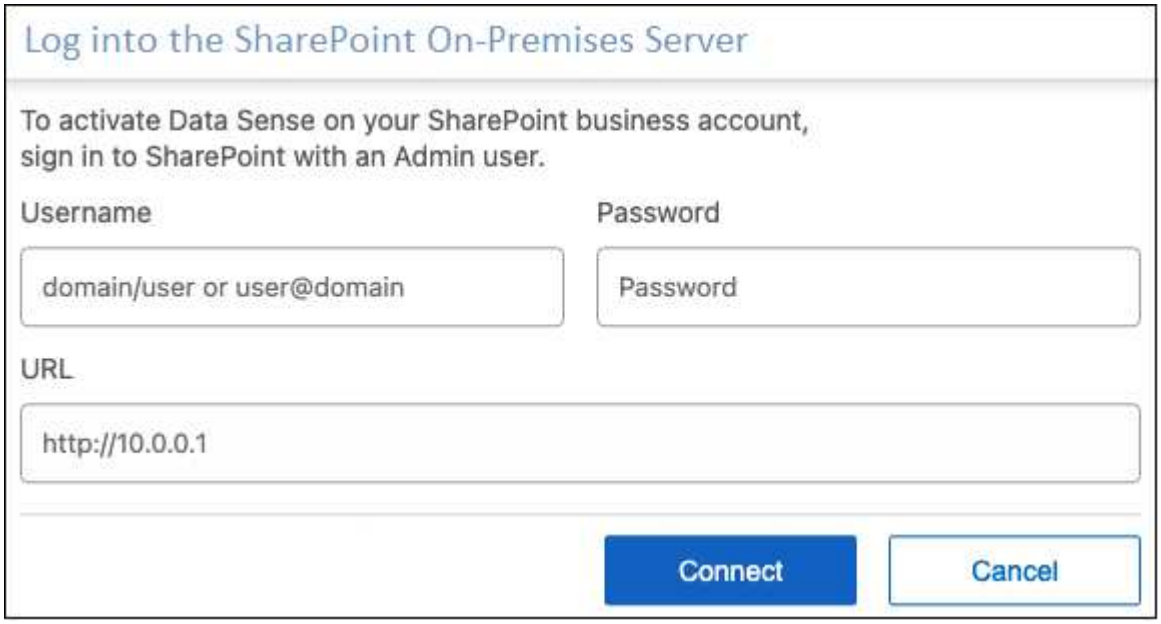
Aggiungere l'account SharePoint on-premise in cui risiedono i file utente.

**Fasi**

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add SharePoint on-premise account** (Aggiungi account SharePoint on-premise).




2. Nella finestra di dialogo Log in the SharePoint on-premise Server (Accedi al server SharePoint on-premise), immettere le seguenti informazioni:
   - Admin user in formato "dominio/utente" o "utente@dominio" e admin password
   - URL di SharePoint Server




3. Fare clic su **Connect** (Connetti).

L'account SharePoint on-premise viene aggiunto all'elenco degli ambienti di lavoro.

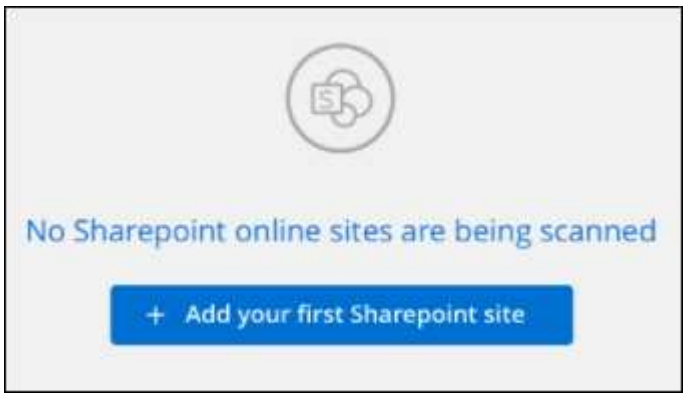
## Aggiunta di siti SharePoint alle scansioni di conformità

È possibile aggiungere singoli siti SharePoint o fino a 1,000 siti SharePoint nell'account, in modo che i file associati vengano sottoposti a scansione in base alla classificazione BlueXP. La procedura è la stessa, sia che si aggiungano siti SharePoint Online o SharePoint on-premise.

