Documentazione NetApp Data Classification

NetApp Data Classification

NetApp
November 03, 2025

Sommario

Documentazione NetApp Data Classification

Note di rilascio

Novità nella NetApp Data Classification

Scopri le novità di NetApp Data Classification.

06 ottobre 2025

Versione 1.47

La BlueXP classification è ora NetApp Data Classification

La BlueXP classification è stata rinominata NetApp Data Classification. Oltre al cambio di nome, è stata migliorata anche l'interfaccia utente.

BlueXP è ora NetApp Console

BlueXP è stato rinominato e riprogettato per riflettere meglio il suo ruolo nella gestione dell'infrastruttura dati.

NetApp Console offre una gestione centralizzata dei servizi di storage e dati in ambienti on-premise e cloud di livello aziendale, offrendo informazioni in tempo reale, flussi di lavoro più rapidi e amministrazione semplificata.

Per i dettagli su cosa è cambiato, vedere il "Note sulla versione NetApp Console" .

Esperienza di indagine migliorata

Trova e comprendi i tuoi dati più velocemente con nuovi filtri di ricerca, conteggi dei risultati per valore, informazioni in tempo reale che riepilogano i risultati principali e una tabella dei risultati aggiornata con colonne personalizzabili e un riquadro dei dettagli scorrevole.

Per ulteriori informazioni, consultare "Indagare i dati" .

Nuove dashboard di governance e conformità

Ottieni informazioni critiche più rapidamente grazie a widget intuitivi, immagini più chiare e prestazioni di caricamento migliorate. Per maggiori informazioni, vedere"Esamina le informazioni di governance sui tuoi dati" E"Visualizza le informazioni sulla conformità dei tuoi dati" .

Criteri per le query salvate (anteprima)

La classificazione dei dati ora consente di automatizzare la governance con azioni condizionali. È possibile creare regole di conservazione con eliminazione automatica e impostare notifiche e-mail periodiche, il tutto gestito da una pagina di query salvate aggiornate.

Per ulteriori informazioni, consultare "Creare politiche" .

Azioni (anteprima)

Assumi il controllo diretto dalla pagina Investigazione: elimina, sposta, copia o tagga i file singolarmente o in blocco, per una gestione e una correzione efficienti dei dati.

Per ulteriori informazioni, consultare "Indagare i dati" .

Supporto per Google Cloud NetApp Volumes

Data Classification ora supporta la scansione su Google Cloud NetApp Volumes. Aggiungi facilmente Google Cloud NetApp Volumes dalla NetApp Console per una scansione e una classificazione dei dati senza interruzioni. Per maggiori informazioni, vedere "Scansiona i Google Cloud NetApp Volumes".

11 agosto 2025

Versione 1.46

Questa versione di Data Classification include correzioni di bug e i seguenti aggiornamenti:

Informazioni dettagliate sugli eventi di scansione migliorate nella pagina di controllo

La pagina Audit ora supporta approfondimenti avanzati sugli eventi di scansione per la BlueXP classification. Nella pagina Audit ora viene visualizzato quando inizia la scansione di un sistema, lo stato dei sistemi e gli eventuali problemi. Gli stati delle condivisioni e dei sistemi sono disponibili solo per le scansioni di mappatura.

Per ulteriori informazioni sulla pagina Audit, vedere"Monitorare le operazioni NetApp Console" .

Supporto per RHEL 9.6

Questa versione aggiunge il supporto per Red Hat Enterprise Linux v9.6 per l'installazione manuale in sede della BlueXP classification, comprese le distribuzioni di siti oscuri.

I seguenti sistemi operativi richiedono l'utilizzo del motore container Podman e la versione BlueXP classification 1.30 o successiva: Red Hat Enterprise Linux versione 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 e 9.5.

14 luglio 2025

Versione 1.45

Questa versione BlueXP classification include modifiche al codice che ottimizzano l'utilizzo delle risorse e:

Flusso di lavoro migliorato per aggiungere condivisioni di file per la scansione

Il flusso di lavoro per aggiungere condivisioni di file a un gruppo di condivisione file è stato semplificato. Il processo ora differenzia anche il supporto del protocollo CIFS in base al tipo di autenticazione (Kerberos o NTLM).

Per ulteriori informazioni, consultare "Scansiona le condivisioni di file" .

Informazioni avanzate sul proprietario del file

Ora è possibile visualizzare maggiori informazioni sui proprietari dei file acquisiti nella scheda Indagine. Quando si visualizzano i metadati di un file nella scheda Indagine, individuare il proprietario del file, quindi selezionare **Visualizza dettagli** per visualizzare il nome utente, l'e-mail e il nome dell'account SAM. Puoi anche visualizzare altri oggetti di proprietà di questo utente. Questa funzionalità è disponibile solo per gli ambienti di lavoro con Active Directory.

Per ulteriori informazioni, consultare "Esamina i dati archiviati nella tua organizzazione" .

10 giugno 2025

Versione 1.44

Questa versione BlueXP classification include:

Tempi di aggiornamento migliorati per la dashboard di Governance

Sono stati migliorati i tempi di aggiornamento dei singoli componenti della dashboard di Governance. Nella tabella seguente viene mostrata la frequenza degli aggiornamenti per ciascun componente.

Componente	Tempi di aggiornamento
L'età dei dati	24 ore
Categorie	24 ore
Panoramica dei dati	5 minuti
File duplicati	2 ore
Tipi di file	24 ore
Dati non aziendali	2 ore
Permessi aperti	24 ore
Ricerche salvate	2 ore
Dati sensibili e permessi estesi	24 ore
Dimensione dei dati	24 ore
Dati obsoleti	2 ore
Principali repository di dati per livello di sensibilità	2 ore

È possibile visualizzare l'ora dell'ultimo aggiornamento e aggiornare manualmente i componenti File duplicati, Dati non aziendali, Ricerche salvate, Dati obsoleti e Repository dati principali per livello di sensibilità. Per ulteriori informazioni sulla dashboard di Governance, vedere"Visualizza i dettagli di governance sui dati archiviati nella tua organizzazione" .

Miglioramenti delle prestazioni e della sicurezza

Sono stati apportati miglioramenti per migliorare le prestazioni, il consumo di memoria e la sicurezza della classificazione BlueXP .

Correzioni di bug

Redis è stato aggiornato per migliorare l'affidabilità della BlueXP classification. La BlueXP classification ora utilizza Elasticsearch per migliorare l'accuratezza dei report sul conteggio dei file durante le scansioni.

12 maggio 2025

Versione 1.43

Questa versione di classificazione dei dati include:

Dare priorità alle scansioni di classificazione

La classificazione dei dati supporta la possibilità di dare priorità alle scansioni Map & Classify oltre alle scansioni di sola mappatura, consentendo di selezionare quali scansioni completare per prime. La definizione delle priorità delle scansioni Map & Classify è supportata durante e prima dell'inizio delle scansioni. Se si sceglie di dare priorità a una scansione mentre è in corso, verrà data priorità sia alla scansione di mappatura che a quella di classificazione.

Per ulteriori informazioni, consultare "Dare priorità alle scansioni" .

Supporto per le categorie di dati di identificazione personale (PII) canadesi

Le scansioni di classificazione dei dati identificano le categorie di dati PII canadesi. Queste categorie includono informazioni bancarie, numeri di passaporto, numeri di previdenza sociale, numeri di patente di guida e numeri di tessera sanitaria per tutte le province e i territori canadesi.

Per ulteriori informazioni, consultare "Categorie di dati personali" .

Classificazione personalizzata (anteprima)

La classificazione dei dati supporta classificazioni personalizzate per le scansioni Map & Classify. Grazie alle classificazioni personalizzate, puoi adattare le scansioni di classificazione dei dati per acquisire dati specifici per la tua organizzazione utilizzando espressioni regolari. Questa funzionalità è attualmente in anteprima.

Per ulteriori informazioni, consultare "Aggiungi classificazioni personalizzate" .

Scheda Ricerche salvate

La scheda **Criteri** è stata rinominata**"Ricerche salvate"** . La funzionalità è invariata.

Invia eventi di scansione alla pagina Audit

La classificazione dei dati supporta l'invio di eventi di classificazione (quando una scansione viene avviata e quando termina) al"Pagina di controllo della console NetApp" .

Aggiornamenti di sicurezza

- Il pacchetto Keras è stato aggiornato, mitigando le vulnerabilità (BDSA-2025-0107 e BDSA-2025-1984).
- La configurazione dei container Docker è stata aggiornata. Il contenitore non ha più accesso alle interfacce di rete dell'host per creare pacchetti di rete non elaborati. Riducendo gli accessi non necessari, l'aggiornamento attenua i potenziali rischi per la sicurezza.

Miglioramenti delle prestazioni

Sono stati implementati miglioramenti al codice per ridurre l'utilizzo della RAM e migliorare le prestazioni complessive della classificazione dei dati.

Correzioni di bug

Sono stati risolti i bug che causavano il fallimento delle scansioni StorageGRID , il mancato caricamento delle opzioni di filtro della pagina di indagine e il mancato download della valutazione Data Discovery per le valutazioni di grandi volumi.

14 aprile 2025

Versione 1.42

Questa versione BlueXP classification include:

Scansione in blocco per ambienti di lavoro

La BlueXP classification supporta operazioni in blocco per ambienti di lavoro. È possibile scegliere di abilitare le scansioni di mappatura, abilitare le scansioni di mappatura e classificazione, disabilitare le scansioni o creare una configurazione personalizzata tra i volumi nell'ambiente di lavoro. Se si effettua una selezione per un singolo volume, questa sostituisce la selezione in blocco. Per eseguire un'operazione in blocco, vai alla pagina **Configurazione** ed effettua la tua selezione.

Scarica localmente il rapporto di indagine

La BlueXP classification supporta la possibilità di scaricare localmente i report di indagine sui dati per visualizzarli nel browser. Se si sceglie l'opzione locale, l'analisi dei dati è disponibile solo nel formato CSV e visualizza solo le prime 10.000 righe di dati.

Per ulteriori informazioni, consultare "Esamina i dati archiviati nella tua organizzazione con la BlueXP classification" .

10 marzo 2025

Versione 1.41

Questa versione BlueXP classification include miglioramenti generali e correzioni di bug. Include anche:

Stato della scansione

La BlueXP classification tiene traccia in tempo reale dell'avanzamento delle scansioni di mappatura e classificazione *iniziali* su un volume. Barre progressive separate tracciano le scansioni di mappatura e classificazione, presentando una percentuale del totale dei file scansionati. È anche possibile passare il mouse sulla barra di avanzamento per visualizzare il numero di file scansionati e il numero totale di file. Monitorare lo stato delle scansioni consente di ottenere informazioni più approfondite sull'avanzamento della scansione, consentendo di pianificare meglio le scansioni e di comprendere l'allocazione delle risorse.

Per visualizzare lo stato delle scansioni, vai a **Configurazione** nella BlueXP classification , quindi seleziona la **configurazione dell'ambiente di lavoro**. L'avanzamento viene visualizzato in riga per ogni volume.

19 febbraio 2025

Versione 1.40

Questa versione BlueXP classification include i seguenti aggiornamenti.

Supporto per RHEL 9.5

Questa versione fornisce supporto per Red Hat Enterprise Linux v9.5 oltre alle versioni supportate in precedenza. Ciò è applicabile a qualsiasi installazione manuale in sede della BlueXP classification, comprese le distribuzioni in dark site.

I seguenti sistemi operativi richiedono l'utilizzo del motore container Podman e la versione BlueXP classification 1.30 o successiva: Red Hat Enterprise Linux versione 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 e 9.5.

Dare priorità alle scansioni di sola mappatura

Quando si eseguono scansioni di sola mappatura, è possibile dare priorità alle scansioni più importanti. Questa funzionalità è utile quando si hanno molti ambienti di lavoro e si desidera garantire che le scansioni ad alta priorità vengano completate per prime.

Per impostazione predefinita, le scansioni vengono messe in coda in base all'ordine in cui vengono avviate. Grazie alla possibilità di dare priorità alle scansioni, è possibile spostarle in cima alla coda. È possibile dare priorità a più scansioni. La priorità viene assegnata in base all'ordine "first-in, first-out", ovvero la prima scansione a cui si dà priorità viene spostata in cima alla coda; la seconda scansione a cui si dà priorità diventa la seconda nella coda e così via.

La priorità viene concessa una sola volta. Le nuove scansioni automatiche dei dati di mappatura avvengono nell'ordine predefinito.

La priorità è limitata a"scansioni solo di mappatura" ; non è disponibile per le scansioni di mappatura e classificazione.

Per ulteriori informazioni, consultare "Dare priorità alle scansioni" .

Riprova tutte le scansioni

La BlueXP classification supporta la possibilità di ripetere in batch tutte le scansioni non riuscite.

È possibile ripetere le scansioni in un'operazione batch con la funzione **Riprova tutto**. Se le scansioni di

classificazione non riescono a causa di un problema temporaneo, ad esempio un'interruzione di rete, è possibile riprovare tutte le scansioni contemporaneamente premendo un pulsante anziché riprovarle singolarmente. È possibile ripetere la scansione tutte le volte che si desidera.

Per riprovare tutte le scansioni:

1. Dal menu BlueXP classification , selezionare **Configurazione**.
2. Per riprovare tutte le scansioni non riuscite, seleziona **Riprova tutte le scansioni**.

Miglioramento della precisione del modello di categorizzazione

L'accuratezza del modello di apprendimento automatico per"categorie predefinite" è migliorato dell'11%.

22 gennaio 2025

Versione 1.39

Questa versione BlueXP classification aggiorna il processo di esportazione per il report di indagine sui dati. Questo aggiornamento dell'esportazione è utile per eseguire analisi aggiuntive sui dati, creare visualizzazioni aggiuntive sui dati o condividere i risultati dell'indagine sui dati con altri.

In precedenza, l'esportazione del report di indagine sui dati era limitata a 10.000 righe. Con questa versione il limite è stato rimosso, così puoi esportare tutti i tuoi dati. Questa modifica ti consente di esportare più dati dai tuoi report di indagine sui dati, garantendoti maggiore flessibilità nell'analisi dei dati.

È possibile scegliere l'ambiente di lavoro, i volumi, la cartella di destinazione e il formato JSON o CSV. Il nome del file esportato include un timestamp per aiutarti a identificare quando i dati sono stati esportati.

Gli ambienti di lavoro supportati includono:

- Cloud Volumes ONTAP
- FSx per ONTAP
- ONTAP
- Condividi gruppo

L'esportazione dei dati dal report di indagine sui dati presenta le seguenti limitazioni:

- Il numero massimo di record da scaricare è 500 milioni per tipo (file, directory e tabelle)
- Si prevede che l'esportazione di un milione di record richiederà circa 35 minuti.

Per i dettagli sull'indagine dei dati e sul rapporto, vedere "Esamina i dati archiviati nella tua organizzazione" .

16 dicembre 2024

Versione 1.38

Questa versione BlueXP classification include miglioramenti generali e correzioni di bug.

4 novembre 2024

Versione 1.37

Questa versione BlueXP classification include i seguenti aggiornamenti.

Supporto per RHEL 8.10

Questa versione fornisce supporto per Red Hat Enterprise Linux v8.10 oltre alle versioni supportate in precedenza. Ciò è applicabile a qualsiasi installazione manuale in sede della BlueXP classification, comprese le distribuzioni in dark site.

I seguenti sistemi operativi richiedono l'utilizzo del motore container Podman e la BlueXP classification versione 1.30 o successiva: Red Hat Enterprise Linux versione 8.8, 8.10, 9.0, 9.1, 9.2, 9.3 e 9.4.

Scopri di più su "BlueXP classification" .

Supporto per NFS v4.1

Questa versione fornisce supporto per NFS v4.1 oltre alle versioni supportate in precedenza.

Scopri di più su "BlueXP classification" .

10 ottobre 2024

Versione 1.36

Supporto per RHEL 9.4

Questa versione fornisce supporto per Red Hat Enterprise Linux v9.4 oltre alle versioni supportate in precedenza. Ciò è applicabile a qualsiasi installazione manuale in sede della BlueXP classification, comprese le distribuzioni in dark site.

I seguenti sistemi operativi richiedono l'utilizzo del motore container Podman e la BlueXP classification versione 1.30 o successiva: Red Hat Enterprise Linux versione 8.8, 9.0, 9.1, 9.2, 9.3 e 9.4.

Scopri di più su "Panoramica delle distribuzioni BlueXP classification" .

Prestazioni di scansione migliorate

Questa versione offre prestazioni di scansione migliorate.

2 settembre 2024

Versione 1.35

Scansiona i dati StorageGRID

La BlueXP classification supporta la scansione dei dati in StorageGRID.

Per i dettagli, fare riferimento a"Scansiona i dati StorageGRID" .

05 agosto 2024

Versione 1.34

Questa versione BlueXP classification include il seguente aggiornamento.

Passaggio da CentOS a Ubuntu

La BlueXP classification ha aggiornato il suo sistema operativo Linux per Microsoft Azure e Google Cloud

Platform (GCP) da CentOS 7.9 a Ubuntu 22.04.

Per i dettagli sulla distribuzione, fare riferimento a "Installare su un host Linux con accesso a Internet e preparare il sistema host Linux" .

01 luglio 2024

Versione 1.33

Ubuntu supportato

Questa versione supporta la piattaforma Linux Ubuntu 24.04.

Le scansioni di mappatura raccolgono metadati

I seguenti metadati vengono estratti dai file durante le scansioni di mappatura e vengono visualizzati nelle dashboard Governance, Conformità e Investigazione:

- Ambiente di lavoro
- Tipo di ambiente di lavoro
- 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

Dati aggiuntivi nei dashboard

Questa versione aggiorna i dati visualizzati nelle dashboard Governance, Conformità e Investigazione durante le scansioni di mappatura.

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

05 giugno 2024

Versione 1.32

Nuova colonna Stato di mappatura nella pagina Configurazione

Questa versione ora mostra una nuova colonna Stato mappatura nella pagina Configurazione. La nuova colonna ti aiuta a identificare se la mappatura è in esecuzione, in coda, in pausa o altro.

Per spiegazioni sugli stati, vedere "Modifica le impostazioni di scansione" .

15 maggio 2024

Versione 1.31

La classificazione è disponibile come servizio principale all'interno di BlueXP

La BlueXP classification è ora disponibile come funzionalità principale di BlueXP senza costi aggiuntivi per un massimo di 500 TiB di dati scansionati per connettore. Non è richiesta alcuna licenza di classificazione o abbonamento a pagamento. Poiché con questa nuova versione concentriamo la funzionalità BlueXP classification sulla scansione dei sistemi di storage NetApp , alcune funzionalità legacy saranno disponibili solo per i clienti che in precedenza avevano pagato una licenza. L'utilizzo di tali funzionalità legacy scadrà quando il contratto a pagamento raggiungerà la data di scadenza.

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" .

01 aprile 2024

Versione 1.30

Aggiunto supporto per la BlueXP classification

Questa versione fornisce supporto per Red Hat Enterprise Linux v8.8 e v9.3, oltre alla versione 9.x precedentemente supportata, che richiede Podman anziché il motore Docker. Ciò è applicabile a qualsiasi installazione manuale in sede della BlueXP classification.

I seguenti sistemi operativi richiedono l'utilizzo del motore container Podman e la BlueXP classification versione 1.30 o successiva: Red Hat Enterprise Linux versione 8.8, 9.0, 9.1, 9.2 e 9.3.

Scopri di più su "Panoramica delle distribuzioni BlueXP classification" .

La BlueXP classification è supportata se si installa il connettore su un host RHEL 8 o 9 residente in locale. Non è supportato se l'host RHEL 8 o 9 risiede in AWS, Azure o Google Cloud.

Opzione per attivare la raccolta del registro di controllo rimossa

L'opzione per attivare la raccolta dei registri di controllo è stata disabilitata.

Velocità di scansione migliorata

Sono state migliorate le prestazioni di scansione sui nodi scanner secondari. È possibile aggiungere altri nodi scanner se è necessaria maggiore potenza di elaborazione per le scansioni. Per i dettagli, fare riferimento a "Installa la BlueXP classification su un host che ha accesso a Internet" .

Aggiornamenti automatici

Se hai distribuito la BlueXP classification su un sistema con accesso a Internet, il sistema si aggiorna automaticamente. In precedenza, l'aggiornamento avveniva dopo un periodo di tempo specifico trascorso dall'ultima attività dell'utente. Con questa versione, la BlueXP classification viene aggiornata automaticamente se l'ora locale è compresa tra l'1:00 e le 5:00. Se l'ora locale è al di fuori di questi orari, l'aggiornamento avviene una volta trascorso un periodo di tempo specifico dall'ultima attività dell'utente. Per i dettagli, fare riferimento a "Installa su un host Linux con accesso a Internet" .

Se hai implementato la BlueXP classification senza accesso a Internet, dovrai effettuare l'aggiornamento

manualmente. Per i dettagli, fare riferimento a "Installa la BlueXP classification su un host Linux senza accesso a Internet" .

04 marzo 2024

Versione 1.29

Ora puoi escludere i dati di scansione che risiedono in determinate directory di origine dati

Se si desidera che la BlueXP classification escluda i dati di scansione che risiedono in determinate directory di origine dati, è possibile aggiungere questi nomi di directory a un file di configurazione elaborato BlueXP classification . Questa funzione consente di evitare la scansione di directory non necessarie o che restituirebbero risultati falsi positivi sui dati personali.

"Saperne di più" .

Il supporto per istanze Extra Large è ora qualificato

Se hai bisogno BlueXP classification per analizzare più di 250 milioni di file, puoi utilizzare un'istanza Extra Large nella tua distribuzione cloud o nell'installazione locale. Questo tipo di sistema può analizzare fino a 500 milioni di file.

"Saperne di più" .

10 gennaio 2024

Versione 1.27

I risultati della pagina di indagine mostrano la dimensione totale oltre al numero totale di elementi

I risultati filtrati nella pagina Indagine mostrano la dimensione totale degli elementi oltre al numero totale di file. Può essere utile quando si spostano file, si eliminano file e altro ancora.

Configurare ID di gruppo aggiuntivi come "Aperti all'organizzazione"

Ora è possibile configurare gli ID di gruppo in NFS in modo che vengano considerati "Aperti all'organizzazione" direttamente dalla BlueXP classification se il gruppo non era stato inizialmente impostato con tale autorizzazione. Tutti i file e le cartelle a cui sono allegati questi ID di gruppo verranno visualizzati come "Aperti all'organizzazione" nella pagina Dettagli indagine. Scopri come"aggiungere ID di gruppo aggiuntivi come "aperti all'organizzazione"" .

14 dicembre 2023

Versione 1.26.6

Questa versione include alcuni piccoli miglioramenti.

La versione ha inoltre rimosso le seguenti opzioni:

- L'opzione per attivare la raccolta dei registri di controllo è stata disabilitata.
- Durante l'indagine di Directories, l'opzione per calcolare il numero di dati di informazioni personali identificabili (PII) da parte di Directories non è disponibile. Fare riferimento a "Esamina i dati archiviati nella tua organizzazione" .
- L'opzione per integrare i dati tramite etichette di Azure Information Protection (AIP) è stata disabilitata.

06 novembre 2023

Versione 1.26.3

In questa versione sono stati risolti i seguenti problemi

- Risolta un'incongruenza nella presentazione del numero di file scansionati dal sistema nelle dashboard.
- Migliorato il comportamento della scansione gestendo e segnalando file e directory con caratteri speciali nel nome e nei metadati.

04 ottobre 2023

Versione 1.26

Supporto per installazioni on-premise della BlueXP classification su RHEL versione 9

Le versioni 8 e 9 di Red Hat Enterprise Linux non supportano il motore Docker, necessario per l'installazione BlueXP classification . Ora supportiamo l'installazione BlueXP classification su RHEL 9.0, 9.1 e 9.2 utilizzando Podman versione 4 o successiva come infrastruttura container. Se il tuo ambiente richiede l'utilizzo delle versioni più recenti di RHEL, ora puoi installare la BlueXP classification (versione 1.26 o successiva) quando utilizzi Podman.

Al momento non supportiamo installazioni di dark site o ambienti di scansione distribuiti (utilizzando un nodo scanner master e remoto) quando si utilizza RHEL 9.x.

05 settembre 2023

Versione 1.25

Piccole e medie implementazioni temporaneamente non disponibili

Quando si distribuisce un'istanza di BlueXP classification in AWS, l'opzione per selezionare **Distribuisci > Configurazione** e scegliere un'istanza di piccole o medie dimensioni non è al momento disponibile. È comunque possibile distribuire l'istanza utilizzando le dimensioni dell'istanza di grandi dimensioni selezionando **Distribuisci > Distribuisci**.

