Attiva la scansione sulle tue fonti dati

NetApp Data Classification

NetApp
February 11, 2026

Sommario

Attiva la scansione sulle tue fonti dati

Scansiona le origini dati con NetApp Data Classification

NetApp Data Classification analizza i dati nei repository (volumi, schemi di database o altri dati utente) selezionati per identificare i dati personali e sensibili. La classificazione dei dati mappa quindi i dati della tua organizzazione, categorizza ogni file e identifica modelli predefiniti nei dati. Il risultato della scansione è un indice di informazioni personali, informazioni personali sensibili, categorie di dati e tipi di file.

Dopo la scansione iniziale, Data Classification analizza continuamente i dati in modalità round-robin per rilevare modifiche incrementali. Ecco perché è importante mantenere l'istanza in esecuzione.

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

Qual è la differenza tra le scansioni di mappatura e classificazione?

È possibile eseguire due tipi di scansioni nella classificazione dei dati:

- Le **scansioni di sola mappatura** forniscono solo una panoramica di alto livello dei dati e vengono eseguite su origini dati selezionate. Le scansioni di sola mappatura richiedono meno tempo rispetto alle scansioni di mappatura e classificazione perché non accedono ai file per visualizzare i dati al loro interno. Potresti volerlo fare inizialmente per identificare le aree di ricerca e poi eseguire una scansione Map & Classify su tali aree.
- **Le scansioni Map & Classify** forniscono una scansione approfondita dei tuoi dati.

La tabella seguente mostra alcune delle differenze:

Caratteristica	Mappa e classifica le scansioni	Scansioni solo di mappatura
Velocità di scansione	Lento	Veloce
Prezzi	Gratuito	Gratuito
Capacità	Limitato a 500 TiB*	Limitato a 500 TiB*
Elenco dei tipi di file e della capacità utilizzata	SÌ	SÌ
Numero di file e capacità utilizzata	SÌ	SÌ
Età e dimensione dei file	SÌ	SÌ
Capacità di eseguire un"Rapporto di mappatura dei dati"	SÌ	SÌ
Pagina di indagine sui dati per visualizzare i dettagli del file	SÌ	NO
Cerca nomi all'interno dei file	SÌ	NO
Creare"query salvate" che forniscono risultati di ricerca personalizzati	SÌ	NO
Possibilità di eseguire altri report	SÌ	NO
Possibilità di visualizzare i metadati dai file**	NO	SÌ

{asterisco} La classificazione dei dati non impone limiti alla quantità di dati che può analizzare. Ogni agente della console supporta la scansione e la visualizzazione di 500 TiB di dati. Per scansionare più di 500 TiB di dati,"installare un altro agente Console" Poi"distribuire un'altra istanza di classificazione dei dati" . + L'interfaccia utente della console visualizza i dati da un singolo connettore. Per suggerimenti sulla visualizzazione dei dati da più agenti della console, vedere"Lavora con più agenti della console" .

{asterisco}{asterisco} I seguenti metadati vengono estratti dai file durante le scansioni di mappatura:

- Sistema
- Tipo di sistema
- Deposito di archiviazione
- Tipo di file
- Capacità utilizzata
- Numero di file
- Dimensione del file
- Creazione di file
- Ultimo accesso al file
- File modificato l'ultima volta
- Ora di scoperta del file
- Estrazione dei permessi

Differenze nella dashboard di governance:

Caratteristica	Mappa e classifica	Mappa
dati obsoleti	SÌ	SÌ
Dati non aziendali	SÌ	SÌ
File duplicati	SÌ	SÌ
Query salvate predefinite	SÌ	NO
Query salvate predefinite	SÌ	SÌ
Rapporto DDA	SÌ	SÌ
Rapporto di mappatura	SÌ	SÌ
Rilevamento del livello di sensibilità	SÌ	NO
Dati sensibili con ampi permessi	SÌ	NO
Permessi aperti	SÌ	SÌ
Età dei dati	SÌ	SÌ
Dimensione dei dati	SÌ	SÌ
Categorie	SÌ	NO
Tipi di file	SÌ	SÌ

Differenze nella dashboard di conformità:

Caratteristica	Mappa e classifica	Mappa
Informazioni personali	SÌ	NO
Informazioni personali sensibili	SÌ	NO
Rapporto di valutazione del rischio per la privacy	SÌ	NO
Rapporto HIPAA	SÌ	NO
Rapporto PCI DSS	SÌ	NO

Differenze nei filtri di indagine:

Caratteristica	Mappa e classifica	Mappa
Query salvate	SÌ	SÌ
Tipo di sistema	SÌ	SÌ
Sistema	SÌ	SÌ
Deposito di archiviazione	SÌ	SÌ
Tipo di file	SÌ	SÌ
Dimensione del file	SÌ	SÌ
Ora di creazione	SÌ	SÌ
Tempo scoperto	SÌ	SÌ
Ultima modifica	SÌ	SÌ
Ultimo accesso	SÌ	SÌ
Permessi aperti	SÌ	SÌ
Percorso della directory del file	SÌ	SÌ
Categoria	SÌ	NO
Livello di sensibilità	SÌ	NO
Numero di identificatori	SÌ	NO
Dati personali	SÌ	NO
Dati personali sensibili	SÌ	NO
Interessato	SÌ	NO
Duplicati	SÌ	SÌ
Stato di classificazione	SÌ	Lo stato è sempre "Approfondimenti limitati"
Evento di analisi della scansione	SÌ	SÌ
Hash del file	SÌ	SÌ
Numero di utenti con accesso	SÌ	SÌ
Autorizzazioni utente/gruppo	SÌ	SÌ
Proprietario del file	SÌ	SÌ
Tipo di directory	SÌ	SÌ

Scansiona Amazon FSx per volumi ONTAP con NetApp Data Classification

Completa alcuni passaggi per eseguire la scansione Amazon FSx per volumi ONTAP con NetApp Data Classification.

Prima di iniziare

- Per distribuire e gestire la classificazione dei dati è necessario un agente Console attivo in AWS.
- Il gruppo di sicurezza selezionato durante la creazione del sistema deve consentire il traffico dall'istanza di classificazione dei dati. È possibile trovare il gruppo di sicurezza associato utilizzando l'ENI connesso al file system FSx for ONTAP e modificarlo tramite AWS Management Console.

  "Gruppi di sicurezza AWS per istanze Linux"

  "Gruppi di sicurezza AWS per istanze Windows"

  "Interfacce di rete elastiche AWS (ENI)"

- Assicurarsi che le seguenti porte siano aperte all'istanza di classificazione dei dati:
  - Per NFS: porte 111 e 2049.
  - Per CIFS: porte 139 e 445.

Distribuisci l'istanza di classificazione dei dati

"Distribuisci la classificazione dei dati"se non è già presente un'istanza distribuita.

È necessario distribuire Data Classification nella stessa rete AWS dell'agente della console per AWS e dei volumi FSx che si desidera analizzare.

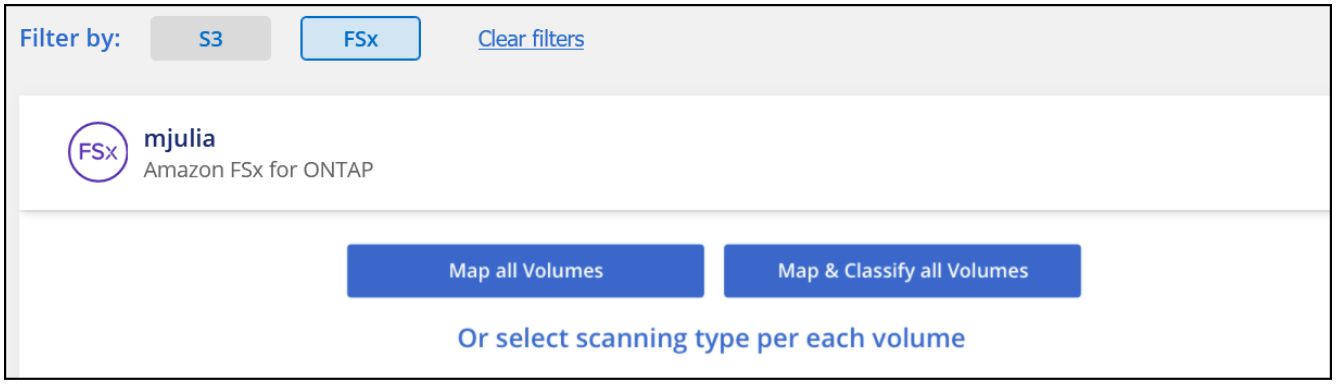
Nota: la distribuzione della classificazione dei dati in una posizione locale non è attualmente supportata durante la scansione dei volumi FSx.

Gli aggiornamenti al software di classificazione dei dati sono automatizzati, a condizione che l'istanza disponga di connettività Internet.

Abilita la classificazione dei dati nei tuoi sistemi

È possibile abilitare la classificazione dei dati per FSx per i volumi ONTAP .

1. Dalla NetApp Console, **Governance > Classificazione**.
2. Dal menu Classificazione dati, selezionare **Configurazione**.



3. Selezionare la modalità di scansione dei volumi in ciascun sistema. "Scopri di più sulle scansioni di mappatura e classificazione":
   - Per mappare tutti i volumi, selezionare **Mappa tutti i volumi**.

- Per mappare e classificare tutti i volumi, selezionare **Mappa e classifica tutti i volumi**.
- Per personalizzare la scansione per ciascun volume, seleziona **Oppure seleziona il tipo di scansione per ciascun volume**, quindi scegli i volumi che desideri mappare e/o classificare.

4. Nella finestra di dialogo di conferma, seleziona **Approva** per far sì che Data Classification inizi la scansione dei volumi.

Risultato

La classificazione dei dati avvia la scansione dei volumi selezionati nel sistema. I risultati saranno disponibili nella dashboard Conformità non appena Data Classification avrà completato le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati: potrebbero volerci pochi minuti o ore. È possibile monitorare l'avanzamento della scansione iniziale accedendo al menu **Configurazione** e selezionando quindi **Configurazione di sistema**. Tieni traccia dell'avanzamento di ogni scansione nella barra di avanzamento; puoi passare il mouse sulla barra di avanzamento per vedere il numero di file scansionati in relazione al totale dei file nel volume.

