# Iniziare

## NetApp Data Classification

NetApp
February 06, 2026

# Sommario

# Iniziare

## Scopri di più sulla NetApp Data Classification

NetApp Data Classification è un servizio di governance dei dati per NetApp Console che analizza le fonti di dati aziendali on-premise e cloud per mappare e classificare i dati e identificare le informazioni private. Ciò può contribuire a ridurre i rischi per la sicurezza e la conformità, a diminuire i costi di archiviazione e ad agevolare i progetti di migrazione dei dati.

A partire dalla versione 1.31, la classificazione dei dati è disponibile come funzionalità principale nella NetApp Console. Non ci sono costi aggiuntivi. Non è richiesta alcuna licenza o abbonamento di classificazione. + Se hai utilizzato la versione legacy 1.30 o una versione precedente, tale versione sarà disponibile fino alla scadenza dell'abbonamento.

### NetApp Console

La classificazione dei dati è accessibile tramite la NetApp Console.

NetApp Console offre una gestione centralizzata dei servizi di storage e dati NetApp in ambienti on-premise e cloud di livello aziendale. La console è necessaria per accedere e utilizzare i servizi dati NetApp . In quanto interfaccia di gestione, consente di gestire numerose risorse di archiviazione da un'unica interfaccia. Gli amministratori della console possono controllare l'accesso allo storage e ai servizi per tutti i sistemi all'interno dell'azienda.

Per iniziare a utilizzare NetApp Console non è necessaria una licenza o un abbonamento e verranno addebitati costi solo quando sarà necessario distribuire gli agenti della console nel cloud per garantire la connettività ai sistemi di storage o ai servizi dati NetApp . Tuttavia, alcuni servizi dati NetApp accessibili dalla Console sono concessi in licenza o basati su abbonamento.

Scopri di più su"NetApp Console" .

### Caratteristiche

La classificazione dei dati utilizza l'intelligenza artificiale (IA), l'elaborazione del linguaggio naturale (NLP) e l'apprendimento automatico (ML) per comprendere il contenuto che analizza, al fine di estrarre entità e categorizzare il contenuto di conseguenza. Ciò consente alla classificazione dei dati di fornire le seguenti aree di funzionalità.

"Scopri i casi d'uso per la classificazione dei dati" .

#### Mantenere la conformità

Data Classification fornisce diversi strumenti che possono aiutarti a raggiungere la conformità. È possibile utilizzare la classificazione dei dati per:

- Identificare le informazioni personali identificabili (PII).
- Identificare un'ampia gamma di informazioni personali sensibili come richiesto dalle normative sulla privacy GDPR, CCPA, PCI e HIPAA.
- Rispondere alle richieste di accesso ai dati personali (DSAR) in base al nome o all'indirizzo e-mail.

**Rafforzare la sicurezza**

La classificazione dei dati può identificare i dati potenzialmente a rischio di accesso per scopi criminali. È possibile utilizzare la classificazione dei dati per:

- Identifica tutti i file e le directory (condivisioni e cartelle) con autorizzazioni aperte che sono accessibili all'intera organizzazione o al pubblico.
- Identificare i dati sensibili che risiedono al di fuori della posizione iniziale dedicata.
- Rispettare le policy di conservazione dei dati.
- Utilizzare *Policies* per rilevare automaticamente nuovi problemi di sicurezza, in modo che il personale addetto alla sicurezza possa intervenire immediatamente.

**Ottimizzare l'utilizzo dello spazio di archiviazione**

La classificazione dei dati fornisce strumenti che possono aiutarti a ridurre il costo totale di proprietà (TCO) del tuo storage. È possibile utilizzare la classificazione dei dati per:

- Aumenta l'efficienza di archiviazione identificando i dati duplicati o non correlati all'attività aziendale.
- Risparmia sui costi di archiviazione identificando i dati inattivi che puoi spostare in un archivio di oggetti meno costoso. "Scopri di più sulla suddivisione in livelli dai sistemi Cloud Volumes ONTAP" . "Scopri di più sulla suddivisione in livelli dai sistemi ONTAP locali" .

## Sistemi supportati e fonti di dati

La classificazione dei dati può analizzare e scansionare dati strutturati e non strutturati provenienti dai seguenti tipi di sistemi e fonti di dati:

**Sistemi**

- Gestione Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP (distribuito in AWS, Azure o GCP)
- Cluster ONTAP on-premise
- StorageGRID
- Google Cloud NetApp Volumes

**Fonti dei dati**

- Condivisioni file NetApp
- Banche dati:
  - Servizio di database relazionale Amazon (Amazon RDS)
  - MongoDB
  - MySQL
  - Oracolo
  - PostgreSQL
  - SAP HANA
  - SQL Server (MSSQL)

Data Classification supporta le versioni NFS 3.x, 4.0 e 4.1 e le versioni CIFS 1.x, 2.0, 2.1 e 3.0.

## Costo

L'utilizzo della classificazione dei dati è gratuito. Non è richiesta alcuna licenza di classificazione o abbonamento a pagamento.

### Costi delle infrastrutture

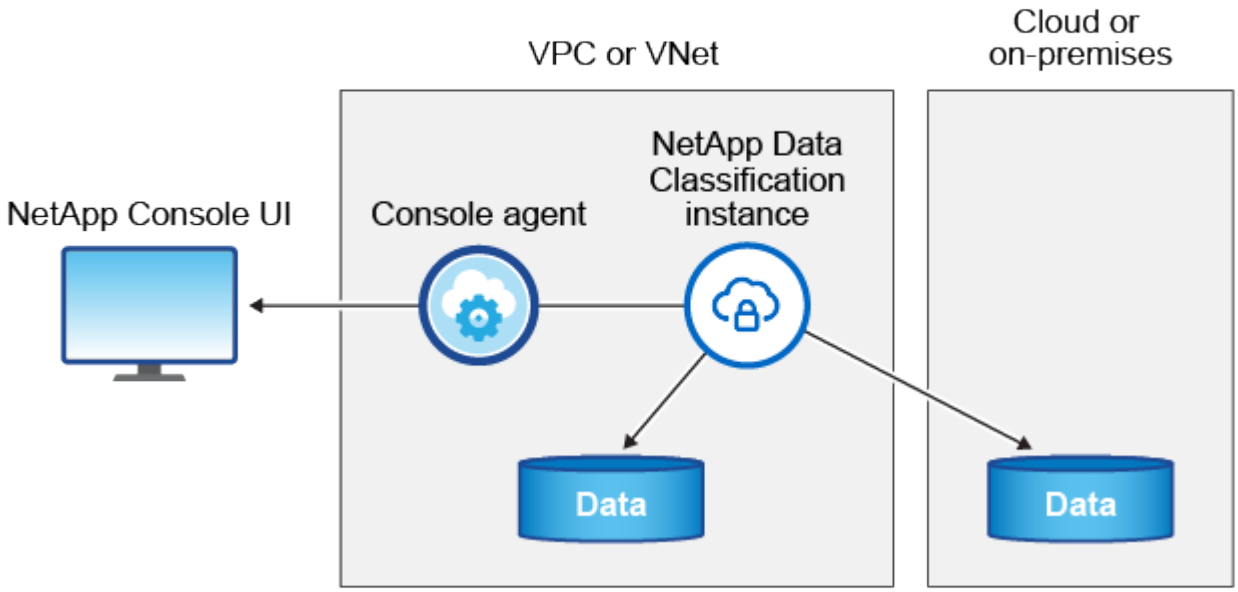
- L'installazione di Data Classification nel cloud richiede la distribuzione di un'istanza cloud, che comporta l'addebito di costi da parte del provider cloud presso cui viene distribuita. Vedere il tipo di istanza distribuita per ciascun provider cloud . Non ci sono costi se si installa Data Classification su un sistema locale.
- Per la classificazione dei dati è necessario aver distribuito un agente Console. In molti casi si dispone già di un agente Console perché si utilizzano altri servizi e risorse di archiviazione nella Console. L'istanza dell'agente Console comporta addebiti da parte del provider cloud presso cui è distribuita. Vedi il "tipo di istanza distribuita per ciascun provider cloud" . Non ci sono costi se si installa l'agente Console su un sistema locale.

### Costi di trasferimento dati

I costi di trasferimento dati dipendono dalla configurazione. Se l'istanza di Data Classification e l'origine dati si trovano nella stessa zona di disponibilità e regione, non vi sono costi di trasferimento dati. Tuttavia, se la fonte dei dati, ad esempio un sistema Cloud Volumes ONTAP , si trova in una zona di disponibilità o regione *diversa*, il tuo provider cloud ti addebiterà i costi di trasferimento dei dati. Per maggiori dettagli consultare questi xref:./* "AWS: Prezzi di Amazon Elastic Compute Cloud (Amazon EC2)" * "Microsoft Azure: dettagli sui prezzi della larghezza di banda" * "Google Cloud: prezzi del servizio di trasferimento dello storage"

## L'istanza di classificazione dei dati

Quando si distribuisce Data Classification nel cloud, la Console distribuisce l'istanza nella stessa subnet dell'agente della Console. "Scopri di più sull'agente Console."




Si noti quanto segue riguardo all'istanza predefinita:

- In AWS, la classificazione dei dati viene eseguita su un "istanza m6i.4xlarge" con un disco GP2 da 500

GiB. L'immagine del sistema operativo è Amazon Linux 2. Se distribuita in AWS, puoi scegliere un'istanza di dimensioni inferiori se stai analizzando una piccola quantità di dati.

- In Azure, la classificazione dei dati viene eseguita su un"Standard_D16s_v3 VM" con un disco da 500 GiB. L'immagine del sistema operativo è Ubuntu 22.04.
- In GCP, la classificazione dei dati viene eseguita su un"VM n2-standard-16" con un disco persistente Standard da 500 GiB. L'immagine del sistema operativo è Ubuntu 22.04.
- Nelle regioni in cui l'istanza predefinita non è disponibile, Data Classification viene eseguito su un'istanza alternativa. "Vedi i tipi di istanza alternativi" .
- L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Per ogni agente console viene distribuita una sola istanza di classificazione dei dati.

Puoi anche distribuire Data Classification su un host Linux nella tua sede o su un host del tuo provider cloud preferito. Il software funziona esattamente allo stesso modo, indipendentemente dal metodo di installazione scelto. Gli aggiornamenti del software di classificazione dei dati sono automatizzati finché l'istanza ha accesso a Internet.

L'istanza deve rimanere sempre in esecuzione perché la classificazione dei dati esegue continuamente la scansione dei dati.

**Distribuisci su diversi tipi di istanza**

Esaminare le seguenti specifiche per i tipi di istanza:

| Dimensioni del sistema | Specifiche | Limitazioni |
|---|---|---|
| Extra Large | 32 CPU, 128 GB di RAM, 1 TiB SSD | Può scansionare fino a 500 milioni di file. |
| Grande (predefinito) | 16 CPU, 64 GB di RAM, SSD da 500 GiB | Può scansionare fino a 250 milioni di file. |

Quando si distribuisce Data Classification in Azure o GCP, inviare un'e-mail a ng-contact-data-sense@netapp.com per ricevere assistenza se si desidera utilizzare un tipo di istanza più piccolo.

## Come funziona la scansione della classificazione dei dati

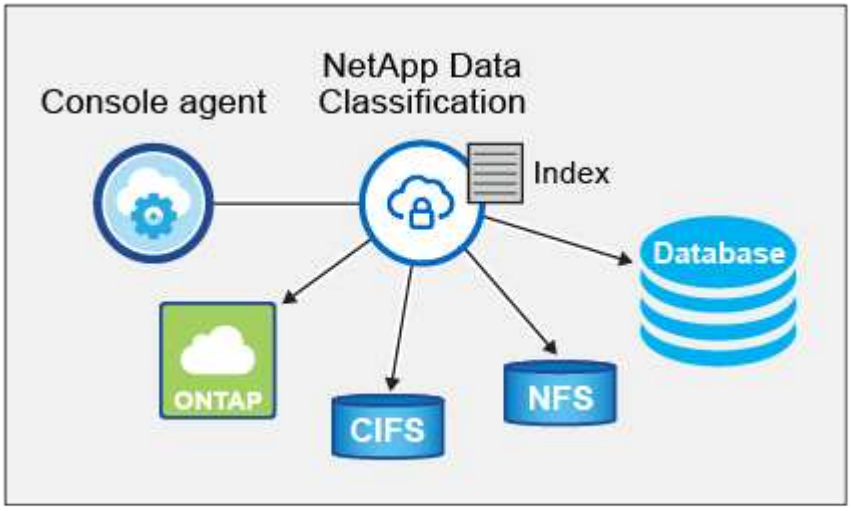
Ad alto livello, la scansione della classificazione dei dati funziona in questo modo:

1. Distribuisci un'istanza di Data Classification nella Console.
2. È possibile abilitare la mappatura di alto livello (chiamata scansione *Solo mappatura*) o la scansione di livello profondo (chiamata scansione *Mappa e classifica*) su una o più origini dati.
3. La classificazione dei dati analizza i dati utilizzando un processo di apprendimento basato sull'intelligenza artificiale.
4. Puoi utilizzare i dashboard e gli strumenti di reporting forniti per aiutarti nei tuoi sforzi di conformità e governance.

Dopo aver abilitato la classificazione dei dati e selezionato i repository che si desidera analizzare (volumi, schemi di database o altri dati utente), la scansione dei dati inizia immediatamente per identificare i dati personali e sensibili. Nella maggior parte dei casi, dovresti concentrarti sulla scansione dei dati di produzione

in tempo reale anziché su backup, mirror o siti DR. Quindi Data Classification mappa i dati della tua organizzazione, categorizza ogni file e identifica ed estrae entità e modelli predefiniti nei dati. Il risultato della scansione è un indice di informazioni personali, informazioni personali sensibili, categorie di dati e tipi di file.

Data Classification si connette ai dati come qualsiasi altro client montando volumi NFS e CIFS. Ai volumi NFS si accede automaticamente in sola lettura, mentre per analizzare i volumi CIFS è necessario fornire le credenziali di Active Directory.




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.

> 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" .

## 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.

Per i dettagli sulle differenze tra le scansioni di mappatura e classificazione, vedere"Qual è la differenza tra le scansioni di mappatura e di classificazione?" .

## Informazioni che la classificazione dei dati categorizza

La classificazione dei dati raccoglie, indicizza e assegna categorie ai seguenti dati:

- **Metadati standard** sui file: tipo di file, dimensioni, date di creazione e modifica, ecc.
- **Dati personali**: informazioni di identificazione personale (PII), come indirizzi e-mail, numeri di identificazione o numeri di carte di credito, che Data Classification identifica utilizzando parole, stringhe e modelli specifici nei file. "Scopri di più sui dati personali" .
- **Dati personali sensibili**: tipologie particolari di informazioni personali sensibili (SPII), come dati sanitari, origine etnica o opinioni politiche, come definito dal Regolamento generale sulla protezione dei dati (GDPR) e da altre normative sulla privacy. "Scopri di più sui dati personali sensibili" .
- **Categorie**: la classificazione dei dati prende i dati scansionati e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi AI del contenuto e dei metadati di ciascun file. "Scopri di più sulle categorie".
- **Riconoscimento dell'entità del nome**: la classificazione dei dati utilizza l'intelligenza artificiale per estrarre i nomi naturali delle persone dai documenti. "Scopri come rispondere alle richieste di accesso ai dati personali" .

### Panoramica della rete

Data Classification distribuisce un singolo server, o cluster, ovunque tu scelga: nel cloud o in sede. I server si connettono tramite protocolli standard alle fonti dati e indicizzano i risultati in un cluster Elasticsearch, anch'esso distribuito sugli stessi server. Ciò consente il supporto per ambienti multi-cloud, cross-cloud, cloud privati e on-premise.