Applica tag a un massimo di 100.000 elementi dalla pagina Risultati dell'indagine

In passato era possibile applicare i tag solo a una pagina alla volta nella pagina Risultati dell'indagine (20 elementi). Ora puoi selezionare **tutti** gli elementi nelle pagine dei risultati dell'indagine e applicare tag a tutti gli elementi, fino a 100.000 elementi alla volta.

Identifica i file duplicati con una dimensione minima di 1 MB

La BlueXP classification veniva utilizzata per identificare i file duplicati solo quando i file erano di 50 MB o più grandi. Ora è possibile identificare i file duplicati che iniziano con 1 MB. È possibile utilizzare i filtri "Dimensioni file" insieme a "Duplicati" della pagina Indagine per vedere quali file di una determinata dimensione sono duplicati nel proprio ambiente.

17 luglio 2023

Versione 1.24

La BlueXP classification identifica due nuovi tipi di dati personali tedeschi

La BlueXP classification può identificare e categorizzare i file che contengono i seguenti tipi di dati:

- Carta d'identità tedesca (Personalausweisnummer)
- Numero di previdenza sociale tedesco (Sozialversicherungsnummer)

"Visualizza tutti i tipi di dati personali che la BlueXP classification può identificare nei tuoi dati" .

La BlueXP classification è completamente supportata in modalità limitata e modalità privata

La BlueXP classification è ora completamente supportata nei siti senza accesso a Internet (modalità privata) e con accesso a Internet in uscita limitato (modalità limitata). "Scopri di più sulle modalità di distribuzione BlueXP per il connettore" .

Possibilità di saltare le versioni durante l'aggiornamento di un'installazione in modalità privata della BlueXP classification

Ora puoi effettuare l'aggiornamento a una versione più recente della BlueXP classification anche se non è sequenziale. Ciò significa che non è più necessario l'attuale limite di aggiornamento BlueXP classification di una versione alla volta. Questa funzionalità è rilevante a partire dalla versione 1.24.

L'API BlueXP classification è ora disponibile

L'API BlueXP classification consente di eseguire azioni, creare query ed esportare informazioni sui dati sottoposti a scansione. La documentazione interattiva è disponibile tramite Swagger. La documentazione è suddivisa in più categorie, tra cui Indagine, Conformità, Governance e Configurazione. Ogni categoria è un riferimento alle schede nell'interfaccia utente BlueXP classification .

"Scopri di più sulle API BlueXP classification" .

06 giugno 2023

Versione 1.23

Ora è supportato il giapponese durante la ricerca dei nomi degli interessati

Ora è possibile inserire nomi giapponesi quando si cerca il nome di un soggetto in risposta a una richiesta di accesso ai dati (DSAR). Puoi generare un"Rapporto sulla richiesta di accesso ai dati dell'interessato" con le informazioni risultanti. Puoi anche inserire nomi giapponesi nel"Filtro "Interessato" nella pagina Indagine sui dati" per identificare i file che contengono il nome del soggetto.

Ubuntu è ora una distribuzione Linux supportata su cui è possibile installare la BlueXP classification

Ubuntu 22.04 è stato qualificato come sistema operativo supportato per la BlueXP classification. È possibile installare la BlueXP classification su un host Ubuntu Linux nella propria rete oppure su un host Linux nel cloud utilizzando la versione 1.23 del programma di installazione. "Scopri come installare la BlueXP classification su un host con Ubuntu installato" .

Red Hat Enterprise Linux 8.6 e 8.7 non sono più supportati con le nuove installazioni BlueXP classification

Queste versioni non sono supportate con le nuove distribuzioni perché Red Hat non supporta più Docker, che è un prerequisito. Se disponi di una macchina BlueXP classification esistente in esecuzione su RHEL 8.6 o 8.7, NetApp continuerà a supportare la tua configurazione.

La BlueXP classification può essere configurata come un FPolicy Collector per ricevere eventi FPolicy dai sistemi ONTAP

È possibile abilitare la raccolta dei registri di controllo degli accessi ai file sul sistema BlueXP classification per gli eventi di accesso ai file rilevati sui volumi negli ambienti di lavoro. La BlueXP classification può acquisire i seguenti tipi di eventi FPolicy e gli utenti che hanno eseguito le azioni sui file: creazione, lettura, scrittura, eliminazione, ridenominazione, modifica proprietario/autorizzazioni e modifica SACL/DACL.

Le licenze BYOL di Data Sense sono ora supportate nei siti oscuri

Ora puoi caricare la tua licenza Data Sense BYOL nel BlueXP digital wallet in un sito buio, così da ricevere una notifica quando la tua licenza sta per esaurirsi.

03 aprile 2023

Versione 1.22

Nuovo rapporto di valutazione della scoperta dei dati

Il rapporto di valutazione della scoperta dei dati fornisce un'analisi di alto livello dell'ambiente scansionato per evidenziare i risultati del sistema e mostrare le aree problematiche e i potenziali passaggi di correzione. L'obiettivo di questo rapporto è quello di aumentare la consapevolezza delle problematiche relative alla governance dei dati, alle vulnerabilità della sicurezza dei dati e alle lacune nella conformità dei dati del tuo set di dati. "Scopri come generare e utilizzare il report di valutazione della scoperta dei dati" .

Possibilità di distribuire la BlueXP classification su istanze più piccole nel cloud

Quando si distribuisce la BlueXP classification da un connettore BlueXP in un ambiente AWS, ora è possibile scegliere tra due tipi di istanza più piccoli rispetto a quelli disponibili con l'istanza predefinita. Se stai eseguendo la scansione di un ambiente di piccole dimensioni, questo può aiutarti a risparmiare sui costi del cloud. Tuttavia, quando si utilizza l'istanza più piccola, ci sono alcune restrizioni. "Visualizza i tipi di istanza disponibili e le limitazioni" .

È ora disponibile uno script autonomo per qualificare il tuo sistema Linux prima dell'installazione BlueXP classification

Se desideri verificare che il tuo sistema Linux soddisfi tutti i prerequisiti indipendentemente dall'esecuzione dell'installazione della BlueXP classification , puoi scaricare uno script separato che verifica solo i prerequisiti. "Scopri come verificare se il tuo host Linux è pronto per installare la BlueXP classification" .

07 marzo 2023

Versione 1.21

Nuova funzionalità per aggiungere le tue categorie personalizzate dall'interfaccia utente BlueXP classification

La BlueXP classification ora consente di aggiungere categorie personalizzate in modo che la BlueXP classification identifichi i file che rientrano in tali categorie. La BlueXP classification ha molti "categorie predefinite" , quindi questa funzionalità ti consente di aggiungere categorie personalizzate per identificare dove si trovano nei tuoi dati le informazioni esclusive della tua organizzazione.

Ora puoi aggiungere parole chiave personalizzate dall'interfaccia utente BlueXP classification

Per un certo periodo la BlueXP classification ha avuto la possibilità di aggiungere parole chiave personalizzate che la BlueXP classification identificherà nelle scansioni future. Tuttavia, era necessario accedere all'host Linux BlueXP classification e utilizzare un'interfaccia a riga di comando per aggiungere le parole chiave. In questa versione, la possibilità di aggiungere parole chiave personalizzate è disponibile nell'interfaccia utente BlueXP classification , rendendo molto semplice l'aggiunta e la modifica di tali parole chiave.

Possibilità di far sì che la BlueXP classification non esegua la scansione dei file quando verrà modificato l'"ultimo orario di accesso"

Per impostazione predefinita, se la BlueXP classification non dispone di autorizzazioni di "scrittura" adeguate, il sistema non eseguirà la scansione dei file nei volumi perché la BlueXP classification non può ripristinare l'"orario dell'ultimo accesso" al timestamp originale. Tuttavia, se non ti interessa che l'ora dell'ultimo accesso venga reimpostata sull'ora originale nei tuoi file, puoi ignorare questo comportamento nella pagina Configurazione in modo che la BlueXP classification esegua la scansione dei volumi indipendentemente dalle autorizzazioni.

Insieme a questa funzionalità, è stato aggiunto un nuovo filtro denominato "Evento analisi scansione" che consente di visualizzare i file che non sono stati classificati perché la BlueXP classification non è riuscita a ripristinare l'orario dell'ultimo accesso oppure i file che sono stati classificati anche se la BlueXP classification non è riuscita a ripristinare l'orario dell'ultimo accesso.

"Scopri di più sul "Timestamp dell'ultimo accesso" e sulle autorizzazioni richieste BlueXP classification" .

La BlueXP classification identifica tre nuovi tipi di dati personali

La BlueXP classification può identificare e categorizzare i file che contengono i seguenti tipi di dati:

- Numero della carta d'identità del Botswana (Omang).
- Numero di passaporto del Botswana
- Carta d'identità nazionale di registrazione di Singapore (NRIC)

"Visualizza tutti i tipi di dati personali che la BlueXP classification può identificare nei tuoi dati" .

Funzionalità aggiornate per le directory

- L'opzione "Light CSV Report" per i Data Investigation Reports ora include informazioni provenienti dalle directory.
- Il filtro temporale "Ultimo accesso" ora mostra l'orario dell'ultimo accesso sia per i file che per le directory.

Miglioramenti dell'installazione

- Il programma di installazione BlueXP classification per i siti senza accesso a Internet (siti oscuri) ora esegue un controllo preliminare per verificare che i requisiti di sistema e di rete siano soddisfatti per un'installazione corretta.
- I file di registro di controllo dell'installazione vengono ora salvati; vengono scritti in `/ops/netapp/install_logs` .

05 febbraio 2023

Versione 1.20

Possibilità di inviare e-mail di notifica basate su policy a qualsiasi indirizzo e-mail

Nelle versioni precedenti della BlueXP classification era possibile inviare avvisi e-mail agli utenti BlueXP nel proprio account quando determinati criteri critici restituivano risultati. Questa funzione ti consente di ricevere notifiche per proteggere i tuoi dati quando non sei online. Ora puoi anche inviare avvisi e-mail da Policies a qualsiasi altro utente (fino a 20 indirizzi e-mail) che non sia presente nel tuo account BlueXP .

"Scopri di più sull'invio di avvisi e-mail in base ai risultati dei criteri" .

Ora puoi aggiungere modelli personali dall'interfaccia utente BlueXP classification

Per un certo periodo, la BlueXP classification ha avuto la possibilità di aggiungere "dati personali" personalizzati che la BlueXP classification identificherà nelle scansioni future. Tuttavia, era necessario accedere all'host Linux BlueXP classification e utilizzare una riga di comando per aggiungere i modelli personalizzati. In questa versione, la possibilità di aggiungere modelli personali utilizzando un'espressione regolare è disponibile nell'interfaccia utente BlueXP classification , rendendo molto semplice l'aggiunta e la modifica di questi modelli personalizzati.

Possibilità di spostare 15 milioni di file utilizzando la BlueXP classification

In passato la BlueXP classification poteva spostare un massimo di 100.000 file sorgente su qualsiasi condivisione NFS. Ora puoi spostare fino a 15 milioni di file alla volta.

Possibilità di visualizzare il numero di utenti che hanno accesso ai file di SharePoint Online

Il filtro "Numero di utenti con accesso" ora supporta i file archiviati nei repository di SharePoint Online. In passato erano supportati solo i file su condivisioni CIFS. Si noti che i gruppi di SharePoint che non sono basati su Active Directory non verranno al momento conteggiati in questo filtro.

È stato aggiunto il nuovo stato "Riuscito parziale" al pannello Stato azione

Il nuovo stato "Riuscito parzialmente" indica che un'azione BlueXP classification è terminata e che alcuni elementi non sono riusciti, mentre altri sono riusciti, ad esempio quando si spostano o si eliminano 100 file. Inoltre, lo stato "Terminata" è stato rinominato "Riuscita". In passato, lo stato "Terminata" poteva elencare le azioni riuscite e quelle fallite. Ora lo stato "Riuscito" significa che tutte le azioni sono riuscite su tutti gli elementi. "Scopri come visualizzare il pannello Stato azioni" .

09 gennaio 2023

Versione 1.19

Possibilità di visualizzare un grafico dei file che contengono dati sensibili e che sono eccessivamente permissivi

Nella dashboard Governance è stata aggiunta una nuova area *Dati sensibili e autorizzazioni estese* che fornisce una mappa termica dei file che contengono dati sensibili (inclusi dati personali sensibili e sensibili) e che sono eccessivamente permissivi. Questo può aiutarti a capire dove potresti correre dei rischi con i dati sensibili. "Saperne di più" .

Sono disponibili tre nuovi filtri nella pagina Indagine sui dati

Sono disponibili nuovi filtri per perfezionare i risultati visualizzati nella pagina Indagine sui dati:

- Il filtro "Numero di utenti con accesso" mostra quali file e cartelle sono aperti a un certo numero di utenti. È possibile scegliere un intervallo numerico per affinare i risultati, ad esempio per vedere quali file sono accessibili a 51-100 utenti.
- I filtri "Ora di creazione", "Ora di scoperta", "Ultima modifica" e "Ultimo accesso" ora consentono di creare un intervallo di date personalizzato anziché selezionare semplicemente un intervallo di giorni predefinito. Ad esempio, puoi cercare file con una data di creazione "più vecchia di 6 mesi" o con una data di ultima modifica "negli ultimi 10 giorni".
- Il filtro "Percorso file" ora consente di specificare i percorsi che si desidera escludere dai risultati della query filtrata. Se si immettono percorsi per includere ed escludere determinati dati, la BlueXP classification trova prima tutti i file nei percorsi inclusi, quindi rimuove i file dai percorsi esclusi e infine visualizza i risultati.

"Visualizza l'elenco di tutti i filtri che puoi utilizzare per analizzare i tuoi dati" .

La BlueXP classification può identificare il numero individuale giapponese

La BlueXP classification può identificare e categorizzare i file che contengono il Japanese Individual Number (noto anche come My Number). Ciò include sia il numero personale che quello aziendale. "Visualizza tutti i tipi di dati personali che la BlueXP classification può identificare nei tuoi dati" .

Limitazioni note nella NetApp Data Classification

Le limitazioni note identificano funzioni che non sono supportate o non interagiscono correttamente in questa versione. Esamina attentamente queste limitazioni.

Opzioni disabilitate NetApp Data Classification

Nella versione di dicembre 2023 (1.26.6) sono state rimosse le seguenti opzioni:

- L'opzione per attivare la raccolta dei registri di controllo è stata disabilitata.
- Durante l'indagine di Directories, l'opzione per calcolare il numero di dati di informazioni personali identificabili (PII) da parte di Directories non è disponibile.
- L'opzione per integrare i dati tramite etichette di Azure Information Protection (AIP) è stata disabilitata.

Scansione della classificazione dei dati

Le scansioni di classificazione dei dati presentano le seguenti limitazioni.

La classificazione dei dati esegue la scansione di una sola condivisione in un volume

Se si dispone di più condivisioni di file in un singolo volume, la classificazione dei dati analizza la condivisione con la gerarchia più elevata. Ad esempio, se hai azioni come le seguenti:

- /UN
- /A/B
- /C
- /D/E

In questa configurazione vengono scansionati solo i dati in /A. I dati in /C e /D non vengono scansionati.

Soluzione alternativa

Esiste una soluzione alternativa per assicurarsi di eseguire la scansione dei dati da tutte le condivisioni nel volume. Segui questi passaggi:

1. Nel sistema, aggiungere il volume da scansionare.
2. Dopo che Data Classification ha completato la scansione del volume, vai alla pagina *Data Investigation* e crea un filtro per vedere quale condivisione è in fase di scansione:

   Filtra i dati in base a "Nome sistema" e "Tipo directory = Condivisione" per vedere quale condivisione viene scansionata.

3. Ottieni l'elenco completo delle condivisioni presenti nel volume, così puoi vedere quali condivisioni non vengono scansionate.
4. "Aggiungi le azioni rimanenti a un gruppo di condivisione" .

   Aggiungi tutte le azioni singolarmente, ad esempio:

   ```
   /C
   /D
   ```

5. Eseguire questi passaggi per ogni volume del sistema che dispone di più condivisioni.

Ultimo timestamp di accesso

Quando Data Classification esegue una scansione di una directory, la scansione ha effetto sul campo **Ultimo accesso** della directory. Quando si visualizza il campo **Ultimo accesso**, i metadati riflettono la data e l'ora della scansione oppure l'ultima volta che un utente ha effettuato l'accesso alla directory.

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

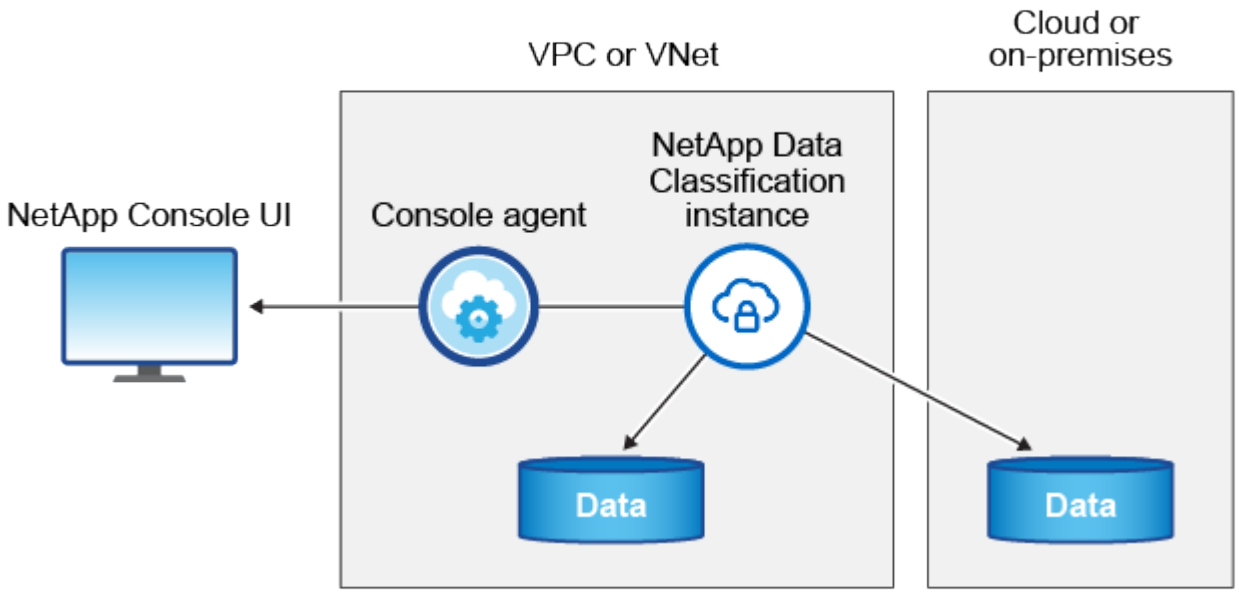
- L'installazione di Data Classification nel cloud richiede la distribuzione di un'istanza cloud, che comporta l'addebito di costi da parte del provider cloud presso cui viene distribuita. Vedere il tipo di istanza distribuita per ciascun provider cloud . Non ci sono costi se si installa Data Classification 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

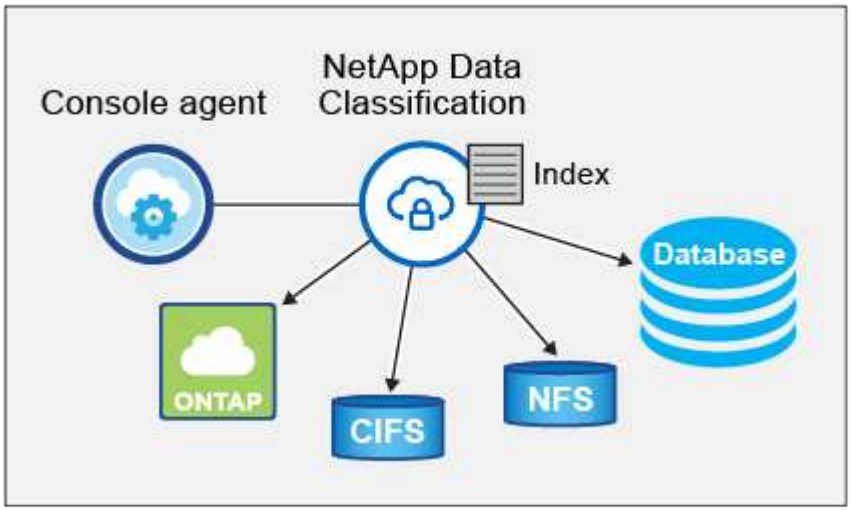
Ad alto livello, la scansione della classificazione dei dati funziona in questo modo:

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" .

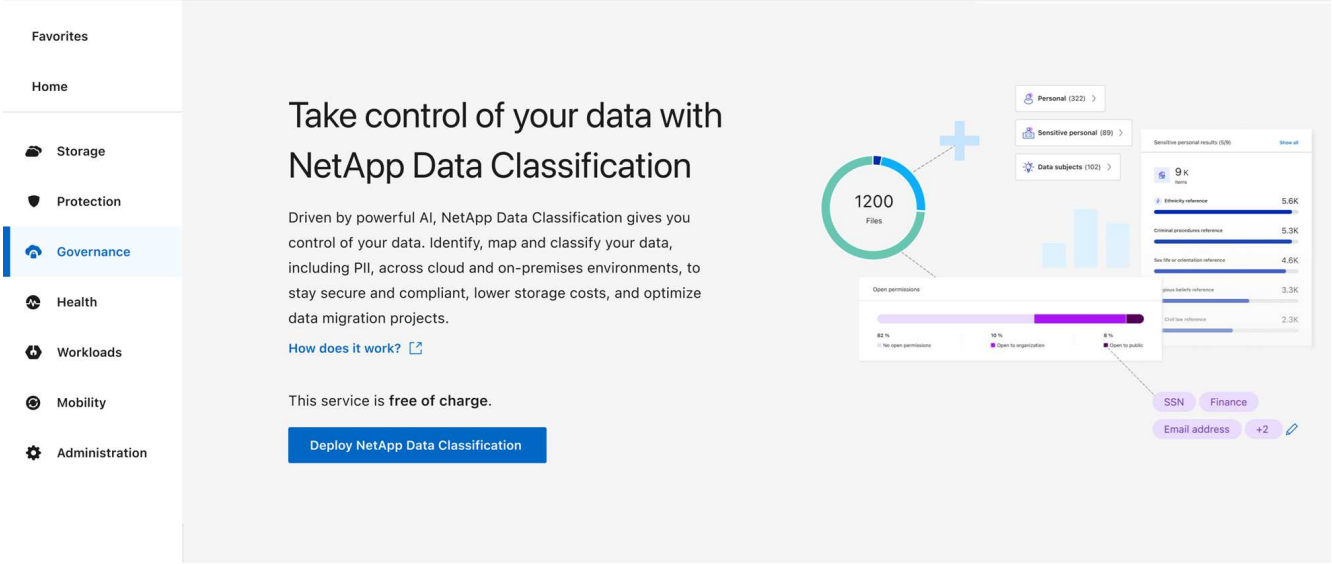
Prima di iniziare

- "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 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. << Prerequisiti,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.