- Per impostazione predefinita, se Data Classification non dispone di autorizzazioni per gli attributi di scrittura in CIFS o di autorizzazioni per la scrittura in NFS, il sistema non eseguirà la scansione dei file nei volumi perché Data Classification non può ripristinare l'"ora dell'ultimo accesso" al timestamp originale. Se non ti interessa che l'ultimo orario di accesso venga reimpostato, seleziona **Oppure seleziona il tipo di scansione per ciascun volume**. La pagina risultante contiene un'impostazione che è possibile abilitare in modo che la classificazione dei dati esegua la scansione dei volumi indipendentemente dalle autorizzazioni.
- La classificazione dei dati analizza solo una condivisione file in un volume. Se nei volumi sono presenti più condivisioni, sarà necessario eseguire la scansione di tali altre condivisioni separatamente, come gruppo di condivisioni. "Vedi maggiori dettagli su questa limitazione della classificazione dei dati" .

Verificare che la classificazione dei dati abbia accesso ai volumi

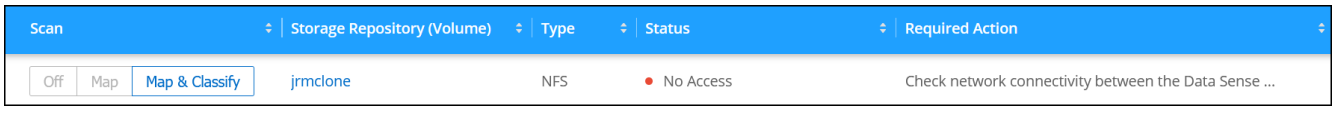
Assicurati che Data Classification possa accedere ai volumi controllando la rete, i gruppi di sicurezza e i criteri di esportazione.

Sarà necessario fornire a Data Classification le credenziali CIFS affinché possa accedere ai volumi CIFS.

Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Nella pagina Configurazione, seleziona **Visualizza dettagli** per rivedere lo stato e correggere eventuali errori.

   Ad esempio, l'immagine seguente mostra un volume che Data Classification non riesce a scansionare a causa di problemi di connettività di rete tra l'istanza di Data Classification e il volume.



3. Assicurarsi che ci sia una connessione di rete tra l'istanza di Data Classification e ciascuna rete che include volumi per FSx per ONTAP.

Per FSx per ONTAP, la classificazione dei dati può eseguire la scansione dei volumi solo nella stessa regione della console.

4. Assicurarsi che i criteri di esportazione del volume NFS includano l'indirizzo IP dell'istanza di classificazione dei dati in modo che possa accedere ai dati su ciascun volume.
5. Se si utilizza CIFS, fornire a Data Classification le credenziali di Active Directory in modo che possa analizzare i volumi CIFS.

   a. Dal menu Classificazione dati, selezionare **Configurazione**.
   b. Per ciascun sistema, selezionare **Modifica credenziali CIFS** e immettere il nome utente e la password necessari a Data Classification per accedere ai volumi CIFS sul sistema.

      Le credenziali possono essere di sola lettura, ma fornendo le credenziali di amministratore si garantisce che Data Classification possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono archiviate nell'istanza di classificazione dei dati.

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

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

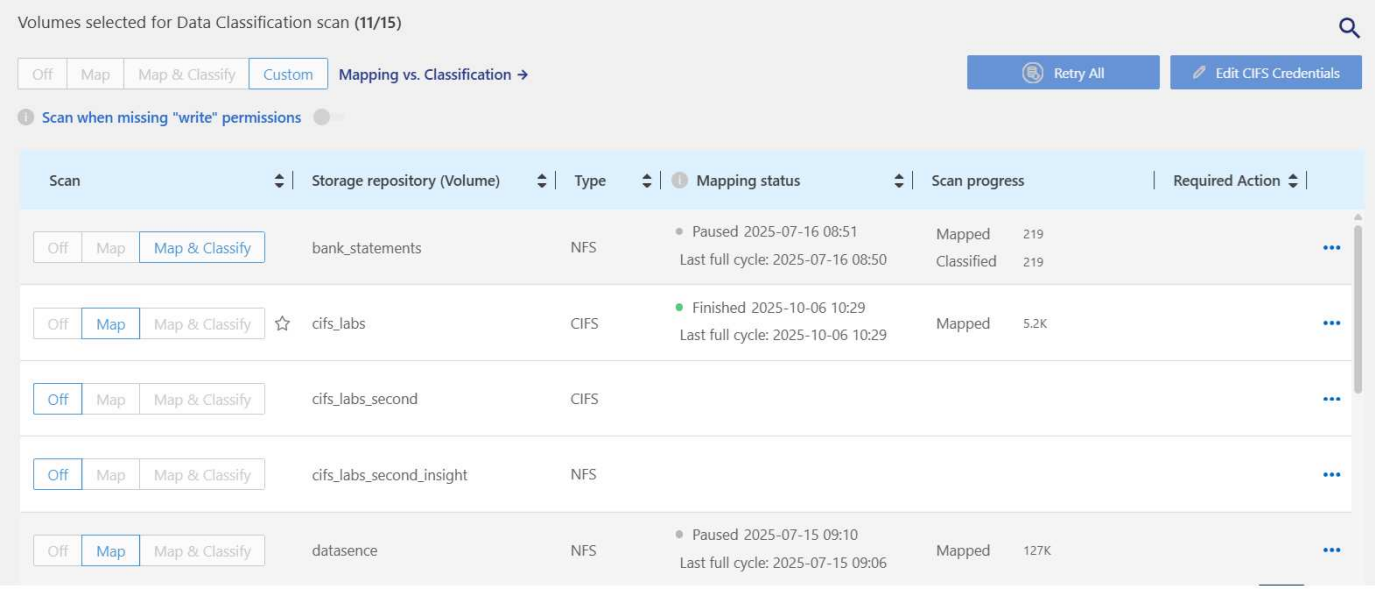
Abilita e disabilita le scansioni sui volumi

È possibile avviare o interrompere le scansioni su qualsiasi sistema in qualsiasi momento dalla pagina Configurazione. È anche 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 di un sistema.

I nuovi volumi aggiunti al sistema vengono automaticamente scansionati solo se è stata selezionata l'impostazione **Mappa** o **Mappa e classifica** nell'area dell'intestazione. Se impostato su **Personalizzato** o **Disattivato** nell'area dell'intestazione, sarà necessario attivare la mappatura e/o la scansione completa su ogni nuovo volume aggiunto al sistema.

Per impostazione predefinita, l'interruttore in cima alla pagina per **Esegui scansione in caso di permessi di "scrittura" mancanti** è disabilitato. Ciò significa che se Data Classification non dispone di autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS, il sistema non eseguirà la scansione dei file perché Data Classification non può ripristinare l'"ora dell'ultimo accesso" al timestamp originale. Se non ti interessa che l'ultimo orario di accesso venga reimpostato, attiva l'interruttore e tutti i file verranno analizzati indipendentemente dalle autorizzazioni. "Saperne di più".

I nuovi volumi aggiunti al sistema vengono automaticamente scansionati solo se nell'area dell'intestazione è stata impostata l'opzione **Mappa** o **Mappa e classifica**. Se l'impostazione per tutti i volumi è **Personalizzata** o **Disattivata**, è necessario attivare manualmente la scansione per ogni nuovo volume aggiunto.



Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Scegli un sistema, quindi seleziona **Configurazione**.
3. Per abilitare o disabilitare le scansioni per tutti i volumi, selezionare **Mappa**, **Mappa e classifica** o **Disattivato** nell'intestazione sopra tutti i volumi.

   Per abilitare o disabilitare le scansioni per singoli volumi, trova i volumi nell'elenco, quindi seleziona **Mappa**, **Mappa e classifica** o **Disattivato** accanto al nome del volume.

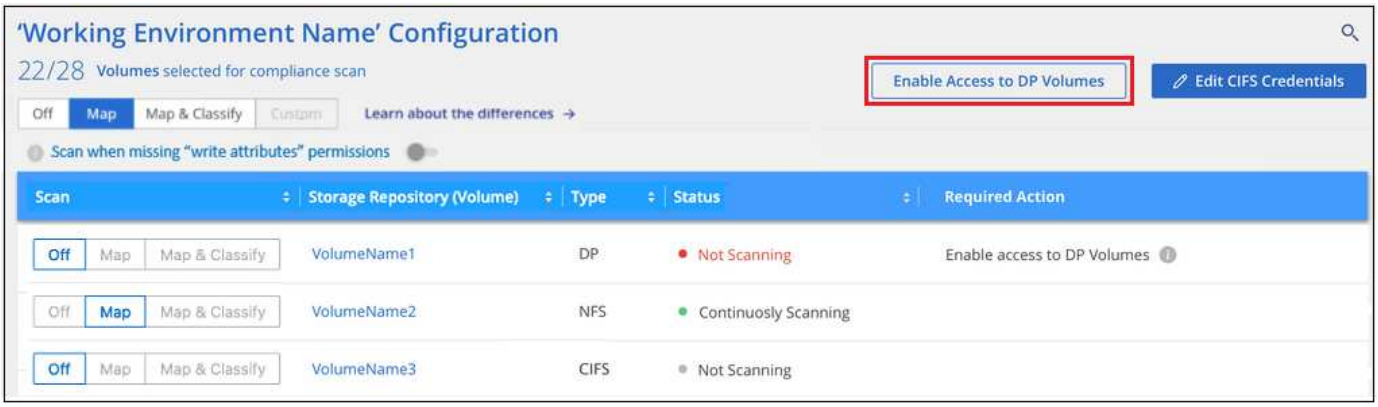
Risultato

Quando si abilita la scansione, Data Classification avvia la scansione dei volumi selezionati nel sistema. I risultati iniziano ad apparire nella dashboard Conformità non appena la Classificazione dei dati avvia la scansione. Il tempo di completamento della scansione dipende dalla quantità di dati e può variare da minuti a ore.

Scansiona i volumi di protezione dei dati

Per impostazione predefinita, i volumi di protezione dati (DP) non vengono scansionati perché non sono esposti esternamente e Data Classification non può accedervi. Questi sono i volumi di destinazione per le operazioni SnapMirror da un file system FSx per ONTAP .