La Console distribuisce l'istanza di classificazione dei dati con un gruppo di sicurezza che abilita le connessioni HTTP in entrata dall'agente della Console.

Quando si utilizza la Console in modalità SaaS, la connessione alla Console viene fornita tramite HTTPS e i dati privati inviati tra il browser e l'istanza di Data Classification sono protetti tramite crittografia end-to-end tramite TLS 1.2, il che significa che NetApp e terze parti non possono leggerli.

Le regole in uscita sono completamente aperte. Per installare e aggiornare il software di classificazione dei dati e per inviare le metriche di utilizzo è necessario l'accesso a Internet.

Se hai requisiti di rete rigorosi,"Scopri gli endpoint contattati da Data Classification" .

# Accedi NetApp Data Classification

È possibile accedere alla NetApp Data Classification tramite la NetApp Console.

Per accedere alla Console, puoi utilizzare le credenziali del sito di supporto NetApp oppure registrarti per accedere alla NetApp Console utilizzando il tuo indirizzo email e una password. "Scopri di più sull'accesso alla Console" .

Attività specifiche richiedono ruoli utente specifici nella Console. "Scopri di più sui ruoli di accesso alla console per tutti i servizi" .

**Prima di iniziare**

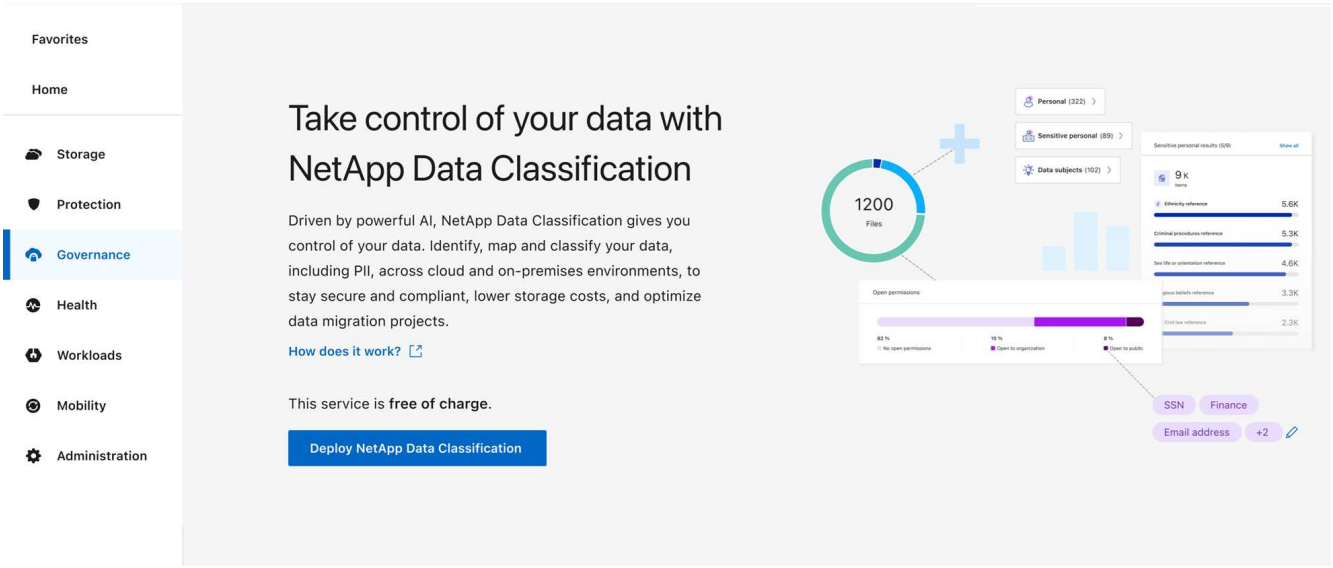
- "Dovresti aggiungere un agente Console."
- "Scopri quale stile di distribuzione della classificazione dei dati è più adatto al tuo carico di lavoro."

**Passi**

1. In un browser web, vai a"Consolle" .

2. Accedi alla Console.
3. Dalla pagina principale della NetApp Console, selezionare **Governance** > **Classificazione dati**.
4. Se è la prima volta che accedi a Data Classification, verrà visualizzata la pagina di destinazione.

   Seleziona **Distribuisci classificazione in locale o nel cloud** per iniziare a distribuire la tua istanza di classificazione. Per maggiori informazioni, vedere"Quale distribuzione di classificazione dei dati dovresti utilizzare?"




   In caso contrario, viene visualizzata la Dashboard di classificazione dei dati.

# Distribuisci la classificazione dei dati

## Quale distribuzione NetApp Data Classification dovresti utilizzare?

È possibile distribuire NetApp Data Classification in diversi modi. Scopri quale metodo soddisfa le tue esigenze.

La classificazione dei dati può essere implementata nei seguenti modi:

- "Distribuisci nel cloud utilizzando la console" . La Console distribuisce l'istanza di classificazione dei dati nella stessa rete del provider cloud dell'agente della Console.
- "Installa su un host Linux con accesso a Internet" . Installa Data Classification su un host Linux nella tua rete o su un host Linux nel cloud che abbia accesso a Internet. Questo tipo di installazione può essere una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP locali utilizzando un'istanza di classificazione dei dati anch'essa ubicata in sede, sebbene non sia un requisito.
- "Installa su un host Linux in un sito locale senza accesso a Internet", nota anche come *modalità privata*. Questo tipo di installazione, che utilizza uno script di installazione, non ha connettività con il livello SaaS della console.

La modalità privata BlueXP (interfaccia BlueXP legacy) viene in genere utilizzata con ambienti locali privi di connessione Internet e con regioni cloud sicure, tra cui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. NetApp continua a supportare questi ambienti con l'interfaccia legacy BlueXP . Per la documentazione sulla modalità privata nell'interfaccia legacy BlueXP , vedere"Documentazione PDF per la modalità privata BlueXP" .

Sia l'installazione su un host Linux con accesso a Internet sia l'installazione in locale su un host Linux senza accesso a Internet utilizzano uno script di installazione. Lo script inizia verificando se il sistema e l'ambiente soddisfano i prerequisiti. Se i prerequisiti sono soddisfatti, l'installazione inizia. Se si desidera verificare i prerequisiti indipendentemente dall'esecuzione dell'installazione di Data Classification, è possibile scaricare un pacchetto software separato che verifica solo i prerequisiti.

Fare riferimento a "Verifica che il tuo host Linux sia pronto per installare Data Classification" .

## Distribuisci NetApp Data Classification nel cloud utilizzando la NetApp Console

È possibile distribuire NetApp Data Classification nel cloud con NetApp Console. La Console distribuisce l'istanza di classificazione dei dati nella stessa rete del provider cloud dell'agente della Console.

Nota che puoi anche"installare Data Classification su un host Linux con accesso a Internet" . Questo tipo di installazione può essere una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP locali utilizzando un'istanza di classificazione dei dati anch'essa ubicata in sede, ma non è un requisito. Il software funziona esattamente allo stesso modo, indipendentemente dal metodo di installazione scelto.

### Avvio rapido

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

**1 Creare un agente Console**

Se non si dispone già di un agente Console, crearne uno. Vedere"creazione di un agente Console in AWS" ,"creazione di un agente Console in Azure" , O"creazione di un agente Console in GCP" .

Puoi anche"installare l'agente Console in locale" su un host Linux nella tua rete o su un host Linux nel cloud.

**2 Prerequisiti**

Assicurati che il tuo ambiente possa soddisfare i prerequisiti. Questi includono outbound accesso a Internet per l'istanza, connettività tra l'agente Console e Data Classification sulla porta 443 e altro ancora. Vedi l'elenco completo.

**3 Distribuisci la classificazione dei dati**

Avviare la procedura guidata di installazione per distribuire l'istanza di Data Classification nel cloud.

### Creare un agente Console

Se non disponi già di un agente Console, creane uno nel tuo provider cloud. Vedere "creazione di un agente

Console in AWS" O "creazione di un agente Console in Azure" , O "creazione di un agente Console in GCP" . Nella maggior parte dei casi sarà probabilmente configurato un agente Console prima di tentare di attivare la classificazione dei dati perché la maggior parte "Le funzionalità della console richiedono un agente della console" , ma ci sono casi in cui sarà necessario impostarne uno ora.

Esistono alcuni scenari in cui è necessario utilizzare un agente Console distribuito in uno specifico provider cloud:

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in AWS o Amazon FSx per i bucket ONTAP , si utilizza un agente Console in AWS.
- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in Azure o in Azure NetApp Files, si utilizza un agente Console in Azure.
  - Per Azure NetApp Files, è necessario distribuirlo nella stessa area dei volumi che si desidera analizzare.
- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in GCP, si utilizza un agente Console in GCP.

È possibile eseguire la scansione dei sistemi ONTAP on-premise, delle condivisioni file NetApp e dei database utilizzando uno qualsiasi di questi agenti della console cloud.

Nota che puoi anche "installare l'agente Console in locale" su un host Linux nella tua rete o nel cloud. Alcuni utenti che intendono installare Data Classification in locale potrebbero anche scegliere di installare l'agente Console in locale.

Potrebbero esserci situazioni in cui è necessario utilizzare "più agenti della console" .

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" .

#### Supporto regionale del governo

La classificazione dei dati è supportata quando l'agente della console viene distribuito in una regione governativa (AWS GovCloud, Azure Gov o Azure DoD). Quando implementata in questo modo, la classificazione dei dati presenta le seguenti restrizioni:

"Scopri come distribuire l'agente Console in una regione governativa".

### Prerequisiti

Esaminare i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata prima di distribuire Data Classification nel cloud. Quando si distribuisce Data Classification nel cloud, questa si trova nella stessa subnet dell'agente Console.

#### Abilita l'accesso a Internet in uscita dalla classificazione dei dati

La classificazione dei dati richiede l'accesso a Internet in uscita. Se la rete virtuale o fisica utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza di Data Classification disponga di accesso a Internet in uscita per contattare i seguenti endpoint. La delega non deve essere trasparente. I proxy trasparenti non sono attualmente supportati.

Consultare la tabella appropriata qui sotto a seconda che si stia distribuendo la classificazione dei dati in AWS, Azure o GCP.

**Endpoint richiesti per AWS**

| Punti finali | Scopo |
|---|---|
| \ https://api.console.netapp.com | Comunicazione con il servizio Console, che include gli account NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicazione con il sito web della Console per l'autenticazione centralizzata degli utenti. |
| \ https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornisce accesso a immagini software, manifesti e modelli. |
| \ https://kinesis.us-east-1.amazonaws.com | Consente a NetApp di trasmettere in streaming i dati dai record di audit. |
| \ https://cognito-idp.us-east-1.amazonaws.com \ https://cognito-identity.us-east-1.amazonaws.com \ https://user-feedback-store-prod.s3.us-west-2.amazonaws.com \ https://customer-data-production.s3.us-west-2.amazonaws.com | Consente a Data Classification di accedere e scaricare manifesti e modelli e di inviare registri e metriche. |

**Endpoint richiesti per Azure**

| Punti finali | Scopo |
|---|---|
| \ https://api.console.netapp.com | Comunicazione con il servizio Console, che include gli account NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicazione con il sito web della Console per l'autenticazione centralizzata degli utenti. |
| \ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornisce accesso a immagini software, manifesti, modelli e consente di inviare log e metriche. |
| \ https://support.compliance.api.console.netapp.com/ | Consente a NetApp di trasmettere in streaming i dati dai record di audit. |

**Endpoint richiesti per GCP**

| Punti finali | Scopo |
|---|---|
| \ https://api.console.netapp.com | Comunicazione con il servizio Console, che include gli account NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicazione con il sito web della Console per l'autenticazione centralizzata degli utenti. |

| Punti finali | Scopo |
| --- | --- |
| \ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornisce accesso a immagini software, manifesti, modelli e consente di inviare log e metriche. |
| \ https://support.compliance.api.console.netapp.com/ | Consente a NetApp di trasmettere in streaming i dati dai record di audit. |

**Assicurarsi che la classificazione dei dati disponga delle autorizzazioni richieste**

Assicurarsi che Data Classification disponga delle autorizzazioni per distribuire risorse e creare gruppi di sicurezza per l'istanza di Data Classification.

- "Autorizzazioni di Google Cloud"
- "Autorizzazioni AWS"
- "Autorizzazioni di Azure"

**Assicurarsi che l'agente della console possa accedere alla classificazione dei dati**

Garantire la connettività tra l'agente della console e l'istanza di classificazione dei dati. Il gruppo di sicurezza per l'agente Console deve consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione dei dati. Questa connessione consente la distribuzione dell'istanza di classificazione dei dati e consente di visualizzare le informazioni nelle schede Conformità e Governance. La classificazione dei dati è supportata nelle regioni governative in AWS e Azure.

Per le distribuzioni AWS e AWS GovCloud sono necessarie regole aggiuntive per i gruppi di sicurezza in entrata e in uscita. Vedere "Regole per l'agente della console in AWS" per i dettagli.

Per le distribuzioni di Azure e Azure Government sono necessarie regole aggiuntive per i gruppi di sicurezza in entrata e in uscita. Vedere "Regole per l'agente Console in Azure" per i dettagli.

**Assicurati di poter mantenere in esecuzione la classificazione dei dati**

L'istanza di classificazione dei dati deve rimanere attiva per analizzare continuamente i dati.

**Assicurare la connettività del browser Web alla classificazione dei dati**

Dopo aver abilitato la classificazione dei dati, assicurarsi che gli utenti accedano all'interfaccia della console da un host che abbia una connessione all'istanza di classificazione dei dati.

L'istanza di classificazione dei dati utilizza un indirizzo IP privato per garantire che i dati indicizzati non siano accessibili da Internet. Di conseguenza, il browser Web utilizzato per accedere alla Console deve disporre di una connessione a tale indirizzo IP privato. Tale connessione può provenire da una connessione diretta al tuo provider cloud (ad esempio, una VPN) oppure da un host che si trova all'interno della stessa rete dell'istanza di classificazione dei dati.

**Controlla i limiti della tua vCPU**

Assicurati che il limite di vCPU del tuo provider cloud consenta la distribuzione di un'istanza con il numero necessario di core. Sarà necessario verificare il limite di vCPU per la famiglia di istanze pertinente nella regione in cui è in esecuzione la Console. "Visualizza i tipi di istanza richiesti" .