Come puoi vedere, potrebbero esserci alcune 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:

"Visualizza ulteriori informazioni sulla distribuzione dell'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

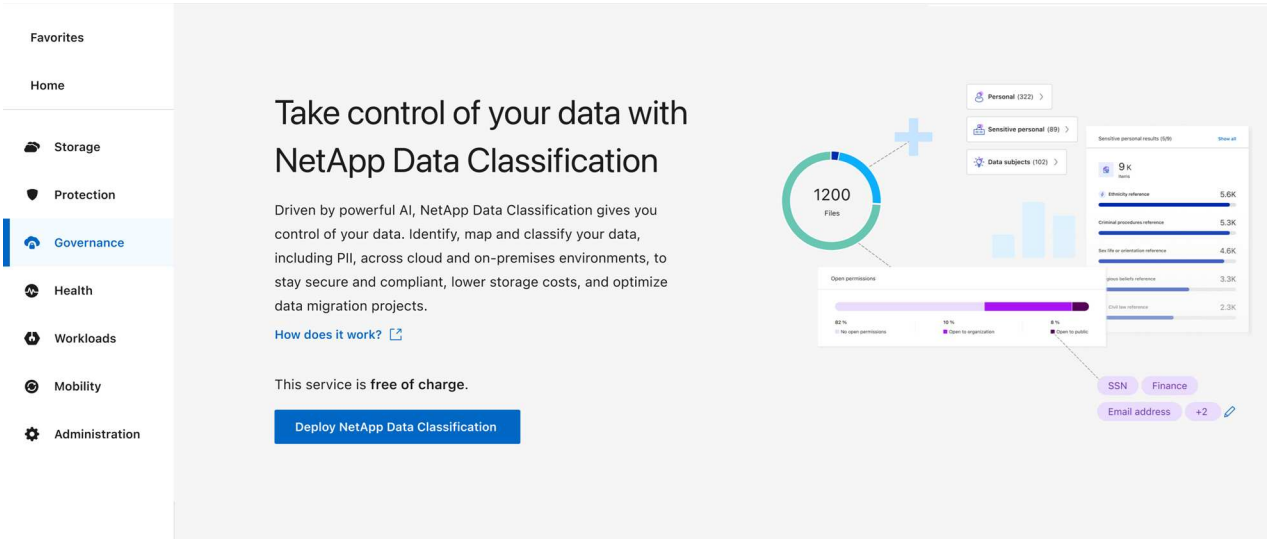
Per distribuire un'istanza di Data Classification nel cloud, seguire questi passaggi. L'agente della console distribuirà l'istanza nel cloud e quindi installerà il software di classificazione dei dati su tale istanza.

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**.

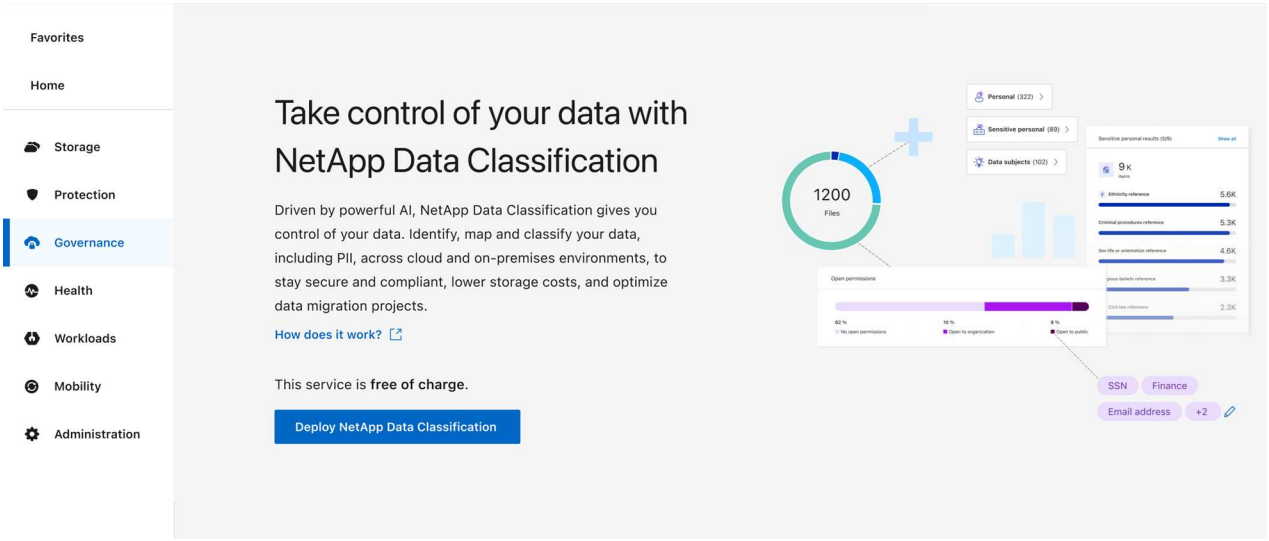


2. Dalla pagina *Installazione*, seleziona **Distribuisci > Distribuisci** per utilizzare la dimensione dell'istanza "Grande" e avviare la procedura guidata di distribuzione cloud.
3. La procedura guidata visualizza l'avanzamento dei passaggi di distribuzione. Quando sono richiesti input o se si verificano 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**.



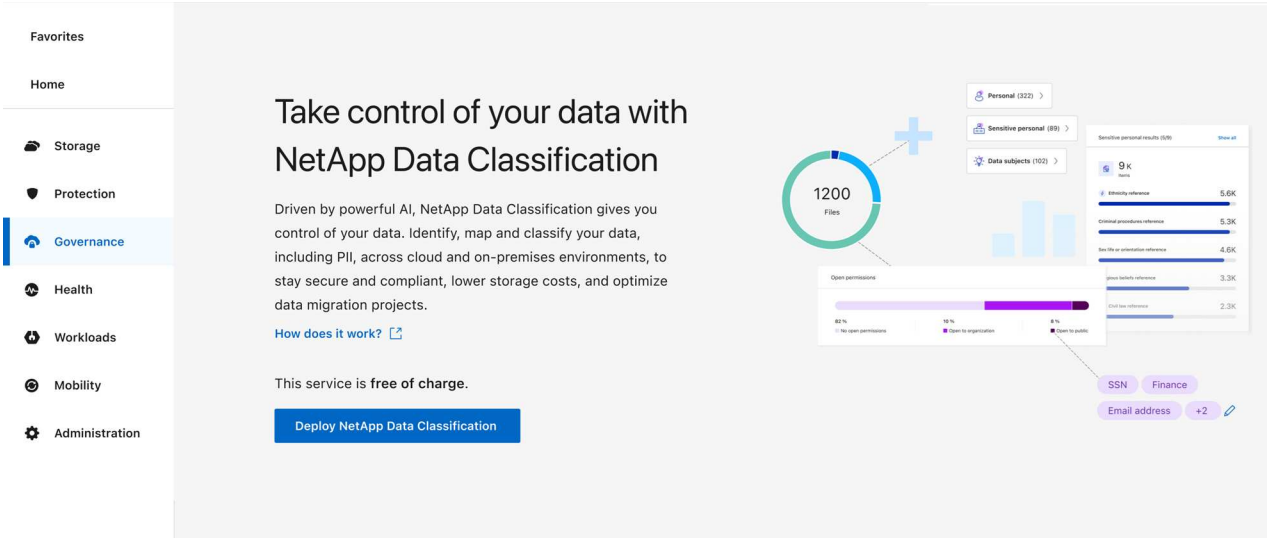
2. Selezionare **Distribuisci** per avviare la procedura guidata di distribuzione cloud.

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

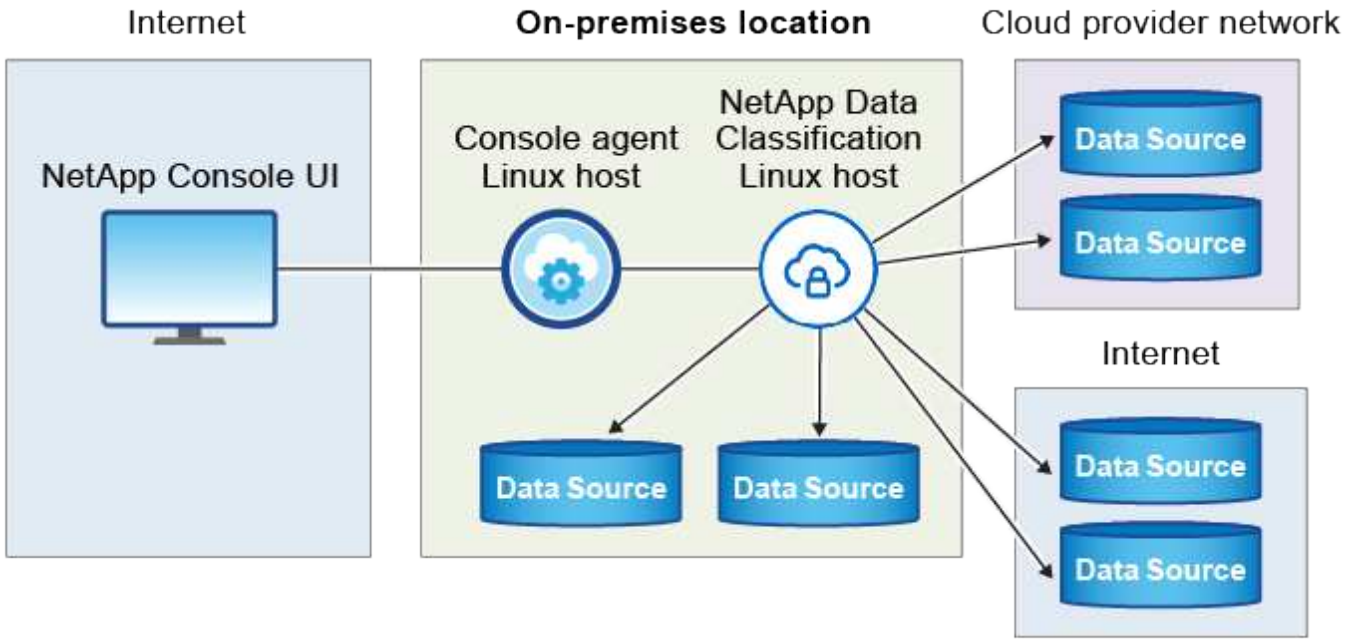
Per distribuire NetApp Data Classification su un host Linux nella tua rete o su un host Linux nel cloud con accesso a Internet, devi distribuire manualmente l'host Linux nella tua rete o nel cloud.

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

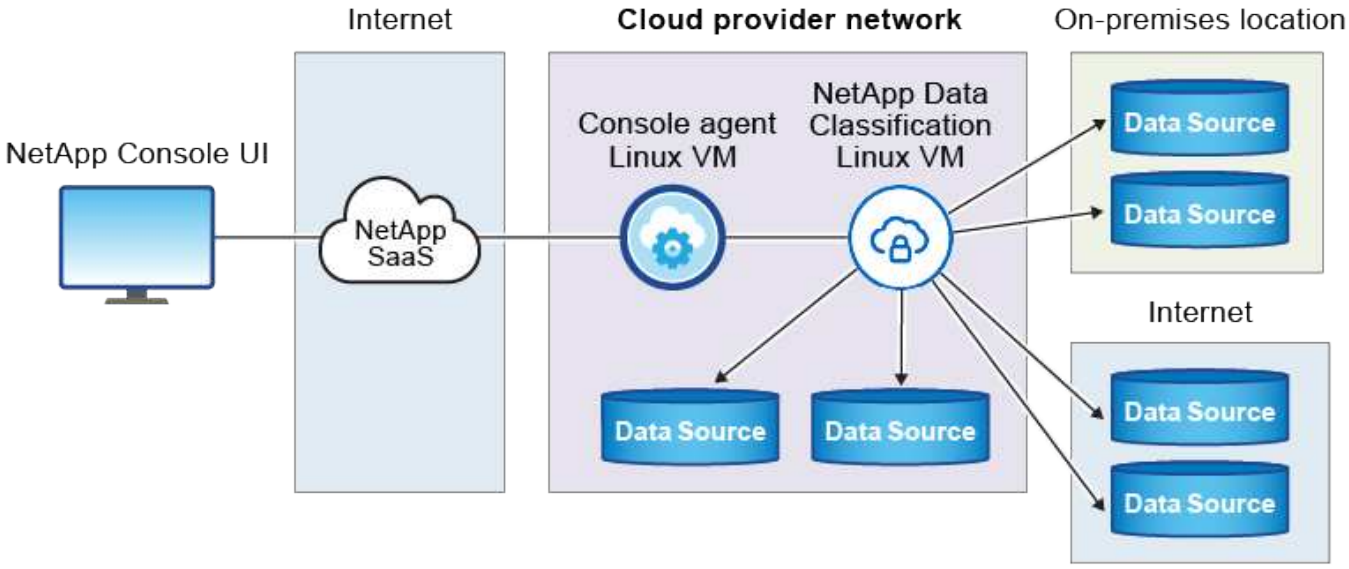
allo stesso modo indipendentemente dal metodo di installazione scelto.

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 non è supportata su un host condiviso con altre applicazioni: l'host deve essere un host dedicato.
- Quando si crea il sistema host nei propri locali, è possibile scegliere tra queste dimensioni di sistema a seconda delle dimensioni del set di dati su cui si prevede di eseguire la scansione di classificazione dei dati.

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 • 895 GiB disponibili su /var/lib/docker • 5 GiB su /tmp • **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 • 400 GiB disponibili su /var/lib/docker o per Podman /var/lib/containers • 5 GiB su /tmp • **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, sarà 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

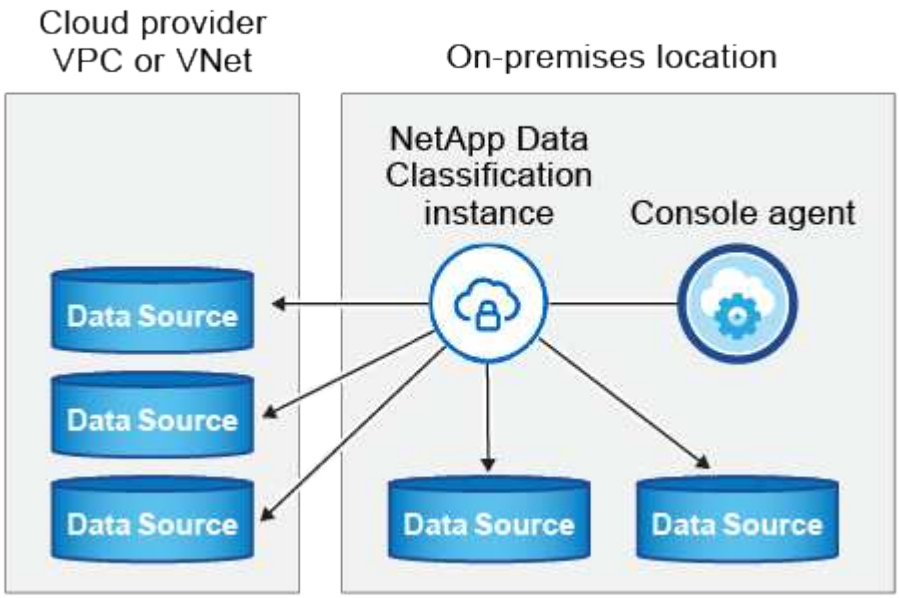
È necessario assicurarsi che tutte le porte necessarie siano aperte per la comunicazione tra l'agente della console, Data Classification, Active Directory e le origini dati.

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: • 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. • 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) • 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. Assicurarsi che queste porte siano aperte all'istanza di classificazione dei dati: • Per NFS - 111 e 2049 • Per CIFS - 139 e 445 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. È necessario disporre delle informazioni per Active Directory: • Indirizzo IP del server DNS o più indirizzi IP • Nome utente e password per il 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)

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

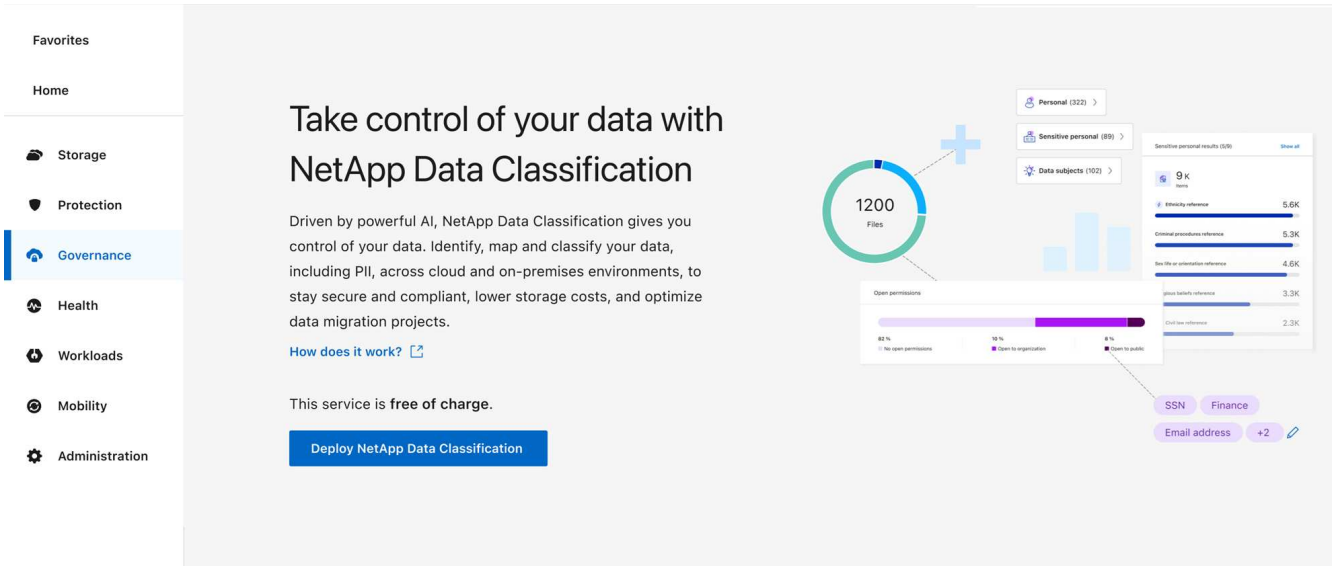
- Verifica che il tuo sistema Linux soddisfi i requisitirequisiti dell'host .
- Verificare che nel sistema siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurati di avere i privilegi di root sul sistema Linux.
- Se utilizzi un proxy per accedere a Internet:
  - 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>` Se stai installando su un'istanza cloud (non nei tuoi locali), aggiungi `--manual-cloud -install <cloud_provider>`. 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. 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. 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: `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*).

Esiste anche uno script di test prerequisito che fa parte dello script di installazione di Data Classification. Lo script descritto qui è progettato specificamente per gli utenti che desiderano verificare l'host Linux indipendentemente dall'esecuzione dello script di installazione di Data Classification.

Iniziare

Dovrai svolgere le seguenti attività.

1. 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.
2. Preparare la macchina host e verificare che soddisfi tutti i requisiti.
3. Abilitare l'accesso a Internet in uscita dalla macchina host di classificazione dei dati.
4. Verificare che tutte le porte richieste siano abilitate su tutti i sistemi.
5. 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. Alcuni utenti che intendono installare Data Classification in locale potrebbero anche scegliere di installare l'agente Console in locale.

Per creare un agente Console 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" .

Quando si esegue lo script dei prerequisiti, 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**.

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, requisiti software e così via.

- La classificazione dei dati non è supportata su un host condiviso con altre applicazioni: l'host deve essere un host dedicato.
- Quando si crea il sistema host nei propri locali, è possibile scegliere tra queste dimensioni di sistema a seconda delle dimensioni del set di dati su cui si prevede di eseguire la scansione di classificazione dei dati.

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 • 895 GiB disponibili su /var/lib/docker • 5 GiB su /tmp • **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 • 400 GiB disponibili su /var/lib/docker o per Podman /var/lib/containers • 5 GiB su /tmp • **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, sarà 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

Con quale rapidità la classificazione dei dati esegue la scansione dei dati

La velocità di scansione è influenzata dalla latenza di rete, dalla latenza del disco, dalla larghezza di banda di rete, dalle dimensioni dell'ambiente e dalle dimensioni di distribuzione dei file.

- Quando si eseguono scansioni di sola mappatura, la classificazione dei dati può analizzare tra 100 e 150

TiB di dati al giorno.

- Quando si eseguono scansioni Map & Classify, Data Classification può analizzare tra 15 e 40 TiB di dati al giorno.

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.

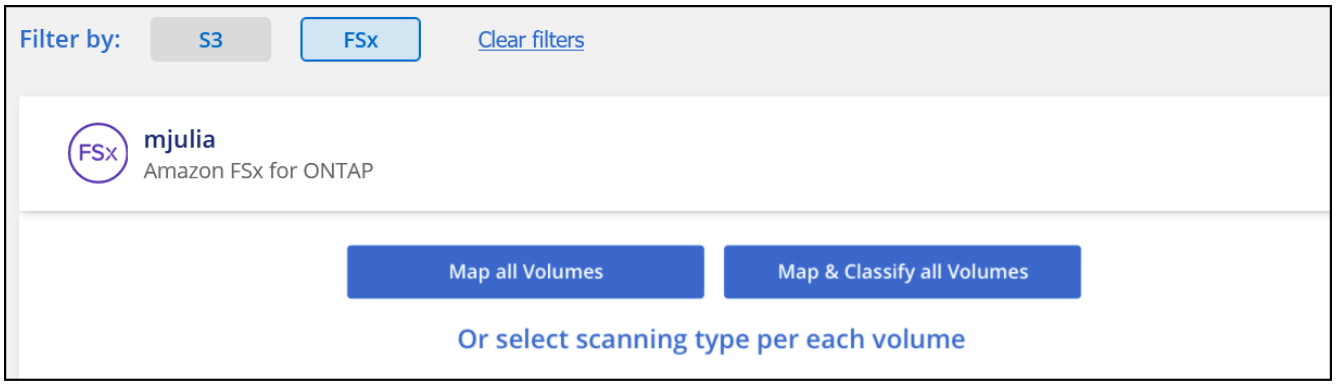
Nota: la distribuzione della classificazione dei dati in una posizione locale non è attualmente supportata durante la scansione dei volumi FSx.

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

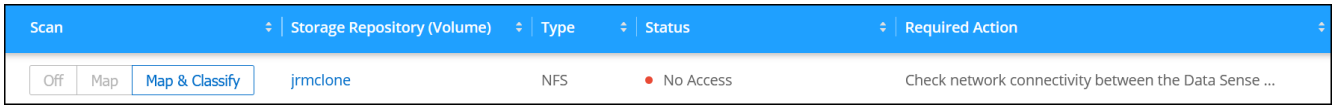
Assicurati che Data Classification possa accedere ai volumi controllando la rete, i gruppi di sicurezza e i criteri di esportazione.

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

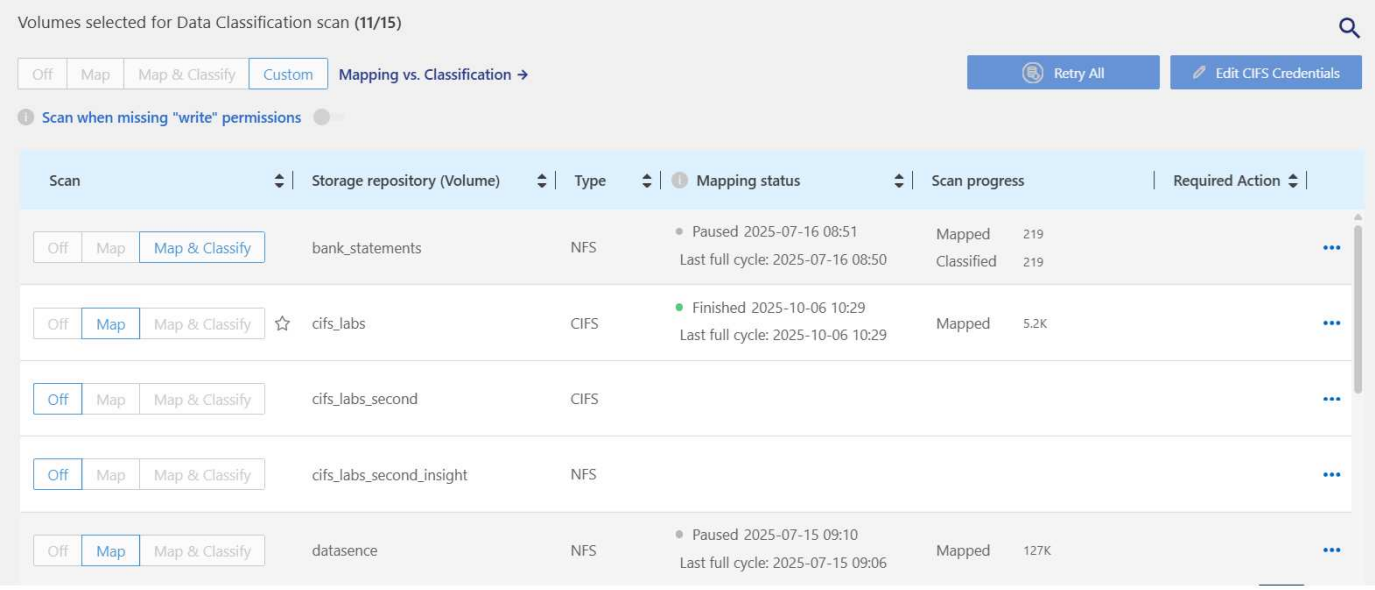
È possibile avviare o interrompere le scansioni su qualsiasi sistema in qualsiasi momento dalla pagina Configurazione. È anche possibile passare da scansioni di sola mappatura a scansioni di mappatura e classificazione e viceversa. Si consiglia di eseguire la scansione di tutti i volumi di un sistema.