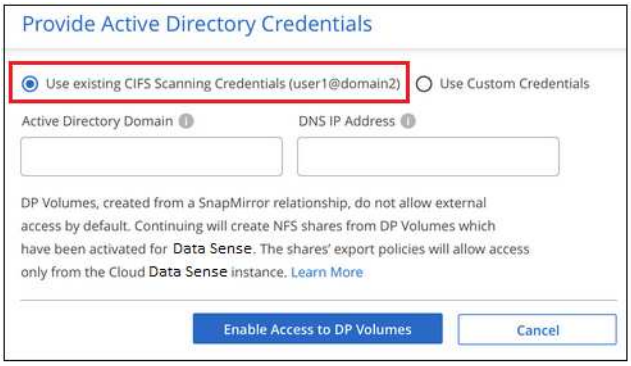
Inizialmente, l'elenco dei volumi identifica questi volumi come *Tipo* **DP** con *Stato* **Non in scansione** e *Azione richiesta* **Abilita accesso ai volumi DP**.

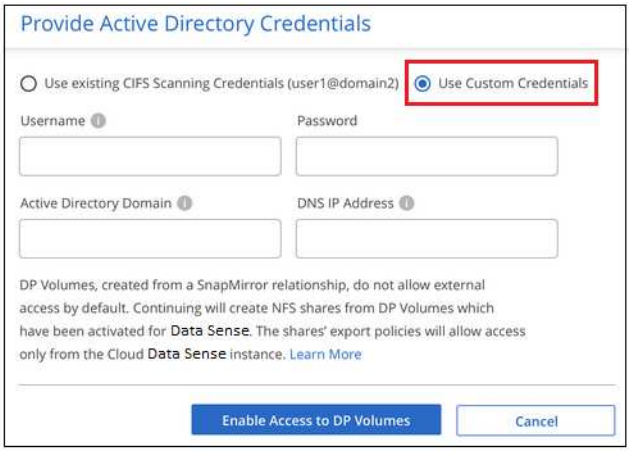


Passi

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

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Selezionare **Abilita accesso ai volumi DP** nella parte superiore della pagina.
3. Rivedere il messaggio di conferma e selezionare nuovamente **Abilita accesso ai volumi DP**.
   - I volumi inizialmente creati come volumi NFS nel file system FSx for ONTAP di origine sono abilitati.
   - I volumi inizialmente creati come volumi CIFS nel file system FSx for ONTAP di origine richiedono l'immissione delle credenziali CIFS per eseguire la scansione di tali volumi DP. Se hai già immesso le credenziali di Active Directory affinché Data Classification possa analizzare i volumi CIFS, puoi utilizzare tali credenziali oppure specificare un set diverso di credenziali di amministratore.





4. Attivare ciascun volume DP che si desidera scansionare.

Risultato

Una volta abilitata, la classificazione dei dati crea una condivisione NFS da ciascun volume DP attivato per la scansione. Le policy di esportazione delle condivisioni consentono l'accesso solo dall'istanza di classificazione dei dati.

Se non erano presenti volumi di protezione dati CIFS quando è stato inizialmente abilitato l'accesso ai volumi DP e in seguito ne sono stati aggiunti alcuni, nella parte superiore della pagina Configurazione viene visualizzato il pulsante **Abilita accesso a CIFS DP**. Selezionare 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 archiviazione del primo volume CIFS DP, pertanto tutti i volumi DP su tale SVM verranno analizzati. Tutti i volumi che risiedono su altre SVM non avranno le credenziali di Active Directory registrate, quindi tali volumi DP non verranno analizzati.

Scansiona i volumi Azure NetApp Files con NetApp Data Classification

Completa alcuni passaggi per iniziare a usare NetApp Data Classification per Azure NetApp Files.

Individuare il sistema Azure NetApp Files che si desidera analizzare

Se il sistema Azure NetApp Files che si desidera analizzare non è già presente nella NetApp Console come sistema,"aggiungilo nella pagina Sistemi" .

Distribuisci l'istanza di classificazione dei dati

"Distribuisci la classificazione dei dati"se non è già presente un'istanza distribuita.

La classificazione dei dati deve essere distribuita nel cloud durante la scansione dei volumi Azure NetApp Files e deve essere distribuita nella stessa area geografica dei volumi che si desidera analizzare.

Nota: la distribuzione della classificazione dei dati in una posizione locale non è attualmente supportata durante la scansione dei volumi Azure NetApp Files .

Abilita la classificazione dei dati nei tuoi sistemi

È possibile abilitare la classificazione dei dati sui volumi Azure NetApp Files .

1. Dal menu Classificazione dati, selezionare **Configurazione**.

2. Selezionare la modalità di scansione dei volumi in ciascun sistema. "Scopri di più sulle scansioni di mappatura e classificazione":
   - Per mappare tutti i volumi, selezionare **Mappa tutti i volumi**.
   - Per mappare e classificare tutti i volumi, selezionare **Mappa e classifica tutti i volumi**.
   - Per personalizzare la scansione per ciascun volume, seleziona **Oppure seleziona il tipo di scansione per ciascun volume**, quindi scegli i volumi che desideri mappare o mappare e classificare.

VedereAbilita o disabilita le scansioni sui volumi per i dettagli.

3. Nella finestra di dialogo di conferma, seleziona **Approva**.

Risultato

La classificazione dei dati avvia la scansione dei volumi selezionati nel sistema. I risultati sono disponibili nella dashboard Conformità non appena la Classificazione dei dati termina le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati: potrebbero volerci pochi minuti o ore. È possibile monitorare l'avanzamento della scansione iniziale accedendo al menu **Configurazione** e selezionando quindi **Configurazione di sistema**. La classificazione dei dati visualizza una barra di avanzamento per ogni scansione. È possibile passare il mouse sulla barra di avanzamento per visualizzare il numero di file scansionati rispetto al numero totale di file presenti nel volume.

- Per impostazione predefinita, se Data Classification non dispone di autorizzazioni per gli attributi di scrittura in CIFS o di autorizzazioni per la scrittura in NFS, il sistema non eseguirà la scansione dei file nei volumi perché Data Classification non può ripristinare l'"ora dell'ultimo accesso" al timestamp originale. Se non ti interessa che l'ultimo orario di accesso venga reimpostato, seleziona **Oppure seleziona il tipo di scansione per ciascun volume**. La pagina risultante contiene un'impostazione che è possibile abilitare in modo che la classificazione dei dati esegua la scansione dei volumi indipendentemente dalle autorizzazioni.
- La classificazione dei dati analizza solo una condivisione file in un volume. Se nei volumi sono presenti più condivisioni, sarà necessario eseguire la scansione delle altre condivisioni separatamente come gruppo di condivisioni. "Scopri di più su questa limitazione della classificazione dei dati" .

Verificare che la classificazione dei dati abbia accesso ai volumi

Assicurarsi che Data Classification possa accedere ai volumi controllando la rete, i gruppi di sicurezza e i criteri di esportazione. È necessario fornire a Data Classification le credenziali CIFS affinché possa accedere ai volumi CIFS.

Per Azure NetApp Files, la classificazione dei dati può analizzare solo i volumi nella stessa area della console.

Lista di controllo

- Assicurarsi che vi sia una connessione di rete tra l'istanza di Data Classification e ciascuna rete che include volumi per Azure NetApp Files.
- Assicurarsi che le seguenti porte siano aperte all'istanza di classificazione dei dati:
  - Per NFS: porte 111 e 2049.
  - Per CIFS: porte 139 e 445.
- Assicurarsi che i criteri di esportazione del volume NFS includano l'indirizzo IP dell'istanza di classificazione dei dati in modo che possa accedere ai dati su ciascun volume.

Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.

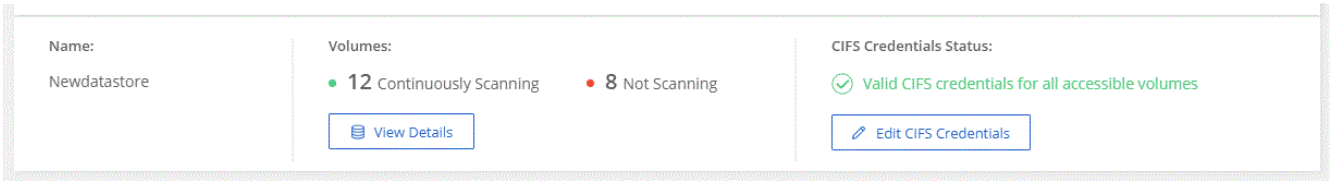
   a. Se si utilizza CIFS (SMB), assicurarsi che le credenziali di Active Directory siano corrette. Per ciascun sistema, selezionare **Modifica credenziali CIFS**, quindi immettere il nome utente e la password necessari a Data Classification per accedere ai volumi CIFS sul sistema.

      Le credenziali possono essere di sola lettura; fornendo le credenziali di amministratore si garantisce che Data Classification possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali

vengono archiviate nell'istanza di classificazione dei dati.

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

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



2. Nella pagina Configurazione, selezionare **Visualizza dettagli** per esaminare lo stato di ciascun volume CIFS e NFS. Se necessario, correggere eventuali errori, ad esempio problemi di connettività di rete.