Per maggiori dettagli sui limiti vCPU, consultare i seguenti xref:./* "Documentazione AWS: quote di servizio Amazon EC2"
* "Documentazione di Azure: quote vCPU delle macchine virtuali"
* "Documentazione di Google Cloud: Quote di risorse"

**Distribuisci la classificazione dei dati nel cloud**

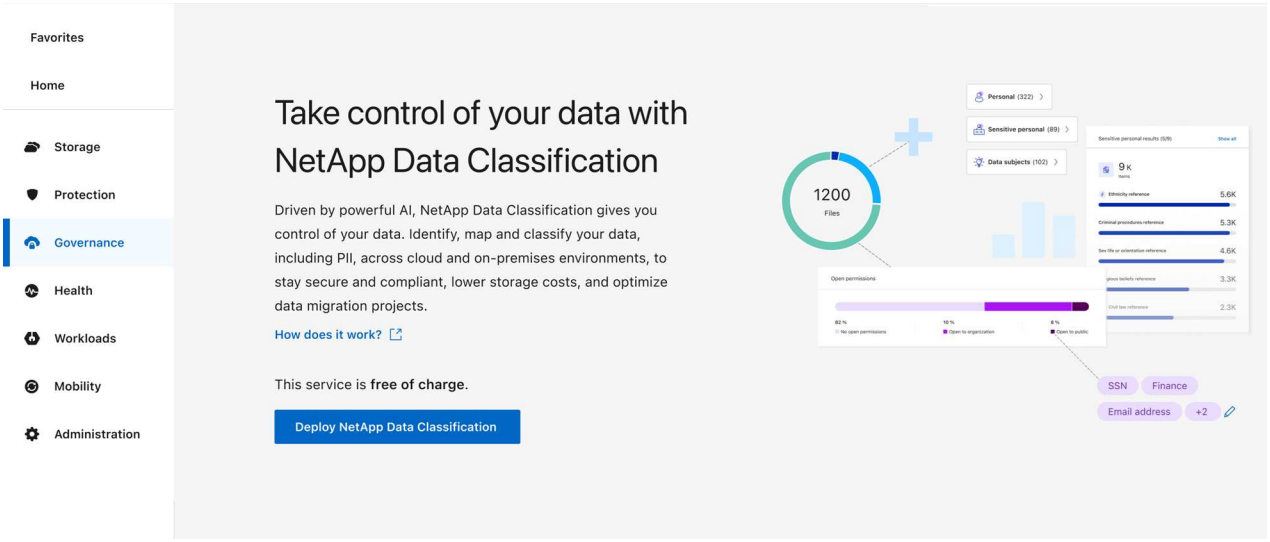
Per distribuire un'istanza di Data Classification nel cloud, seguire questi passaggi. L'agente della console distribuirà l'istanza nel cloud e quindi installerà il software di classificazione dei dati su tale istanza.

Nelle regioni in cui il tipo di istanza predefinito non è disponibile, la classificazione dei dati viene eseguita su un"tipo di istanza alternativo" .

### Distribuisci in AWS

#### Passi

1. Dalla pagina principale di Data Classification, seleziona **Distribuisci classificazione in locale o nel cloud**.

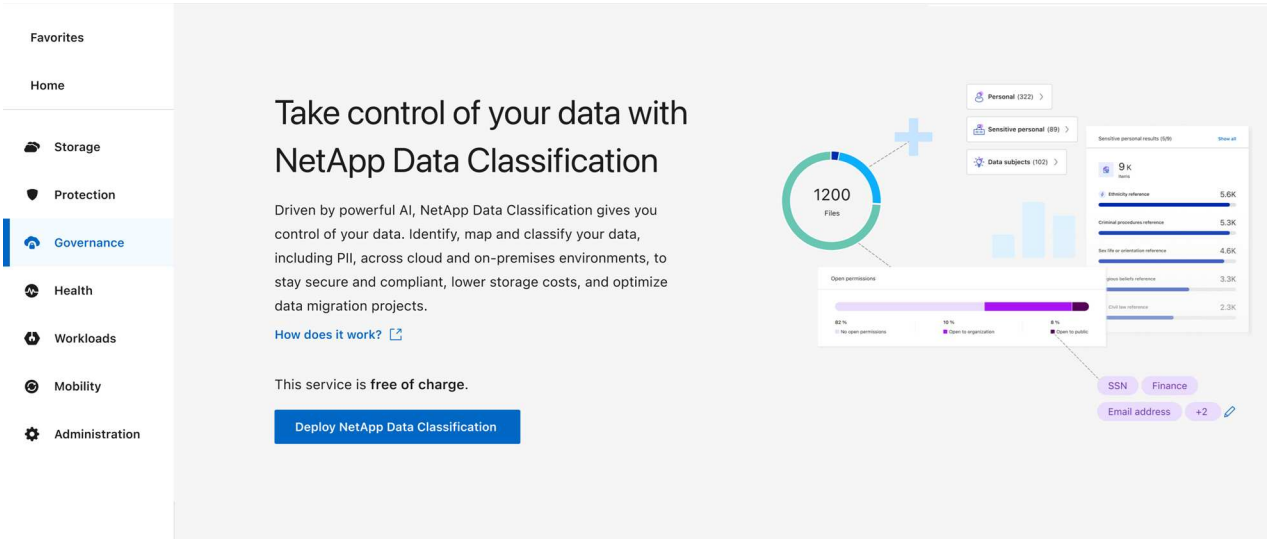



2. Dalla pagina *Installazione*, seleziona **Distribuisci > Distribuisci** per utilizzare la dimensione dell'istanza "Grande" e avviare la procedura guidata di distribuzione cloud.
3. La procedura guidata visualizza l'avanzamento dei passaggi di distribuzione. Quando sono richiesti input o se si verificano problemi, viene visualizzato un messaggio.
4. Una volta distribuita l'istanza e installata la classificazione dei dati, selezionare **Continua alla configurazione** per andare alla pagina *Configurazione*.

### Distribuisci in Azure

#### Passi

1. Dalla pagina principale di Data Classification, seleziona **Distribuisci classificazione in locale o nel cloud**.



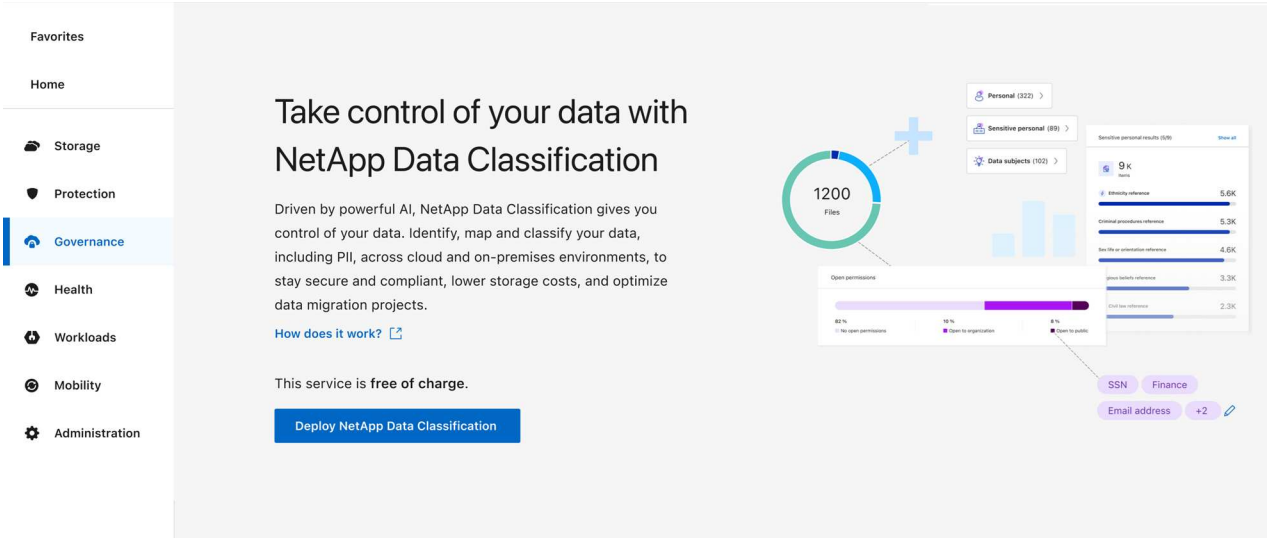

2. Selezionare **Distribuisci** per avviare la procedura guidata di distribuzione cloud.

3. La procedura guidata visualizza l'avanzamento dei passaggi di distribuzione. Se riscontra qualche problema, si fermerà e chiederà un input.
4. Una volta distribuita l'istanza e installata la classificazione dei dati, selezionare **Continua alla configurazione** per andare alla pagina *Configurazione*.

**Distribuisci in Google Cloud**

**Passi**

1. Dalla pagina principale di Data Classification, selezionare **Governance > Classificazione**.
2. Selezionare **Distribuisci classificazione in locale o nel cloud**.




3. Selezionare **Distribuisci** per avviare la procedura guidata di distribuzione cloud.
4. La procedura guidata visualizza l'avanzamento dei passaggi di distribuzione. Se riscontra qualche problema, si fermerà e chiederà un input.
5. Una volta distribuita l'istanza e installata la classificazione dei dati, selezionare **Continua alla configurazione** per andare alla pagina *Configurazione*.

**Risultato**

La Console distribuisce l'istanza di classificazione dei dati nel tuo provider cloud.

Gli aggiornamenti all'agente della console e al software di classificazione dei dati sono automatizzati, a condizione che le istanze dispongano di connettività Internet.

**Cosa succederà dopo?**

Dalla pagina Configurazione è possibile selezionare le origini dati che si desidera analizzare.

## Installa NetApp Data Classification su un host con accesso a Internet

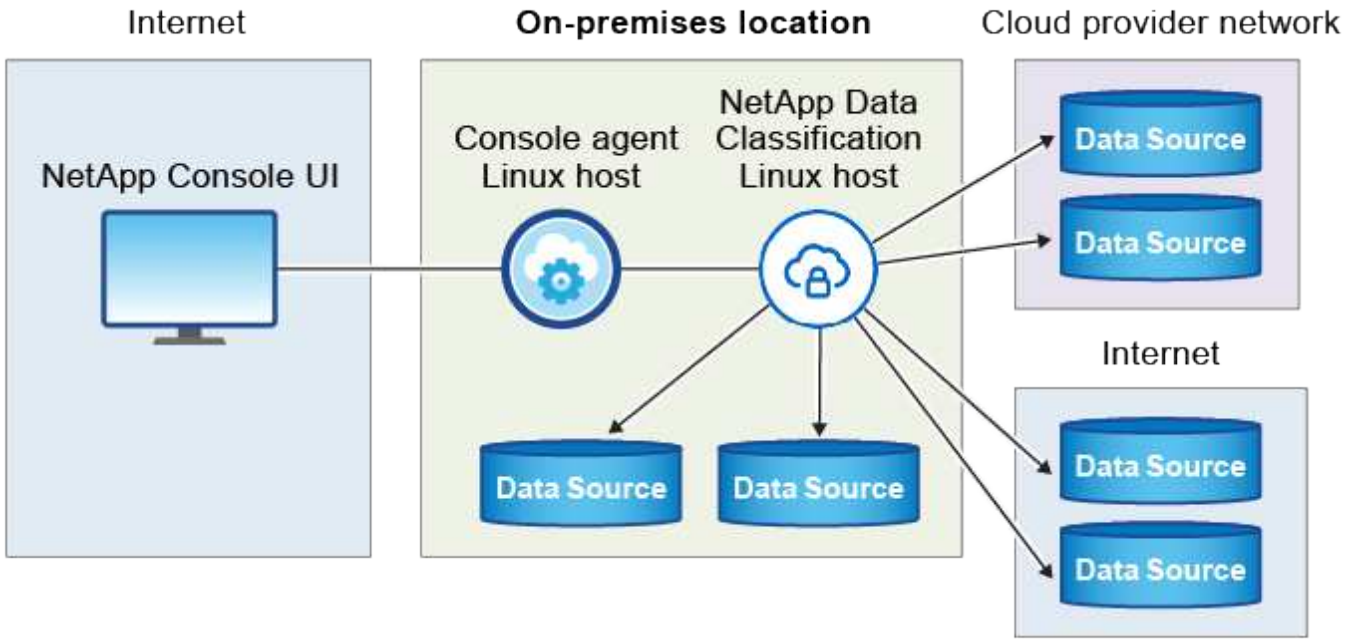
Per distribuire NetApp Data Classification su un host Linux nella tua rete o su un host Linux nel cloud con accesso a Internet, devi distribuire manualmente l'host Linux nella tua rete o nel cloud.

L'installazione in sede è una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP in sede utilizzando un'istanza di Data Classification anch'essa in sede. Questo non è un requisito. Il software funziona

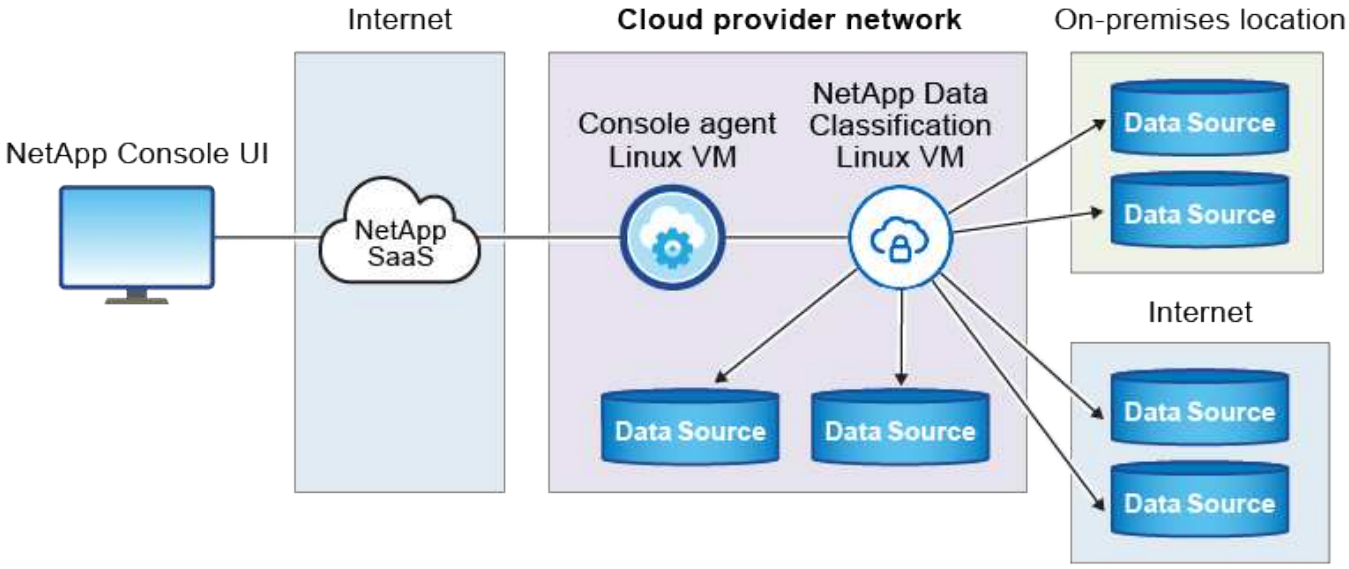
allo stesso modo indipendentemente dal metodo di installazione scelto.

Lo script di installazione di Data Classification inizia verificando se il sistema e l'ambiente soddisfano i prerequisiti richiesti. Se tutti i prerequisiti sono soddisfatti, l'installazione avrà inizio. Se si desidera verificare i prerequisiti indipendentemente dall'esecuzione dell'installazione di Data Classification, è possibile scaricare un pacchetto software separato che verifica solo i prerequisiti. "Scopri come verificare se il tuo host Linux è pronto per installare Data Classification" .

L'installazione tipica su un host Linux *nei tuoi locali* presenta i seguenti componenti e connessioni.




L'installazione tipica su un host Linux *nel cloud* presenta i seguenti componenti e connessioni.




**Avvio rapido**

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

### 1 Creare un agente Console

Se non hai ancora un agente Console, "distribuire l'agente della console in locale" su un host Linux nella tua rete o su un host Linux nel cloud.

Puoi anche creare un agente Console con il tuo provider cloud. Vedere "creazione di un agente Console in AWS" , "creazione di un agente Console in Azure" , O "creazione di un agente Console in GCP" .

### 2 Rivedere i prerequisiti

Assicurati che il tuo ambiente soddisfi i prerequisiti. Ciò include l'accesso a Internet in uscita per l'istanza, la connettività tra l'agente della console e la classificazione dei dati sulla porta 443 e altro ancora. Vedi l'elenco completo .

Hai anche bisogno di un sistema Linux che soddisfi i requisitiseguenti requisiti .

### 3 Scarica e distribuisci la classificazione dei dati

Scarica il software Cloud Data Classification dal sito di supporto NetApp e copia il file di installazione sull'host Linux che intendi utilizzare. Quindi avviare la procedura guidata di installazione e seguire le istruzioni per distribuire l'istanza di Data Classification.