**Fasi**

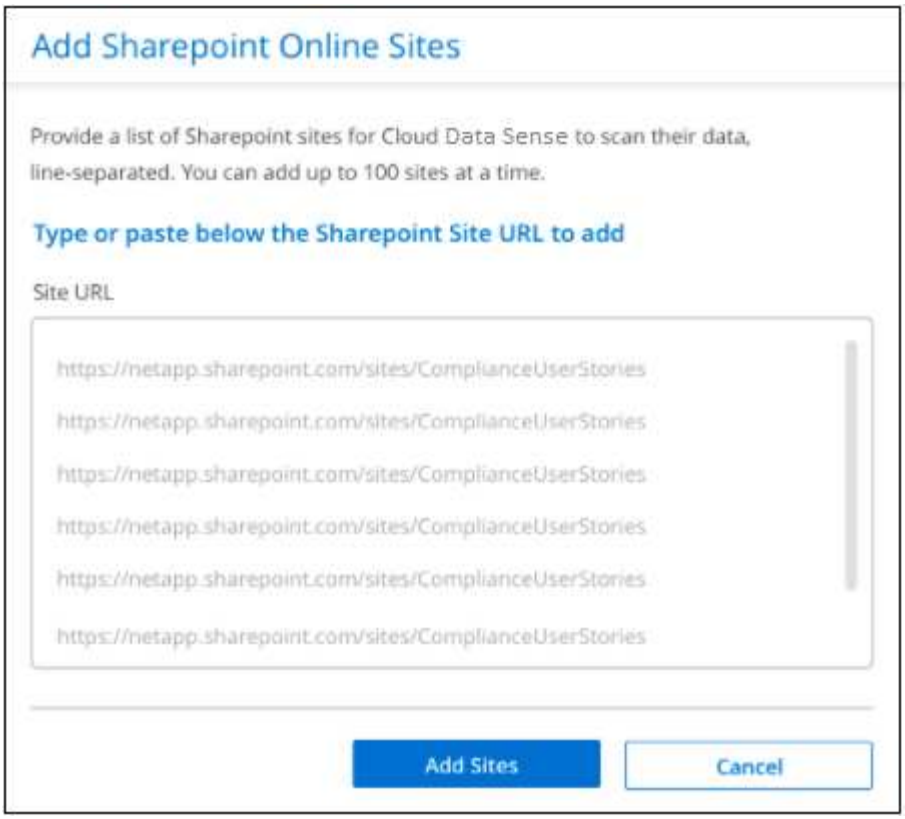
1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** dell'account SharePoint.


2. Se questa è la prima volta che si aggiungono siti per questo account SharePoint, fare clic su **Aggiungi il primo sito SharePoint**.




Se si aggiungono altri utenti da un account SharePoint, fare clic su **Aggiungi siti SharePoint**.


3. Aggiungere gli URL dei siti di cui si desidera eseguire la scansione - un URL per riga (fino a 100 per sessione) - e fare clic su **Aggiungi siti**.




Una finestra di dialogo di conferma visualizza il numero di siti aggiunti.

Se la finestra di dialogo elenca i siti che non è stato possibile aggiungere, acquisire queste informazioni in modo da risolvere il problema. In alcuni casi è possibile aggiungere nuovamente il sito con un URL corretto.

4. Se è necessario aggiungere più di 100 siti per questo account, fare clic nuovamente su **Aggiungi siti SharePoint** fino a quando non sono stati aggiunti tutti i siti per questo account (fino a un totale di 1,000 siti per ciascun account).
5. Attivare scansioni di sola mappatura o scansioni di mappatura e classificazione sui file nei siti SharePoint.

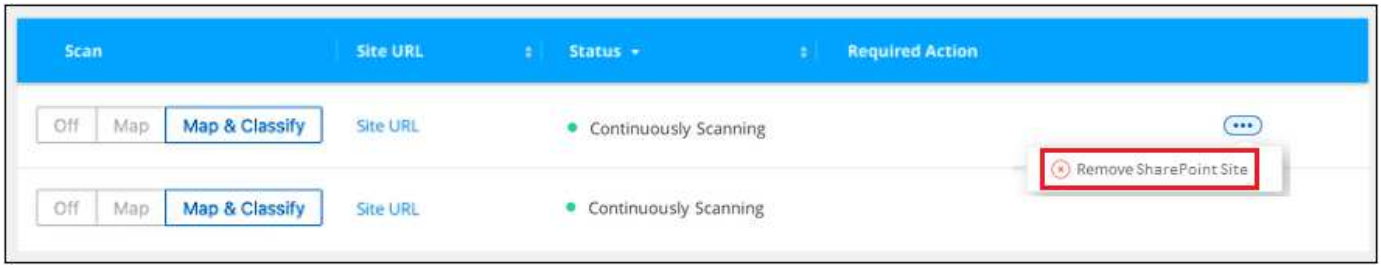
| A: | Eseguire questa operazione: |
|---|---|
| Abilitare le scansioni di sola mappatura sui file | Fare clic su **Map** (Mappa) |
| Attivare scansioni complete sui file | Fare clic su **Map & Classify** (Mappa e classificazione) |
| Disattivare la scansione dei file | Fare clic su **Off** |

**Risultato**

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

## Rimozione di un sito SharePoint dalle scansioni di conformità

Se si rimuove un sito SharePoint in futuro o si decide di non eseguire la scansione dei file in un sito SharePoint, è possibile rimuovere singoli siti SharePoint dall'eseguire la scansione dei file in qualsiasi momento. Fai clic su **Rimuovi sito SharePoint** dalla pagina di configurazione.




Nota: È possibile "Eliminare l'intero account SharePoint dalla classificazione BlueXP" Se non si desidera più eseguire la scansione dei dati utente dall'account SharePoint.

# Scansione di account Google Drive

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

## Avvio rapido

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

1. **Esaminare i prerequisiti di Google Drive**

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

2. **Implementare la classificazione BlueXP**

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

3. **Accedere all'account Google Drive**

Utilizzando le credenziali dell'utente Admin, accedere all'account Google Drive a cui si desidera accedere in modo che venga aggiunto come nuova origine dati.