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.

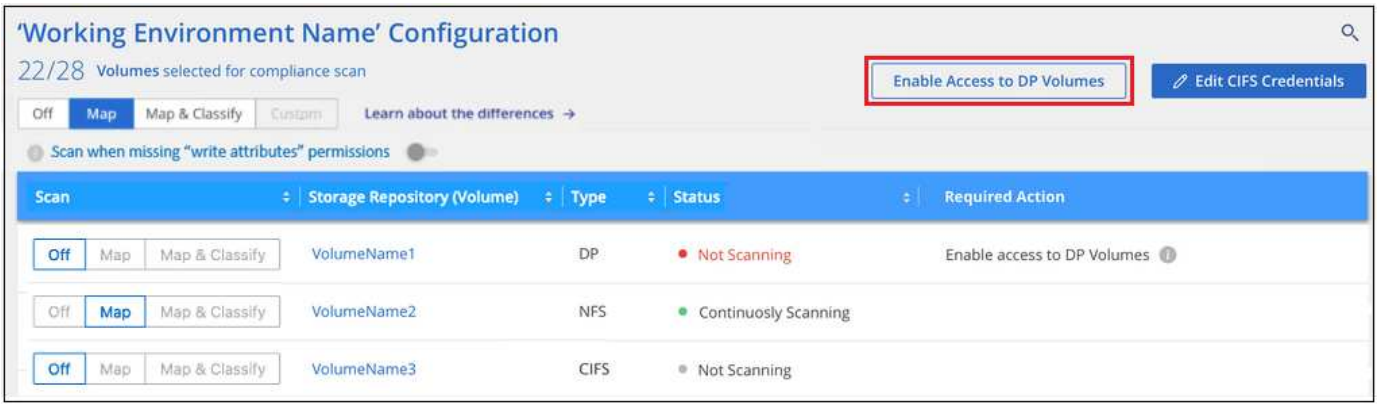
Risultato

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 .

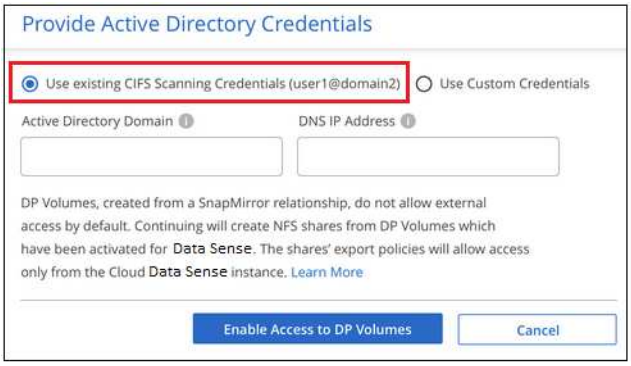
Inizialmente, l'elenco dei volumi identifica questi volumi come *Tipo* **DP** con *Stato* **Non in scansione** e *Azione richiesta* **Abilita accesso ai volumi DP**.

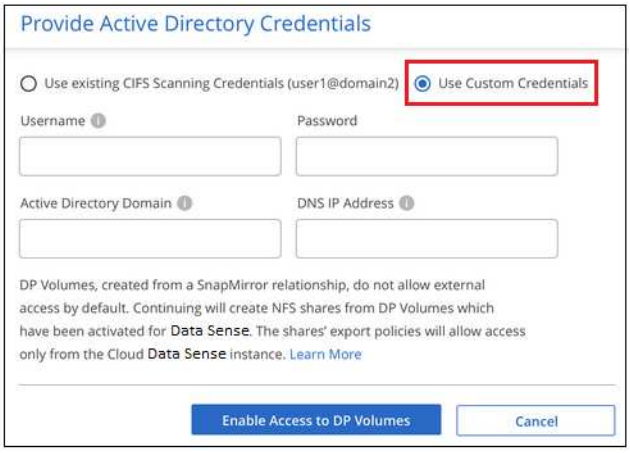


Passi

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**.

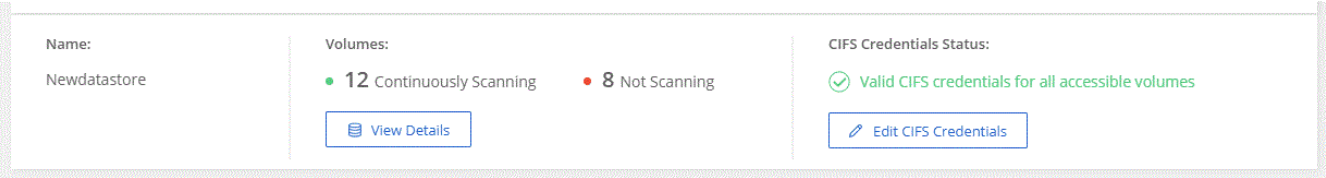
   a. Se si utilizza CIFS (SMB), assicurarsi che le credenziali di Active Directory siano corrette. Per ciascun sistema, selezionare **Modifica credenziali CIFS**, quindi immettere il nome utente e la password necessari a Data Classification per accedere ai volumi CIFS sul sistema.

      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.

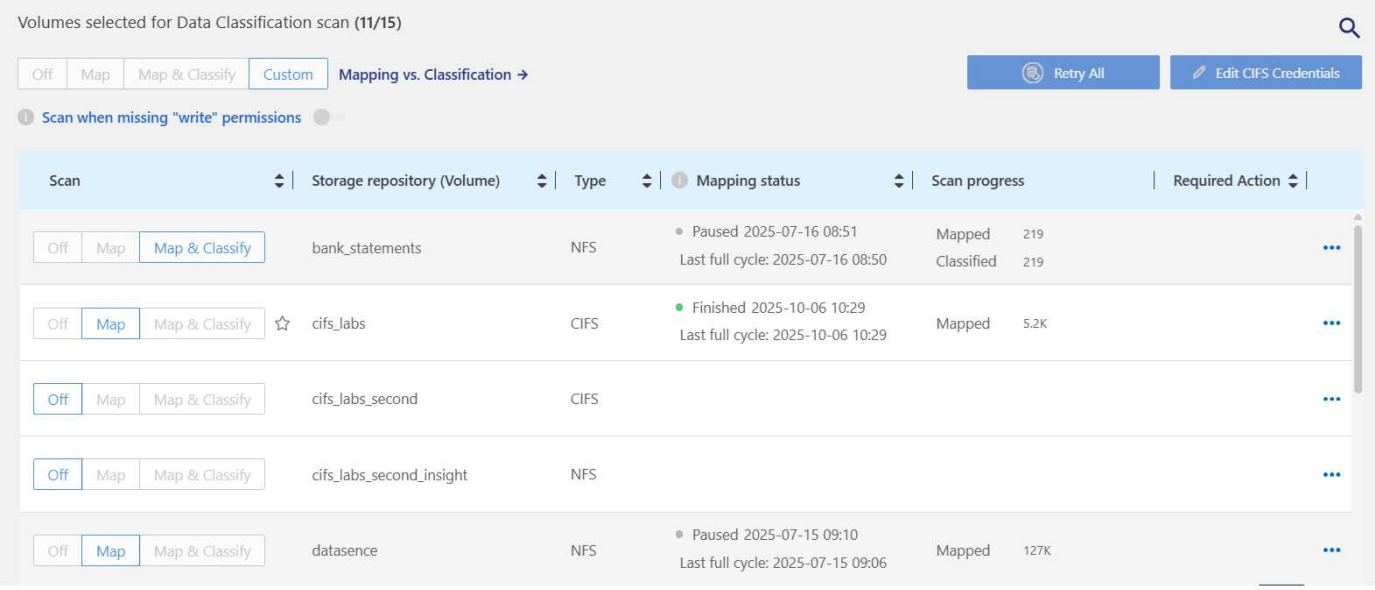
Abilita o disabilita le scansioni sui volumi

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

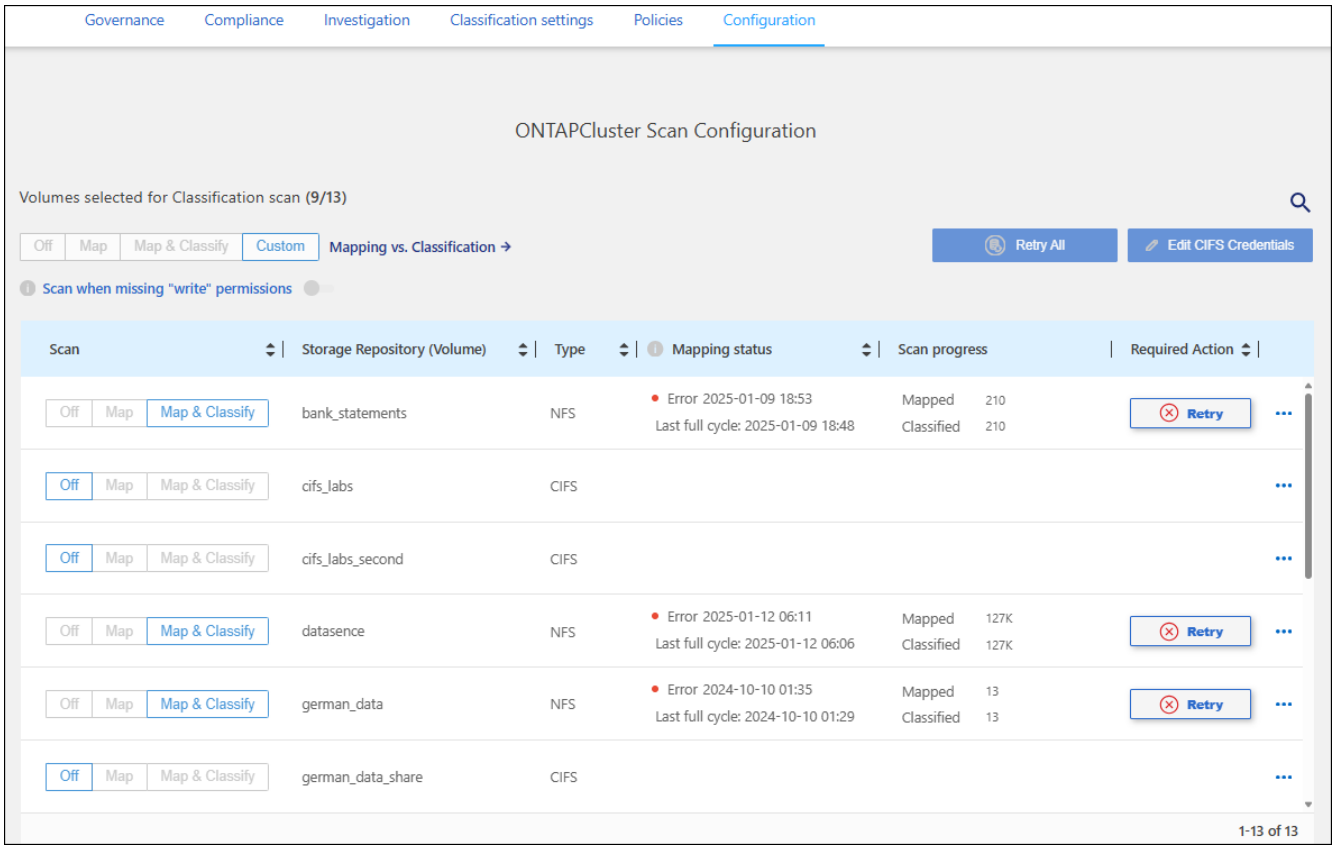
- Assicurarsi che vi sia una connessione di rete tra l'istanza di Data Classification e ciascuna rete che include volumi per Cloud Volumes ONTAP o cluster ONTAP on-prem.
- Assicurarsi che il gruppo di sicurezza per Cloud Volumes ONTAP consenta il traffico in entrata dall'istanza di classificazione dei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

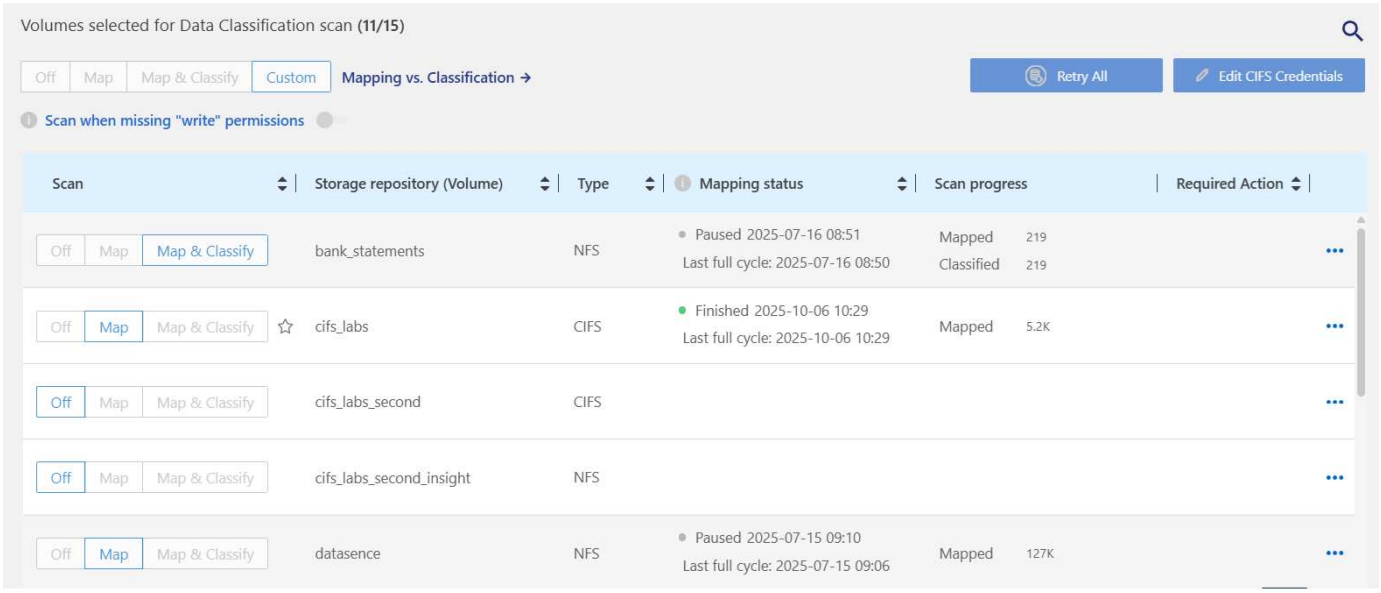
Abilita o disabilita le scansioni sui volumi

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.

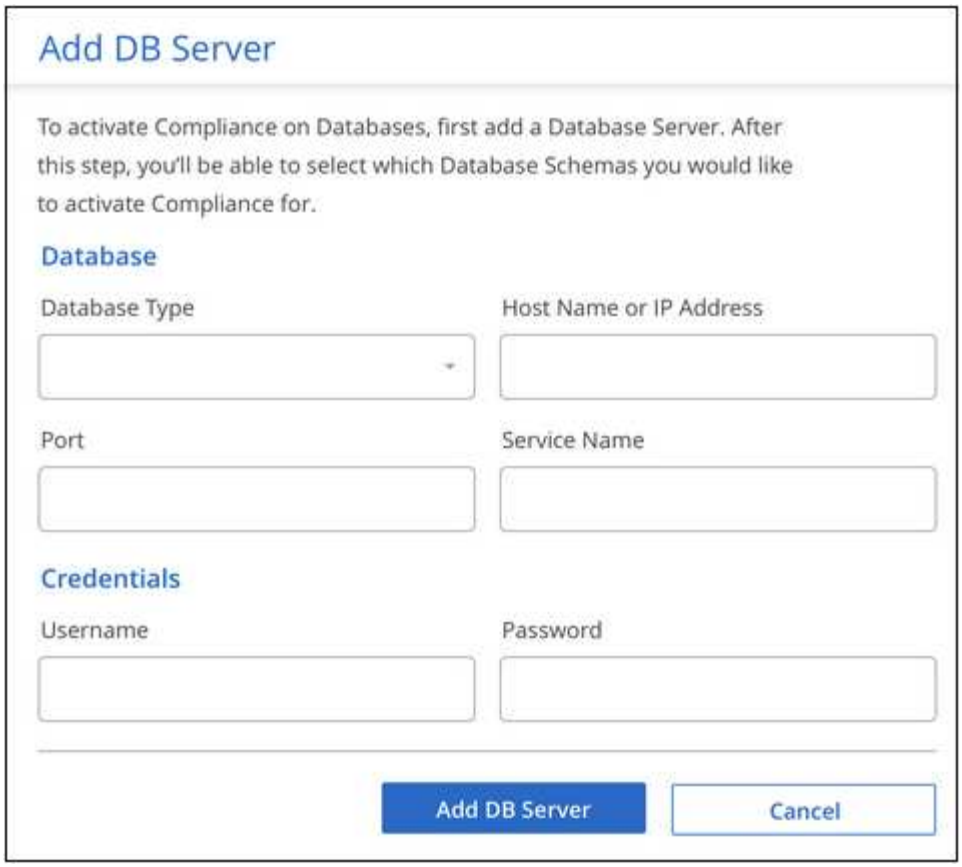
Se si esegue la scansione di schemi di database accessibili tramite Internet, è possibile"distribuire la classificazione dei dati nel cloud" O"distribuire la classificazione dei dati in una posizione locale dotata di accesso a Internet" .

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.

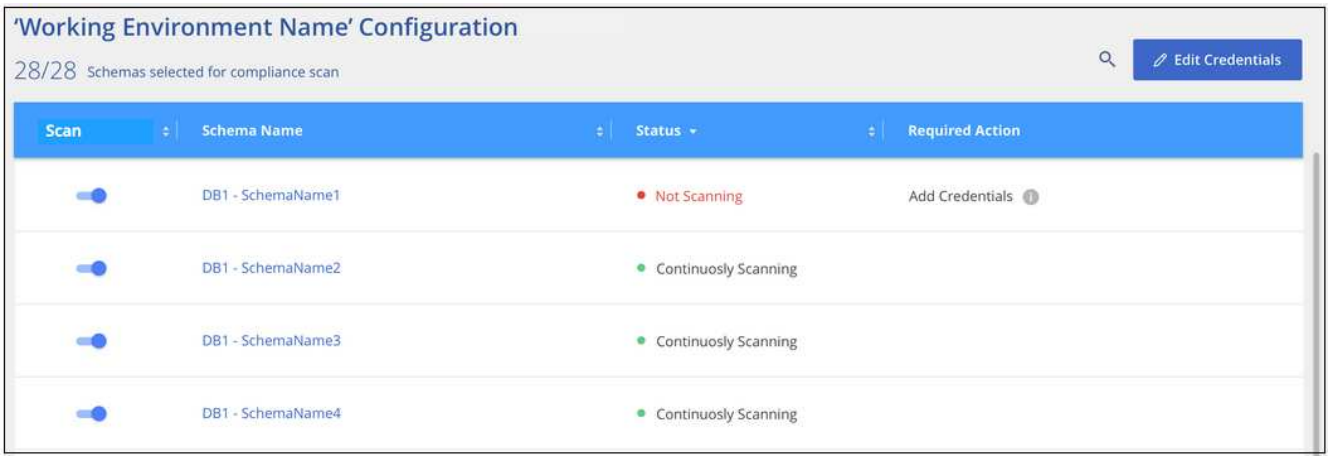
Abilita e disabilita le scansioni sugli schemi del database

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 di conformità 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**.

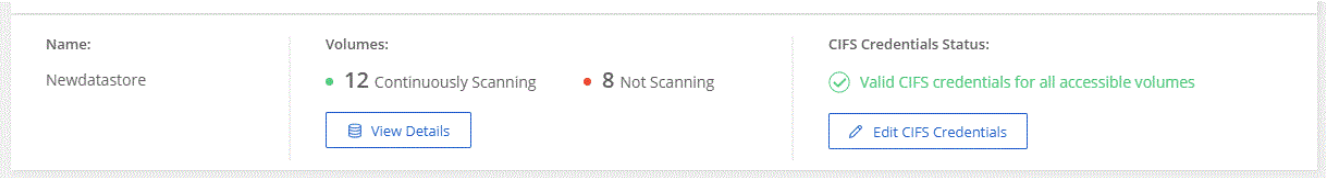
   a. Se si utilizza CIFS (SMB), assicurarsi che le credenziali di Active Directory siano corrette. Per ciascun sistema, selezionare **Modifica credenziali CIFS**, quindi immettere il nome utente e la password

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.

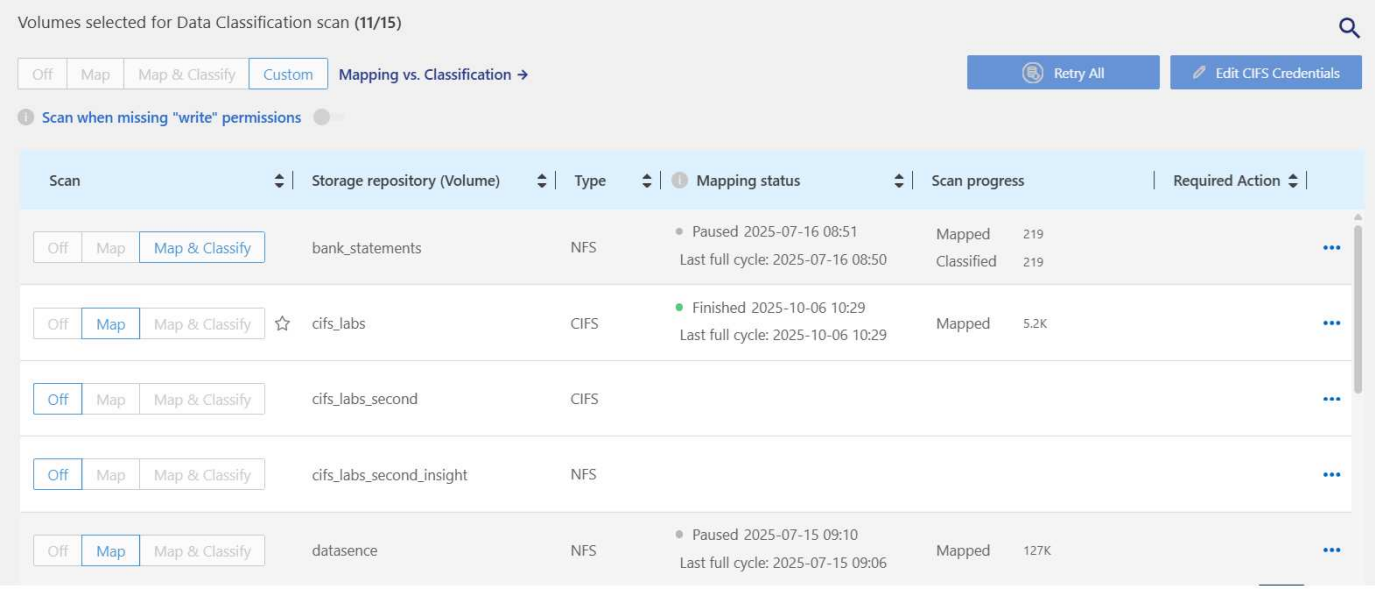
Abilita e disabilita le scansioni sui volumi

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.