#### Creare un agente Console

Per poter installare e utilizzare Data Classification è necessario un agente Console. Nella maggior parte dei casi, probabilmente avrai configurato un agente Console prima di tentare di attivare la classificazione dei dati perché la maggior parte "Le funzionalità della console richiedono un agente della console" , ma ci sono casi in cui sarà necessario impostarne uno ora.

Per crearne uno nell'ambiente del tuo provider cloud, vedi "creazione di un agente Console in AWS" , "creazione di un agente Console in Azure" , O "creazione di un agente Console in GCP" .

Esistono alcuni scenari in cui è necessario utilizzare un agente Console distribuito in uno specifico provider cloud:

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in AWS o Amazon FSx per ONTAP, si utilizza un agente Console in AWS.
- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in Azure o in Azure NetApp Files, si utilizza un agente Console in Azure.

  Per Azure NetApp Files, è necessario distribuirlo nella stessa area dei volumi che si desidera analizzare.

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in GCP, si utilizza un agente Console in GCP.

I sistemi ONTAP on-premise, le condivisioni file NetApp e gli account di database possono essere scansionati utilizzando uno qualsiasi di questi agenti della console cloud.

Nota che puoi anche "distribuire l'agente della console in locale" su un host Linux nella tua rete o su un host Linux nel cloud. Alcuni utenti che intendono installare Data Classification in locale potrebbero anche scegliere di installare l'agente Console in locale.

Durante l'installazione di Data Classification sarà necessario l'indirizzo IP o il nome host del sistema agente della console. Queste informazioni saranno disponibili se hai installato l'agente Console nella tua sede. Se l'agente della console è distribuito nel cloud, è possibile trovare queste informazioni nella console: selezionare l'icona della Guida, quindi **Supporto** e infine **Agente della console**.

### Preparare il sistema host Linux

Il software di classificazione dei dati deve essere eseguito su un host che soddisfi specifici requisiti del sistema operativo, requisiti di RAM, requisiti software e così via. L'host Linux può trovarsi nella tua rete o nel cloud.

Assicurarsi di poter mantenere in esecuzione la classificazione dei dati. La macchina di classificazione dei dati deve rimanere accesa per analizzare continuamente i dati.

- La classificazione dei dati deve avvenire su un host dedicato. L'host non può essere condiviso con altre applicazioni o software di terze parti, come gli antivirus.
- Scegli la dimensione più adatta al set di dati che intendi analizzare con Data Classification.

| Dimensioni del sistema | processore | RAM (la memoria di swap deve essere disabilitata) | Disco |
|---|---|---|---|
| **Extra Large** | 32 CPU | 128 GB di RAM | • SSD da 1 TiB su /, oppure 100 GiB disponibili su /opt<br>• 895 GiB disponibili su /var/lib/docker<br>• 5 GiB su /tmp<br>• **Per Podman, 30 GB su /var/tmp** |
| **Grande** | 16 CPU | 64 GB di RAM | • SSD da 500 GiB su /, oppure 100 GiB disponibili su /opt<br>• 400 GiB disponibili su /var/lib/docker o per Podman /var/lib/containers<br>• 5 GiB su /tmp<br>• **Per Podman, 30 GB su /var/tmp** |

- Quando si distribuisce un'istanza di elaborazione nel cloud per l'installazione di Data Classification, si consiglia di utilizzare un sistema che soddisfi i requisiti di sistema "Large" sopra indicati:
  - **Tipo di istanza Amazon Elastic Compute Cloud (Amazon EC2)**: "m6i.4xlarge". "Vedi altri tipi di istanze AWS" .
  - **Dimensioni della VM di Azure**: "Standard_D16s_v3". "Visualizza altri tipi di istanze di Azure" .
  - **Tipo di macchina GCP**: "n2-standard-16". "Vedi altri tipi di istanza GCP" .
- **Autorizzazioni cartella UNIX**: sono richieste le seguenti autorizzazioni UNIX minime:

| Cartella | Permessi minimi |
|---|---|
| /tmp | `rwxrwxrwt` |

| Cartella | Permessi minimi |
| --- | --- |
| /optare | `rwxr-xr-x` |
| /var/lib/docker | `rwx------` |
| /usr/lib/systemd/sistema | `rwxr-xr-x` |

- **Sistema operativo**:
  - I seguenti sistemi operativi richiedono l'utilizzo del motore container Docker:
    - Red Hat Enterprise Linux versione 7.8 e 7.9
    - Ubuntu 22.04 (richiede Data Classification versione 1.23 o successiva)
    - Ubuntu 24.04 (richiede Data Classification versione 1.23 o successiva)
  - I seguenti sistemi operativi richiedono l'utilizzo del motore contenitore Podman e la versione 1.30 o successiva di Data Classification:
    - Red Hat Enterprise Linux versione 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 e 9.6.
  - Le estensioni vettoriali avanzate (AVX2) devono essere abilitate sul sistema host.
- **Red Hat Subscription Management**: l'host deve essere registrato presso Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.
- **Software aggiuntivo**: è necessario installare il seguente software sull'host prima di installare Data Classification:
  - A seconda del sistema operativo utilizzato, è necessario installare uno dei seguenti motori container:
    - Docker Engine versione 19.3.1 o successiva. "Visualizza le istruzioni di installazione" .
    - Podman versione 4 o successiva. Per installare Podman, inserisci(`sudo yum install podman netavark -y` ).
- Python versione 3.6 o successiva. "Visualizza le istruzioni di installazione" .
  - **Considerazioni su NTP**: NetApp consiglia di configurare il sistema di classificazione dei dati per utilizzare un servizio Network Time Protocol (NTP). L'ora deve essere sincronizzata tra il sistema di classificazione dei dati e il sistema agente della console.
- **Considerazioni su Firewalld**: se si prevede di utilizzare `firewalld` , ti consigliamo di abilitarlo prima di installare Data Classification. Eseguire i seguenti comandi per configurare `firewalld` in modo che sia compatibile con la classificazione dei dati:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Se si prevede di utilizzare host di classificazione dati aggiuntivi come nodi scanner, aggiungere subito queste regole al sistema primario:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Tieni presente che devi riavviare Docker o Podman ogni volta che abiliti o aggiorni `firewalld` impostazioni.

L'indirizzo IP del sistema host di classificazione dei dati non può essere modificato dopo l'installazione.

### Abilita l'accesso a Internet in uscita dalla classificazione dei dati

La classificazione dei dati richiede l'accesso a Internet in uscita. Se la rete virtuale o fisica utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza di Data Classification disponga di accesso a Internet in uscita per contattare i seguenti endpoint.

| Punti finali | Scopo |
|---|---|
| \ https://api.console.netapp.com | Comunicazione con la Console, che include gli account NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicazione con il sito web della Console per l'autenticazione centralizzata degli utenti. |
| \ https://support.compliance.api.bluexp.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornisce accesso a immagini software, manifesti, modelli e consente di inviare log e metriche. |
| \ https://support.compliance.api.bluexp.netapp.com/ | Consente a NetApp di trasmettere in streaming i dati dai record di audit. |
| \ https://github.com/docker \ https://download.docker.com | Fornisce i pacchetti prerequisiti per l'installazione di Docker. |
| \ http://packages.ubuntu.com/ \ http://archive.ubuntu.com | Fornisce i pacchetti prerequisiti per l'installazione di Ubuntu. |

### Verificare che tutte le porte richieste siano abilitate

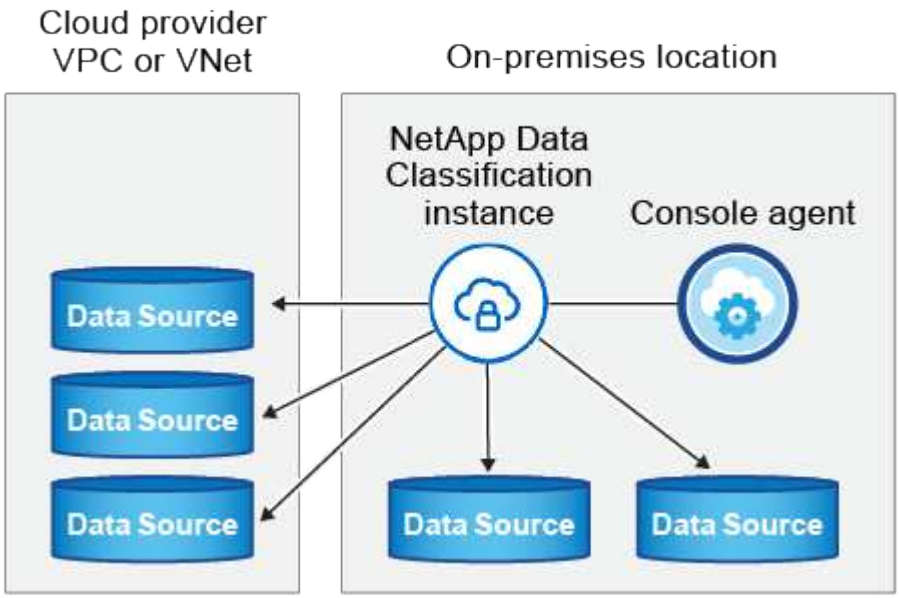
È necessario assicurarsi che tutte le porte necessarie siano aperte per la comunicazione tra l'agente della console, Data Classification, Active Directory e le origini dati.

| Tipo di connessione | porti | Descrizione |
| --- | --- | --- |
| Agente console <> Classificazione dati | 8080 (TCP), 443 (TCP) e 80. 9000 | Le regole del firewall o di routing per l'agente della console devono consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione dei dati. Assicurati che la porta 8080 sia aperta in modo da poter visualizzare l'avanzamento dell'installazione nella Console. Se sull'host Linux viene utilizzato un firewall, per i processi interni di un server Ubuntu è richiesta la porta 9000. |
| Agente console <> cluster ONTAP (NAS) | 443 (TCP) | La console rileva i cluster ONTAP tramite HTTPS. Se si utilizzano criteri firewall personalizzati, questi devono soddisfare i seguenti requisiti:<br>• L'host dell'agente della console deve consentire l'accesso HTTPS in uscita tramite la porta 443. Se l'agente della console si trova nel cloud, tutte le comunicazioni in uscita sono consentite dalle regole di routing o dal firewall predefiniti.<br>• Il cluster ONTAP deve consentire l'accesso HTTPS in entrata tramite la porta 443. Il criterio firewall predefinito "mgmt" consente l'accesso HTTPS in entrata da tutti gli indirizzi IP. Se hai modificato questa policy predefinita o se hai creato una policy firewall personalizzata, devi associare il protocollo HTTPS a tale policy e abilitare l'accesso dall'host dell'agente della console. |
| Classificazione dei dati <> cluster ONTAP | • Per NFS - 111 (TCP\UDP) e 2049 (TCP\UDP)<br>• Per CIFS - 139 (TCP\UDP) e 445 (TCP\UDP) | La classificazione dei dati necessita di una connessione di rete a ciascuna subnet Cloud Volumes ONTAP o sistema ONTAP locale. I firewall o le regole di routing per Cloud Volumes ONTAP devono consentire le connessioni in ingresso dall'istanza di classificazione dei dati.<br>Assicurarsi che queste porte siano aperte all'istanza di classificazione dei dati:<br>• Per NFS - 111 e 2049<br>• Per CIFS - 139 e 445<br>I criteri di esportazione del volume NFS devono consentire l'accesso dall'istanza di classificazione dei dati. |

| Tipo di connessione | porti | Descrizione |
| --- | --- | --- |
| Classificazione dei dati <> Active Directory | 389 (TCP e UDP), 636 (TCP), 3268 (TCP) e 3269 (TCP) | È necessario che sia già stata configurata una Active Directory per gli utenti della propria azienda. Inoltre, la classificazione dei dati necessita delle credenziali di Active Directory per analizzare i volumi CIFS.<br><br>È necessario disporre delle informazioni per Active Directory:<br><br>• Indirizzo IP del server DNS o più indirizzi IP<br>• Nome utente e password per il server<br>• Nome di dominio (nome di Active Directory)<br>• Se stai utilizzando LDAP sicuro (LDAPS) o meno<br>• Porta del server LDAP (in genere 389 per LDAP e 636 per LDAP sicuro) |

### Installa Data Classification sull'host Linux

Nelle configurazioni tipiche, il software verrà installato su un singolo sistema host. Guarda i passaggi qui .




VederePreparazione del sistema host Linux ERevisione dei prerequisiti per l'elenco completo dei requisiti prima di implementare Data Classification.

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

Al momento, Data Classification non è in grado di analizzare bucket S3, Azure NetApp Files o FSx per ONTAP quando il software è installato in locale. In questi casi sarà necessario distribuire un agente Console separato e un'istanza di Data Classification nel cloud e "passare da un connettore all'altro" per le tue diverse fonti di dati.

#### Installazione a host singolo per configurazioni tipiche

Esaminare i requisiti e seguire questi passaggi quando si installa il software di classificazione dei dati su un singolo host locale.

"Guarda questo video"per vedere come installare Data Classification.

Si noti che tutte le attività di installazione vengono registrate durante l'installazione di Data Classification. Se si verificano problemi durante l'installazione, è possibile visualizzare il contenuto del registro di controllo dell'installazione. È scritto a `/opt/netapp/install_logs/` .

**Prima di iniziare**

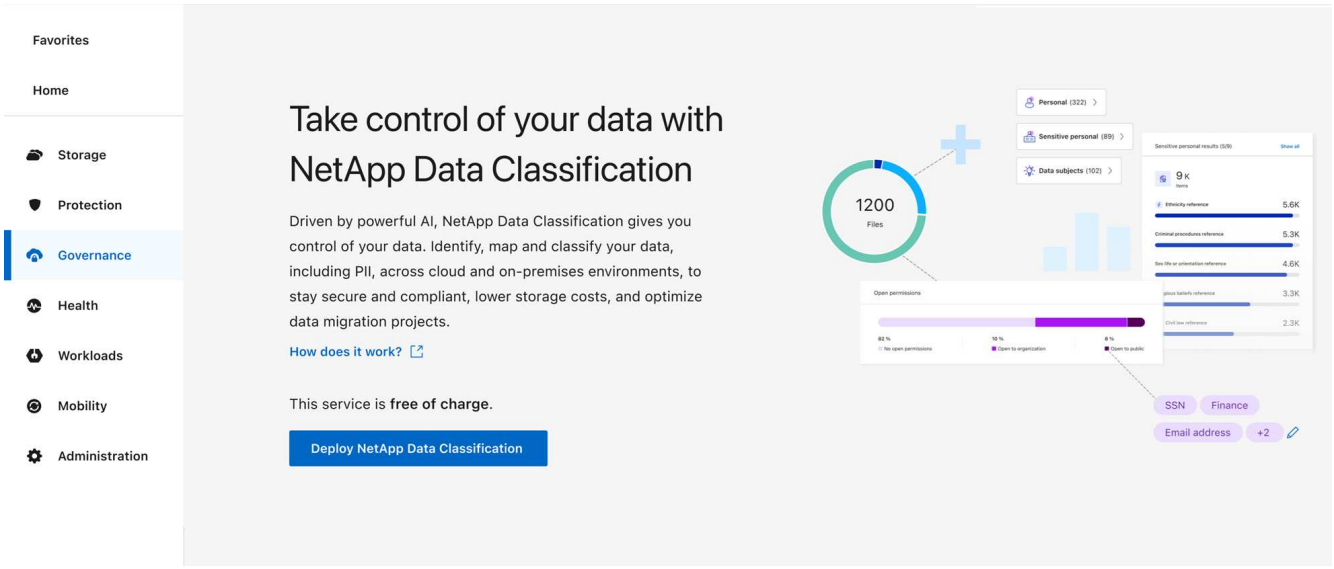
- Verifica che il tuo sistema Linux soddisfi i requisitirequisiti dell'host .
- Verificare che nel sistema siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurati di avere i privilegi di root sul sistema Linux.
- Se utilizzi un proxy per accedere a Internet:
  - Avrai bisogno delle informazioni sul server proxy (indirizzo IP o nome host, porta di connessione, schema di connessione: https o http, nome utente e password).
  - Se il proxy esegue l'intercettazione TLS, è necessario conoscere il percorso sul sistema Data Classification Linux in cui sono archiviati i certificati TLS CA.
  - La delega non deve essere trasparente. Attualmente la classificazione dei dati non supporta proxy trasparenti.
  - L'utente deve essere un utente locale. Gli utenti di dominio non sono supportati.
- Verifica che il tuo ambiente offline soddisfi i requisiti richiestipermessi e connettività .