4. **Selezionare il tipo di scansione dei file utente**

Selezionare il tipo di scansione che si desidera eseguire sui file dell'utente; mappatura o mappatura e classificazione.

## Analisi dei requisiti di Google Drive

Esaminare i seguenti prerequisiti per assicurarsi di essere pronti per attivare la classificazione BlueXP su un account Google Drive.

- È necessario disporre delle credenziali di accesso Admin per l'account Google Drive che fornisce l'accesso in lettura ai file dell'utente

### Restrizioni attuali

Le seguenti funzionalità di classificazione BlueXP non sono attualmente supportate con Google Drive Files:

- Quando si visualizzano i file nella pagina Data Investigation (analisi dati), le azioni nella barra dei pulsanti non sono attive. Non è possibile copiare, spostare, eliminare, ecc. alcun file.
- Non è possibile identificare le autorizzazioni all'interno dei file in Google Drive, pertanto non vengono visualizzate informazioni sulle autorizzazioni nella pagina di analisi.

## Implementazione della classificazione BlueXP

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

La classificazione BlueXP può essere "implementato nel cloud" oppure "in una sede on-premise con accesso a internet".

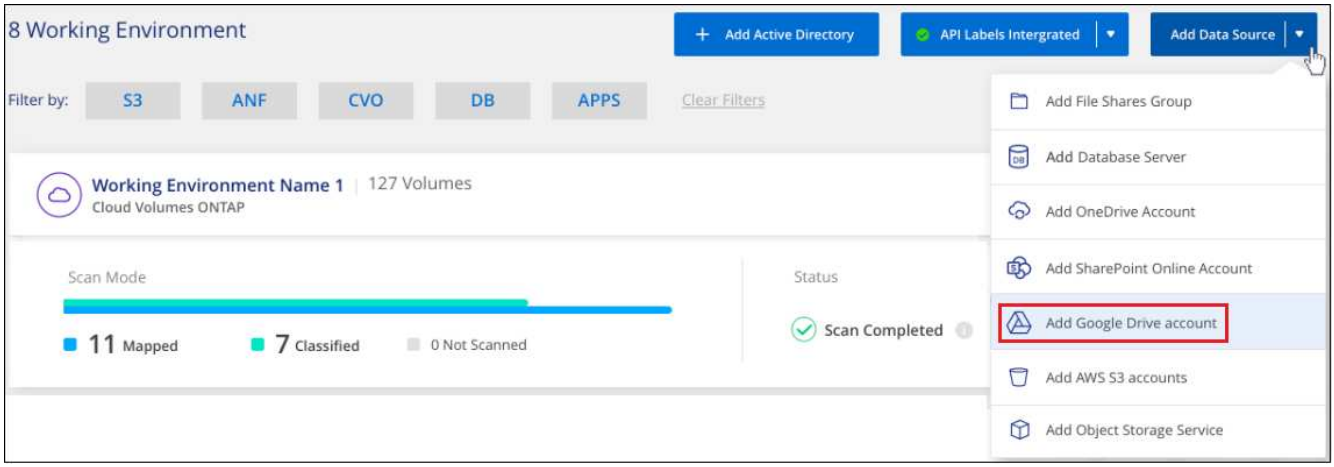
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

## Aggiunta dell'account Google Drive

Aggiungere l'account Google Drive in cui risiedono i file utente. Se si desidera eseguire la scansione di file da più utenti, è necessario eseguire questa procedura per ciascun utente.

### Fasi

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add Google Drive account** (Aggiungi account Google Drive).




2. Nella finestra di dialogo Aggiungi un account Google Drive, fare clic su **Accedi a Google Drive**.
3. Nella pagina Google visualizzata, selezionare l'account Google Drive e immettere l'utente e la password di amministratore richiesti, quindi fare clic su **Accept** (Accetta) per consentire alla classificazione BlueXP di leggere i dati da questo account.

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

## Selezione del tipo di scansione per i dati dell'utente

Selezionare il tipo di scansione che verrà eseguita dalla classificazione BlueXP sui dati dell'utente.

**Fasi**

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


2. Abilitare le scansioni di sola mappatura, o le scansioni di mappatura e classificazione, sui file nell'account Google Drive.


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

**Risultato**

La classificazione BlueXP avvia la scansione dei file nell'account Google Drive aggiunto e i risultati vengono visualizzati nella dashboard e in altre posizioni.

### Rimozione di un account Google Drive dalle scansioni di conformità

Poiché solo i file Google Drive di un singolo utente fanno parte di un singolo account Google Drive, se si desidera interrompere la scansione dei file dall'account Google Drive di un utente, è necessario "Eliminare l'account Google Drive dalla classificazione BlueXP".

# Scansione delle condivisioni di file

Completare alcuni passaggi per avviare la scansione di condivisioni di file NFS o CIFS non NetApp direttamente con la classificazione BlueXP. Queste condivisioni di file possono risiedere on-premise o nel cloud.

## Avvio rapido

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

1 **Verificare i prerequisiti per la condivisione dei file**

Per le condivisioni CIFS (SMB), assicurarsi di disporre delle credenziali per accedere alle condivisioni.