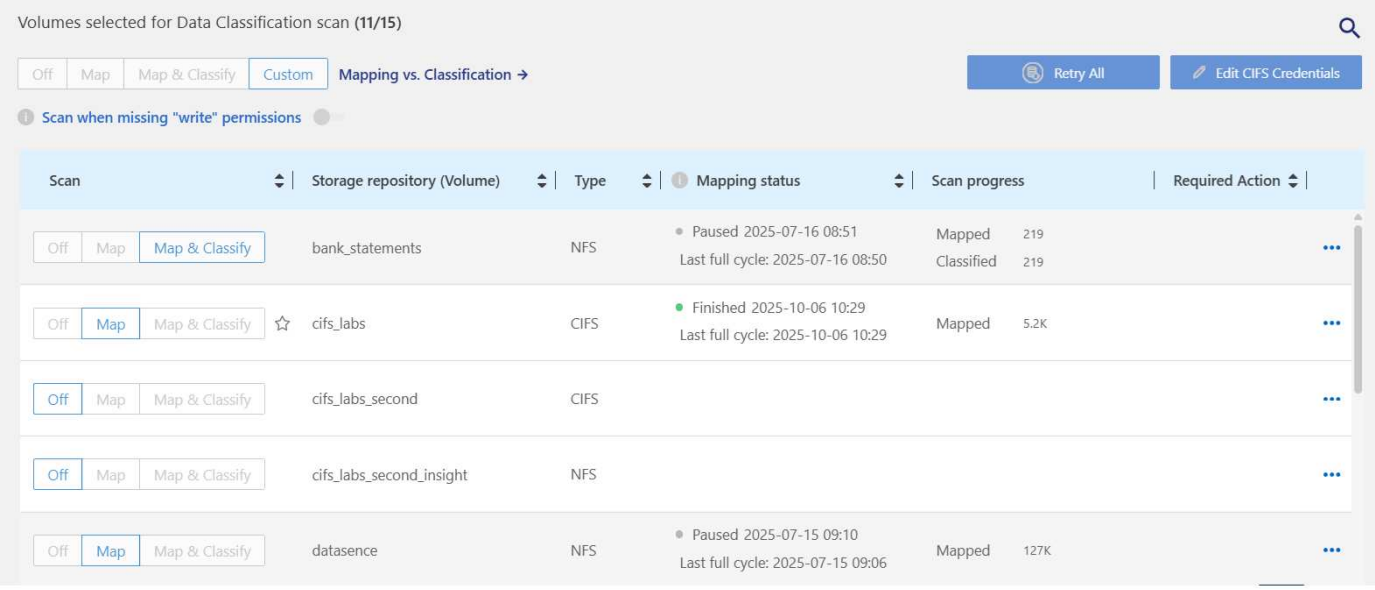
Abilita o disabilita le scansioni sui volumi

È possibile avviare o interrompere le scansioni su qualsiasi sistema in qualsiasi momento dalla pagina Configurazione. È anche 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 di un sistema.

I nuovi volumi aggiunti al sistema vengono automaticamente scansionati solo se è stata selezionata l'impostazione **Mappa** o **Mappa e classifica** nell'area dell'intestazione. Se impostato su **Personalizzato** o **Disattivato** nell'area dell'intestazione, sarà necessario attivare la mappatura e/o la scansione completa su ogni nuovo volume aggiunto al sistema.

Per impostazione predefinita, l'interruttore in cima alla pagina per **Esegui scansione in caso di permessi di "scrittura" mancanti** è disabilitato. Ciò significa che se Data Classification non dispone di autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS, il sistema non eseguirà la scansione dei file perché Data Classification non può ripristinare l'"ora dell'ultimo accesso" al timestamp originale. Se non ti interessa che l'ultimo orario di accesso venga reimpostato, attiva l'interruttore e tutti i file verranno analizzati indipendentemente dalle autorizzazioni. "Saperne di più".

I nuovi volumi aggiunti al sistema vengono automaticamente scansionati solo se nell'area dell'intestazione è stata impostata l'opzione **Mappa** o **Mappa e classifica**. Se l'impostazione per tutti i volumi è **Personalizzata** o **Disattivata**, è necessario attivare manualmente la scansione per ogni nuovo volume aggiunto.



Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Scegli un sistema, quindi seleziona **Configurazione**.
3. Per abilitare o disabilitare le scansioni per tutti i volumi, selezionare **Mappa**, **Mappa e classifica** o **Disattivato** nell'intestazione sopra tutti i volumi.

   Per abilitare o disabilitare le scansioni per singoli volumi, trova i volumi nell'elenco, quindi seleziona **Mappa**, **Mappa e classifica** o **Disattivato** accanto al nome del volume.

Risultato

Quando si abilita la scansione, Data Classification avvia la scansione dei volumi selezionati nel sistema. I risultati iniziano ad apparire nella dashboard Conformità non appena la Classificazione dei dati avvia la scansione. Il tempo di completamento della scansione dipende dalla quantità di dati e può variare da minuti a ore.

Scansiona i Cloud Volumes ONTAP e i volumi ONTAP locali con NetApp Data Classification

Completa alcuni passaggi per iniziare a scansionare i tuoi Cloud Volumes ONTAP e ONTAP locali utilizzando NetApp Data Classification.

Prerequisiti

Prima di abilitare la classificazione dei dati, assicurati di disporre di una configurazione supportata.

- Se si esegue la scansione di sistemi Cloud Volumes ONTAP e ONTAP locali accessibili tramite Internet, è possibile"distribuire la classificazione dei dati nel cloud" O"in una sede locale dotata di accesso a Internet" .
- Se si esegue la scansione di sistemi ONTAP locali installati in un sito buio senza accesso a Internet, è necessario"distribuire la classificazione dei dati nella stessa posizione locale che non ha accesso a Internet" . Ciò richiede che l'agente della console venga distribuito nella stessa posizione locale.

Verificare che la classificazione dei dati abbia accesso ai volumi

Assicurarsi che Data Classification possa accedere ai volumi controllando la rete, i gruppi di sicurezza e i criteri di esportazione. Sarà necessario fornire a Data Classification le credenziali CIFS affinché possa accedere ai volumi CIFS.

Lista di controllo

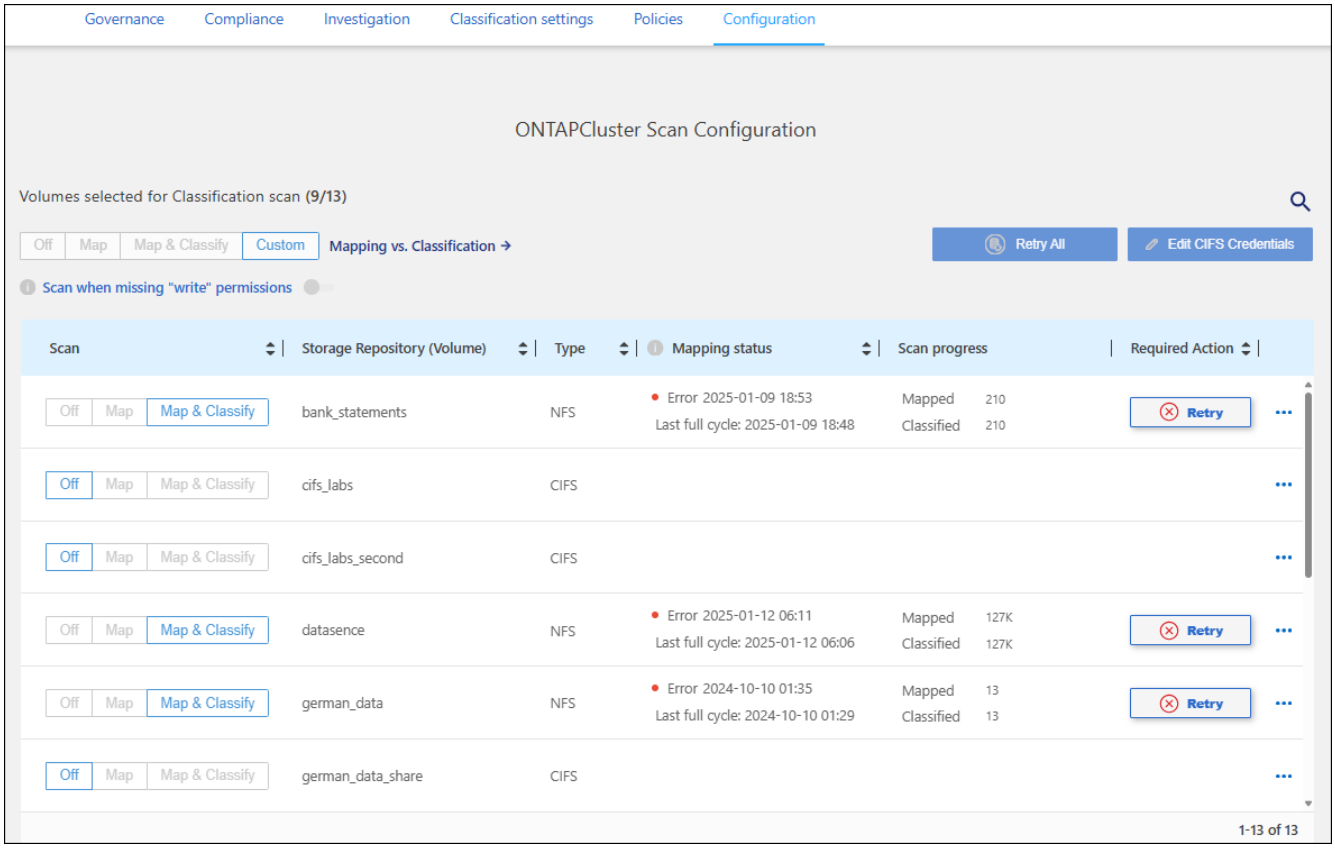
- Assicurarsi che vi sia una connessione di rete tra l'istanza di Data Classification e ciascuna rete che include volumi per Cloud Volumes ONTAP o cluster ONTAP on-prem.
- Assicurarsi che il gruppo di sicurezza per Cloud Volumes ONTAP consenta il traffico in entrata dall'istanza di classificazione dei dati.

  È possibile aprire il gruppo di sicurezza per il traffico proveniente dall'indirizzo IP dell'istanza di classificazione dei dati oppure per tutto il traffico dall'interno della rete virtuale.

- Assicurarsi che i criteri di esportazione del volume NFS includano l'indirizzo IP dell'istanza di classificazione dei dati in modo che possa accedere ai dati su ciascun volume.

Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.



2. Se si utilizza CIFS, fornire a Data Classification le credenziali di Active Directory in modo che possa analizzare i volumi CIFS. Per ciascun sistema, selezionare **Modifica credenziali CIFS** e immettere il nome utente e la password necessari a Data Classification per accedere ai volumi CIFS sul sistema.

   Le credenziali possono essere di sola lettura, ma fornendo le credenziali di amministratore si garantisce che Data Classification possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono archiviate nell'istanza di classificazione dei dati.

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

Se le credenziali sono state immesse correttamente, un messaggio conferma che tutti i volumi CIFS sono stati autenticati correttamente.