**Passi**

1. Scarica il software di classificazione dei dati da "Sito di supporto NetApp" . Il file da selezionare si chiama **DATASENSE-INSTALLER-<versione>.tar.gz**.
2. Copia il file di installazione sull'host Linux che intendi utilizzare (utilizzando `scp` o qualche altro metodo).
3. Decomprimere il file di installazione sul computer host, ad esempio:

   ```
   tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
   ```

4. Nella Console, seleziona **Governance > Classificazione**.
5. Selezionare **Distribuisci classificazione in locale o nel cloud**.




6. A seconda che si stia installando Data Classification su un'istanza preparata nel cloud o su un'istanza preparata in sede, selezionare l'opzione **Distribuisci** appropriata per avviare l'installazione di Data Classification.
7. Viene visualizzata la finestra di dialogo *Distribuisci classificazione dati in locale*. Copia il comando fornito (ad esempio: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq` ) e incollalo in un file di testo in modo da poterlo utilizzare in seguito. Quindi seleziona **Chiudi** per chiudere la finestra di dialogo.
8. Sulla macchina host, immetti il comando che hai copiato e segui una serie di prompt, oppure puoi fornire il comando completo, inclusi tutti i parametri richiesti, come argomenti della riga di comando.

   Tieni presente che il programma di installazione esegue un controllo preliminare per assicurarsi che i requisiti di sistema e di rete siano soddisfatti per un'installazione corretta. "Guarda questo video" per comprendere i messaggi e le implicazioni del pre-controllo.

| Inserire i parametri come richiesto: | Inserisci il comando completo: |
| --- | --- |
| a. Incolla il comando che hai copiato dal passaggio 7: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>`<br><br>Se stai installando su un'istanza cloud (non nei tuoi locali), aggiungi `--manual-cloud -install <cloud_provider>`.<br><br>b. Immettere l'indirizzo IP o il nome host della macchina host di classificazione dei dati in modo che sia accessibile al sistema agente della console.<br>c. Immettere l'indirizzo IP o il nome host della macchina host dell'agente Console in modo che sia accessibile al sistema di classificazione dei dati.<br>d. Inserisci i dettagli del proxy come richiesto. Se l'agente della console utilizza già un proxy, non è necessario immettere nuovamente queste informazioni qui, poiché la classificazione dei dati utilizzerà automaticamente il proxy utilizzato dall'agente della console. | In alternativa, è possibile creare l'intero comando in anticipo, fornendo i parametri host e proxy necessari:<br>`sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>` |

Valori variabili:

- *account_id* = ID account NetApp
- *client_id* = ID client dell'agente della console (aggiungere il suffisso "client" all'ID client se non è già presente)
- *user_token* = token di accesso utente JWT
- *ds_host* = Indirizzo IP o nome host del sistema Linux di classificazione dei dati.
- *cm_host* = Indirizzo IP o nome host del sistema agente della console.
- *cloud_provider* = Quando si esegue l'installazione su un'istanza cloud, immettere "AWS", "Azure" o "Gcp" a seconda del provider cloud.
- *proxy_host* = IP o nome host del server proxy se l'host si trova dietro un server proxy.
- *proxy_port* = Porta per connettersi al server proxy (predefinita 80).
- *proxy_scheme* = Schema di connessione: https o http (predefinito http).
- *proxy_user* = Utente autenticato per connettersi al server proxy, se è richiesta l'autenticazione di base. L'utente deve essere un utente locale: gli utenti di dominio non sono supportati.
- *proxy_password* = Password per il nome utente specificato.
- *ca_cert_dir* = Percorso sul sistema Linux di classificazione dei dati contenente bundle di certificati TLS CA aggiuntivi. Richiesto solo se il proxy esegue l'intercettazione TLS.

**Risultato**

Il programma di installazione di Data Classification installa i pacchetti, registra l'installazione e installa Data

Classification. L'installazione può richiedere dai 10 ai 20 minuti.

Se è presente connettività sulla porta 8080 tra la macchina host e l'istanza dell'agente Console, l'avanzamento dell'installazione verrà visualizzato nella scheda Classificazione dati nella Console.

**Cosa succederà dopo?**

Dalla pagina Configurazione è possibile selezionare le origini dati che si desidera analizzare.

## Installa NetApp Data Classification su un host Linux senza accesso a Internet

L'installazione di NetApp Data Classification su un host Linux in un sito locale che non dispone di accesso a Internet è nota come *modalità privata*. Questo tipo di installazione, che utilizza uno script di installazione, non ha connettività con il livello SaaS NetApp Console .

> La modalità privata BlueXP (interfaccia BlueXP legacy) viene in genere utilizzata con ambienti locali privi di connessione Internet e con regioni cloud sicure, tra cui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. NetApp continua a supportare questi ambienti con l'interfaccia legacy BlueXP . Per la documentazione sulla modalità privata nell'interfaccia legacy BlueXP , vedere"Documentazione PDF per la modalità privata BlueXP" .

## Verifica che il tuo host Linux sia pronto per installare NetApp Data Classification

Prima di installare manualmente NetApp Data Classification su un host Linux, è possibile eseguire uno script sull'host per verificare che siano soddisfatti tutti i prerequisiti per l'installazione di Data Classification. Puoi eseguire questo script su un host Linux nella tua rete o su un host Linux nel cloud. L'host può essere connesso a Internet oppure risiedere in un sito che non ha accesso a Internet (un *dark site*).

Lo script di installazione di Data Classification comprende uno script di test per garantire che l'ambiente soddisfi i requisiti. È possibile eseguire questo script separatamente per verificare la disponibilità dell'host Linux prima di eseguire lo script di installazione.

### Iniziare

Dovrai svolgere le seguenti attività.

- Facoltativamente, installa un agente Console se non ne hai già installato uno. È possibile eseguire lo script di test senza avere installato un agente Console, ma lo script verifica la connettività tra l'agente Console e la macchina host di Data Classification, pertanto è consigliabile disporre di un agente Console.
- Preparare la macchina host e verificare che soddisfi tutti i requisiti.
- Abilitare l'accesso a Internet in uscita dalla macchina host di classificazione dei dati.
- Verificare che tutte le porte richieste siano abilitate su tutti i sistemi.
- Scarica ed esegui lo script di test dei prerequisiti.

### Creare un agente Console

Per poter installare e utilizzare Data Classification è necessario un agente Console. Tuttavia, è possibile eseguire lo script Prerequisiti senza un agente Console.

Puoi "installare l'agente Console in locale" su un host Linux nella tua rete o su un host Linux nel cloud. È anche possibile installare Data Classification in locale se l'agente Console è installato in locale.

Per creare un agente Console nell'ambiente del tuo provider cloud, consulta:

- "creazione di un agente Console in AWS"
- "creazione di un agente Console in Azure"
- "creazione di un agente Console in GCP"

Quando si esegue lo script dei prerequisiti, è necessario l'indirizzo IP o il nome host del sistema agente della console. Queste informazioni sono disponibili se hai installato l'agente Console nei tuoi locali. Se l'agente della Console è distribuito nel cloud, è possibile trovare queste informazioni nella Console: selezionare l'icona della Guida, quindi **Supporto**; nella sezione Agente e audit, selezionare **Vai all'agente**.

### Verifica i requisiti dell'host

Il software di classificazione dei dati deve essere eseguito su un host che soddisfi specifici requisiti del sistema operativo, requisiti di RAM e requisiti software.

- La classificazione dei dati deve avvenire su un host dedicato. L'host non può essere condiviso con altre applicazioni o software di terze parti, come gli antivirus.
- Scegli la dimensione più adatta al set di dati che intendi analizzare con Data Classification.

| Dimensioni del sistema | processore | RAM (la memoria di swap deve essere disabilitata) | Disco |
|---|---|---|---|
| **Extra Large** | 32 CPU | 128 GB di RAM | • SSD da 1 TiB su /, oppure 100 GiB disponibili su /opt<br>• 895 GiB disponibili su /var/lib/docker<br>• 5 GiB su /tmp<br>• **Per Podman, 30 GB su /var/tmp** |
| **Grande** | 16 CPU | 64 GB di RAM | • SSD da 500 GiB su /, oppure 100 GiB disponibili su /opt<br>• 400 GiB disponibili su /var/lib/docker o per Podman /var/lib/containers<br>• 5 GiB su /tmp<br>• **Per Podman, 30 GB su /var/tmp** |

- Quando si distribuisce un'istanza di elaborazione nel cloud per l'installazione di Data Classification, si consiglia di utilizzare un sistema che soddisfi i requisiti di sistema "Large" sopra indicati:
  - **Tipo di istanza Amazon Elastic Compute Cloud (Amazon EC2)**: "m6i.4xlarge". "Vedi altri tipi di istanze AWS" .
  - **Dimensioni della VM di Azure**: "Standard_D16s_v3". "Visualizza altri tipi di istanze di Azure" .

- **Tipo di macchina GCP**: "n2-standard-16". "Vedi altri tipi di istanza GCP" .

- **Autorizzazioni cartella UNIX**: sono richieste le seguenti autorizzazioni UNIX minime:

| Cartella | Permessi minimi |
|---|---|
| /tmp | `rwxrwxrwt` |
| /optare | `rwxr-xr-x` |
| /var/lib/docker | `rwx------` |
| /usr/lib/systemd/sistema | `rwxr-xr-x` |

- **Sistema operativo**:
  - I seguenti sistemi operativi richiedono l'utilizzo del motore container Docker:
    - Red Hat Enterprise Linux versione 7.8 e 7.9
    - Ubuntu 22.04 (richiede Data Classification versione 1.23 o successiva)
    - Ubuntu 24.04 (richiede Data Classification versione 1.23 o successiva)
  - I seguenti sistemi operativi richiedono l'utilizzo del motore contenitore Podman e la versione 1.30 o successiva di Data Classification:
    - Red Hat Enterprise Linux versione 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 e 9.6.
  - Le estensioni vettoriali avanzate (AVX2) devono essere abilitate sul sistema host.
- **Red Hat Subscription Management**: l'host deve essere registrato presso Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.
- **Software aggiuntivo**: è necessario installare il seguente software sull'host prima di installare Data Classification:
  - A seconda del sistema operativo utilizzato, è necessario installare uno dei seguenti motori container:
    - Docker Engine versione 19.3.1 o successiva. "Visualizza le istruzioni di installazione" .
    - Podman versione 4 o successiva. Per installare Podman, inserisci(`sudo yum install podman netavark -y` ).
- Python versione 3.6 o successiva. "Visualizza le istruzioni di installazione" .
  - **Considerazioni su NTP**: NetApp consiglia di configurare il sistema di classificazione dei dati per utilizzare un servizio Network Time Protocol (NTP). L'ora deve essere sincronizzata tra il sistema di classificazione dei dati e il sistema agente della console.
- **Considerazioni su Firewalld**: se si prevede di utilizzare `firewalld` , ti consigliamo di abilitarlo prima di installare Data Classification. Eseguire i seguenti comandi per configurare `firewalld` in modo che sia compatibile con la classificazione dei dati:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Se si prevede di utilizzare host di classificazione dati aggiuntivi come nodi scanner (in un modello distribuito), aggiungere subito queste regole al sistema primario:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Tieni presente che devi riavviare Docker o Podman ogni volta che abiliti o aggiorni `firewalld` impostazioni.

### Abilita l'accesso a Internet in uscita dalla classificazione dei dati

La classificazione dei dati richiede l'accesso a Internet in uscita. Se la rete virtuale o fisica utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza di Data Classification disponga di accesso a Internet in uscita per contattare i seguenti endpoint.

Questa sezione non è richiesta per i sistemi host installati in siti senza connettività Internet.

| Punti finali | Scopo |
|---|---|
| \ https://api.console.netapp.com | Comunicazione con il servizio Console, che include gli account NetApp . |
| \ https://netapp-cloud-account.auth0.com \ https://auth0.com | Comunicazione con il sito web della Console per l'autenticazione centralizzata degli utenti. |
| \ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/ | Fornisce accesso a immagini software, manifesti, modelli e consente di inviare log e metriche. |
| \ https://support.compliance.api.console.netapp.com/ | Consente a NetApp di trasmettere in streaming i dati dai record di audit. |
| \ https://github.com/docker \ https://download.docker.com | Fornisce i pacchetti prerequisiti per l'installazione di Docker. |
| \ http://packages.ubuntu.com/ \ http://archive.ubuntu.com | Fornisce i pacchetti prerequisiti per l'installazione di Ubuntu. |

### Verificare che tutte le porte richieste siano abilitate

È necessario assicurarsi che tutte le porte necessarie siano aperte per la comunicazione tra l'agente della console, Data Classification, Active Directory e le origini dati.

| Tipo di connessione | porti | Descrizione |
| --- | --- | --- |
| Agente console <> Classificazione dati | 8080 (TCP), 443 (TCP) e 80. 9000 | Le regole del firewall o di routing per l'agente della console devono consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione dei dati. Assicurati che la porta 8080 sia aperta in modo da poter visualizzare l'avanzamento dell'installazione nella Console. Se sull'host Linux viene utilizzato un firewall, per i processi interni di un server Ubuntu è richiesta la porta 9000. |
| Agente console <> cluster ONTAP (NAS) | 443 (TCP) | La console rileva i cluster ONTAP tramite HTTPS. Se si utilizzano criteri firewall personalizzati, l'host dell'agente della console deve consentire l'accesso HTTPS in uscita tramite la porta 443. Se l'agente della console si trova nel cloud, tutte le comunicazioni in uscita sono consentite dalle regole di routing o dal firewall predefiniti. |

### Eseguire lo script dei prerequisiti per la classificazione dei dati

Per eseguire lo script dei prerequisiti per la classificazione dei dati, seguire questi passaggi.

"Guarda questo video"per vedere come eseguire lo script Prerequisiti e interpretare i risultati.

#### Prima di iniziare

- Verifica che il tuo sistema Linux soddisfi i requisitirequisiti dell'host .
- Verificare che nel sistema siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurati di avere i privilegi di root sul sistema Linux.

#### Passi

1. Scarica lo script dei prerequisiti per la classificazione dei dati da "Sito di supporto NetApp" . Il file da selezionare si chiama **standalone-pre-requisite-tester-<versione>**.
2. Copia il file sull'host Linux che intendi utilizzare (utilizzando `scp` o qualche altro metodo).
3. Assegnare le autorizzazioni per eseguire lo script.

   ```
   chmod +x standalone-pre-requisite-tester-v1.25.0
   ```

4. Eseguire lo script utilizzando il seguente comando.

   ```
   ./standalone-pre-requisite-tester-v1.25.0 <--darksite>
   ```

   Aggiungere l'opzione "--darksite" solo se si esegue lo script su un host che non ha accesso a Internet. Alcuni test preliminari vengono saltati quando l'host non è connesso a Internet.