**2 Distribuire l'istanza di classificazione BlueXP**

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

**3 Creare un gruppo per conservare le condivisioni di file**

Il gruppo è un contenitore per le condivisioni di file che si desidera sottoporre a scansione e viene utilizzato come nome dell'ambiente di lavoro per tali condivisioni di file.

**4 Aggiungere le condivisioni di file al gruppo**

Aggiungere l'elenco delle condivisioni di file che si desidera acquisire e selezionare il tipo di scansione. È possibile aggiungere fino a 100 condivisioni di file alla volta.

## Revisione dei requisiti di condivisione dei file

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

- Le condivisioni possono essere ospitate ovunque, anche nel cloud o on-premise. Nella maggior parte dei casi si tratta di condivisioni di file che risiedono su sistemi di storage non NetApp. Tuttavia, le condivisioni CIFS dei sistemi storage NetApp 7-Mode precedenti possono essere sottoposte a scansione come condivisioni di file.

  Si noti che la classificazione BlueXP non può estrarre le autorizzazioni o il "tempo di accesso ultimo" dai sistemi 7-Mode. Inoltre, a causa di un problema noto tra alcune versioni di Linux e le condivisioni CIFS su sistemi 7-Mode, è necessario configurare la condivisione in modo che utilizzi solo SMB v1 con l'autenticazione NTLM attivata.

- È necessario disporre di una connettività di rete tra l'istanza di classificazione BlueXP e le condivisioni.
- Assicurarsi che queste porte siano aperte per l'istanza di classificazione BlueXP:
  - Per NFS: Porte 111 e 2049.
  - Per CIFS – porte 139 e 445.
- È possibile aggiungere una condivisione DFS (Distributed file System) come normale condivisione CIFS. Tuttavia, poiché la classificazione BlueXP non è consapevole che la condivisione è costruita su più server/volumi combinati come una singola CIFS share, potresti ricevere errori di permessi o connettività sulla condivisione quando il messaggio si applica davvero solo a una delle cartelle/condivisioni che si trova su un server/volume diverso.
- Per le condivisioni CIFS (SMB), assicurarsi di disporre delle credenziali Active Directory che forniscono l'accesso in lettura alle condivisioni. Le credenziali di amministratore sono preferite nel caso in cui la classificazione BlueXP debba eseguire la scansione di qualsiasi dato che richieda autorizzazioni elevate.

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

- Sarà necessario l'elenco delle condivisioni che si desidera aggiungere nel formato

`<host_name>:/<share_path>`. È possibile immettere le condivisioni singolarmente oppure fornire un elenco separato da riga delle condivisioni di file che si desidera acquisire.

## Implementazione dell'istanza di classificazione BlueXP

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

Se si esegue la scansione di condivisioni di file NFS o CIFS non NetApp accessibili tramite Internet, è possibile "Implementare la classificazione BlueXP nel cloud" oppure "Implementare la classificazione BlueXP in una posizione on-premise con accesso a Internet".

Se si esegue la scansione di condivisioni di file NFS o CIFS non NetApp installate in un sito buio che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella stessa posizione on-premise.

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

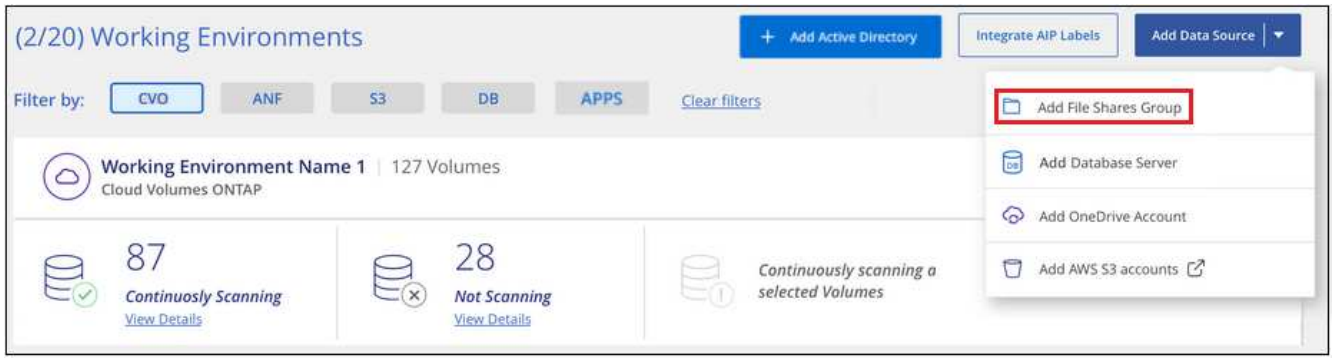
## Creazione del gruppo per le condivisioni file

È necessario aggiungere un "gruppo" di condivisioni file prima di poter aggiungere le condivisioni file. Il gruppo è un contenitore per le condivisioni di file che si desidera sottoporre a scansione e il nome del gruppo viene utilizzato come nome dell'ambiente di lavoro per tali condivisioni di file.