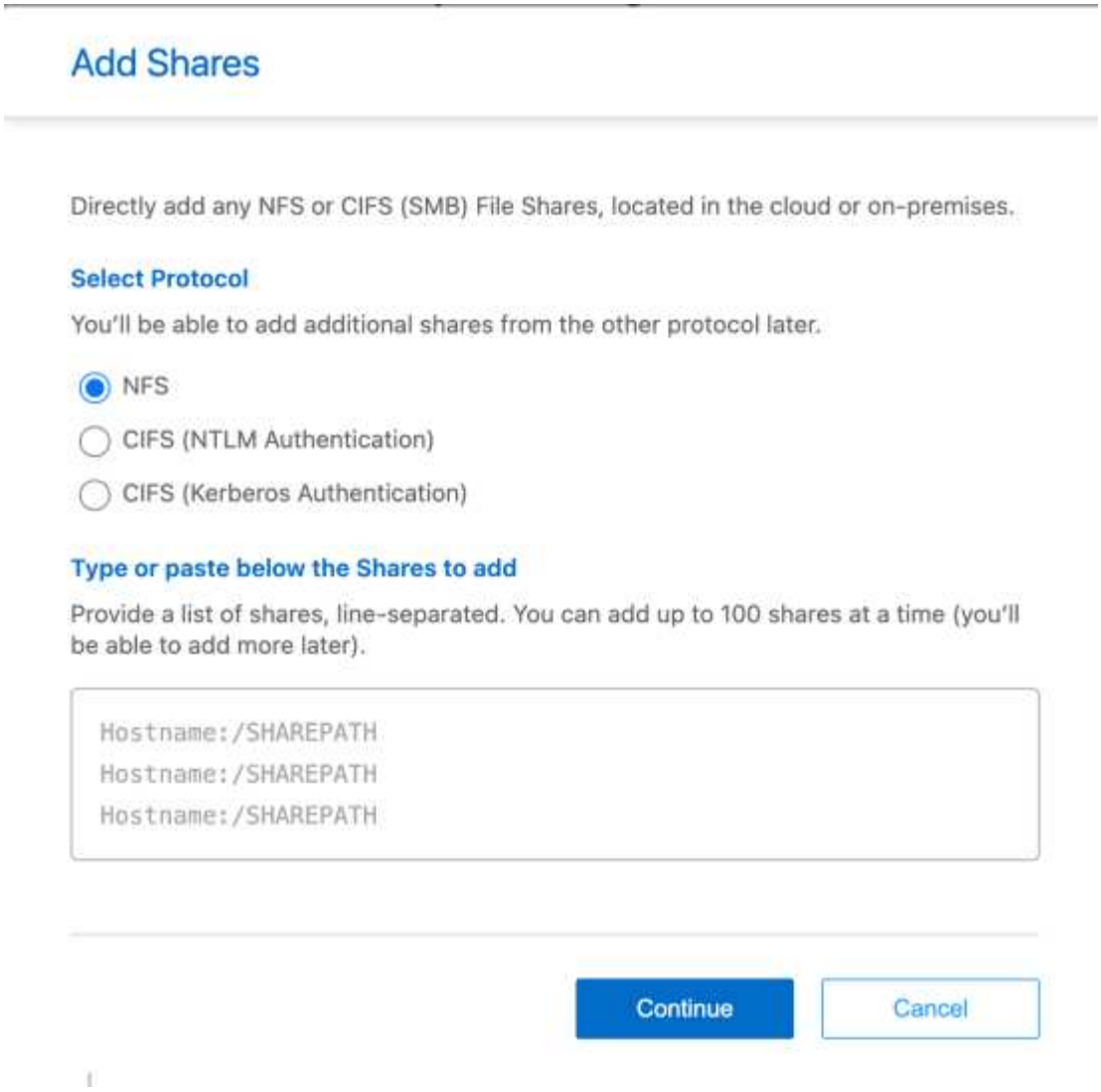
Crea un gruppo di condivisione file

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.

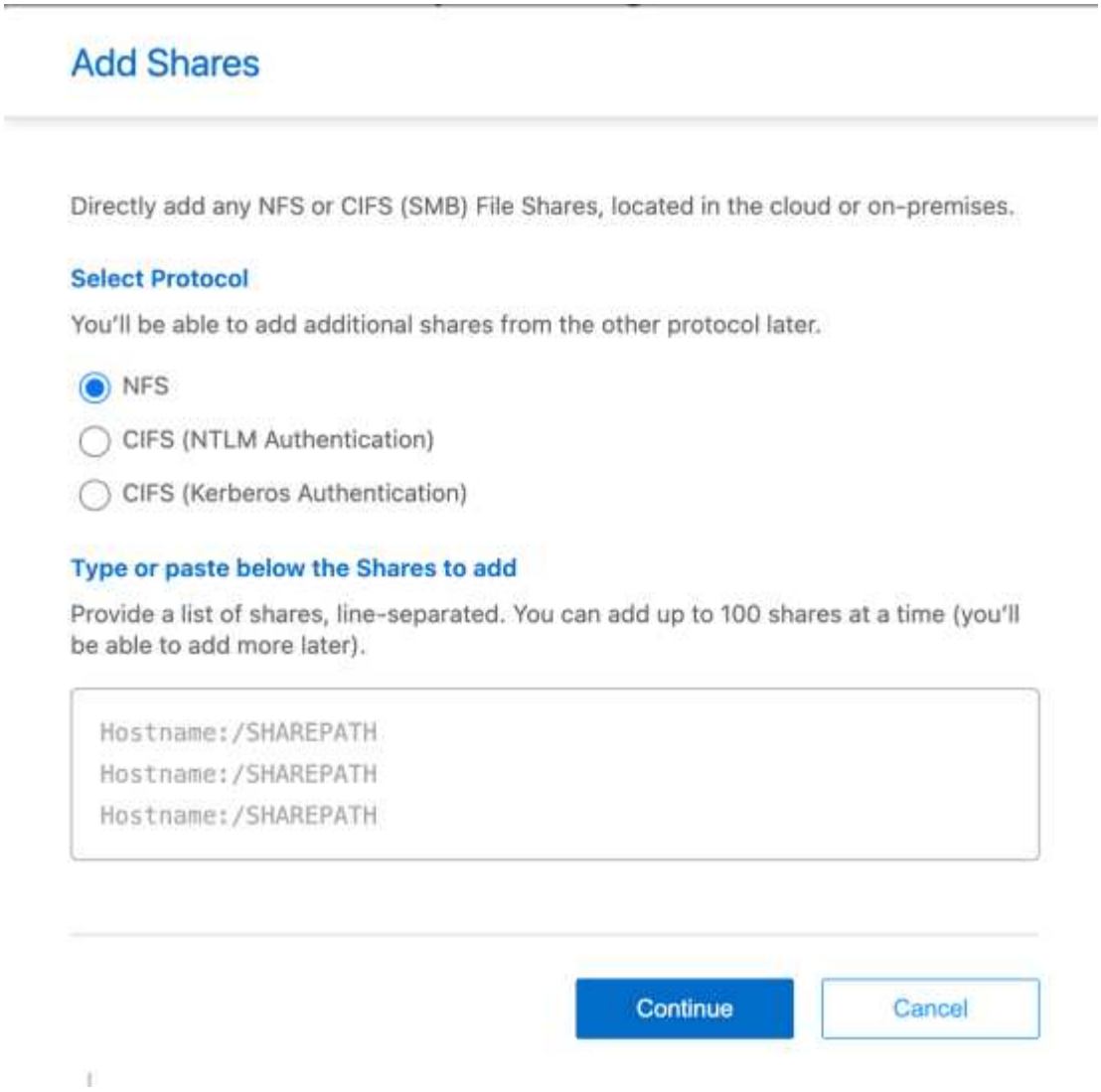
Modifica la configurazione del protocollo CIFS

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" .

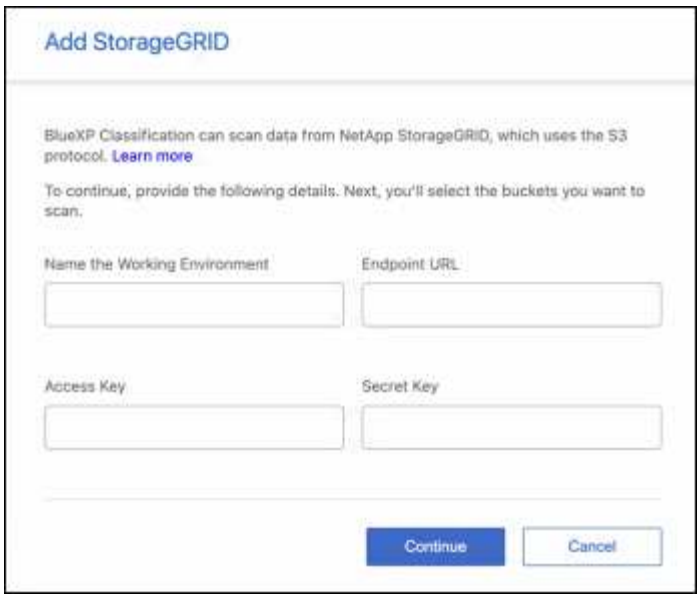
Se si stanno eseguendo la scansione dei dati da StorageGRID installato in un sito buio senza accesso a Internet, è necessario"distribuire la classificazione dei dati nella stessa posizione locale che non ha accesso a Internet" . Ciò richiede anche che l'agente della console venga distribuito nella stessa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

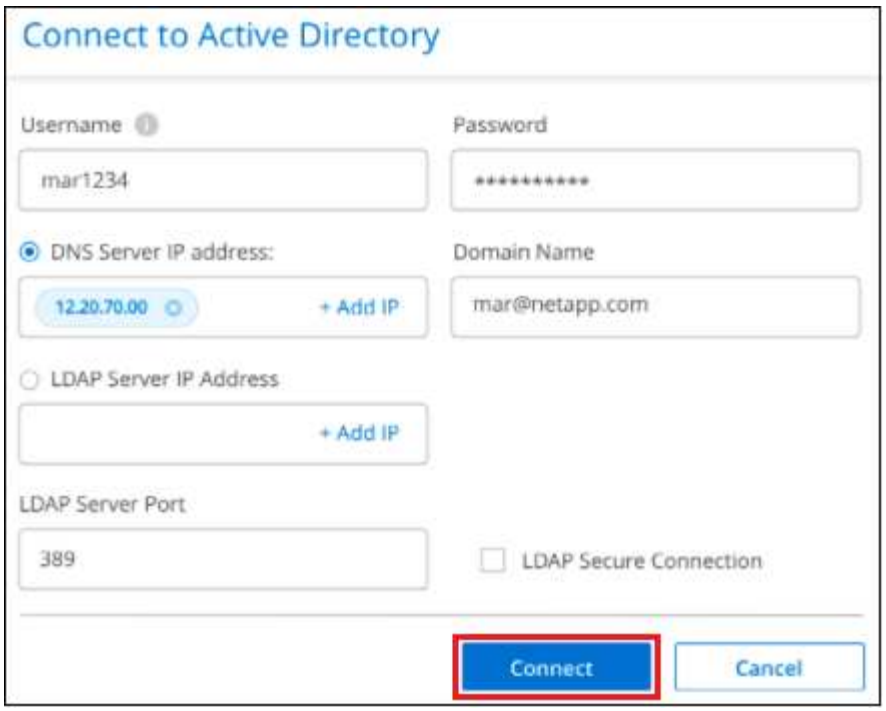
Protocollo	Porta	Destinazione	Scopo
TCP e UDP	389	Directory attiva	LDAP
TCP	636	Directory attiva	LDAP su SSL
TCP	3268	Directory attiva	Catalogo globale
TCP	3269	Directory attiva	Catalogo globale su SSL

Passi

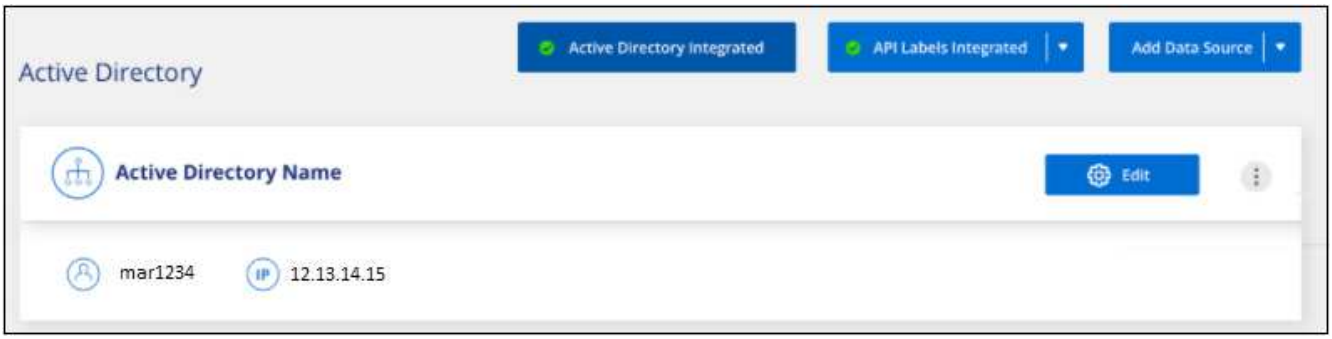
1. Nella pagina Configurazione classificazione dati, fare clic su **Aggiungi Active Directory**.

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**.

Utilizzare la classificazione dei dati

Visualizza i dettagli di governance sui dati archiviati nella tua organizzazione con NetApp Data Classification

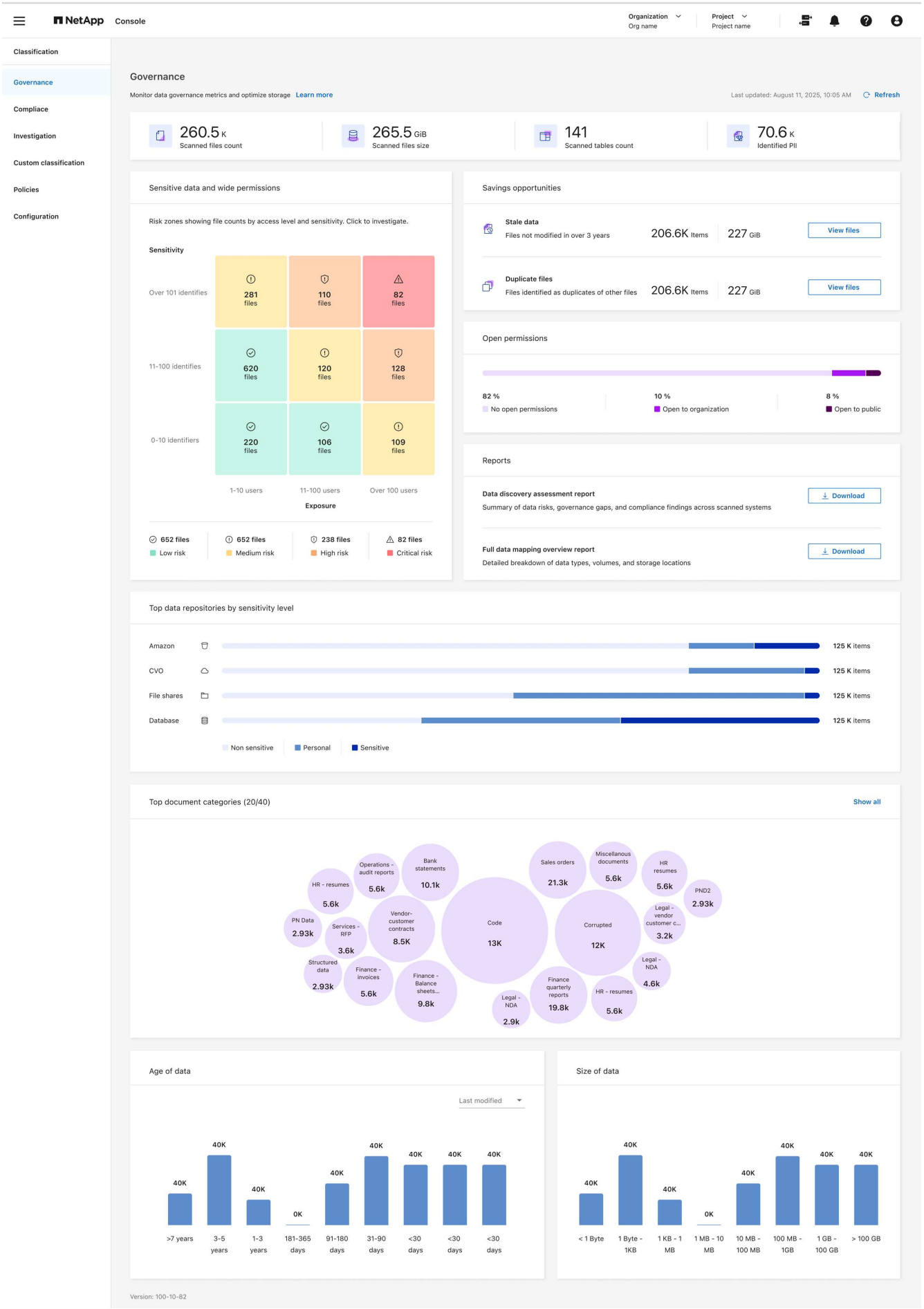
Ottieni il controllo dei costi relativi ai dati sulle risorse di archiviazione della tua organizzazione. NetApp Data Classification identifica la quantità di dati obsoleti, file duplicati e file di grandi dimensioni presenti nei tuoi sistemi, così puoi decidere se rimuovere o spostare alcuni file in un archivio di oggetti meno costoso.

È qui che dovresti iniziare la tua ricerca. Dalla dashboard Governance è possibile selezionare un'area su cui effettuare ulteriori indagini.

Inoltre, se si prevede di migrare i dati da sedi locali al cloud, è possibile visualizzare le dimensioni dei dati e verificare se contengono informazioni sensibili prima di spostarli.

Esaminare la dashboard di governance

La dashboard Governance fornisce informazioni che consentono di aumentare l'efficienza e controllare i costi relativi ai dati archiviati nelle risorse di storage.


NetApp Console
Organization
Org name
Project
Project name
Classification
Governance
Compliace
Investigation
Custom classification
Policies
Configuration
Governance
Monitor data governance metrics and optimize storage Learn more
Last updated: August 11, 2025, 10:05 AM
Refresh
260.5 K
Scanned files count
265.5 GiB
Scanned files size
141
Scanned tables count
70.6 K
Identified PII
Sensitive data and wide permissions
Risk zones showing file counts by access level and sensitivity. Click to investigate.
Sensitivity
Over 101 identifies
11-100 identifies
0-10 identifiers
281 files
110 files
82 files
620 files
120 files
128 files
220 files
106 files
109 files
1-10 users
11-100 users
Over 100 users
Exposure
652 files
Low risk
652 files
Medium risk
238 files
High risk
82 files
Critical risk
Savings opportunities
Stale data
Files not modified in over 3 years
206.6K Items
227 GiB
View files
Duplicate files
Files identified as duplicates of other files
206.6K Items
227 GiB
View files
Open permissions
82 %
No open permissions
10 %
Open to organization
8 %
Open to public
Reports
Data discovery assessment report
Summary of data risks, governance gaps, and compliance findings across scanned systems
Download
Full data mapping overview report
Detailed breakdown of data types, volumes, and storage locations
Download
Top data repositories by sensitivity level
Amazon
CVO
File shares
Database
125 K items
Non sensitive
Personal
Sensitive
Top document categories (20/40)
Show all
Operations - audit reports 5.6k
Bank statements 10.1k
Sales orders 21.3k
Miscellanous documents 5.6k
HR resumes 5.6k
PND2 2.93k
HR - resumes 5.6k
PN Data 2.93k
Services - RFP 3.6k
Vendor-customer contracts 8.5K
Code 13K
Corrupted 12K
Legal - vendor customer c... 3.2k
Structured data 2.93k
Finance - invoices 5.6k
Finance - Balance sheets... 9.8k
Legal - NDA 2.9k
Finance quarterly reports 19.8k
HR - resumes 5.6k
Legal - NDA 4.6k
Age of data
Last modified
40K
>7 years
40K
3-5 years
40K
1-3 years
0K
181-365 days
40K
91-180 days
40K
31-90 days
40K
<30 days
40K
<30 days
40K
<30 days
Size of data
40K
< 1 Byte
40K
1 Byte - 1KB
40K
1 KB - 1 MB
0K
1 MB - 10 MB
40K
10 MB - 100 MB
40K
100 MB - 1GB
40K
1 GB - 100 GB
40K
> 100 GB
Version: 100-10-82

Passi

1. Dal menu NetApp Console , selezionare **Governance > Classificazione**.
2. Selezionare **Governance**.

   Viene visualizzata la dashboard Governance.

Esaminare le opportunità di risparmio

Il componente *Opportunità di risparmio* mostra i dati che è possibile eliminare o spostare in un archivio di oggetti meno costoso. I dati in *Opportunità di risparmio* vengono aggiornati ogni 2 ore. È anche possibile aggiornare manualmente i dati.

Passi

1. Dal menu Classificazione dati, selezionare **Governance**.
2. In ogni riquadro Opportunità di risparmio della dashboard Governance, seleziona **Ottimizza archiviazione** per visualizzare i risultati filtrati nella pagina Indagine. Per scoprire quali dati dovresti eliminare o spostare in un archivio meno costoso, esamina le *Opportunità di risparmio*.
   - **Dati obsoleti** - Dati modificati l'ultima volta più di 3 anni fa.
   - **File duplicati**: file duplicati in altre posizioni nelle origini dati sottoposte a scansione. "Visualizza quali tipi di file duplicati vengono visualizzati" .

> Se una qualsiasi delle tue origini dati implementa la suddivisione in livelli dei dati, i vecchi dati che risiedono già nell'archiviazione degli oggetti possono essere identificati nella categoria *Dati obsoleti*.

Creare il report di valutazione della scoperta dei dati

Il rapporto di valutazione della scoperta dei dati fornisce un'analisi di alto livello dell'ambiente scansionato per evidenziare le aree problematiche e i potenziali interventi di risanamento. I risultati si basano sia sulla mappatura che sulla classificazione dei dati. L'obiettivo di questo rapporto è quello di aumentare la consapevolezza di tre aspetti significativi del tuo set di dati:

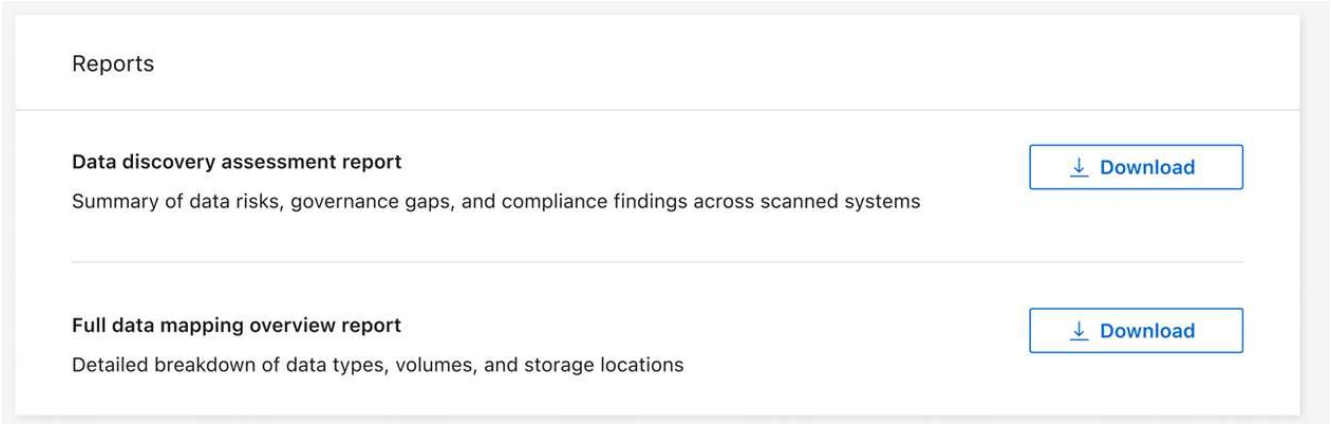
Caratteristica	Descrizione
Preoccupazioni sulla governance dei dati	Un quadro dettagliato di tutti i dati in tuo possesso e delle aree in cui potresti ridurre la quantità di dati per risparmiare sui costi.
Esposizioni alla sicurezza dei dati	Aree in cui i tuoi dati sono accessibili ad attacchi interni o esterni grazie ad ampi permessi di accesso.
Lacune nella conformità dei dati	Dove si trovano i tuoi dati personali o sensibili, sia per motivi di sicurezza che per le richieste di accesso ai dati (DSAR).

Con il report puoi intraprendere le seguenti azioni:

- Riduci i costi di archiviazione modificando i criteri di conservazione oppure spostando o eliminando determinati dati (obsoleti o duplicati).
- Proteggi i tuoi dati con autorizzazioni estese rivedendo le policy di gestione del gruppo globale.
- Proteggi i tuoi dati contenenti informazioni personali o sensibili spostando le informazioni personali identificabili (PII) in archivi dati più sicuri.

Passi

1. Da Classificazione dati, seleziona **Governance**.
2. Nel riquadro dei report, seleziona **Report di valutazione della scoperta dei dati**.



Risultato

La classificazione dei dati genera un report in formato PDF che puoi rivedere e condividere.