5. Lo script richiede l'indirizzo IP della macchina host di classificazione dei dati.

◦ Immettere l'indirizzo IP o il nome host.

6. Lo script chiede se è installato un agente Console.
   ◦ Immettere **N** se non è installato un agente Console.
   ◦ Inserisci **Y** se hai un agente Console installato. Quindi immettere l'indirizzo IP o il nome host dell'agente della console in modo che lo script di test possa testare questa connettività.
7. Lo script esegue una serie di test sul sistema e ne visualizza i risultati man mano che procede. Quando termina, scrive un registro della sessione in un file denominato `prerequisites-test-<timestamp>.log` nella directory `/opt/netapp/install_logs` .

**Risultato**

Se tutti i test dei prerequisiti sono stati eseguiti correttamente, puoi installare Data Classification sull'host quando sei pronto.

Se vengono rilevati problemi, questi vengono classificati come "Consigliati" o "Obbligatori" per essere risolti. I problemi consigliati sono in genere elementi che potrebbero rallentare le attività di scansione e categorizzazione della classificazione dei dati. Non è necessario correggere questi elementi, ma potresti volerli risolvere.

Se si verificano problemi "obbligatori", è necessario risolverli ed eseguire nuovamente lo script di test dei prerequisiti.

# 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.

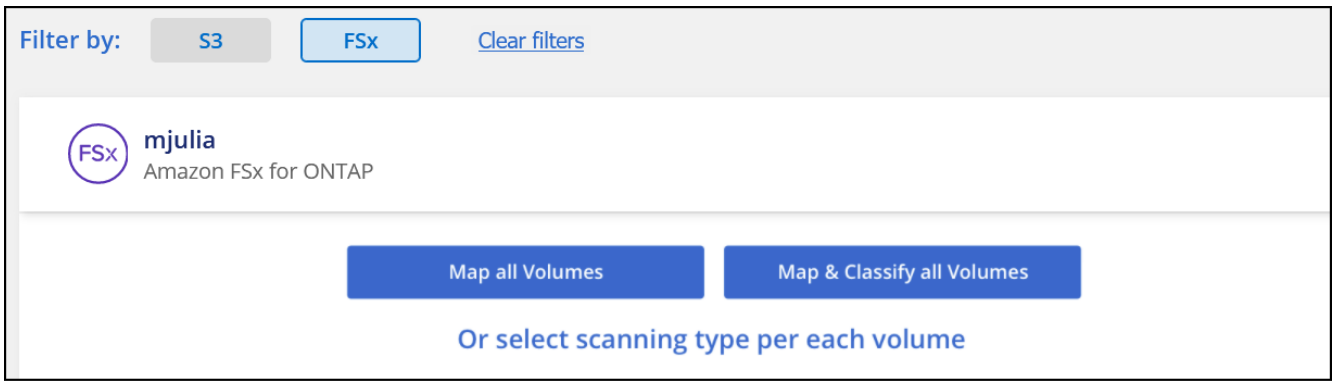
**Nota:** la distribuzione della classificazione dei dati in una posizione locale non è attualmente supportata durante la scansione dei volumi FSx.

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

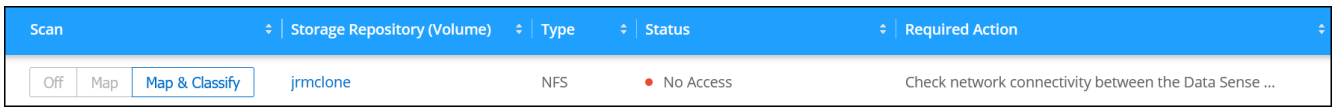
Assicurati che Data Classification possa accedere ai volumi controllando la rete, i gruppi di sicurezza e i criteri di esportazione.

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.

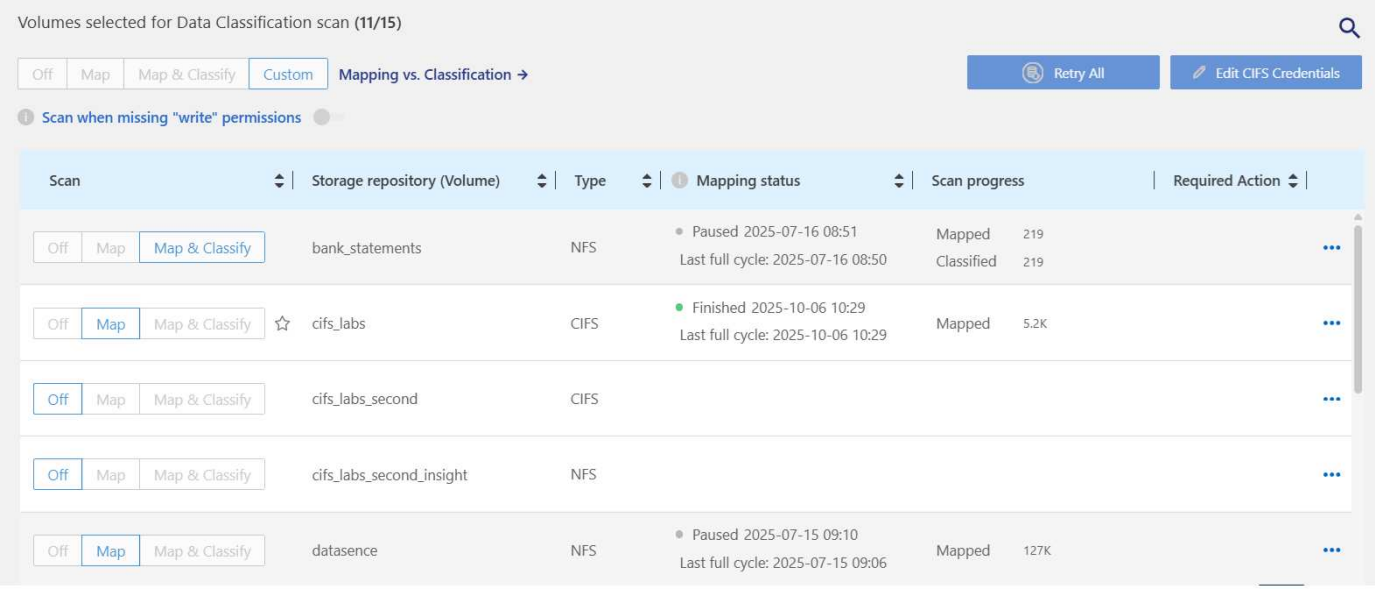
### Abilita e disabilita le scansioni sui volumi

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.

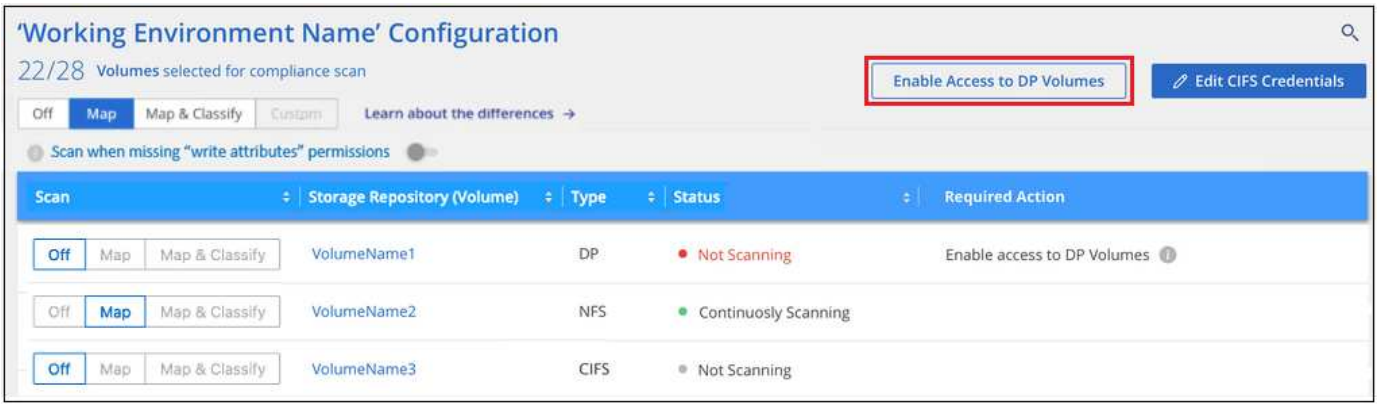
**Risultato**

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 .

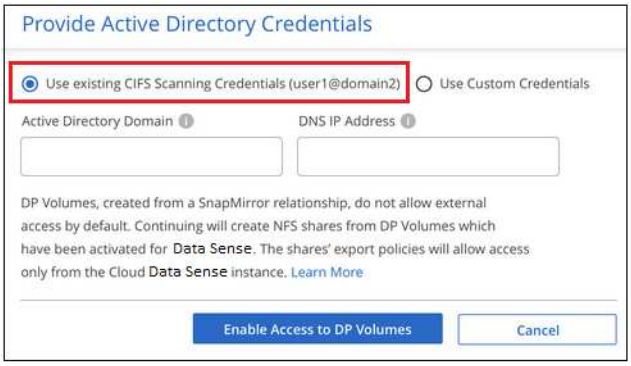
Inizialmente, l'elenco dei volumi identifica questi volumi come *Tipo* **DP** con *Stato* **Non in scansione** e *Azione richiesta* **Abilita accesso ai volumi DP**.

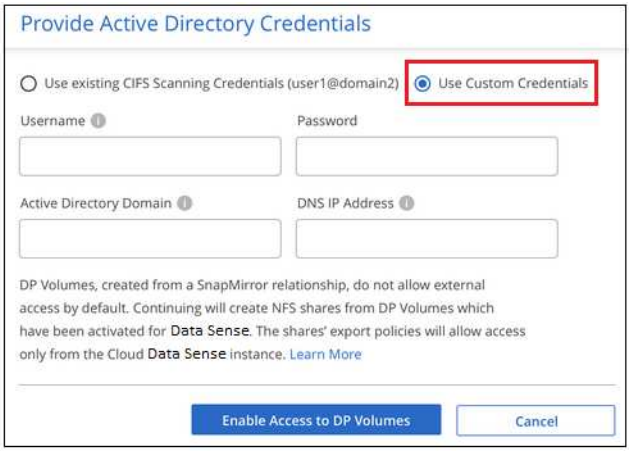



**Passi**

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**.

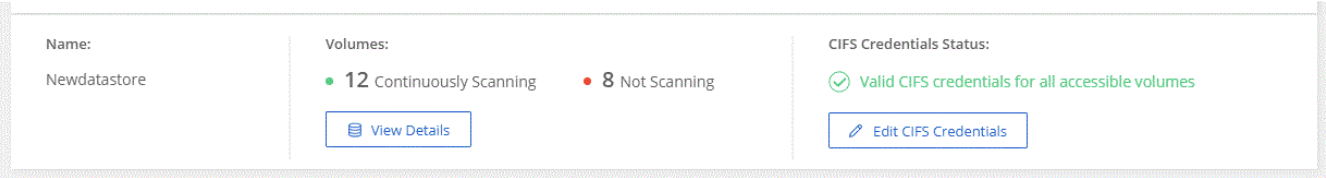
   a. Se si utilizza CIFS (SMB), assicurarsi che le credenziali di Active Directory siano corrette. Per ciascun sistema, selezionare **Modifica credenziali CIFS**, quindi immettere il nome utente e la password necessari a Data Classification per accedere ai volumi CIFS sul sistema.

      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.

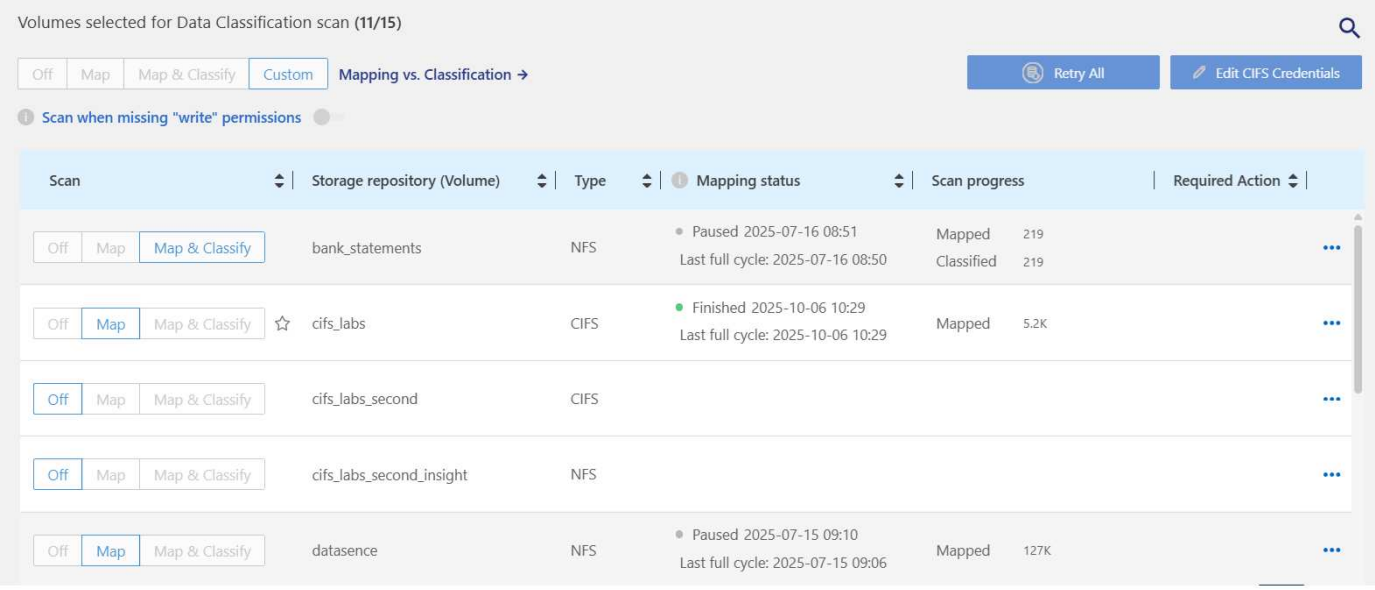
### Abilita o disabilita le scansioni sui volumi