3. Nella pagina Configurazione, selezionare **Configurazione** per rivedere lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

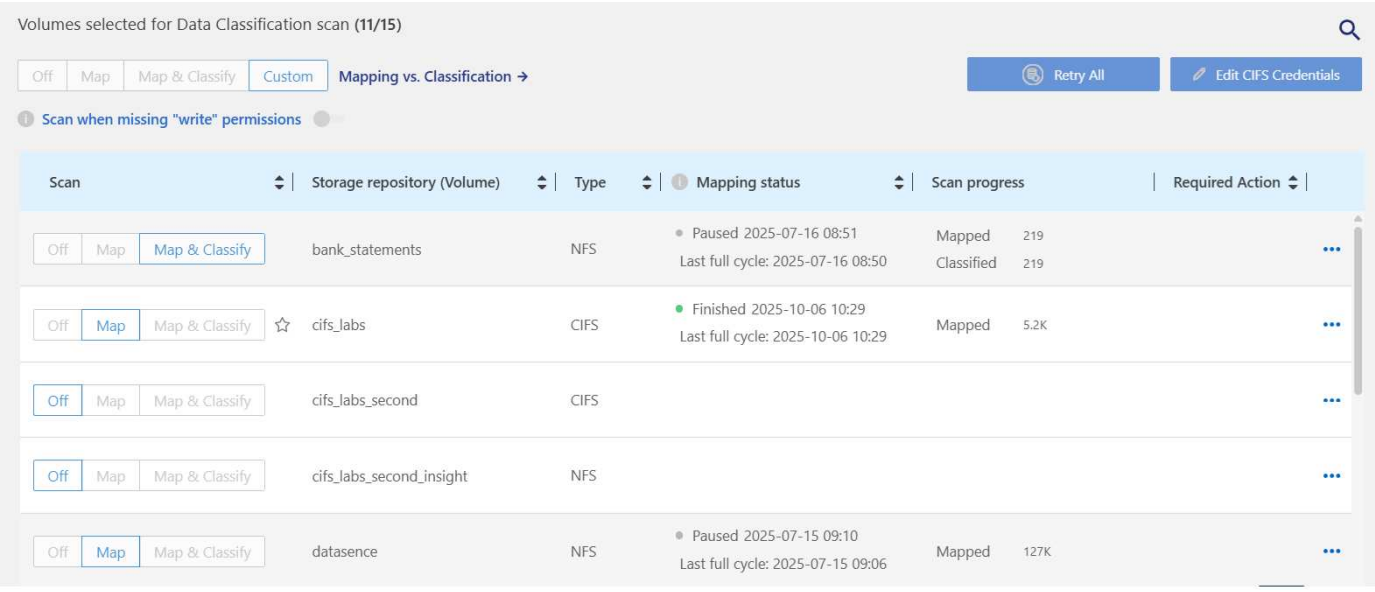
Abilita o disabilita le scansioni sui volumi

È possibile avviare o interrompere le scansioni su qualsiasi sistema in qualsiasi momento dalla pagina Configurazione. È anche 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 di un sistema.

I nuovi volumi aggiunti al sistema vengono automaticamente scansionati solo se è stata selezionata l'impostazione **Mappa** o **Mappa e classifica** nell'area dell'intestazione. Se impostato su **Personalizzato** o **Disattivato** nell'area dell'intestazione, sarà necessario attivare la mappatura e/o la scansione completa su ogni nuovo volume aggiunto al sistema.

Per impostazione predefinita, l'interruttore in cima alla pagina per **Esegui scansione in caso di permessi di "scrittura" mancanti** è disabilitato. Ciò significa che se Data Classification non dispone di autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS, il sistema non eseguirà la scansione dei file perché Data Classification non può ripristinare l'"ora dell'ultimo accesso" al timestamp originale. Se non ti interessa che l'ultimo orario di accesso venga reimpostato, attiva l'interruttore e tutti i file verranno analizzati indipendentemente dalle autorizzazioni. "Saperne di più".

I nuovi volumi aggiunti al sistema vengono automaticamente scansionati solo se nell'area dell'intestazione è stata impostata l'opzione **Mappa** o **Mappa e classifica**. Se l'impostazione per tutti i volumi è **Personalizzata** o **Disattivata**, è necessario attivare manualmente la scansione per ogni nuovo volume aggiunto.



Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Scegli un sistema, quindi seleziona **Configurazione**.
3. Per abilitare o disabilitare le scansioni per tutti i volumi, selezionare **Mappa**, **Mappa e classifica** o **Disattivato** nell'intestazione sopra tutti i volumi.

   Per abilitare o disabilitare le scansioni per singoli volumi, trova i volumi nell'elenco, quindi seleziona **Mappa**, **Mappa e classifica** o **Disattivato** accanto al nome del volume.

Risultato

Quando si abilita la scansione, Data Classification avvia la scansione dei volumi selezionati nel sistema. I risultati iniziano ad apparire nella dashboard Conformità non appena la Classificazione dei dati avvia la scansione. Il tempo di completamento della scansione dipende dalla quantità di dati e può variare da minuti a ore.

> La classificazione dei dati analizza solo una condivisione file in un volume. Se nei volumi sono presenti più condivisioni, sarà necessario eseguire la scansione di tali altre condivisioni separatamente, come gruppo di condivisioni. "Vedi maggiori dettagli su questa limitazione della classificazione dei dati" .

Scansiona gli schemi del database con NetApp Data Classification

Completa alcuni passaggi per iniziare a scansionare gli schemi del tuo database con NetApp Data Classification.

Rivedere i prerequisiti

Prima di abilitare la classificazione dei dati, rivedere i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata.

Database supportati

La classificazione dei dati può analizzare gli schemi dai seguenti database:

- Servizio di database relazionale Amazon (Amazon RDS)
- MongoDB
- MySQL
- Oracolo
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

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

Requisiti del database

È possibile eseguire la scansione di qualsiasi database con connettività all'istanza di classificazione dei dati,

indipendentemente da dove sia 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 di autorizzazioni di lettura complete per tutti gli schemi e le tabelle che si desidera analizzare. Ti consigliamo di creare un utente dedicato per il sistema di classificazione dei dati con tutte le autorizzazioni necessarie.

Per MongoDB è richiesto un ruolo di amministratore di sola lettura.

Distribuisci l'istanza di classificazione dei dati

Distribuisci Data Classification se non è già stata distribuita un'istanza.

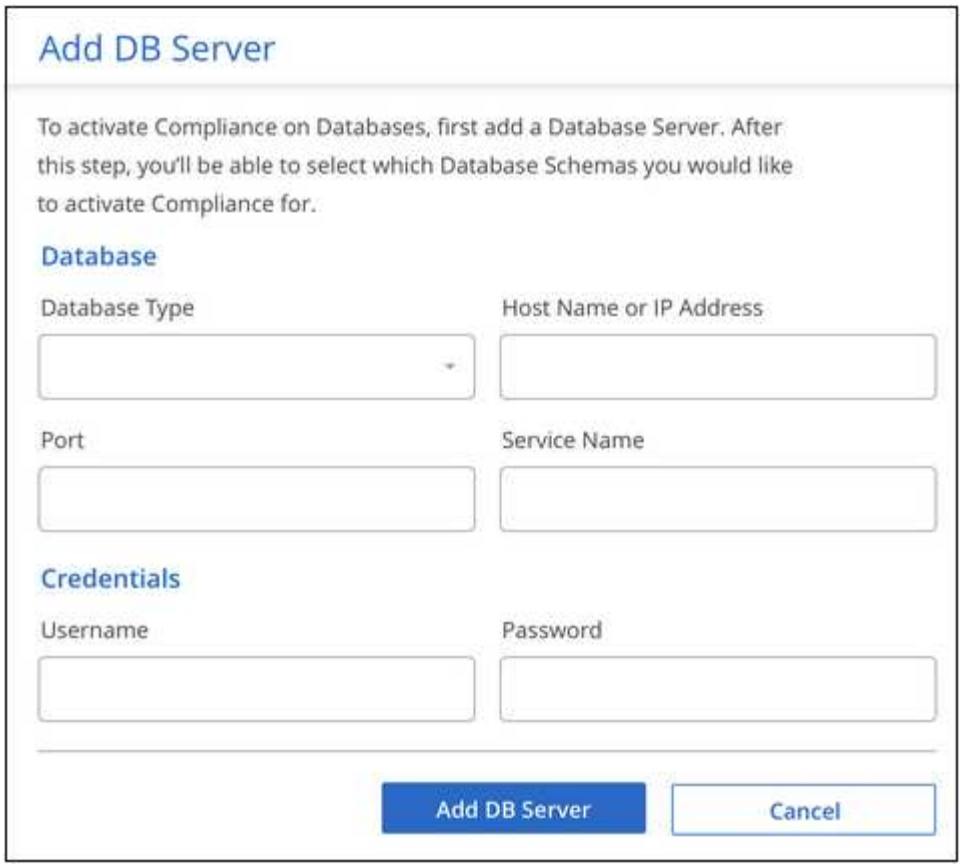
Se si esegue la scansione di schemi di database accessibili tramite Internet, è possibile"distribuire la classificazione dei dati nel cloud" O"distribuire la classificazione dei dati in una posizione locale dotata di accesso a Internet" .

Se si stanno eseguendo la scansione di schemi di database installati in un sito buio che non ha accesso a Internet, è necessario"distribuire la classificazione dei dati nella stessa posizione locale che non ha accesso a Internet" . Ciò richiede anche che l'agente della console venga distribuito nella stessa posizione locale.

Aggiungere il server del database

Aggiungere il server del database in cui risiedono gli schemi.

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Dalla pagina Configurazione, seleziona **Aggiungi sistema** > **Aggiungi server database**.
3. Immettere le informazioni richieste per identificare il server del database.
   a. Selezionare il tipo di database.
   b. Immettere la porta e il nome host o l'indirizzo IP per connettersi al database.
   c. Per i database Oracle, immettere il nome del servizio.
   d. Immettere le credenziali affinché Data Classification possa accedere al server.
   e. Selezionare **Aggiungi server DB**.



Il database viene aggiunto all'elenco dei sistemi.