Creare il report di panoramica della mappatura dei dati

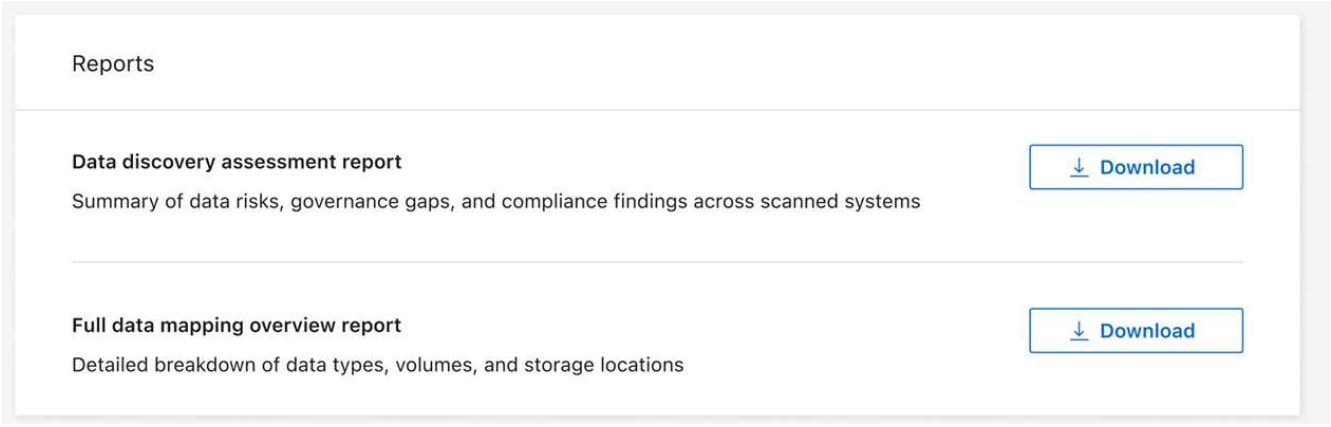
Il report di panoramica sulla mappatura dei dati fornisce una panoramica dei dati archiviati nelle fonti dati aziendali per assisterti nelle decisioni relative ai processi di migrazione, backup, sicurezza e conformità. Il rapporto riassume tutti i sistemi e le fonti di dati. Fornisce inoltre un'analisi per ciascun sistema.

Il rapporto include le seguenti informazioni:

Categoria	Descrizione
Capacità di utilizzo	Per tutti i sistemi: elenca il numero di file e la capacità utilizzata per ciascun sistema. Per sistemi singoli: elenca i file che utilizzano la maggiore capacità.
L'età dei dati	Fornisce tre grafici e diagrammi che indicano quando i file sono stati creati, modificati per l'ultima volta o a cui è stato effettuato l'ultimo accesso. Elenca il numero di file e la loro capacità utilizzata in base a determinati intervalli di date.
Dimensione dei dati	Elenca il numero di file presenti nei tuoi sistemi entro determinati intervalli di dimensioni.

Passi

1. Da Classificazione dati, seleziona **Governance**.
2. Nel riquadro dei report, seleziona **Report di panoramica completa della mappatura dei dati**.



Risultato

La classificazione dei dati genera un report PDF che puoi rivedere e inviare ad altri gruppi, se necessario.

Se il report è più grande di 1 MB, il file PDF viene conservato nell'istanza di Data Classification e verrà visualizzato un messaggio pop-up con la posizione esatta. Quando Data Classification è installato su una macchina Linux in sede o su una macchina Linux distribuita nel cloud, è possibile accedere direttamente al file PDF. Quando Data Classification viene distribuito nel cloud, è necessario autorizzare tramite SSH l'istanza di Data Classification per scaricare il file PDF.

Esamina i principali repository di dati elencati in base alla sensibilità dei dati

L'area *Principali repository di dati per livello di sensibilità* del report Panoramica mappatura dati elenca i quattro principali repository di dati (sistemi e origini dati) che contengono gli elementi più sensibili. Il grafico a barre per ciascun sistema è suddiviso in:

- Dati non sensibili
- Dati personali
- Dati personali sensibili

Questi dati vengono aggiornati ogni due ore e possono essere aggiornati manualmente.

Passi

1. Per visualizzare il numero totale di elementi in ogni categoria, posiziona il cursore su ogni sezione della barra.
2. Per filtrare i risultati che appariranno nella pagina Indagine, seleziona ciascuna area nella barra e prosegui nell'indagine.

Esaminare i dati sensibili e le autorizzazioni estese

L'area *Dati sensibili e autorizzazioni estese* della dashboard Governance mostra i conteggi dei file che contengono dati sensibili e dispongono di autorizzazioni estese. Nella tabella sono riportati i seguenti tipi di autorizzazioni:

- Dai permessi più restrittivi alle restrizioni più permissive sull'asse orizzontale.
- Dai dati meno sensibili a quelli più sensibili sull'asse verticale.

Passi

1. Per visualizzare il numero totale di file in ogni categoria, posiziona il cursore su ogni casella.

2. Per filtrare i risultati che appariranno nella pagina Indagine, seleziona una casella e prosegui l'indagine.

Esaminare i dati elencati in base ai tipi di autorizzazioni aperte

L'area *Autorizzazioni aperte* del report Panoramica mappatura dati mostra la percentuale per ciascun tipo di autorizzazioni esistenti per tutti i file sottoposti a scansione. Il grafico mostra i seguenti tipi di autorizzazioni:

- Nessuna autorizzazione aperta
- Aperto all'organizzazione
- Aperto al pubblico
- Accesso sconosciuto

Passi

1. Per visualizzare il numero totale di file in ogni categoria, posiziona il cursore su ogni casella.
2. Per filtrare i risultati che appariranno nella pagina Indagine, seleziona una casella e prosegui l'indagine.

Esaminare l'età e la dimensione dei dati

È possibile esaminare gli elementi nei grafici *Età* e *Dimensione* del report Panoramica mappatura dati per verificare se vi sono dati da eliminare o da spostare in un archivio di oggetti meno costoso.

Passi

1. Nel grafico Età dei dati, per visualizzare i dettagli sull'età dei dati, posizionare il cursore su un punto del grafico.
2. Per filtrare in base a un intervallo di età o di taglia, seleziona l'età o la taglia desiderata.
    - **Grafico Età dei dati** - Categorizza i dati in base all'ora in cui sono stati creati, all'ultima volta che vi si è avuto accesso o all'ultima volta che sono stati modificati.
    - **Grafico Dimensioni dei dati** - Categorizza i dati in base alle dimensioni.

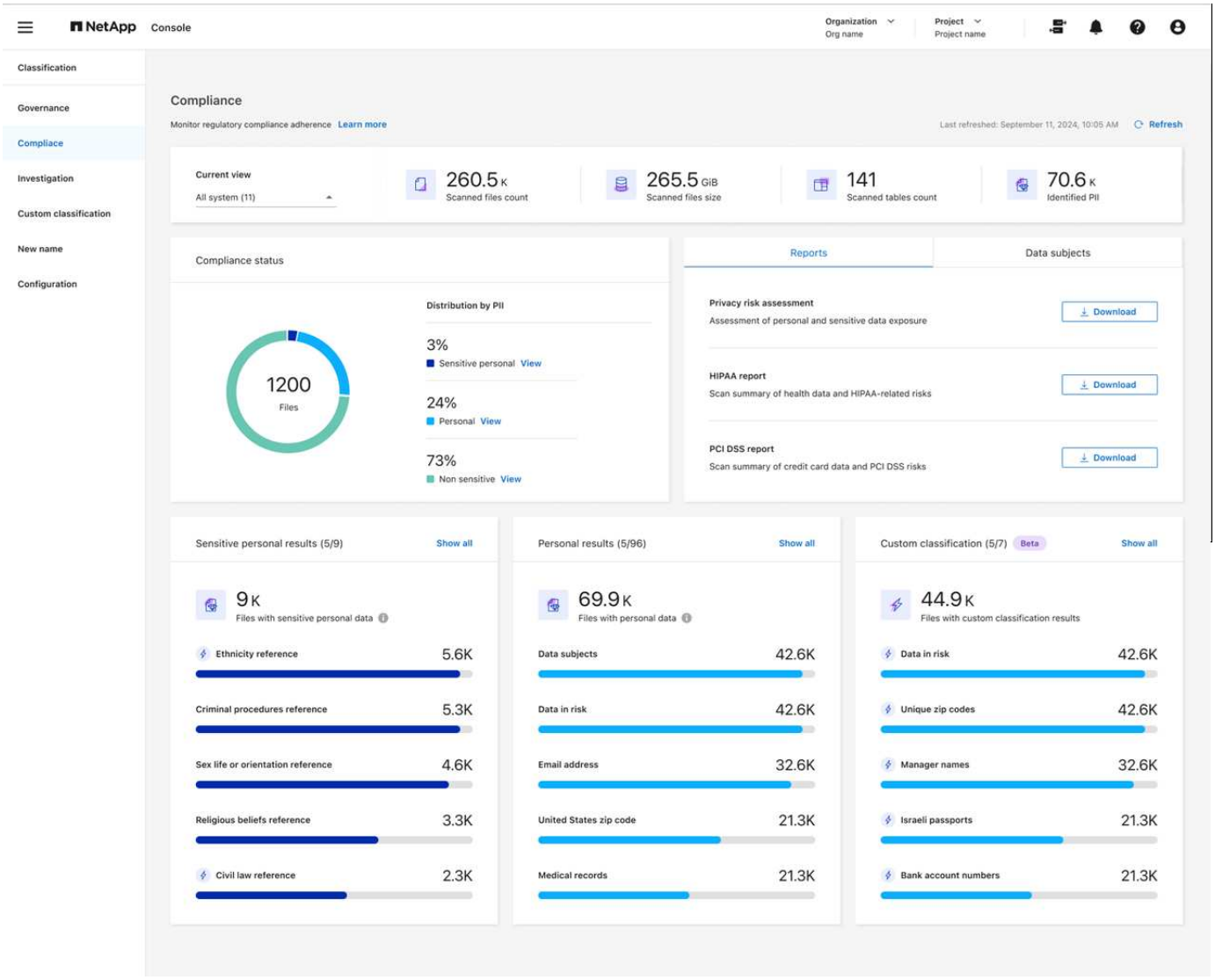
Se una qualsiasi delle tue origini dati implementa la suddivisione in livelli dei dati, i vecchi dati già presenti nell'archiviazione degli oggetti potrebbero essere identificati nel grafico *Age of Data*.

Visualizza i dettagli di conformità sui dati privati archiviati nella tua organizzazione con NetApp Data Classification

Ottieni il controllo dei tuoi dati privati visualizzando i dettagli sui dati personali (PII) e sui dati personali sensibili (SPII) nella tua organizzazione. Puoi anche ottenere visibilità esaminando le categorie e i tipi di file che NetApp Data Classification ha trovato nei tuoi dati.

I dettagli sulla conformità a livello di file sono disponibili solo se si esegue una scansione completa della classificazione. Le scansioni di sola mappatura non forniscono dettagli a livello di file.

Per impostazione predefinita, la dashboard Classificazione dati visualizza i dati di conformità per tutti i sistemi e database. Per visualizzare i dati solo di alcuni sistemi, selezionarli.



È possibile filtrare i risultati dalla pagina Indagine dati e scaricare un report dei risultati come file CSV. Vedere"Filtraggio dei dati nella pagina Indagine sui dati" per i dettagli.

Visualizza i file che contengono dati personali

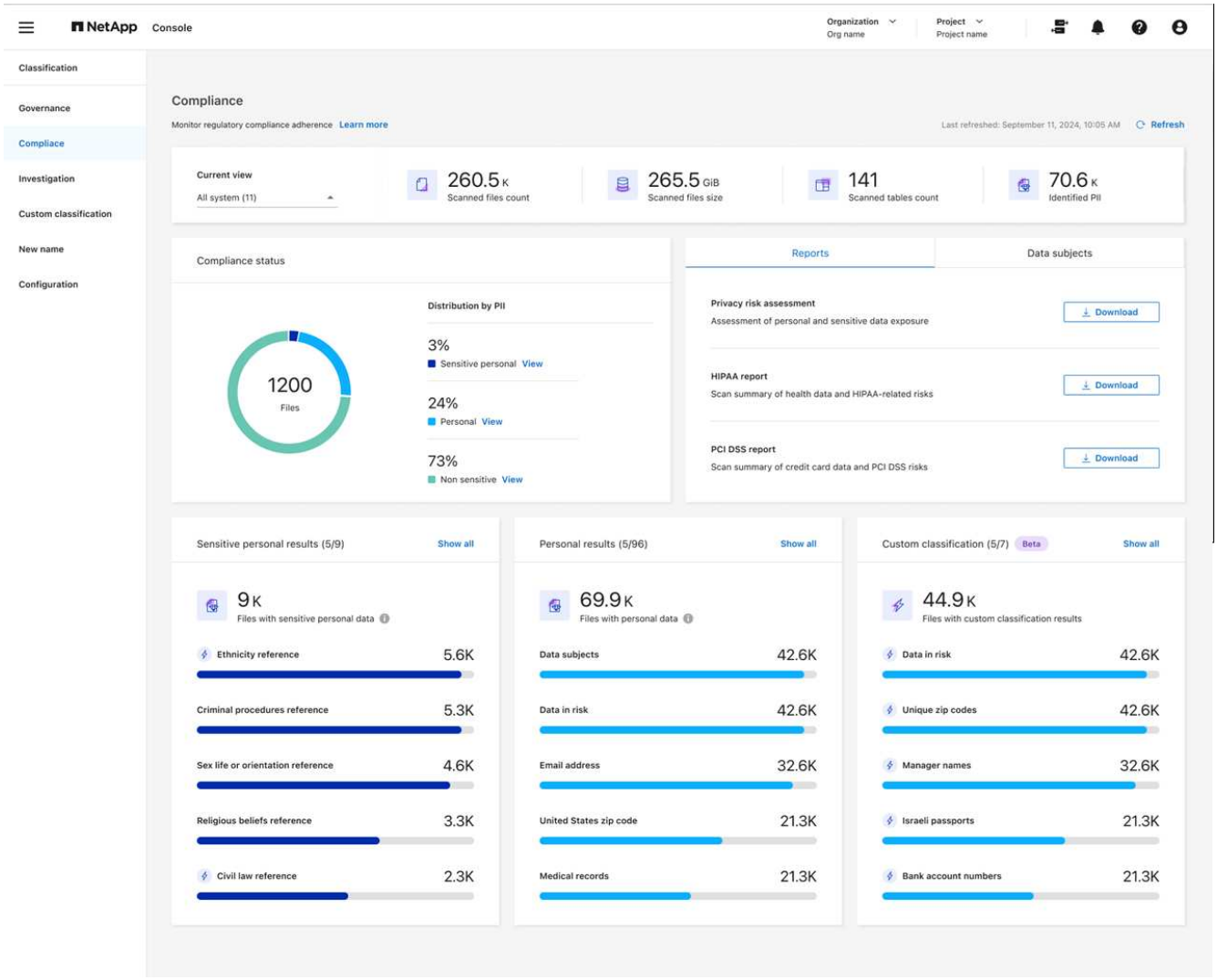
La classificazione dei dati identifica automaticamente parole, stringhe e modelli specifici (Regex) all'interno dei dati. "Ad esempio, numeri di carte di credito, numeri di previdenza sociale, numeri di conti bancari, password e altro ancora."La classificazione dei dati identifica questo tipo di informazioni nei singoli file, nei file all'interno delle directory (condivisioni e cartelle) e nelle tabelle del database.

Puoi anche creare termini di ricerca personalizzati per identificare dati personali specifici della tua organizzazione. Per ulteriori informazioni, consultare "Crea una classificazione personalizzata" .

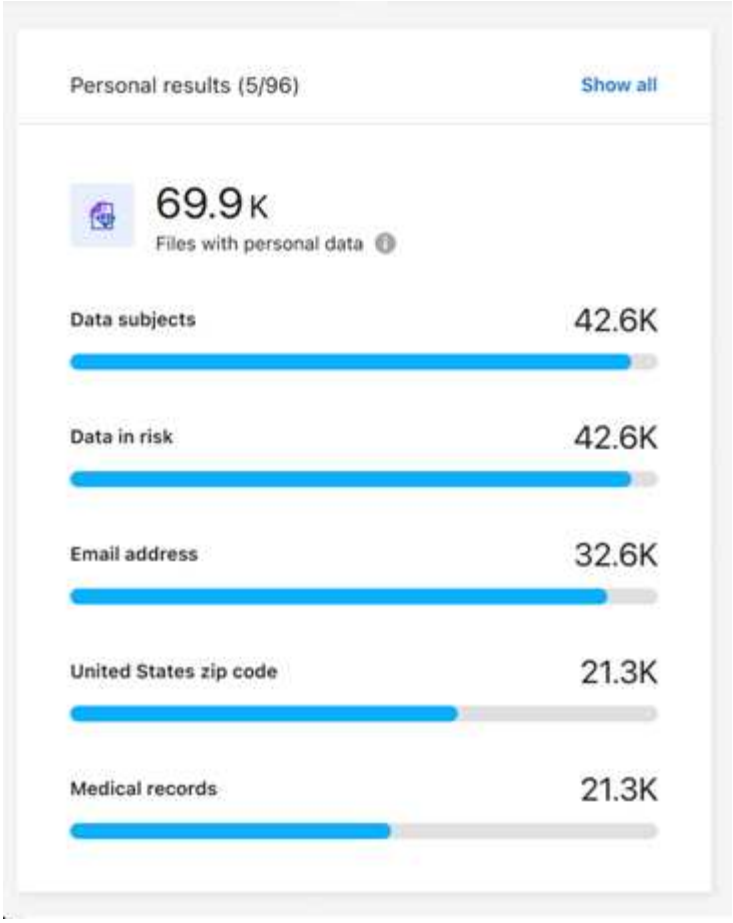
Per alcuni tipi di dati personali, la classificazione dei dati utilizza la *validazione di prossimità* per convalidare i propri risultati. La validazione avviene ricercando una o più parole chiave predefinite in prossimità dei dati personali trovati. Ad esempio, la classificazione dei dati identifica un numero di previdenza sociale (SSN) statunitense come SSN se vede una parola di prossimità accanto ad esso, ad esempio *SSN* o *previdenza sociale*. "La tabella dei dati personali" mostra quando la classificazione dei dati utilizza la convalida di prossimità.

Passi

1. Dal menu Classificazione dati, selezionare la scheda **Conformità**.
2. Per esaminare i dettagli di tutti i dati personali, selezionare l'icona accanto alla percentuale dei dati personali.

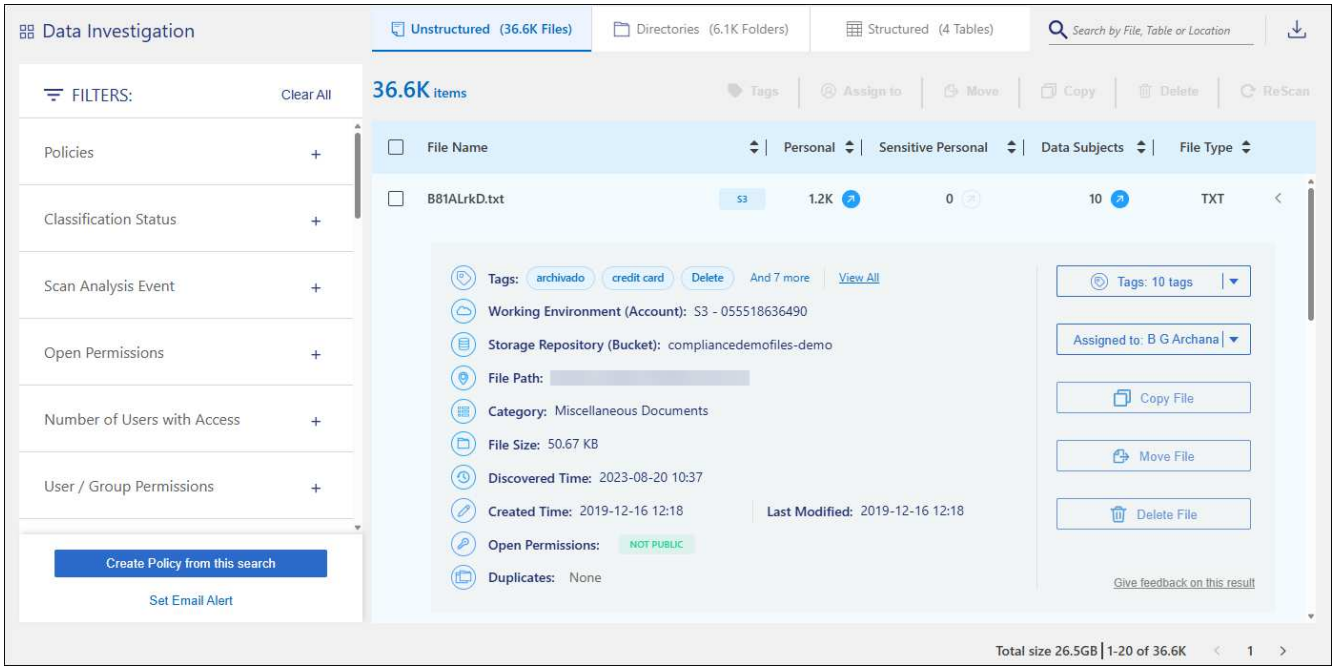


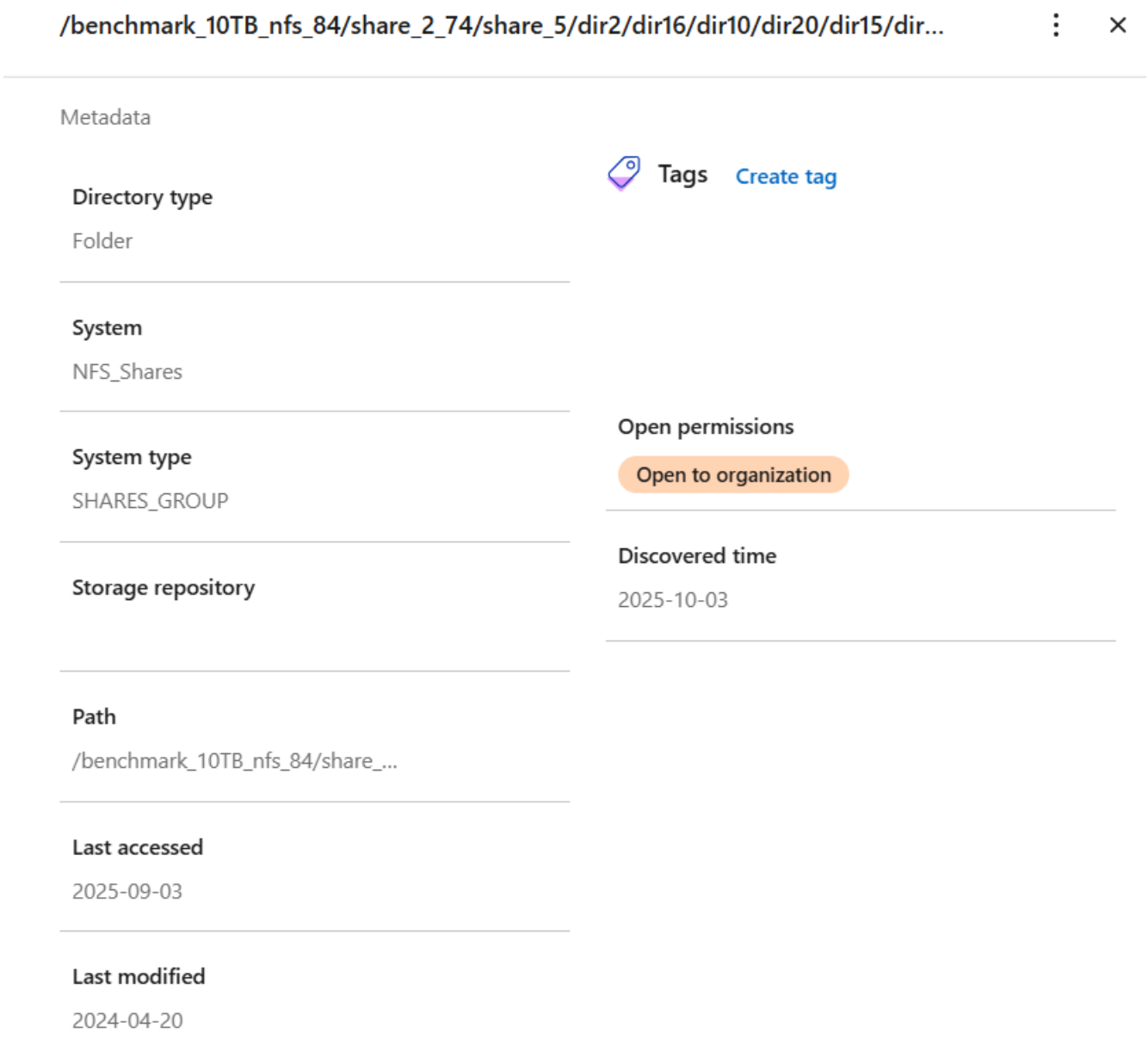
3. Per esaminare i dettagli di un tipo specifico di dati personali, seleziona **Visualizza tutto** e poi seleziona l'icona a freccia **Esamina risultati** per un tipo specifico di dati personali, ad esempio indirizzi e-mail.