È possibile combinare condivisioni NFS e CIFS nello stesso gruppo, tuttavia tutte le condivisioni file CIFS di un gruppo devono utilizzare le stesse credenziali Active Directory. Se si prevede di aggiungere condivisioni CIFS che utilizzano credenziali diverse, è necessario creare un gruppo separato per ogni set univoco di credenziali.

**Fasi**

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add file Shares Group** (Aggiungi gruppo condivisioni file).




2. Nella finestra di dialogo Add Files shares Group (Aggiungi gruppo condivisioni file), immettere il nome del gruppo di condivisioni e fare clic su **Continue** (continua).

Il nuovo file shares Group viene aggiunto all'elenco degli ambienti di lavoro.

## Aggiunta di condivisioni di file a un gruppo

Le condivisioni di file vengono aggiunte al file shares Group in modo che i file in tali condivisioni vengano sottoposti a scansione in base alla classificazione BlueXP. Le condivisioni vengono aggiunte nel formato

`<host_name>:/<share_path>`.

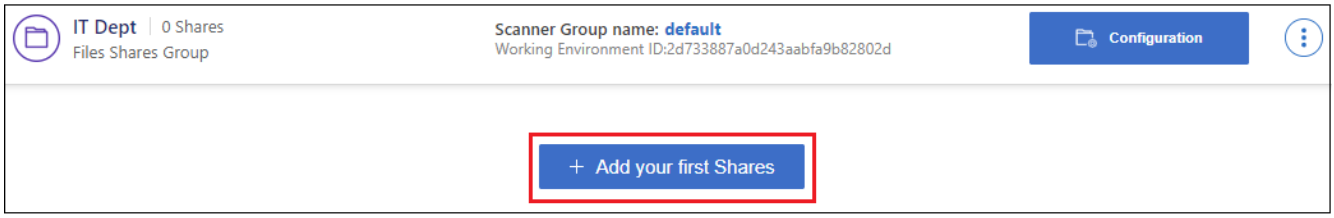
È possibile aggiungere singole condivisioni di file oppure fornire un elenco separato da righe delle condivisioni di file che si desidera sottoporre a scansione. È possibile aggiungere fino a 100 condivisioni alla volta.

Quando si aggiungono sia le condivisioni NFS che CIFS in un singolo gruppo, è necessario eseguire il processo due volte, una volta aggiunte le condivisioni NFS e quindi di nuovo le condivisioni CIFS.

**Fasi**

1. Dalla pagina *ambienti di lavoro*, fare clic sul pulsante **Configurazione** per il gruppo condivisioni file.

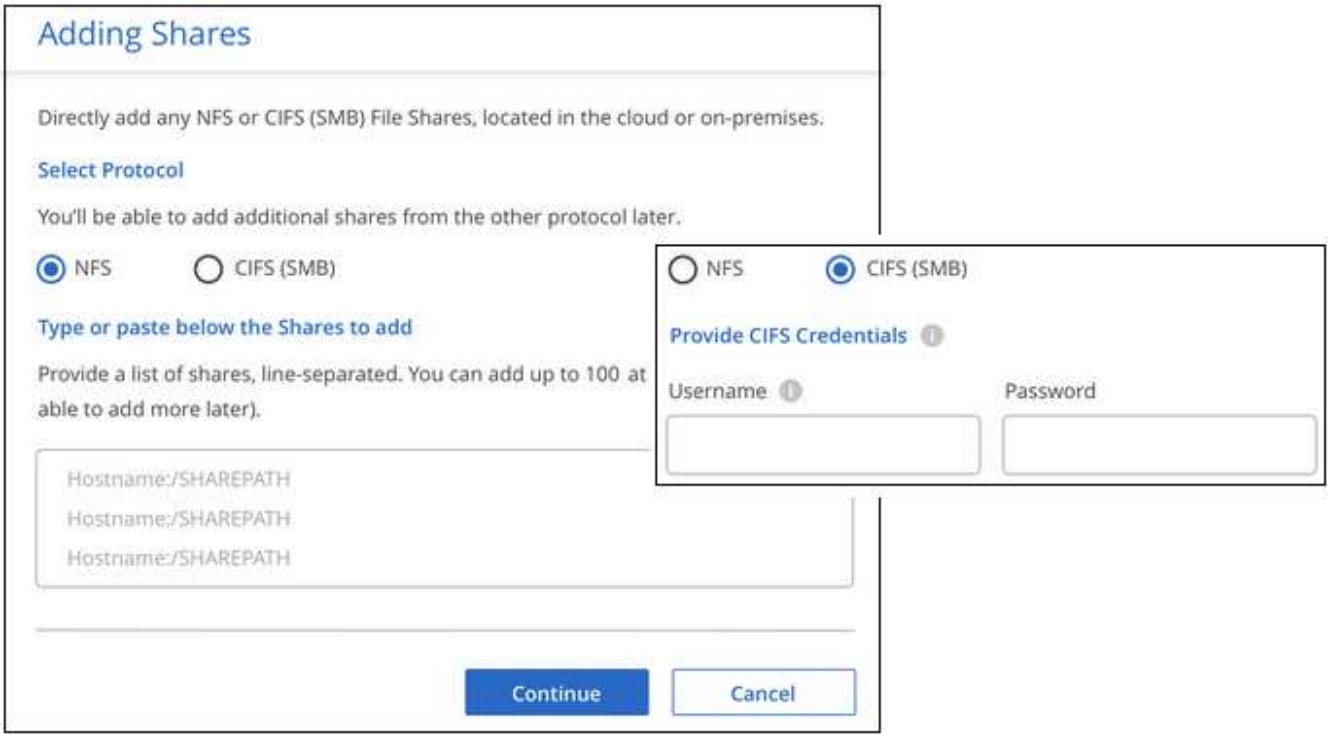

2. Se è la prima volta che si aggiungono condivisioni file per questo gruppo di condivisioni file, fare clic su **Aggiungi le prime condivisioni**.