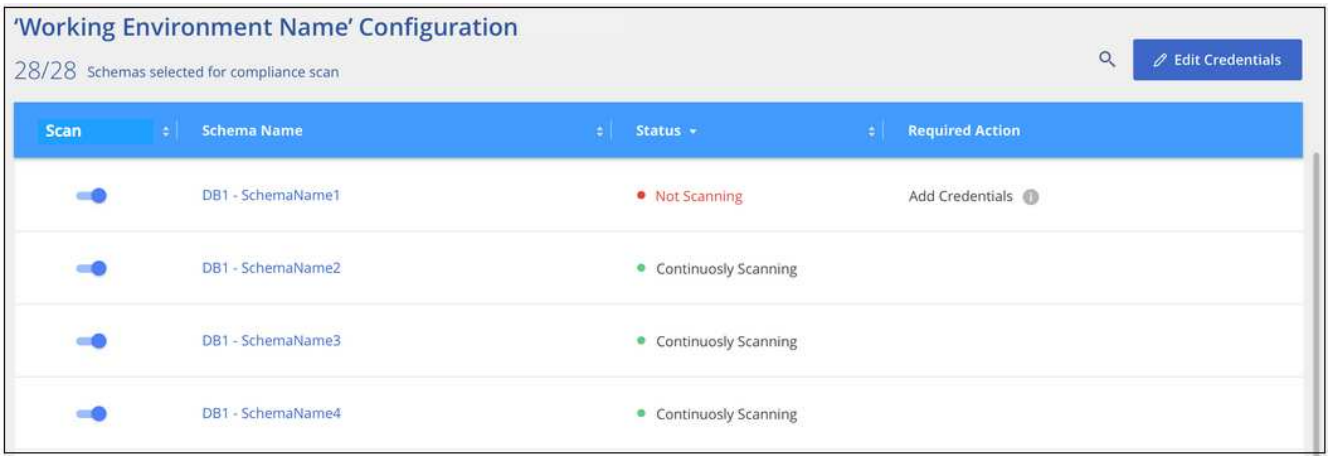
Abilita e disabilita le scansioni sugli schemi del database

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

Non è possibile selezionare scansioni di sola mappatura per gli schemi del database.

1. Dalla pagina Configurazione, seleziona il pulsante **Configurazione** per il database che desideri configurare.

2. Selezionare gli schemi che si desidera analizzare spostando il cursore verso destra.



Risultato

La classificazione dei dati avvia la scansione degli schemi del database abilitati. È possibile monitorare l'avanzamento della scansione iniziale accedendo al menu **Configurazione** e selezionando quindi **Configurazione di sistema**. L'avanzamento di ogni scansione viene visualizzato tramite una barra di avanzamento. È anche possibile passare il mouse sulla barra di avanzamento per visualizzare il numero di file scansionati rispetto al numero totale di file presenti nel volume. Se ci sono errori, questi appariranno nella colonna Stato, insieme alle azioni necessarie per correggerli.

Data Classification esegue la scansione dei database una volta al giorno; i database non vengono scansionati continuamente come altre fonti di dati.

Scansiona i Google Cloud NetApp Volumes con NetApp Data Classification

NetApp Data Classification supporta Google Cloud NetApp Volumes come sistema. Scopri come eseguire la scansione del tuo sistema Google Cloud NetApp Volumes .

Scopri il sistema Google Cloud NetApp Volumes che desideri scansionare

Se il sistema Google Cloud NetApp Volumes che si desidera analizzare non è già presente nella NetApp Console come sistema,"aggiungilo alla pagina Sistemi" .

Distribuisci l'istanza di classificazione dei dati

"Distribuisci la classificazione dei dati"se non è già presente un'istanza distribuita.

La classificazione dei dati deve essere distribuita nel cloud durante la scansione di Google Cloud NetApp Volumes e deve essere distribuita nella stessa regione dei volumi che si desidera analizzare.

Nota: la distribuzione della classificazione dei dati in una posizione locale non è attualmente supportata durante la scansione di Google Cloud NetApp Volumes.

Abilita la classificazione dei dati nei tuoi sistemi

Puoi abilitare la classificazione dei dati sul tuo sistema Google Cloud NetApp Volumes .

1. Dal menu Classificazione dati, selezionare **Configurazione**.

2. Selezionare la modalità di scansione dei volumi in ciascun sistema. "Scopri di più sulle scansioni di mappatura e classificazione":
   - Per mappare tutti i volumi, selezionare **Mappa tutti i volumi**.
   - Per mappare e classificare tutti i volumi, selezionare **Mappa e classifica tutti i volumi**.
   - Per personalizzare la scansione per ciascun volume, seleziona **Oppure seleziona il tipo di scansione per ciascun volume**, quindi scegli i volumi che desideri mappare e/o classificare.

     VedereAbilita e disabilita le scansioni sui volumi per i dettagli.
3. Nella finestra di dialogo di conferma, seleziona **Approva**.

Risultato

La classificazione dei dati avvia la scansione dei volumi selezionati nel sistema. I risultati sono disponibili nella dashboard Conformità non appena la Classificazione dei dati termina le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati: da pochi minuti a qualche ora. È possibile monitorare l'avanzamento della scansione iniziale nella sezione **Configurazione di sistema** del menu **Configurazione**. La classificazione dei dati visualizza una barra di avanzamento per ogni scansione. È anche possibile passare il mouse sulla barra di avanzamento per visualizzare il numero di file scansionati rispetto al totale dei file presenti nel volume.

- Per impostazione predefinita, se Data Classification non dispone di autorizzazioni per gli attributi di scrittura in CIFS o di autorizzazioni per la scrittura in NFS, il sistema non eseguirà la scansione dei file nei volumi perché Data Classification non può ripristinare l'"ora dell'ultimo accesso" al timestamp originale. Se non ti interessa che l'ultimo orario di accesso venga reimpostato, seleziona **Oppure seleziona il tipo di scansione per ciascun volume**. La pagina risultante contiene un'impostazione che è possibile abilitare in modo che la classificazione dei dati esegua la scansione dei volumi indipendentemente dalle autorizzazioni.
- La classificazione dei dati analizza solo una condivisione file in un volume. Se nei volumi sono presenti più condivisioni, è necessario eseguire la scansione delle altre condivisioni separatamente come gruppo di condivisioni. "Scopri di più su questa limitazione della classificazione dei dati".

Verificare che la classificazione dei dati abbia accesso ai volumi

Verificare che Data Classification possa accedere ai volumi controllando la rete, i gruppi di sicurezza e i criteri di esportazione. Per i volumi CIFS, è necessario fornire la classificazione dei dati con le credenziali CIFS.

Per Google Cloud NetApp Volumes, Data Classification può eseguire la scansione solo dei volumi nella stessa regione della Console.

Lista di controllo

- Assicurarsi che vi sia una connessione di rete tra l'istanza di Data Classification e ciascuna rete che include volumi per Google Cloud NetApp Volumes.
- Assicurarsi che le seguenti porte siano aperte all'istanza di classificazione dei dati:
  - Per NFS: porte 111 e 2049.
  - Per CIFS: porte 139 e 445.
- Assicurarsi che i criteri di esportazione del volume NFS includano l'indirizzo IP dell'istanza di classificazione dei dati in modo che possa accedere ai dati su ciascun volume.

Passi

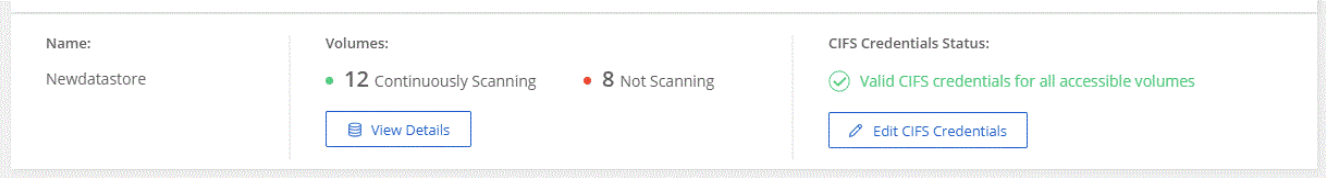
1. Dal menu Classificazione dati, selezionare **Configurazione**.

a. Se si utilizza CIFS (SMB), assicurarsi che le credenziali di Active Directory siano corrette. Per ciascun sistema, selezionare **Modifica credenziali CIFS**, quindi immettere il nome utente e la password necessari a Data Classification per accedere ai volumi CIFS sul sistema.

   Le credenziali possono essere di sola lettura, ma fornendo le credenziali di amministratore si garantisce che Data Classification possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono archiviate nell'istanza di classificazione dei dati.

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

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



2. Nella pagina Configurazione, seleziona **Visualizza dettagli** per rivedere lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

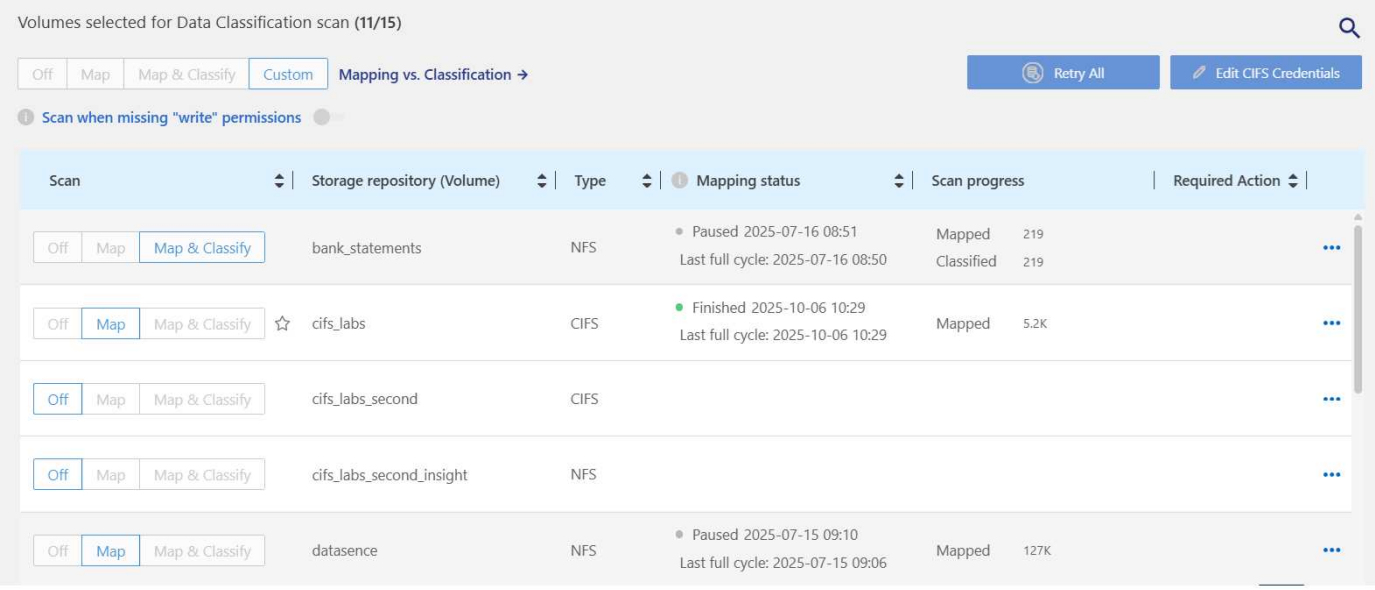
Abilita e disabilita le scansioni sui volumi

È possibile avviare o interrompere le scansioni su qualsiasi sistema in qualsiasi momento dalla pagina Configurazione. È anche 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 di un sistema.