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

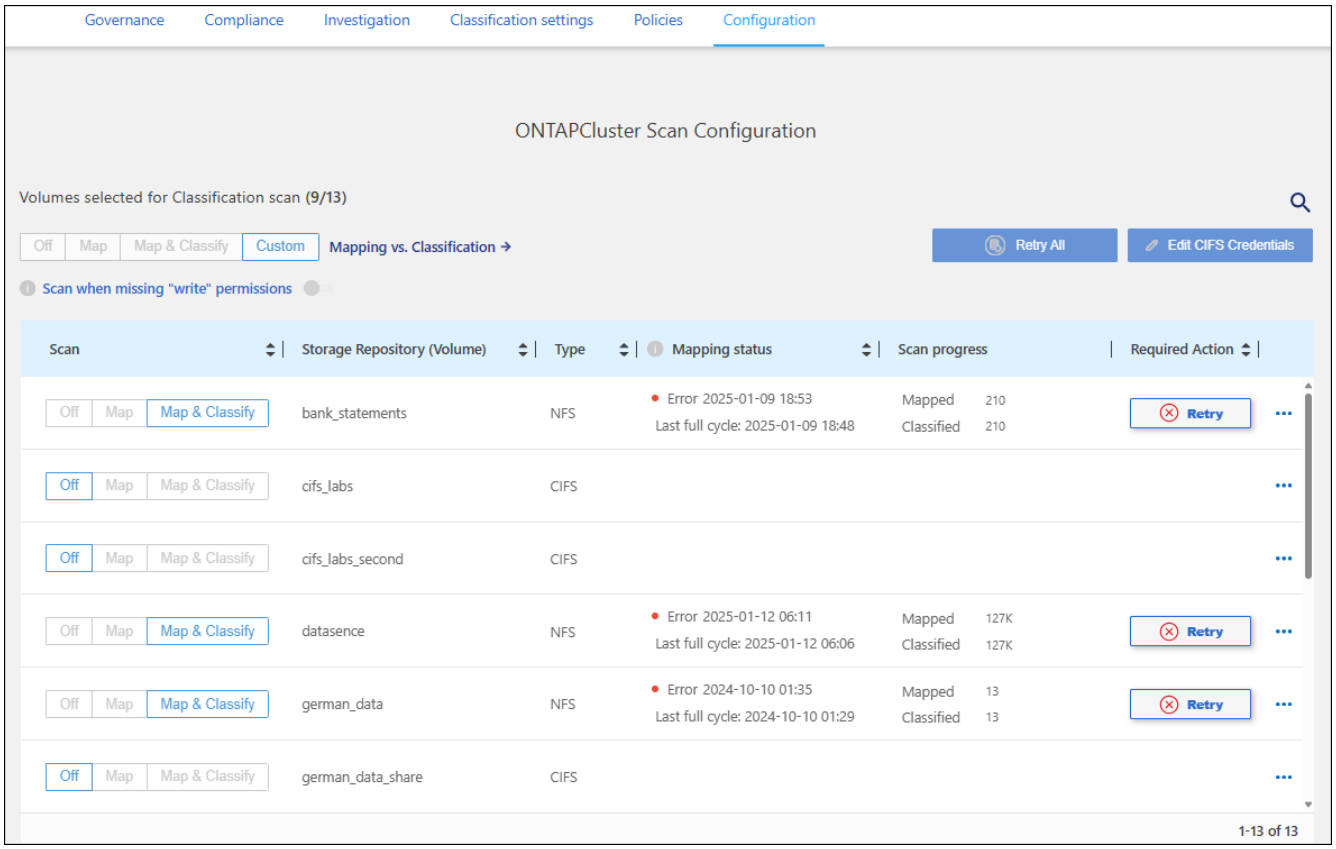
- Assicurarsi che vi sia una connessione di rete tra l'istanza di Data Classification e ciascuna rete che include volumi per Cloud Volumes ONTAP o cluster ONTAP on-prem.
- Assicurarsi che il gruppo di sicurezza per Cloud Volumes ONTAP consenta il traffico in entrata dall'istanza di classificazione dei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

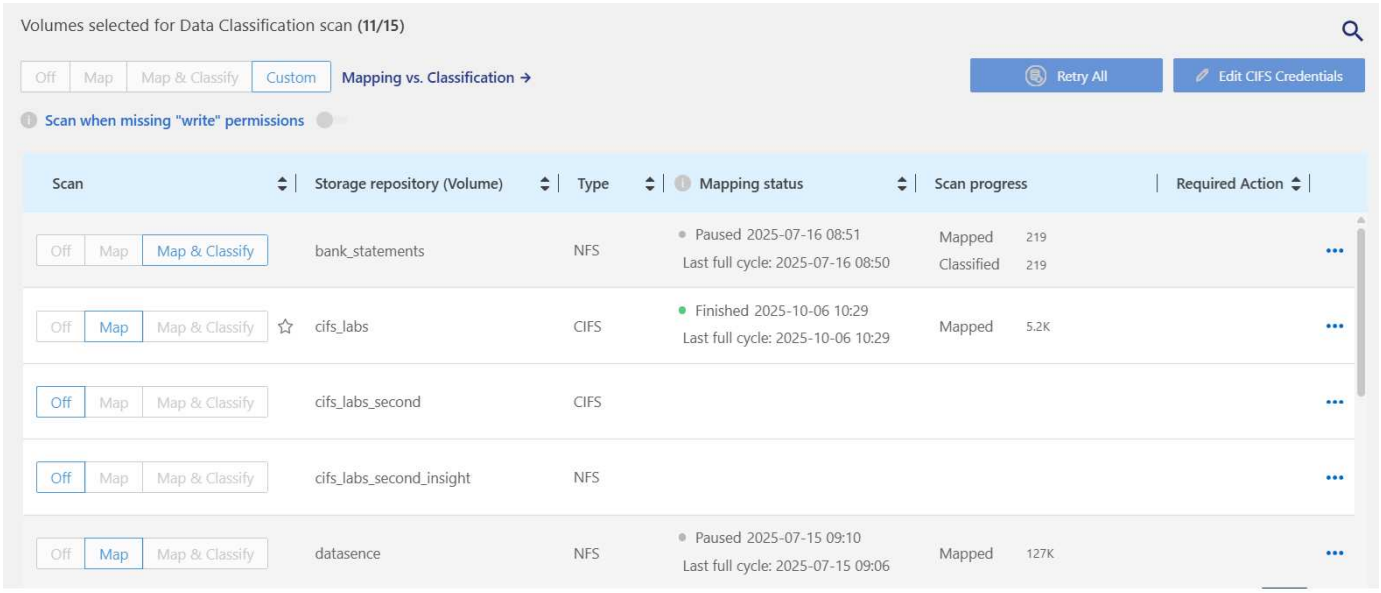
### Abilita o disabilita le scansioni sui volumi

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.

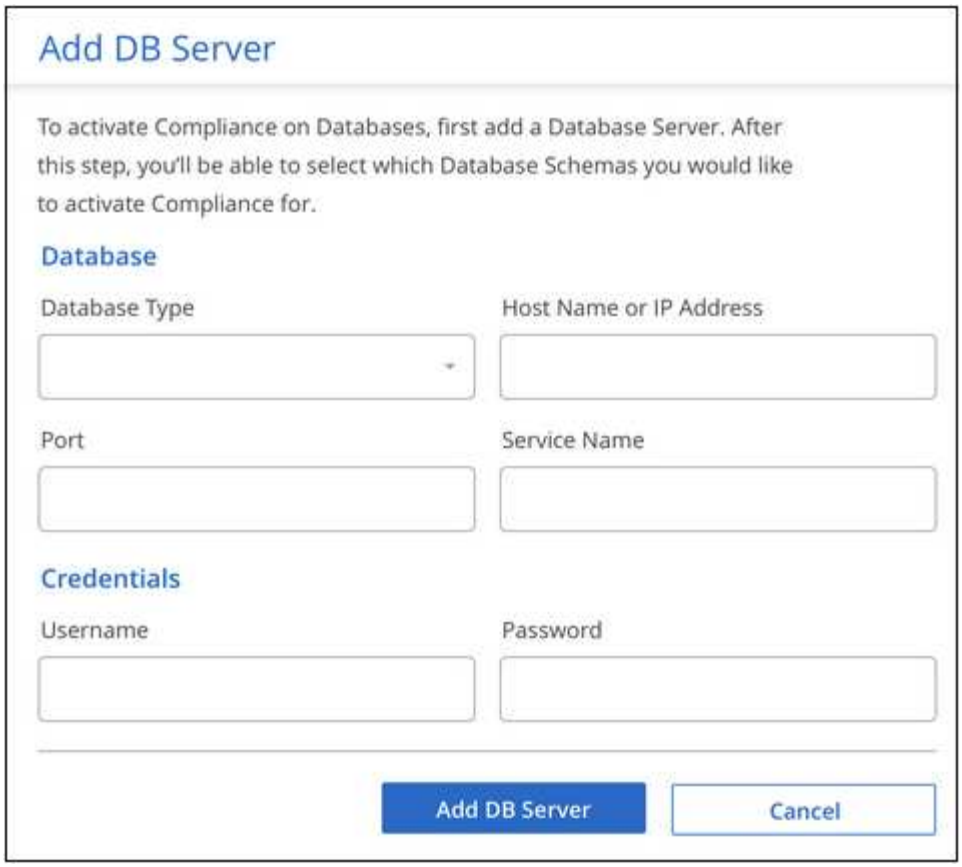
Se si esegue la scansione di schemi di database accessibili tramite Internet, è possibile"distribuire la classificazione dei dati nel cloud" O"distribuire la classificazione dei dati in una posizione locale dotata di accesso a Internet" .

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.

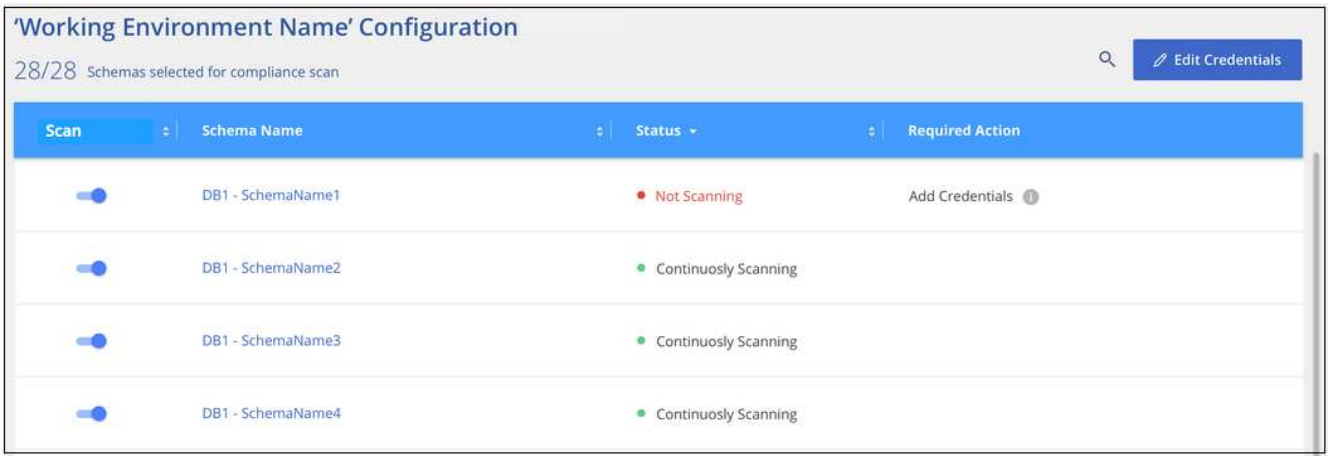
**Abilita e disabilita le scansioni sugli schemi del database**

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**.

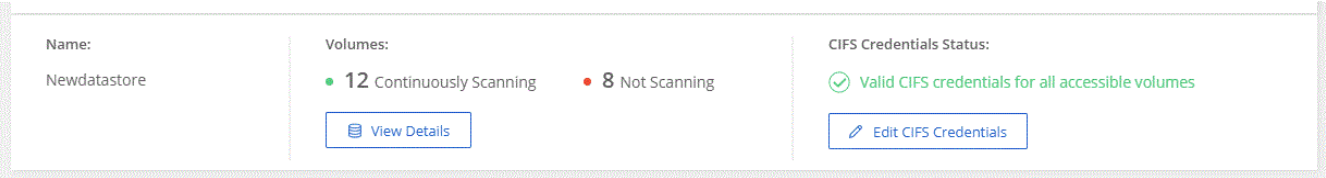
   a. Se si utilizza CIFS (SMB), assicurarsi che le credenziali di Active Directory siano corrette. Per ciascun sistema, selezionare **Modifica credenziali CIFS**, quindi immettere il nome utente e la password

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.

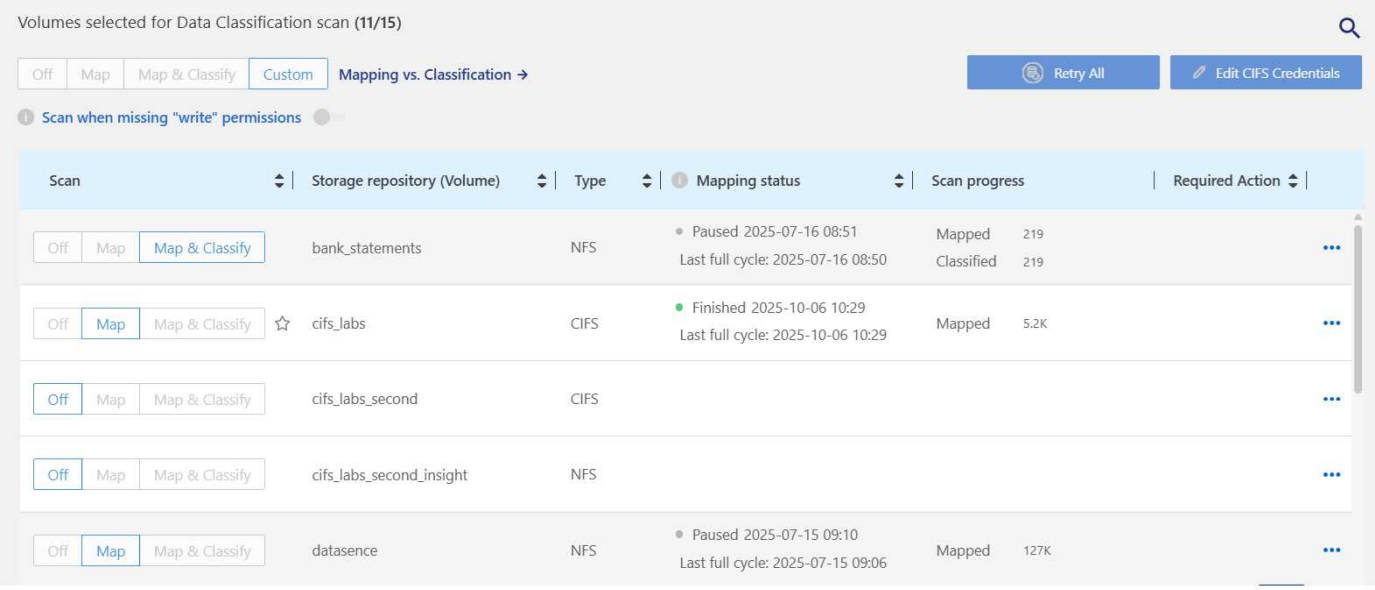
### Abilita e disabilita le scansioni sui volumi

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.