Se si stanno aggiungendo condivisioni di file a un gruppo esistente, fare clic su **Aggiungi condivisioni**.


3. Selezionare il protocollo per le condivisioni di file che si desidera aggiungere, aggiungere le condivisioni di file che si desidera sottoporre a scansione (una condivisione di file per riga) e fare clic su **continua**.

   Quando si aggiungono condivisioni CIFS (SMB), è necessario immettere le credenziali Active Directory che forniscono l'accesso in lettura alle condivisioni. Si preferiscono le credenziali di amministratore.




Viene visualizzata una finestra di dialogo di conferma del numero di condivisioni aggiunte.

Se la finestra di dialogo elenca le condivisioni che non è stato possibile aggiungere, acquisire queste informazioni in modo da risolvere il problema. In alcuni casi è possibile aggiungere nuovamente la condivisione con un nome host o un nome di condivisione corretto.

4. Abilitare scansioni di sola mappatura o scansioni di mappatura e classificazione su ogni condivisione di file.

| A: | Eseguire questa operazione: |
|---|---|
| Abilitare le scansioni di sola mappatura sulle condivisioni di file | Fare clic su **Map** (Mappa) |
| Attiva scansioni complete sulle condivisioni di file | Fare clic su **Map & Classify** (Mappa e classificazione) |
| Disattivare la scansione sulle condivisioni di file | Fare clic su **Off** |

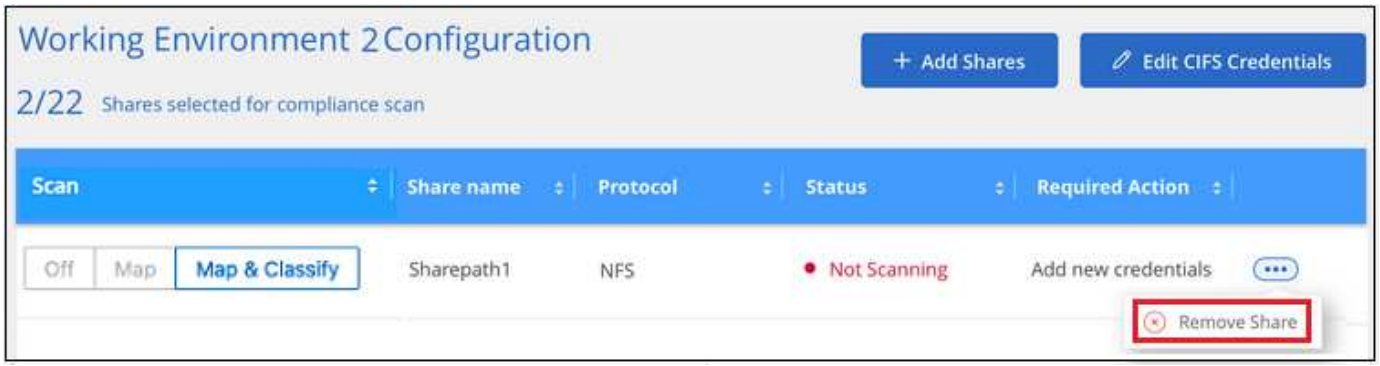
Per impostazione predefinita, lo switch nella parte superiore della pagina per le autorizzazioni **Scan when missing "write attributa" (Esegui scansione quando mancano gli attributi di scrittura)** è disattivato. Ciò significa che se la classificazione di BlueXP non dispone di permessi di scrittura in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

**Risultato**

La classificazione BlueXP avvia la scansione dei file nelle condivisioni di file aggiunte e i risultati vengono visualizzati nella dashboard e in altre posizioni.

### Rimozione di una condivisione file dalle scansioni di conformità

Se non è più necessario eseguire la scansione di determinate condivisioni di file, è possibile rimuovere singole condivisioni di file dal fatto che i file siano sottoposti a scansione in qualsiasi momento. Fare clic su **Remove Share** (Rimuovi condivisione) dalla pagina di configurazione.




# Scansione dello storage a oggetti che utilizza il protocollo S3

Completare alcuni passaggi per avviare la scansione dei dati all'interno dello storage a oggetti direttamente con la classificazione BlueXP. La classificazione BlueXP consente di eseguire la scansione dei dati da qualsiasi servizio di storage a oggetti che utilizza il protocollo S3 (Simple Storage Service). Tra cui NetApp StorageGRID, IBM Cloud Object Store, Linode, B2 Cloud Storage, Amazon S3 e molto altro ancora.