I nuovi volumi aggiunti al sistema vengono automaticamente scansionati solo se è stata selezionata l'impostazione **Mappa** o **Mappa e classifica** nell'area dell'intestazione. Se impostato su **Personalizzato** o **Disattivato** nell'area dell'intestazione, sarà necessario attivare la mappatura e/o la scansione completa su ogni nuovo volume aggiunto al sistema.

Per impostazione predefinita, l'interruttore in cima alla pagina per **Esegui scansione in caso di permessi di "scrittura" mancanti** è disabilitato. Ciò significa che se Data Classification non dispone di autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS, il sistema non eseguirà la scansione dei file perché Data Classification non può ripristinare l'"ora dell'ultimo accesso" al timestamp originale. Se non ti interessa che l'ultimo orario di accesso venga reimpostato, attiva l'interruttore e tutti i file verranno analizzati indipendentemente dalle autorizzazioni. "Saperne di più".

I nuovi volumi aggiunti al sistema vengono automaticamente scansionati solo se nell'area dell'intestazione è stata impostata l'opzione **Mappa** o **Mappa e classifica**. Se l'impostazione per tutti i volumi è **Personalizzata** o **Disattivata**, è necessario attivare manualmente la scansione per ogni nuovo volume aggiunto.



Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Scegli un sistema, quindi seleziona **Configurazione**.
3. Per abilitare o disabilitare le scansioni per tutti i volumi, selezionare **Mappa**, **Mappa e classifica** o **Disattivato** nell'intestazione sopra tutti i volumi.

   Per abilitare o disabilitare le scansioni per singoli volumi, trova i volumi nell'elenco, quindi seleziona **Mappa**, **Mappa e classifica** o **Disattivato** accanto al nome del volume.

Risultato

Quando si abilita la scansione, Data Classification avvia la scansione dei volumi selezionati nel sistema. I risultati iniziano ad apparire nella dashboard Conformità non appena la Classificazione dei dati avvia la scansione. Il tempo di completamento della scansione dipende dalla quantità di dati e può variare da minuti a ore.

Scansiona le condivisioni di file con NetApp Data Classification

Per eseguire la scansione delle condivisioni file, è necessario prima creare un gruppo di condivisioni file in NetApp Data Classification. I gruppi di condivisione file sono per condivisioni NFS o CIFS (SMB) ospitate in locale o nel cloud.

La scansione dei dati provenienti da condivisioni file non NetApp non è supportata nella versione core di Data Classification.

Prerequisiti

Prima di abilitare la classificazione dei dati, rivedere i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata.

- Le condivisioni possono essere ospitate ovunque, anche nel cloud o in locale. Le condivisioni CIFS dei vecchi sistemi di archiviazione NetApp 7-Mode possono essere scansionate come condivisioni di file.

    - La classificazione dei dati non può estrarre le autorizzazioni o l'"ultimo orario di accesso" dai sistemi 7-Mode.
    - A causa di un problema noto tra alcune versioni di Linux e le condivisioni CIFS sui sistemi 7-Mode, è necessario configurare la condivisione in modo che utilizzi solo SMBv1 con l'autenticazione NTLM abilitata.
- È necessaria la connettività di rete tra l'istanza di classificazione dei dati e le condivisioni.
- È possibile aggiungere una condivisione DFS (Distributed File System) come una normale condivisione CIFS. Poiché Data Classification non è a conoscenza del fatto che la condivisione è basata su più server/volumi combinati in un'unica condivisione CIFS, potrebbero essere visualizzati errori di autorizzazione o connettività relativi alla condivisione quando in realtà il messaggio si applica solo a una delle cartelle/condivisioni che si trova su un server/volume diverso.
- Per le condivisioni CIFS (SMB), assicurati di disporre delle credenziali di Active Directory che forniscano l'accesso in lettura alle condivisioni. Le credenziali di amministratore sono preferibili nel caso in cui Data Classification debba analizzare dati che richiedono autorizzazioni elevate.

  Se si desidera assicurarsi che gli "ultimi orari di accesso" dei file non vengano modificati dalle scansioni di classificazione dei dati, si consiglia che l'utente disponga delle autorizzazioni di scrittura degli attributi in CIFS o delle autorizzazioni di scrittura in NFS. Se possibile, configurare l'utente di Active Directory come parte di un gruppo padre nell'organizzazione che dispone delle autorizzazioni per tutti i file.
- Tutte le condivisioni file CIFS in un gruppo devono utilizzare le stesse credenziali di Active Directory.
- È possibile combinare condivisioni NFS e CIFS (utilizzando Kerberos o NTLM). È necessario aggiungere le azioni al gruppo separatamente. Ciò significa che è necessario completare il processo due volte, una volta per protocollo.
    - Non è possibile creare un gruppo di condivisioni file che combini i tipi di autenticazione CIFS (Kerberos e NTLM).
- Se si utilizza CIFS con autenticazione Kerberos, assicurarsi che l'indirizzo IP fornito sia accessibile alla classificazione dei dati. Le condivisioni di file non possono essere aggiunte se l'indirizzo IP non è raggiungibile.

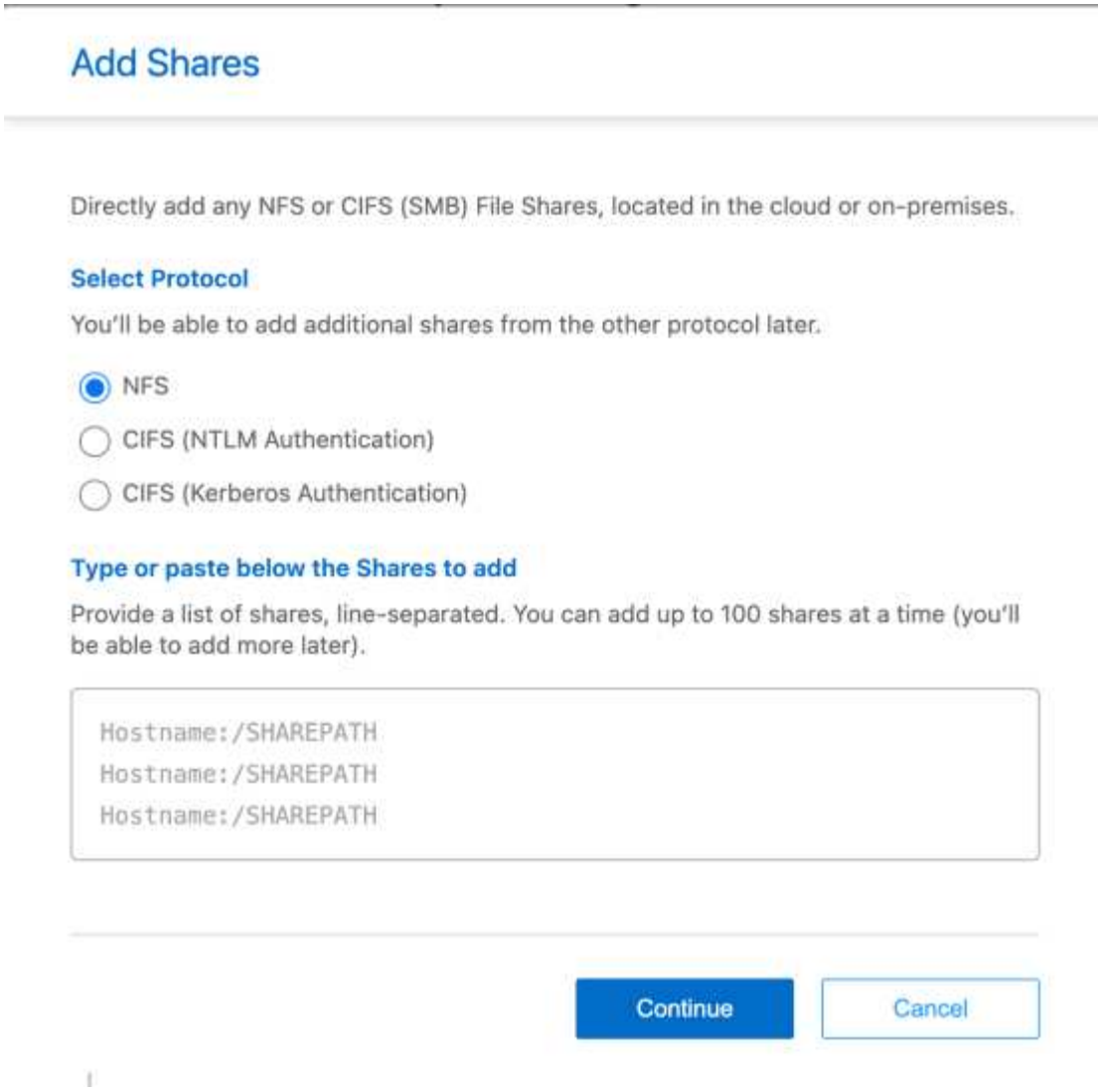
Crea un gruppo di condivisione file

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

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

Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Dalla pagina Configurazione, seleziona **Aggiungi sistema** > **Aggiungi gruppo di condivisioni file**.
3. Nella finestra di dialogo Aggiungi gruppo di condivisioni file, immettere il nome del gruppo di condivisioni, quindi selezionare **Continua**.
4. Seleziona il protocollo per le condivisioni file che stai aggiungendo.



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

5. Aggiungere le condivisioni file che si desidera analizzare (una condivisione file per riga). Quindi seleziona **Continua**.
6. Una finestra di dialogo di conferma visualizza il numero di condivisioni aggiunte.

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

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

Per impostazione predefinita, l'interruttore in cima alla pagina per **Esegui scansione quando mancano i permessi "attributi di scrittura"** è disabilitato. Ciò significa che se Data Classification non dispone di autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS, il sistema non eseguirà la scansione dei file perché Data Classification non può ripristinare l'"ora dell'ultimo accesso" al timestamp originale. + Se si imposta **Scansione in caso di mancanza di autorizzazioni "attributi di scrittura"** su **Attivato**, la scansione reimposta l'orario dell'ultimo accesso ed esegue la scansione di tutti i file indipendentemente dalle autorizzazioni. + Per saperne di più sull'ultimo timestamp di accesso, vedere"Metadati raccolti da fonti di dati nella classificazione dei dati" .