4. Esamina i dati cercando, ordinando, espandendo i dettagli per un file specifico, selezionando la freccia **Esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

   Le immagini seguenti mostrano i dati personali presenti in una directory (condivisioni e cartelle). Nella scheda **Strutturato** puoi visualizzare i dati personali presenti nei database. Nella scheda **Non strutturato** è possibile visualizzare i dati a livello di file.





Visualizza i file che contengono dati personali sensibili

La classificazione dei dati identifica automaticamente tipi speciali di informazioni personali sensibili, come definito dalle normative sulla privacy come "articoli 9 e 10 del GDPR" . Ad esempio, informazioni riguardanti la salute, l'origine etnica o l'orientamento sessuale di una persona. "Vedi l'elenco completo" . La classificazione dei dati identifica questo tipo di informazioni nei singoli file, nei file all'interno delle directory (condivisioni e cartelle) e nelle tabelle del database.

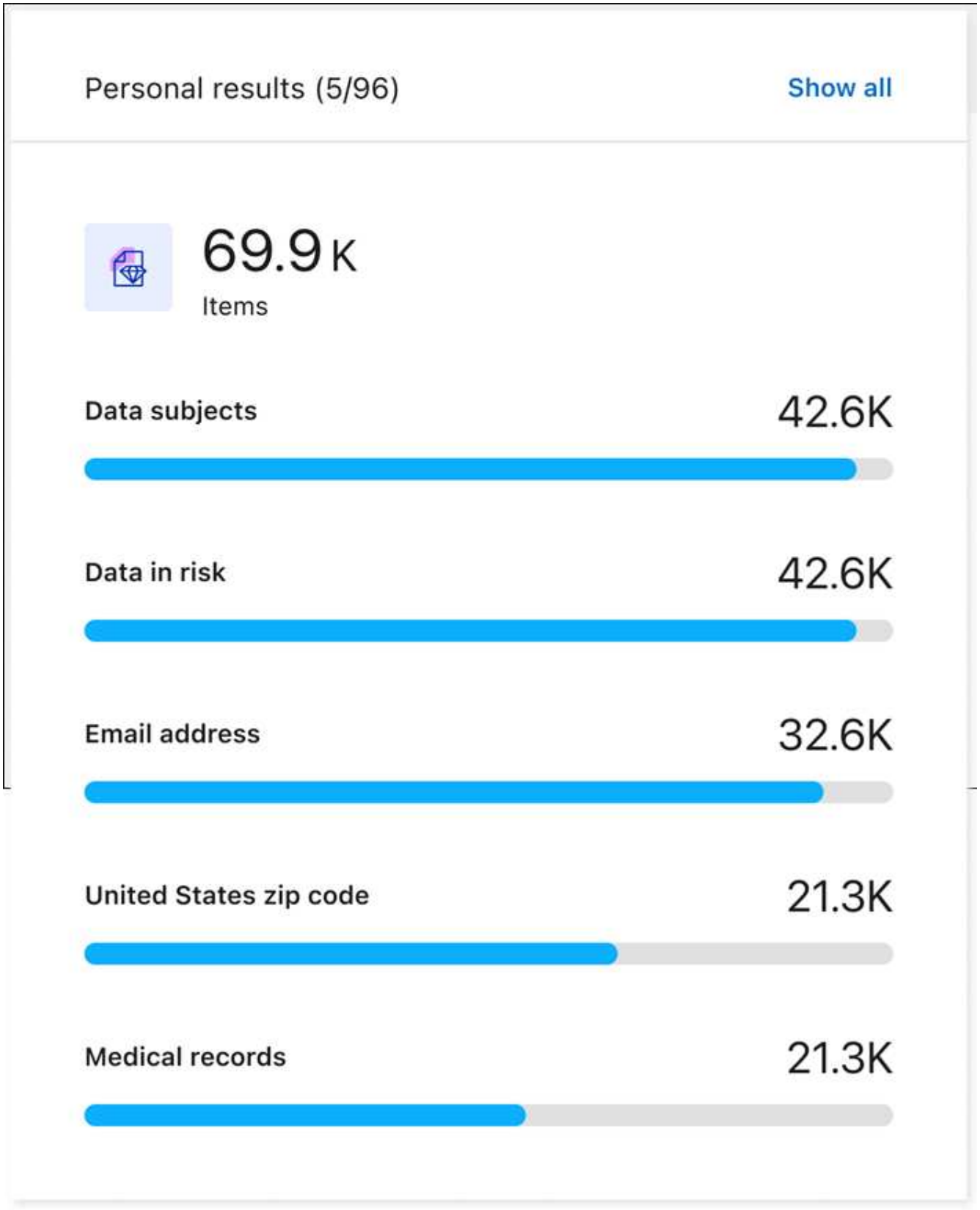
La classificazione dei dati utilizza l'intelligenza artificiale, l'elaborazione del linguaggio naturale (NLP), l'apprendimento automatico (ML) e il cognitive computing (CC) per comprendere il significato del contenuto analizzato, al fine di estrarre entità e categorizzarle di conseguenza.

Ad esempio, una categoria di dati sensibili del GDPR è l'origine etnica. Grazie alle sue capacità di NLP, la classificazione dei dati è in grado di distinguere tra una frase che recita "George è messicano" (che indica dati sensibili come specificato nell'articolo 9 del GDPR) e una frase che dice "George sta mangiando cibo messicano".

Per la scansione dei dati personali sensibili è supportata solo la lingua inglese. In seguito verrà aggiunto il supporto per altre lingue.

Passi

1. Dal menu Classificazione dati, selezionare **Conformità**.
2. Per esaminare i dettagli di tutti i dati personali sensibili, individua la scheda **Risultati personali sensibili**, quindi seleziona **Mostra tutto**.



.

3. Per esaminare i dettagli di un tipo specifico di dati personali sensibili, seleziona **Visualizza tutto**, quindi seleziona l'icona a freccia **Esamina risultati** per un tipo specifico di dati personali sensibili.
4. Esamina i dati cercando, ordinando, espandendo i dettagli per un file specifico, cliccando su **Esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

Categorie di dati privati nella NetApp Data Classification

Esistono molti tipi di dati privati che NetApp Data Classification può identificare nei volumi e nei database.

La classificazione dei dati identifica due tipi di dati personali:

- **Informazioni personali identificabili (PII)**
- **Informazioni personali sensibili (SPII)**

Se hai bisogno della classificazione dei dati per identificare altri tipi di dati privati, come numeri di identificazione nazionali aggiuntivi o identificatori sanitari, contatta il tuo account manager.

Tipi di dati personali

I dati personali, o *informazioni di identificazione personale* (PII), presenti nei file possono essere dati personali generali o identificatori nazionali. La terza colonna nella tabella sottostante identifica se la classificazione dei dati utilizza"convalida di prossimità" per convalidare i risultati per l'identificatore.

Nella tabella sono indicate le lingue in cui questi elementi possono essere riconosciuti.

Tipo	Identificatore	Validazione di prossimità?	Inglese	tedesco	spagnolo	francese	giapponese
Generale	Numero di carta di credito	SÌ	✓	✓	✓		✓
	Interessati	NO	✓	✓	✓		
	Indirizzo e-mail	NO	✓	✓	✓		✓
	Numero IBAN (numero di conto bancario internazionale)	NO	✓	✓	✓		✓
	Indirizzo IP	NO	✓	✓	✓		✓
	Password	SÌ	✓	✓	✓		✓

Tipo	Identificatore	Validazione di prossimità?	Inglese	tedesco	spagnolo	francese	giapponese
Identificatori nazionali							

Tipo	Identificatore	Validazione di prossimità?	Inglese	tedesco	spagnolo	francese	giapponese

Tipo	Identificatore	Validazione di prossimità?	Inglese	tedesco	spagnolo	francese	giapponese

Tipo	Identificatore	Validazione di prossimità?	Inglese	tedesco	spagnolo	francese	giapponese
	aziendale)						
	Carta d’identità lettone	SÌ	✓	✓	✓		
	Carta d’identità lituana	SÌ	✓	✓	✓		
	Carta d’identità lussemburghese	SÌ	✓	✓	✓		
	Carta d’identità maltese	SÌ	✓	✓	✓		
	Numero del Servizio Sanitario Nazionale (NHS)	SÌ	✓	✓	✓		
	Conto bancario in Nuova Zelanda	SÌ	✓	✓	✓		
	Patente di guida neozelandese	SÌ	✓	✓	✓		
	Numero IRD (codice fiscale) della Nuova Zelanda	SÌ	✓	✓	✓		
	Numero NHI (Indice Nazionale di Salute) della Nuova Zelanda	SÌ	✓	✓	✓		
	Numero di passaporto neozelandese	SÌ	✓	✓	✓		
	Carta d’identità polacca (PESEL)	SÌ	✓	✓	✓		
	Numero di identificazione fiscale portoghese (NIF)	SÌ	✓	✓	✓		
	Carta d’identità rumena (CNP)	SÌ	✓	✓	✓		
	Carta d’identità nazionale di registrazione di Singapore (NRIC)	SÌ	✓	✓	✓		
	Carta d’identità slovena (EMSO)	SÌ	✓	✓	✓		
	Documento d’identità sudafricano	SÌ	✓	✓	✓		
	Codice fiscale spagnolo	SÌ	✓	✓	✓		
	Carta d’identità svedese	SÌ	✓	✓	✓		
	ID UK (NINO)	SÌ	✓	✓	✓		
	Patente di guida USA California	SÌ	✓	✓	✓		
	Patente di guida USA Indiana	SÌ	✓	✓	✓		
	Patente di guida USA New York	SÌ	✓	✓	✓		
	Patente di guida USA Texas	SÌ	✓	✓	✓		
	Numero di previdenza sociale (SSN) degli Stati Uniti	SÌ	✓	✓	✓		

Tipi di dati personali sensibili

La classificazione dei dati può trovare le seguenti informazioni personali sensibili (SPII) nei file.

I seguenti SPII possono attualmente essere riconosciuti solo in inglese:

- **Riferimento di procedura penale**: dati relativi alle condanne penali e ai reati di una persona fisica.
- **Riferimento etnico**: dati relativi all’origine razziale o etnica di una persona fisica.
- **Riferimento sanitario**: dati relativi alla salute di una persona fisica.

- **Codici medici ICD-9-CM**: codici utilizzati nel settore medico e sanitario.
- **Codici medici ICD-10-CM**: codici utilizzati nel settore medico e sanitario.
- **Riferimento alle convinzioni filosofiche**: dati relativi alle convinzioni filosofiche di una persona fisica.
- **Riferimento alle opinioni politiche**: Dati relativi alle opinioni politiche di una persona fisica.
- **Riferimento alle convinzioni religiose**: dati relativi alle convinzioni religiose di una persona fisica.
- **Riferimento alla vita sessuale o all'orientamento sessuale**: dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Tipi di categorie

La classificazione dei dati categorizza i dati come segue.

La maggior parte di queste categorie può essere riconosciuta in inglese, tedesco e spagnolo.

Categoria	Tipo	Inglese	tedesco	spagnolo
Finanza	Bilanci	✓	✓	✓
	Ordini di acquisto	✓	✓	✓
	Fatture	✓	✓	✓
	Rapporti trimestrali	✓	✓	✓
Risorse umane	Verifiche dei precedenti	✓		✓
	Piani di compensazione	✓	✓	✓
	Contratti dei dipendenti	✓		✓
	Recensioni dei dipendenti	✓		✓
	Salute	✓		✓
	Curriculum	✓	✓	✓
Legal	NDA	✓	✓	✓
	Contratti fornitore-cliente	✓	✓	✓
Marketing	Campagne	✓	✓	✓
	Conferenze	✓	✓	✓
Operazioni	Rapporti di revisione	✓	✓	✓
Saldi	Ordini di vendita	✓	✓	
Servizi	Richiesta di informazioni	✓		✓
	Richiesta di proposta	✓		✓
	SEMINARE	✓	✓	✓
	Formazione	✓	✓	✓
Supporto	Reclami e biglietti	✓	✓	✓

Anche i seguenti metadati sono categorizzati e identificati nelle stesse lingue supportate:

- Dati dell’applicazione
- File di archivio
- Audio
- Breadcrumb da Classificazione dei dati Dati delle applicazioni aziendali
- File CAD
- Codice
- Corrotto
- File di database e indice
- File di progettazione
- Dati dell’applicazione e-mail
- Crittografato (file con un punteggio di entropia elevato)
- Eseguibili
- Dati di applicazione finanziaria
- Dati delle applicazioni sanitarie
- Immagini
- Registri
- Documenti vari
- Presentazioni varie
- Fogli di calcolo vari
- Miscellanea "Sconosciuto"
- File protetti da password
- Dati strutturati
- Video
- File a zero byte

Tipi di file

La classificazione dei dati analizza tutti i file per ottenere informazioni dettagliate su categorie e metadati e visualizza tutti i tipi di file nella sezione Tipi di file della dashboard. Quando la classificazione dei dati rileva informazioni personali identificabili (PII) o quando esegue una ricerca DSAR, sono supportati solo i seguenti formati di file:

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

Accuratezza delle informazioni trovate

NetApp non può garantire l’accuratezza al 100% dei dati personali e dei dati personali sensibili identificati dalla classificazione dei dati. Dovresti sempre convalidare le informazioni esaminando i dati.

Sulla base dei nostri test, la tabella seguente mostra l’accuratezza delle informazioni rilevate da Data Classification. Lo suddividiamo in *precisione* e *richiamo*:

Precisione

La probabilità che ciò che la classificazione dei dati rileva sia stato identificato correttamente. Ad esempio, un tasso di precisione del 90% per i dati personali significa che 9 file su 10 identificati come contenenti informazioni personali, in realtà contengono informazioni personali. 1 file su 10 sarebbe un falso positivo.

Richiamo

La probabilità che la classificazione dei dati trovi ciò che dovrebbe. Ad esempio, un tasso di richiamo del 70% per i dati personali significa che Data Classification può identificare 7 file su 10 che contengono effettivamente informazioni personali nella tua organizzazione. La classificazione dei dati perderebbe il 30% dei dati e questi non verrebbero visualizzati nella dashboard.

Miglioriamo costantemente la precisione dei nostri risultati. Tali miglioramenti saranno automaticamente disponibili nelle future versioni di Data Classification.

Tipo	Precisione	Richiamo
Dati personali - Generale	90%-95%	60%-80%
Dati personali - Identificatori del Paese	30%-60%	40%-60%
Dati personali sensibili	80%-95%	20%-30%
Categorie	90%-97%	60%-80%

Crea una classificazione personalizzata in NetApp Data Classification

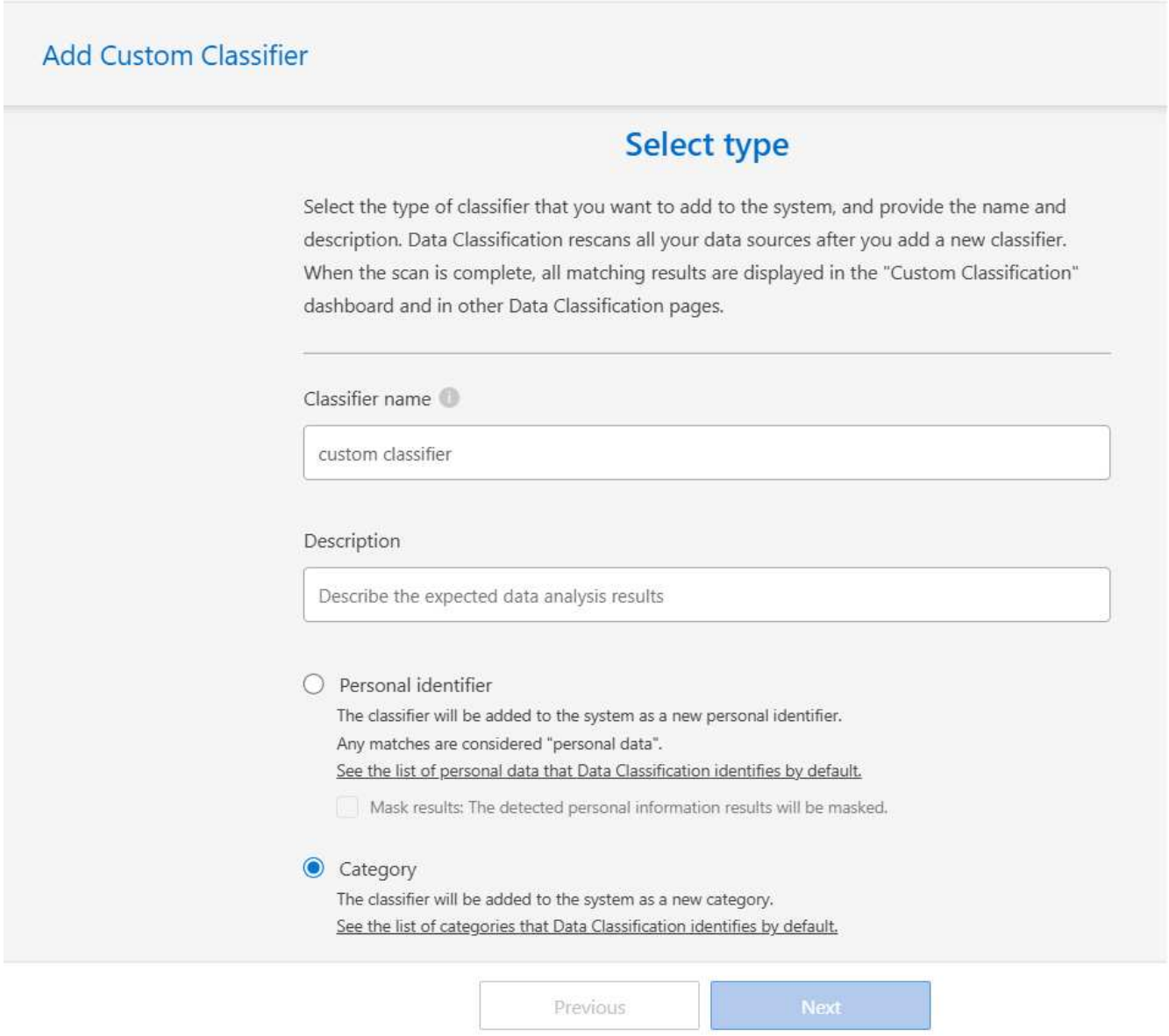
Con NetApp Data Classification puoi creare una ricerca personalizzata per informazioni sensibili. La ricerca può essere limitata a un'espressione regolare (regex).

Crea una classificazione personalizzata

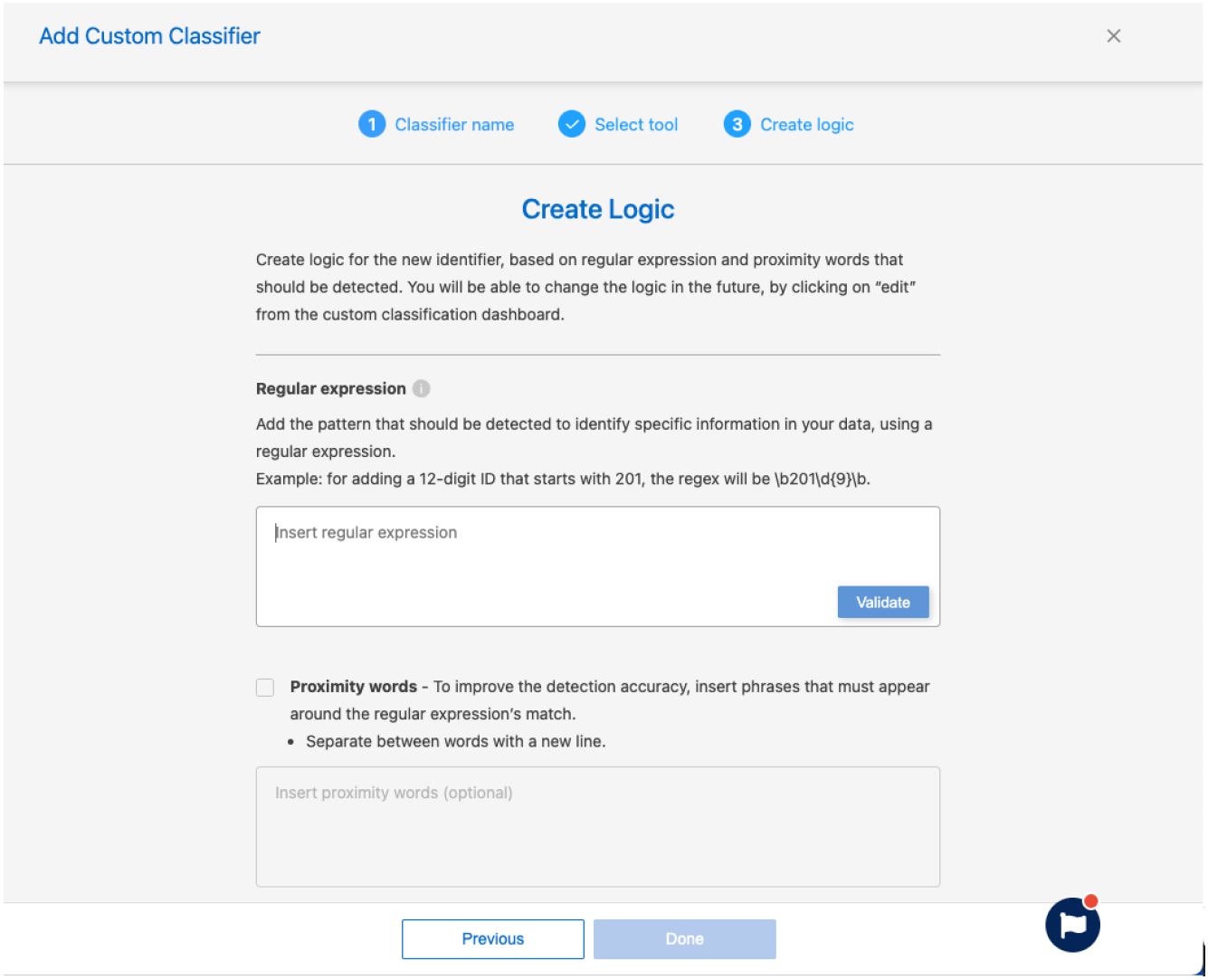
La classificazione personalizzata è disponibile solo per le scansioni Map & Classify, non per le scansioni di sola mappatura. Questa funzionalità è attualmente in anteprima.

Passi

1. Selezionare la scheda **Classificazione personalizzata**.
2. Selezionare il pulsante **Aggiungi nuovo classificatore**.
3. Aggiungere un nome e una descrizione per il nuovo classificatore.
4. Scegli di aggiungere il classificatore come **Identificatore personale** o **Categoria**.



5. Selezionare **Avanti**.
6. Per aggiungere la personalizzazione come espressione regolare, seleziona **Espressione regolare personalizzata**, quindi **Avanti**.
7. Aggiungi uno schema per rilevare le informazioni specifiche dei tuoi dati. Selezionare **Convalida** per confermare la sintassi della
voce.



8. Selezionare **Fine** per creare la classificazione personalizzata.

La nuova personalizzazione verrà acquisita nella successiva scansione pianificata. Per visualizzare i risultati, vedereGenerare report di conformità .

Esamina i dati archiviati nella tua organizzazione con NetApp Data Classification

La dashboard di Data Investigation visualizza informazioni dettagliate sui dati a livello di file e directory, consentendo di ordinare e filtrare i risultati. La pagina Analisi dati fornisce approfondimenti sui metadati e sulle autorizzazioni di file e directory, nonché sull'identificazione dei file duplicati. Grazie alle informazioni a livello di file, directory e database, puoi adottare misure per migliorare la conformità della tua organizzazione e risparmiare spazio di archiviazione. La pagina di analisi dei dati supporta anche lo spostamento, la copia e l'eliminazione dei file.

Per ottenere informazioni dalla pagina Indagine, è necessario eseguire una scansione completa della classificazione sulle origini dati. Le origini dati sottoposte a scansione solo di mappatura non mostrano dettagli a livello di file.