## Avvio rapido

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

1. **Esaminare i prerequisiti dello storage a oggetti**

Per connettersi al servizio di storage a oggetti, è necessario disporre dell'URL dell'endpoint.

È necessario disporre della chiave di accesso e della chiave segreta del provider di storage a oggetti, in modo che la classificazione BlueXP possa accedere ai bucket.

2. **Distribuire l'istanza di classificazione BlueXP**

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

3. **Aggiungere il servizio di storage a oggetti**

Aggiungere il servizio di storage a oggetti alla classificazione BlueXP.

4. **Selezionare i bucket da sottoporre a scansione**

Selezionare i bucket che si desidera sottoporre a scansione e la classificazione BlueXP inizierà a eseguirne la scansione.

## Analisi dei requisiti di storage a oggetti

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

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

## Implementazione dell'istanza di classificazione BlueXP

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

Se si esegue la scansione di dati dallo storage a oggetti S3 accessibile tramite Internet, è possibile "Implementare la classificazione BlueXP nel cloud" oppure "Implementare la classificazione BlueXP in una posizione on-premise con accesso a Internet".

Se si esegue la scansione di dati dallo storage a oggetti S3 installato in un sito buio che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella stessa posizione on-premise.

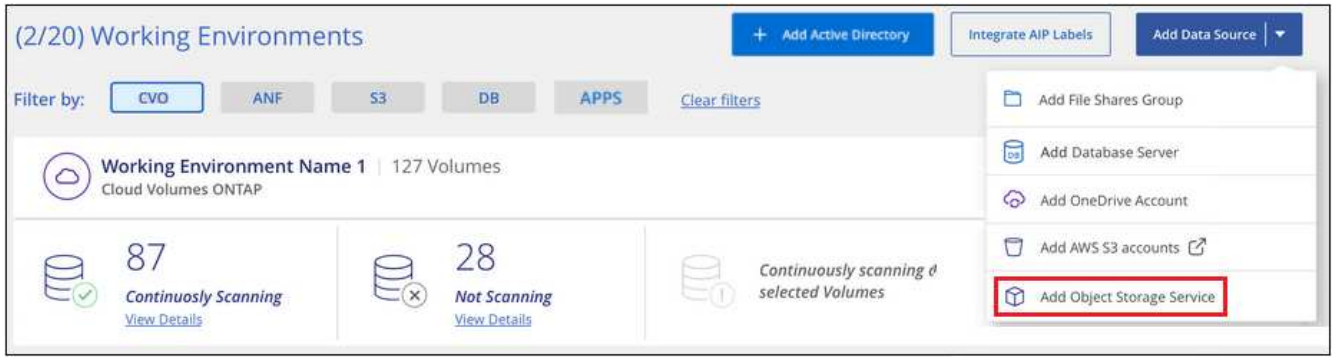
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

## Aggiunta del servizio di storage a oggetti alla classificazione BlueXP

Aggiungere il servizio di storage a oggetti.

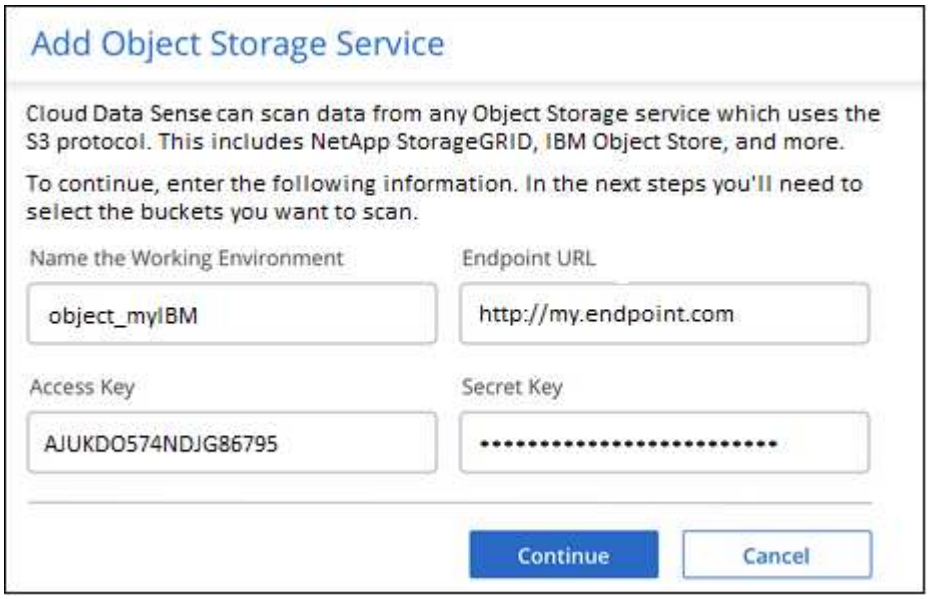
**Fasi**

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add Object Storage Service** (Aggiungi servizio di storage a oggetti).