Risultato

La classificazione dei dati avvia la scansione dei file nelle condivisioni file aggiunte. PuoiMonitora l'avanzamento della scansione e visualizzare i risultati della scansione nella **Dashboard**.

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

Modifica un gruppo di condivisione file

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

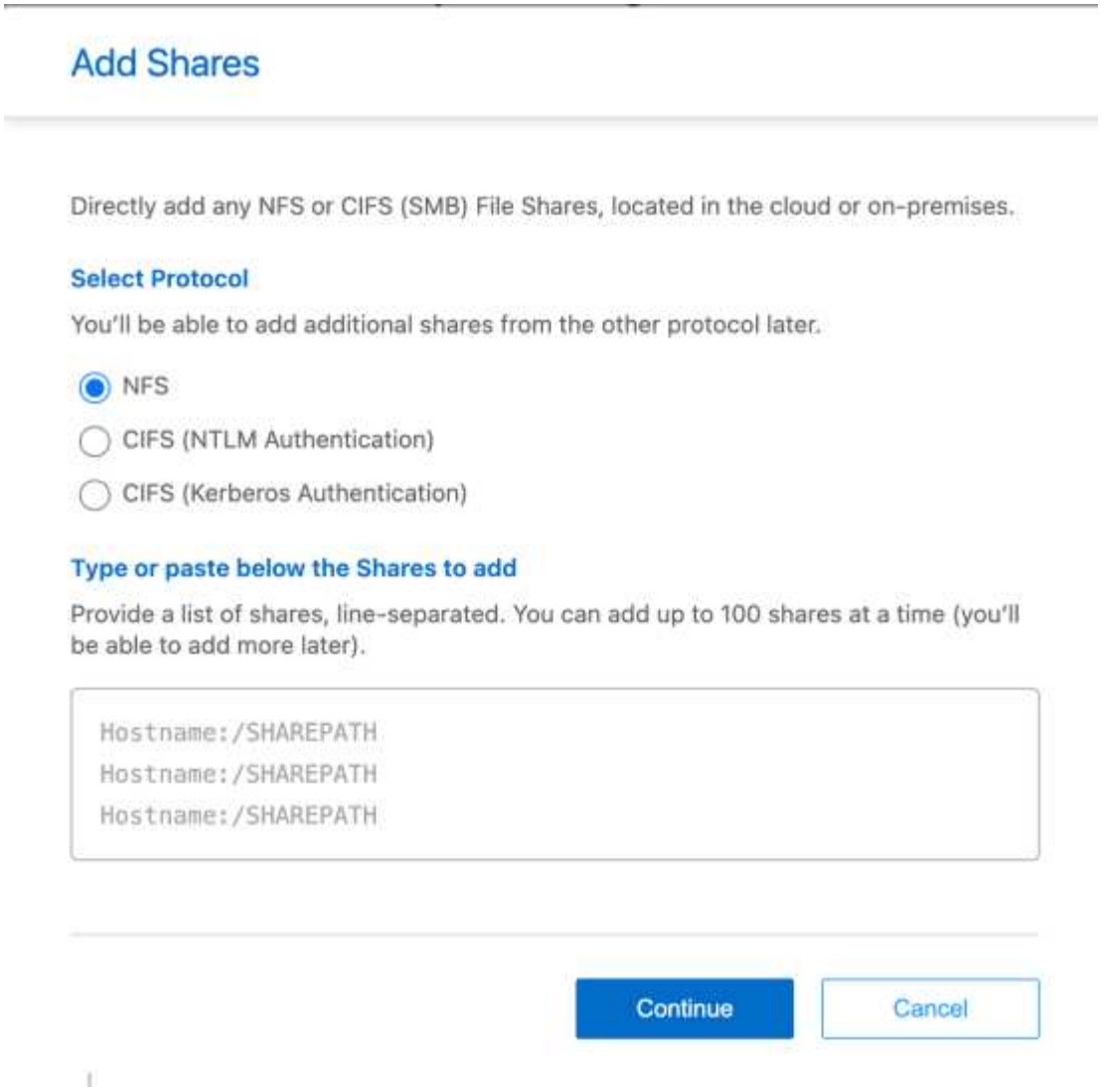
Modifica la configurazione del protocollo CIFS

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

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

Aggiungi condivisioni di file alle scansioni

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Dalla pagina Configurazione, seleziona il gruppo di condivisioni file che desideri modificare.
3. Seleziona **+ Aggiungi azioni**.
4. Seleziona il protocollo per le condivisioni file che stai aggiungendo.



Se si aggiungono condivisioni file a un protocollo già configurato, non sono necessarie modifiche.

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

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

Rimuovere una condivisione file dalle scansioni

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Seleziona il sistema da cui desideri rimuovere le condivisioni file.
3. Selezionare **Configurazione**.
4. Dalla pagina Configurazione, seleziona Azioni ••• per la condivisione file che vuoi rimuovere.
5. Dal menu Azioni, seleziona **Rimuovi condivisione**.

Monitora l'avanzamento della scansione

È possibile monitorare l'avanzamento della scansione iniziale.

1. Selezionare il menu **Configurazione**.
2. Selezionare **Configurazione di sistema**.
3. Per il repository di archiviazione, controllare la colonna Avanzamento scansione per visualizzarne lo stato.

Scansiona i dati StorageGRID con NetApp Data Classification

Completare alcuni passaggi per avviare la scansione dei dati all'interno StorageGRID direttamente con NetApp Data Classification.

Esaminare i requisiti di StorageGRID

Prima di abilitare la classificazione dei dati, rivedere i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata.

- È necessario disporre dell'URL dell'endpoint per connettersi al servizio di archiviazione degli oggetti.
- È necessario disporre della chiave di accesso e della chiave segreta di StorageGRID affinché Data Classification possa accedere ai bucket.

Distribuisci l'istanza di classificazione dei dati

Distribuisci Data Classification se non è già stata distribuita un'istanza.

Se si esegue la scansione di dati da StorageGRID accessibili tramite Internet, è possibile"distribuire la classificazione dei dati nel cloud" O"distribuire la classificazione dei dati in una posizione locale dotata di accesso a Internet" .

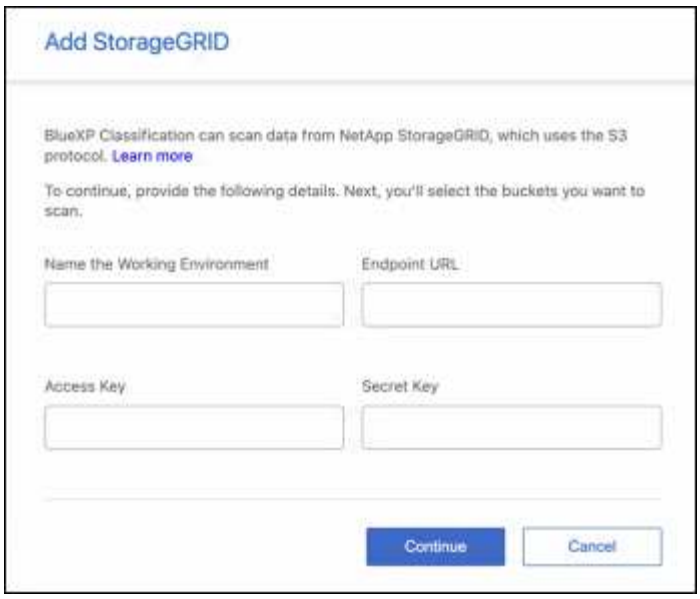
Se si stanno eseguendo la scansione dei dati da StorageGRID installato in un sito buio senza accesso a Internet, è necessario"distribuire la classificazione dei dati nella stessa posizione locale che non ha accesso a Internet" . Ciò richiede anche che l'agente della console venga distribuito nella stessa posizione locale.

Aggiungere il servizio StorageGRID alla classificazione dei dati

Aggiungere il servizio StorageGRID .

Passi

1. Dal menu Classificazione dati, selezionare l'opzione **Configurazione**.
2. Dalla pagina Configurazione, seleziona **Aggiungi sistema** > **Aggiungi StorageGRID**.
3. Nella finestra di dialogo Aggiungi servizio StorageGRID , immettere i dettagli per il servizio StorageGRID e selezionare **Continua**.
   a. Inserisci il nome che vuoi usare per il sistema. Questo nome dovrebbe riflettere il nome del servizio StorageGRID a cui ci si sta connettendo.
   b. Immettere l'URL dell'endpoint per accedere al servizio di archiviazione degli oggetti.
   c. Immettere la chiave di accesso e la chiave segreta in modo che Data Classification possa accedere ai bucket in StorageGRID.



Risultato

StorageGRID viene aggiunto all'elenco dei sistemi.

Abilita e disabilita le scansioni sui bucket StorageGRID

Dopo aver abilitato la classificazione dei dati su StorageGRID, il passaggio successivo consiste nel configurare i bucket che si desidera analizzare. La classificazione dei dati rileva tali bucket e li visualizza nel sistema creato.

Passi

1. Nella pagina Configurazione, individuare il sistema StorageGRID .
2. Nel riquadro del sistema StorageGRID , seleziona **Configurazione**.
3. Per abilitare o disabilitare la scansione, completare uno dei seguenti passaggi:
   - Per abilitare le scansioni di sola mappatura su un bucket, selezionare **Mappa**.
   - Per abilitare le scansioni complete su un bucket, seleziona **Mappa e classifica**.
   - Per disattivare la scansione su un bucket, selezionare **Off**.

Risultato

La classificazione dei dati avvia la scansione dei bucket abilitati. È possibile monitorare l'avanzamento della scansione iniziale accedendo al menu **Configurazione** e selezionando quindi **Configurazione di sistema**. L'avanzamento di ogni scansione viene visualizzato tramite una barra di avanzamento. È anche possibile passare il mouse sulla barra di avanzamento per visualizzare il numero di file scansionati rispetto al totale dei file presenti nel volume. Se sono presenti errori, questi appariranno nella colonna Stato, insieme all'azione richiesta per correggerli.

Informazioni sul copyright

Informazioni sul marchio commerciale