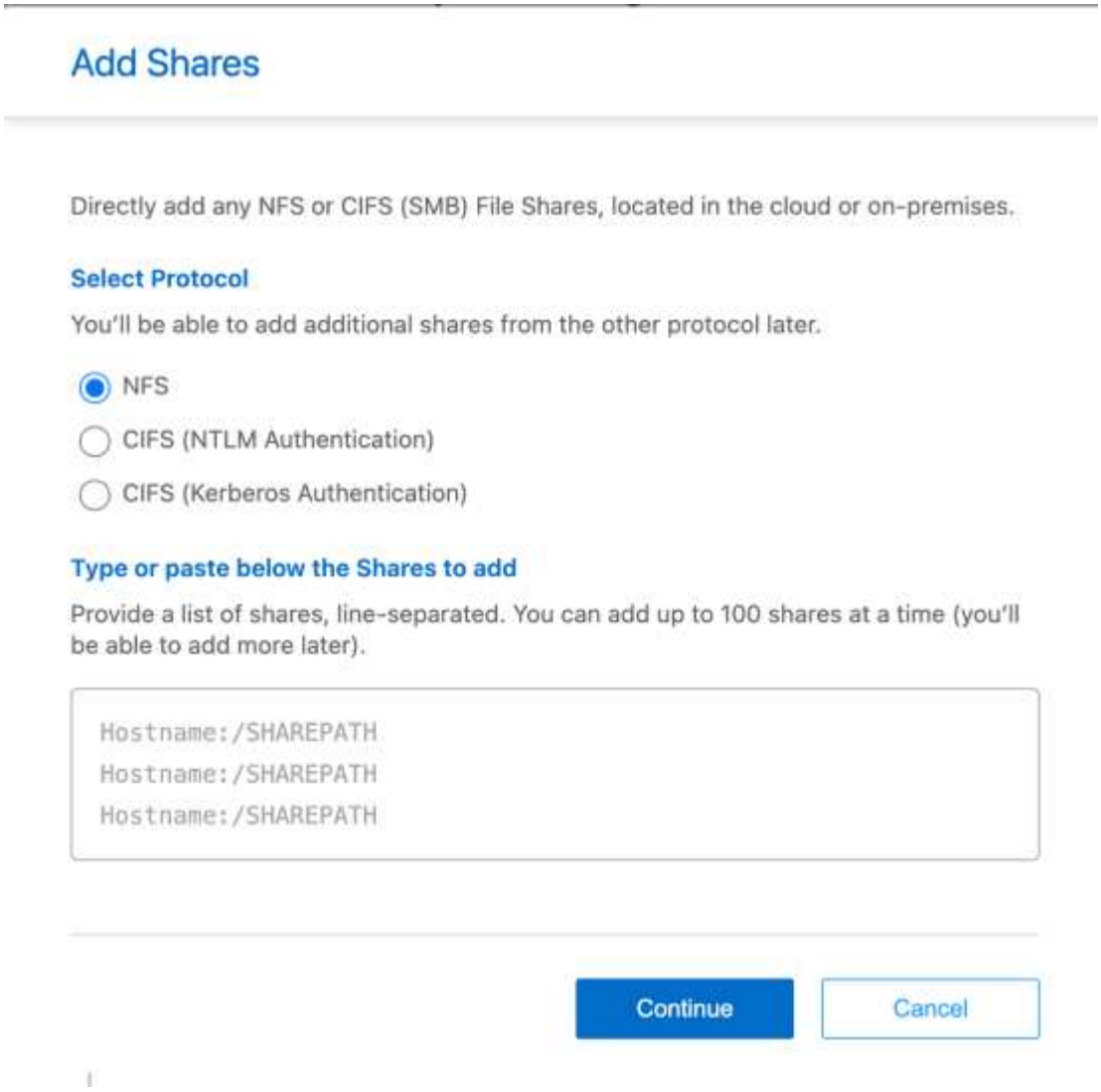
**Crea un gruppo di condivisione file**

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.

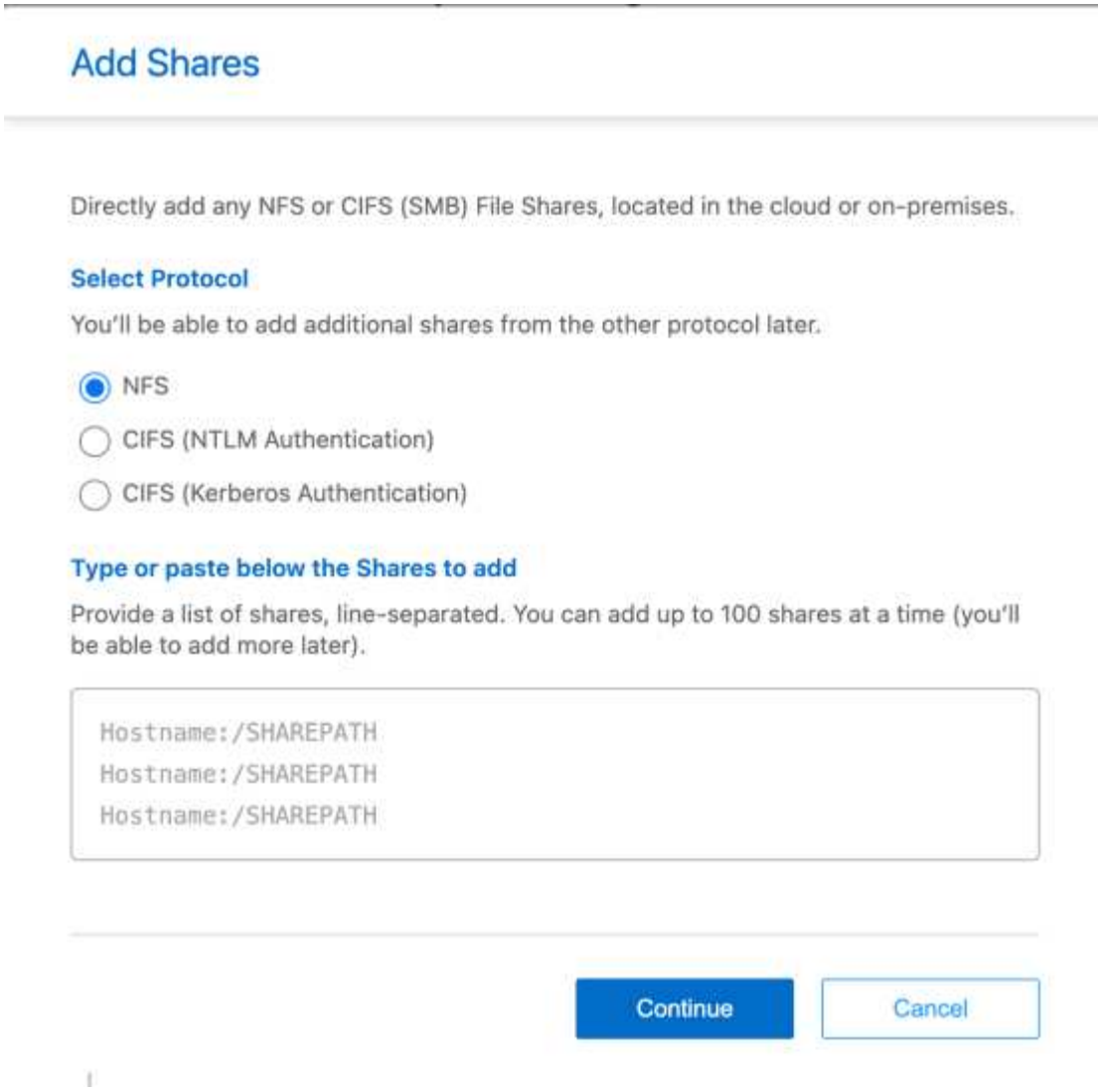
#### Modifica la configurazione del protocollo CIFS

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" .

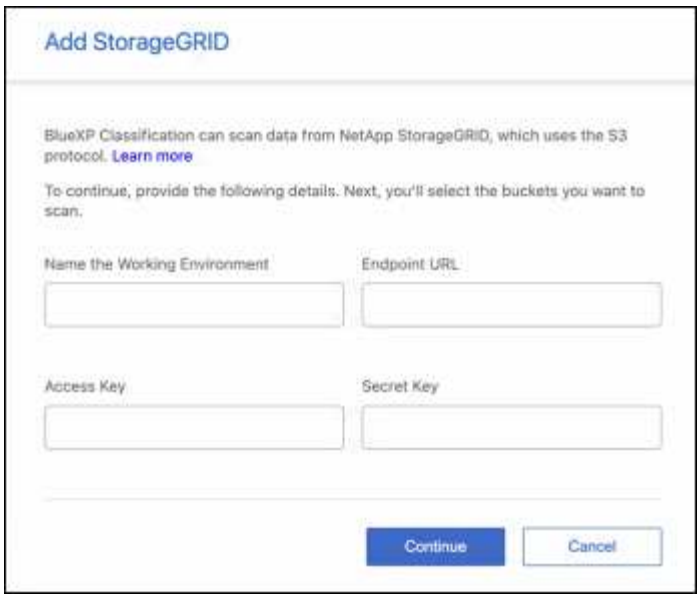
Se si stanno eseguendo la scansione dei dati da StorageGRID installato in un sito buio senza accesso a Internet, è necessario"distribuire la classificazione dei dati nella stessa posizione locale che non ha accesso a Internet" . Ciò richiede anche che l'agente della console venga distribuito nella stessa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

# Integra Active Directory con NetApp Data Classification

È possibile integrare un Active Directory globale con NetApp Data Classification per migliorare i risultati che Data Classification riporta sui proprietari dei file e sugli utenti e gruppi che hanno accesso ai file.

Quando si configurano determinate origini dati (elencate di seguito), è necessario immettere le credenziali di

Active Directory affinché Data Classification esegua la scansione dei volumi CIFS. Questa integrazione fornisce alla classificazione dei dati i dettagli sul proprietario del file e sulle autorizzazioni per i dati che risiedono in tali origini dati. Le credenziali di Active Directory immesse per tali origini dati potrebbero essere diverse dalle credenziali di Active Directory globali immesse qui. La classificazione dei dati cercherà in tutte le Active Directory integrate i dettagli degli utenti e delle autorizzazioni.

Questa integrazione fornisce informazioni aggiuntive nelle seguenti posizioni nella Classificazione dei dati:

- Puoi usare il "Proprietario del file""filtro" e visualizza i risultati nei metadati del file nel riquadro Indagine. Invece del proprietario del file contenente il SID (Security IDentifier), viene inserito il nome utente effettivo.

  È inoltre possibile visualizzare maggiori dettagli sul proprietario del file: nome dell'account, indirizzo e-mail e nome dell'account SAM, oppure visualizzare gli elementi di proprietà di tale utente.

- Puoi vedere"permessi completi del file" per ogni file e directory quando si fa clic sul pulsante "Visualizza tutte le autorizzazioni".
- Nel"Dashboard di governance" , il pannello Autorizzazioni aperte mostrerà un livello di dettaglio maggiore sui tuoi dati.

> I SID degli utenti locali e i SID di domini sconosciuti non vengono tradotti nel nome utente effettivo.

## Fonti dati supportate

Un'integrazione di Active Directory con Data Classification può identificare i dati dalle seguenti origini dati:

- Sistemi ONTAP on-premise
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSx per ONTAP

## Connettiti al tuo server Active Directory

Dopo aver distribuito Data Classification e attivato la scansione sulle origini dati, è possibile integrare Data Classification con Active Directory. È possibile accedere ad Active Directory tramite un indirizzo IP del server DNS o un indirizzo IP del server LDAP.

Le credenziali di Active Directory 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.

Per i volumi/condivisioni file CIFS, se si desidera assicurarsi che gli "ultimi orari di accesso" dei file non vengano modificati dalle scansioni di classificazione dei dati, l'utente deve disporre dell'autorizzazione di scrittura degli attributi. Se possibile, consigliamo di far sì che l'utente configurato in Active Directory faccia parte di un gruppo padre nell'organizzazione che dispone delle autorizzazioni per tutti i file.

**Requisiti**

- È necessario che sia già stata configurata una Active Directory per gli utenti della propria azienda.
- È necessario disporre delle informazioni per Active Directory:
  - Indirizzo IP del server DNS o più indirizzi IP

O

Indirizzo IP del server LDAP o più indirizzi IP

- Nome utente e password per accedere al server
- Nome di dominio (nome di Active Directory)
- Se stai utilizzando LDAP sicuro (LDAPS) o meno
- Porta del server LDAP (in genere 389 per LDAP e 636 per LDAP sicuro)

- Le seguenti porte devono essere aperte per la comunicazione in uscita da parte dell'istanza di classificazione dei dati:

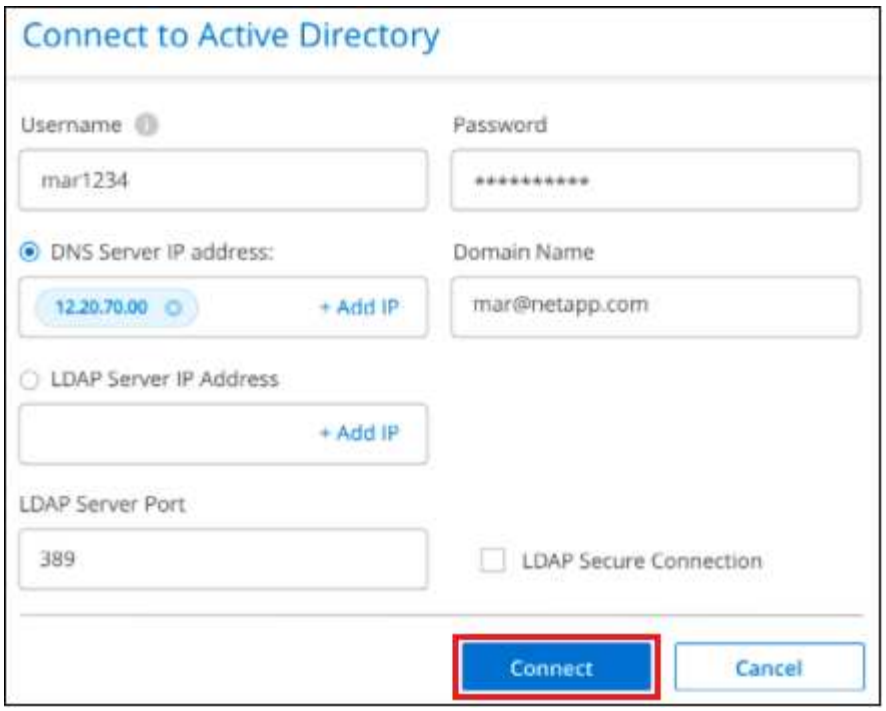
| Protocollo | Porta | Destinazione | Scopo |
|---|---|---|---|
| TCP e UDP | 389 | Directory attiva | LDAP |
| TCP | 636 | Directory attiva | LDAP su SSL |
| TCP | 3268 | Directory attiva | Catalogo globale |
| TCP | 3269 | Directory attiva | Catalogo globale su SSL |

**Passi**

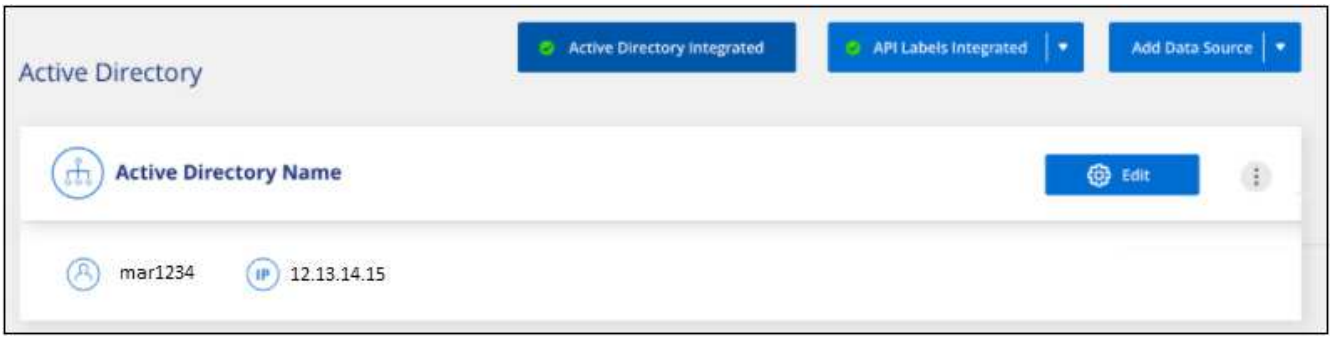
1. Nella pagina Configurazione classificazione dati, fare clic su **Aggiungi Active Directory**.


2. Nella finestra di dialogo Connetti ad Active Directory, immettere i dettagli di Active Directory e fare clic su **Connetti**.

   Se necessario, è possibile aggiungere più indirizzi IP selezionando **Aggiungi IP**.




La classificazione dei dati si integra con Active Directory e una nuova sezione viene aggiunta alla pagina Configurazione.




## Gestisci la tua integrazione con Active Directory

Se è necessario modificare dei valori nell'integrazione di Active Directory, fare clic sul pulsante **Modifica** e apportare le modifiche.

Puoi anche eliminare l'integrazione selezionando l'opzione pulsante quindi **Rimuovi Active Directory**.

## Informazioni sul copyright



## Informazioni sul marchio commerciale