2. Nella finestra di dialogo Add Object Storage Service (Aggiungi servizio di storage a oggetti), immettere i dettagli del servizio di storage a oggetti e fare clic su **Continue** (continua).
   a. Immettere il nome che si desidera utilizzare per l'ambiente di lavoro. Questo nome deve riflettere il nome del servizio di storage a oggetti a cui ci si connette.
   b. Inserire l'URL dell'endpoint per accedere al servizio di storage a oggetti.

c. Inserire la chiave di accesso e la chiave segreta in modo che la classificazione BlueXP possa accedere ai bucket nello storage a oggetti.




**Risultato**

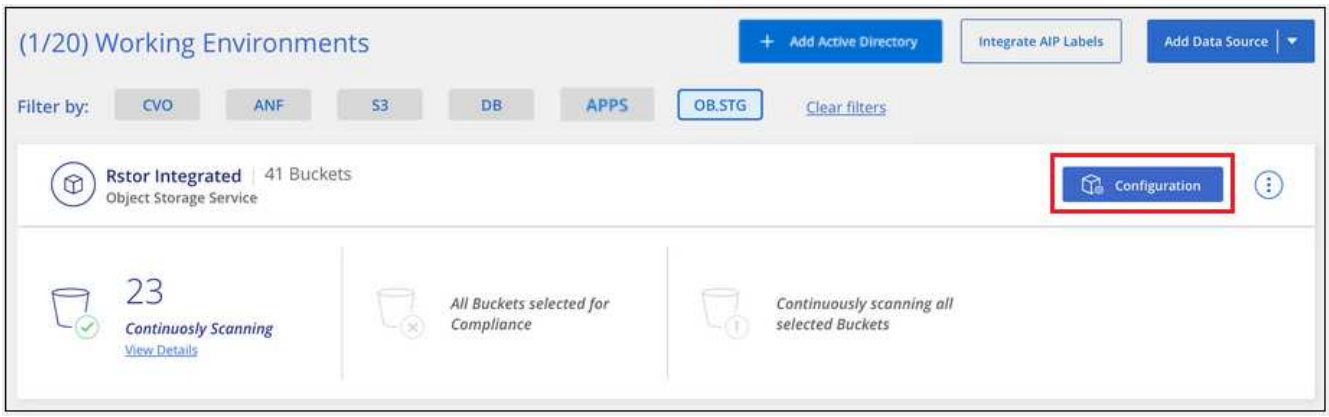
Il nuovo servizio di storage a oggetti viene aggiunto all'elenco degli ambienti di lavoro.

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

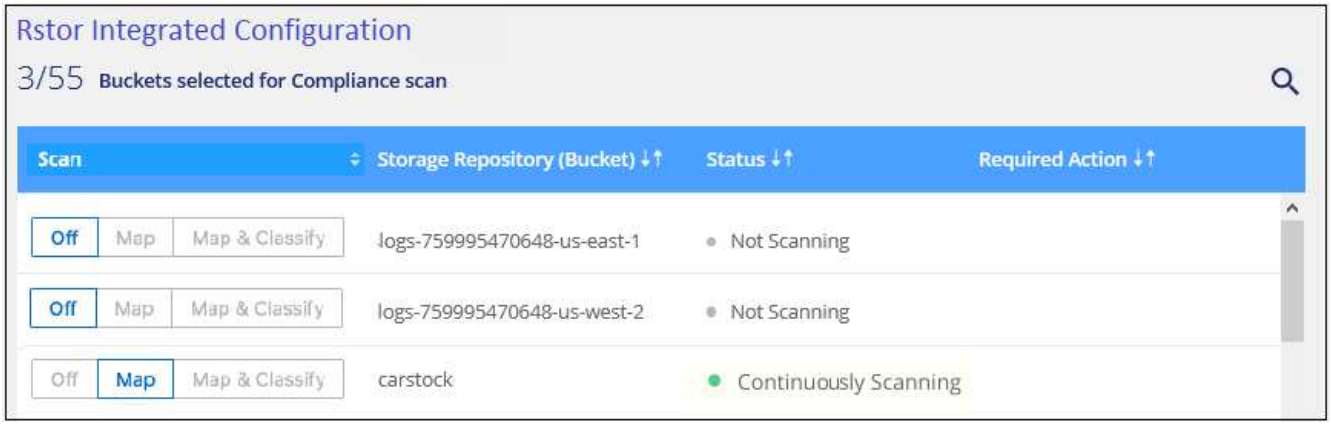
Dopo aver attivato la classificazione BlueXP sul servizio di storage a oggetti, il passaggio successivo consiste nel configurare i bucket che si desidera sottoporre a scansione. La classificazione BlueXP rileva tali bucket e li visualizza nell'ambiente di lavoro creato.

**Fasi**

1. Nella pagina Configuration (Configurazione), fare clic su **Configuration** (Configurazione) dall'ambiente di lavoro Object Storage Service (Servizio di archiviazione oggetti).




2. Abilita scansioni di sola mappatura o scansioni di mappatura e classificazione sui bucket.




| A: | Eseguire questa operazione: |
|---|---|
| Attivare scansioni solo mappatura su un bucket | Fare clic su **Map** (Mappa) |
| Abilitare scansioni complete su un bucket | Fare clic su **Map & Classify** (Mappa e classificazione) |
| Disattivare la scansione su un bucket | Fare clic su **Off** |

**Risultato**

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