Struttura dell'indagine sui dati

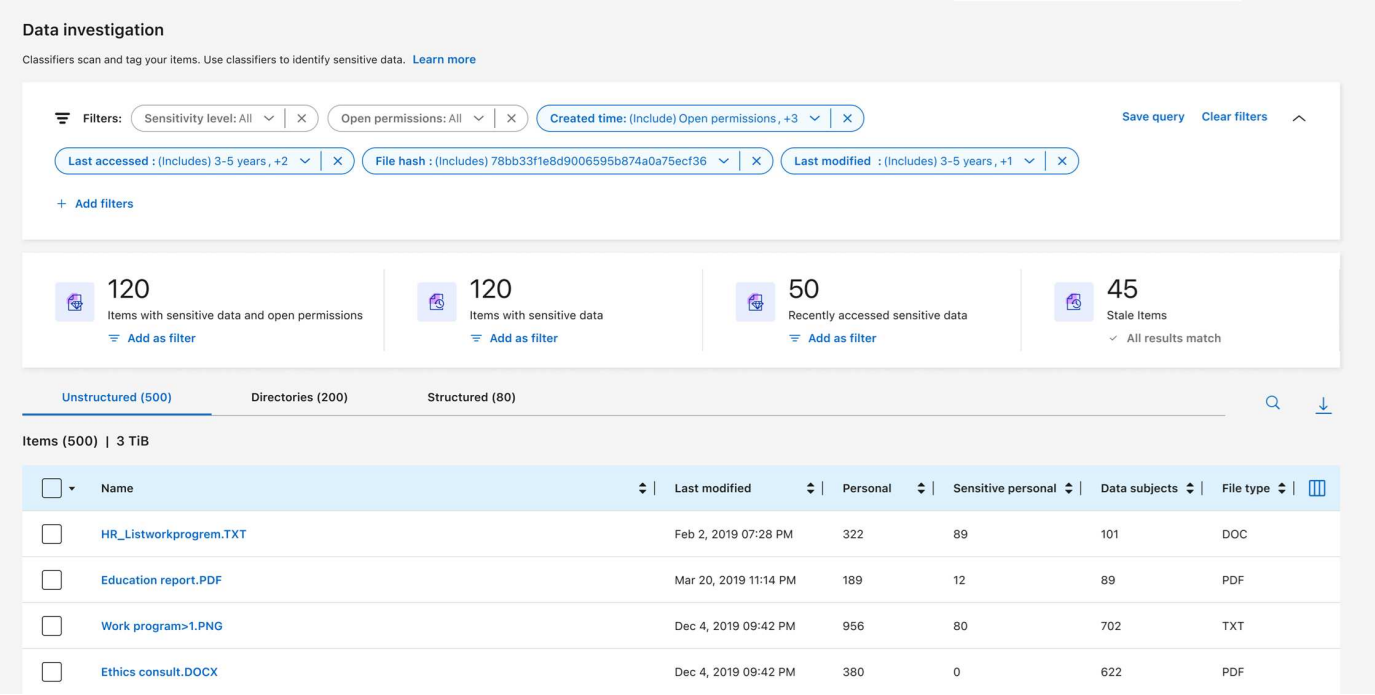
La pagina Indagine sui dati ordina i dati in tre schede:

- **Dati non strutturati**: dati di file
- **Directory**: cartelle e condivisioni di file
- **Strutturato**: database

Filtri dati

La pagina Analisi dati fornisce numerosi filtri per ordinare i dati in modo da poter trovare ciò di cui hai bisogno. È possibile utilizzare più filtri contemporaneamente.

Per aggiungere un filtro, seleziona il pulsante **Aggiungi filtro**.



Sensibilità e contenuto del filtro

Utilizza i seguenti filtri per visualizzare la quantità di informazioni sensibili contenute nei tuoi dati.

Filtro	Dettagli
Categoria	Seleziona il"tipi di categorie" .
Livello di sensibilità	Selezionare il livello di sensibilità: Personale, Personale sensibile o Non sensibile.
Numero di identificatori	Selezionare l'intervallo di identificatori sensibili rilevati per file. Include dati personali e dati personali sensibili. Quando si filtra nelle directory, la classificazione dei dati somma le corrispondenze di tutti i file in ogni cartella (e sottocartelle). NOTA: nella versione di dicembre 2023 (1.26.6) è stata rimossa l'opzione per calcolare il numero di dati di informazioni personali identificabili (PII) per directory.

Filtro	Dettagli
Dati personali	Seleziona il"tipi di dati personali" .
Dati personali sensibili	Seleziona il"tipi di dati personali sensibili" .
Interessato	Inserire il nome completo o un identificativo noto dell'interessato. "Scopri di più sugli interessati qui" .

Filtra il proprietario dell'utente e i permessi dell'utente

Utilizza i seguenti filtri per visualizzare i proprietari dei file e le autorizzazioni per accedere ai tuoi dati.

Filtro	Dettagli
Permessi aperti	Selezionare il tipo di autorizzazioni all'interno dei dati e all'interno delle cartelle/condivisioni.
Autorizzazioni utente/gruppo	Selezionare uno o più nomi utente e/o nomi di gruppo oppure immettere un nome parziale.
Proprietario del file	Inserisci il nome del proprietario del file.
Numero di utenti con accesso	Selezionare uno o più intervalli di categorie per mostrare quali file e cartelle sono aperti a un determinato numero di utenti.

Filtra cronologicamente

Utilizzare i seguenti filtri per visualizzare i dati in base a criteri temporali.

Filtro	Dettagli
Tempo di creazione	Selezionare un intervallo di tempo in cui è stato creato il file. È anche possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca.
Tempo scoperto	Selezionare un intervallo di tempo in cui Data Classification ha rilevato il file. È anche possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca.
Ultima modifica	Seleziona un intervallo di tempo in cui il file è stato modificato l'ultima volta. È anche possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca.
Ultimo accesso	Selezionare un intervallo di tempo in cui è avvenuto l'ultimo accesso al file o alla directory*. È anche possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca. Per i tipi di file analizzati da Data Classification, questa è l'ultima volta che Data Classification ha analizzato il file.

{asterisco} L'orario dell'ultimo accesso a una directory è disponibile solo per le condivisioni NFS o CIFS.

Filtra metadati

Utilizzare i seguenti filtri per visualizzare i dati in base a posizione, dimensione e tipo di directory o file.

Filtro	Dettagli
Percorso del file	Inserisci fino a 20 percorsi parziali o completi che desideri includere o escludere dalla query. Se si immettono sia percorsi di inclusione che percorsi di esclusione, Data Classification trova prima tutti i file nei percorsi inclusi, quindi rimuove i file dai percorsi esclusi e infine visualizza i risultati. Tieni presente che l'utilizzo di "*" in questo filtro non ha alcun effetto e che non puoi escludere cartelle specifiche dalla scansione: verranno scansionate tutte le directory e i file in una condivisione configurata.
Tipo di directory	Selezionare il tipo di directory: "Condividi" o "Cartella".
Tipo di file	Seleziona il"tipi di file" .
Dimensione del file	Seleziona l'intervallo di dimensioni del file.
Hash del file	Inserisci l'hash del file per trovare un file specifico, anche se il nome è diverso.

Tipo di archiviazione filtro

Utilizzare i seguenti filtri per visualizzare i dati in base al tipo di archiviazione.

Filtro	Dettagli
Tipo di sistema	Selezionare il tipo di sistema.
Nome dell'ambiente di sistema	Selezionare sistemi specifici.
Deposito di archiviazione	Selezionare il repository di archiviazione, ad esempio un volume o uno schema.

Query filtro

Utilizzare il seguente filtro per visualizzare i dati in base alle query salvate.

Filtro	Dettagli
Query salvata	Selezionare una o più query salvate. Vai al"scheda query salvate" per visualizzare l'elenco delle query salvate esistenti e crearne di nuove.
Etichette	Selezionare"il tag o i tag" che sono assegnati ai tuoi file.

Stato dell'analisi del filtro

Utilizzare il seguente filtro per visualizzare i dati in base allo stato della scansione di classificazione dei dati.

Filtro	Dettagli
Stato dell'analisi	Selezionare un'opzione per visualizzare l'elenco dei file in attesa della prima scansione, in fase di scansione completata, in attesa di nuova scansione o la cui scansione non è riuscita.

Filtro	Dettagli
Evento di analisi della scansione	Seleziona se desideri visualizzare i file che non sono stati classificati perché la classificazione dei dati non è riuscita a ripristinare l'orario dell'ultimo accesso oppure i file che sono stati classificati anche se la classificazione dei dati non è riuscita a ripristinare l'orario dell'ultimo accesso.

"Visualizza i dettagli sul timestamp "ultimo accesso""per maggiori informazioni sugli elementi che compaiono nella pagina Indagine quando si filtra tramite l'evento Analisi scansione.

Filtra i dati per duplicati

Utilizza il seguente filtro per visualizzare i file duplicati nel tuo archivio.

Filtro	Dettagli
Duplicati	Selezionare se il file è duplicato nei repository.

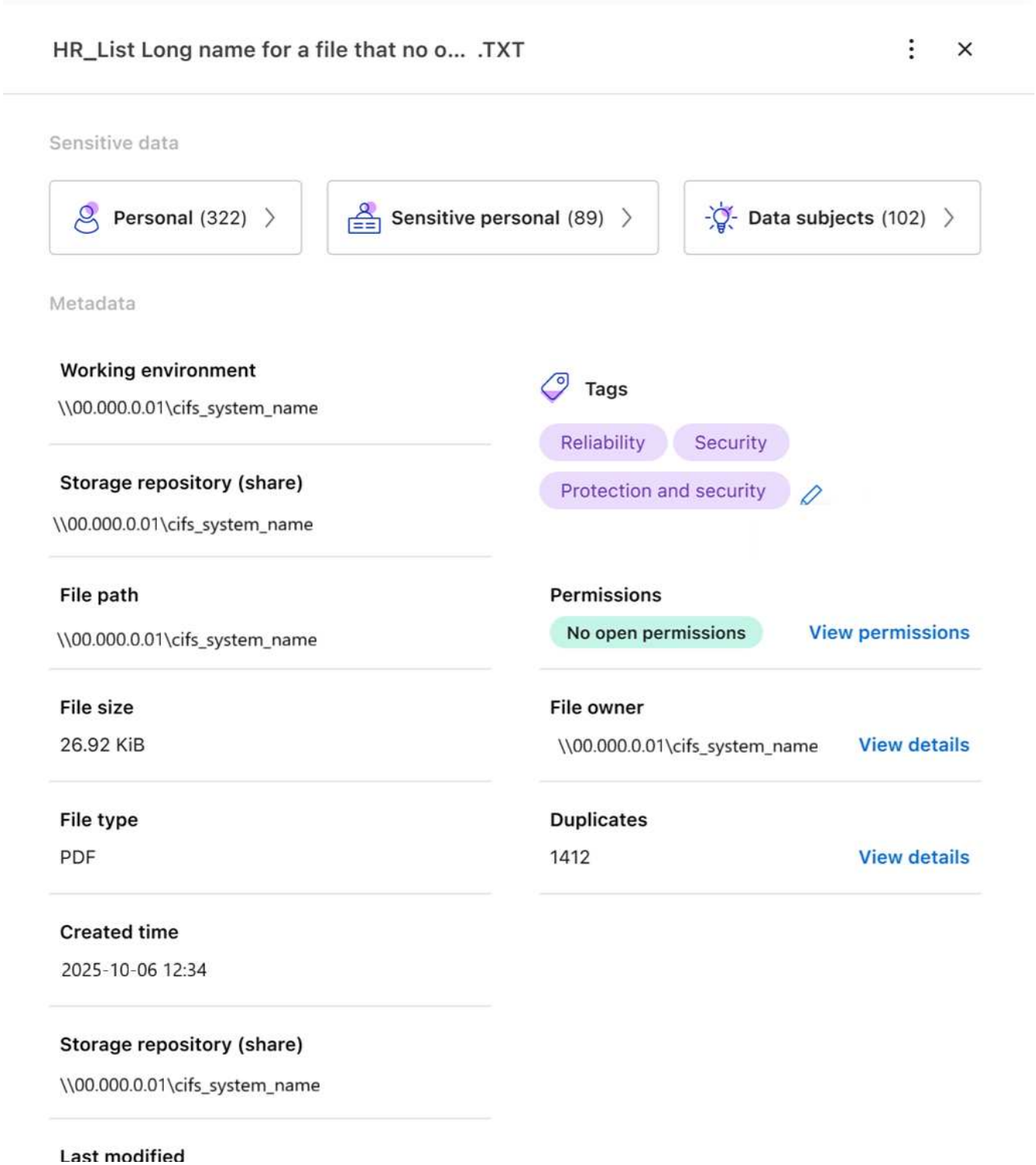
Visualizza i metadati del file

Oltre a mostrare il sistema e il volume in cui risiede il file, i metadati mostrano molte altre informazioni, tra cui le autorizzazioni del file, il proprietario del file e se sono presenti duplicati di questo file. Questa informazione è utile se stai pianificando di"creare query salvate" perché puoi vedere tutte le informazioni che puoi utilizzare per filtrare i tuoi dati.

La disponibilità delle informazioni dipende dalla fonte dei dati. Ad esempio, il nome del volume e le autorizzazioni non vengono condivisi per i file del database.

Passi

1. Dal menu Classificazione dati, selezionare **Indagine**.
2. Nell'elenco Indagine dati a destra, seleziona il cursore verso il basso sulla destra per ogni singolo file per visualizzare i metadati del file.



3. Facoltativamente, puoi creare o aggiungere un tag al file con il pulsante **Crea tag**. Seleziona un tag esistente dal menu a discesa oppure aggiungi un nuovo tag con il pulsante **+ Aggiungi**. I tag possono essere utilizzati per filtrare i dati.

Visualizza i permessi utente per file e directory

Per visualizzare un elenco di tutti gli utenti o gruppi che hanno accesso a un file o a una directory e i tipi di autorizzazioni di cui dispongono, selezionare **Visualizza tutte le autorizzazioni**. Questa opzione è disponibile solo per i dati nelle condivisioni CIFS.

Se si utilizzano identificatori di sicurezza (SID) anziché nomi di utenti e gruppi, è consigliabile integrare Active Directory in Data Classification. Per ulteriori informazioni, consultare "aggiungi Active Directory alla classificazione dei dati" .

Passi

1. Dal menu Classificazione dati, selezionare **Indagine**.
2. Nell'elenco Indagine dati a destra, seleziona il cursore verso il basso sulla destra per ogni singolo file per visualizzare i metadati del file.
3. Per visualizzare un elenco di tutti gli utenti o gruppi che hanno accesso a un file o a una directory e i tipi di autorizzazioni di cui dispongono, nel campo Apri autorizzazioni, selezionare **Visualizza tutte le autorizzazioni**.

   La classificazione dei dati mostra fino a 100 utenti nell'elenco.

4. Seleziona il cursore verso il basso pulsante per qualsiasi gruppo per visualizzare l'elenco degli utenti che fanno parte del gruppo.

   È possibile espandere un livello del gruppo per visualizzare gli utenti che ne fanno parte.

5. Seleziona il nome di un utente o di un gruppo per aggiornare la pagina Indagine, in modo da poter visualizzare tutti i file e le directory a cui l'utente o il gruppo ha accesso.

Controlla i file duplicati nei tuoi sistemi di archiviazione

Puoi verificare se nei tuoi sistemi di archiviazione sono archiviati file duplicati. Questa funzione è utile se si desidera identificare le aree in cui è possibile risparmiare spazio di archiviazione. È inoltre opportuno assicurarsi che determinati file con autorizzazioni specifiche o informazioni sensibili non vengano duplicati inutilmente nei sistemi di archiviazione.

Tutti i file (esclusi i database) che hanno una dimensione pari o superiore a 1 MB o che contengono informazioni personali o sensibili vengono confrontati per verificare se sono presenti duplicati.

La classificazione dei dati utilizza la tecnologia di hashing per individuare i file duplicati. Se un file ha lo stesso codice hash di un altro file, puoi essere sicuro al 100% che i file sono duplicati esatti, anche se i nomi dei file sono diversi.

Passi

1. Dal menu Classificazione dati, selezionare **Indagine**.
2. Nel riquadro Filtro, seleziona "Dimensione file" insieme a "Duplicati" ("Contiene duplicati") per vedere quali file di un certo intervallo di dimensioni sono duplicati nel tuo ambiente.
3. Facoltativamente, scarica l'elenco dei file duplicati e invialo all'amministratore dell'archiviazione, in modo che possa decidere quali file, se presenti, possono essere eliminati.
4. Facoltativamente, puoi eliminare, contrassegnare o spostare i file duplicati. Selezionare i file su cui si desidera eseguire un'azione, quindi selezionare l'azione appropriata.

Visualizza se un file specifico è duplicato

Puoi vedere se un singolo file ha dei duplicati.

Passi

1. Dal menu Classificazione dati, selezionare **Indagine**.
2. Nell'elenco Indagine sui dati, selezionare sulla destra per ogni singolo file per visualizzare i metadati del file.

   Se per un file esistono duplicati, questa informazione viene visualizzata accanto al campo *Duplicati*.

3. Per visualizzare l'elenco dei file duplicati e la loro posizione, selezionare **Visualizza dettagli**.
4. Nella pagina successiva seleziona **Visualizza duplicati** per visualizzare i file nella pagina Indagine.
5. Facoltativamente, puoi eliminare, contrassegnare o spostare i file duplicati. Selezionare i file su cui si desidera eseguire un'azione, quindi selezionare l'azione appropriata.

È possibile utilizzare il valore "hash del file" fornito in questa pagina e inserirlo direttamente nella pagina Indagine per cercare in qualsiasi momento uno specifico file duplicato, oppure è possibile utilizzarlo in una query salvata.

Scarica il tuo report

Puoi scaricare i risultati filtrati in formato CSV o JSON.

Se la classificazione dei dati esegue la scansione di file (dati non strutturati), directory (cartelle e condivisioni di file) e database (dati strutturati), è possibile scaricare fino a tre file di report.

I file vengono suddivisi in file con un numero fisso di righe o record:

- JSON: 100.000 record per report, la cui generazione richiede circa 5 minuti
- CSV: 200.000 record per report, la cui generazione richiede circa 4 minuti

È possibile scaricare una versione del file CSV da visualizzare in questo browser. Questa versione è limitata a 10.000 record.

Cosa è incluso nel report scaricabile

Il **Rapporto dati file non strutturati** include le seguenti informazioni sui tuoi file:

- Nome del file
- Tipo di posizione
- Nome del sistema
- Repository di archiviazione (ad esempio, un volume, un bucket, condivisioni)
- Tipo di repository
- Percorso del file
- Tipo di file
- Dimensione del file (in MB)
- Ora di creazione
- Ultima modifica
- Ultimo accesso
- Proprietario del file

    - I dati del proprietario del file comprendono il nome dell'account, il nome dell'account SAM e l'indirizzo e-mail quando Active Directory è configurato.
- Categoria
- Informazioni personali
- Informazioni personali sensibili
- Permessi aperti
- Errore di analisi della scansione
- Data di rilevamento dell'eliminazione

  La data di rilevamento dell'eliminazione identifica la data in cui il file è stato eliminato o spostato. Ciò consente di identificare quando sono stati spostati file sensibili. I file eliminati non contribuiscono al conteggio dei file visualizzato nella dashboard o nella pagina Indagine. I file vengono visualizzati solo nei report CSV.

Il **Rapporto dati directory non strutturate** include le seguenti informazioni sulle cartelle e sulle condivisioni file:

- Tipo di sistema
- Nome del sistema
- Nome della directory
- Repository di archiviazione (ad esempio, una cartella o condivisioni di file)
- Proprietario della directory
- Ora di creazione
- Tempo scoperto
- Ultima modifica
- Ultimo accesso
- Permessi aperti
- Tipo di directory

Il **Rapporto dati strutturati** include le seguenti informazioni sulle tabelle del database:

- Nome della tabella DB
- Tipo di posizione
- Nome del sistema
- Repository di archiviazione (ad esempio, uno schema)
- Numero di colonne
- Conteggio delle righe
- Informazioni personali
- Informazioni personali sensibili

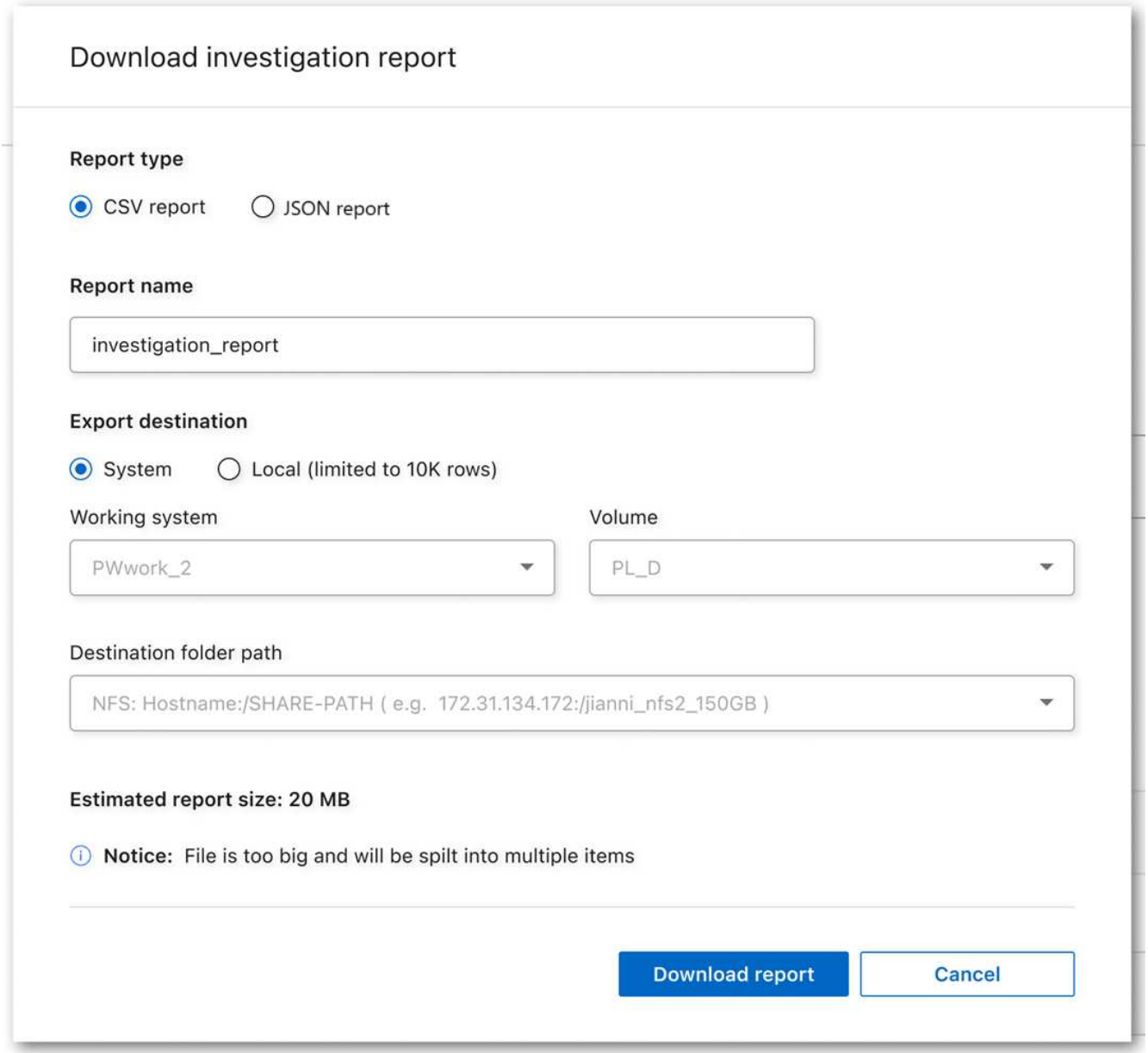
Passaggi per generare il report

1. Dalla pagina Indagine sui dati, selezionare pulsante in alto a destra della pagina.
2. Scegli il tipo di report: CSV o JSON.

3. Inserisci un **Nome del report**.
4. Per scaricare il report completo, seleziona **Sistema**, quindi scegli **Sistema** e **Volume** dai rispettivi menu a discesa. Fornire un **percorso per la cartella di destinazione**.

   Per scaricare il report nel browser, seleziona **Locale**. Si noti che questa opzione limita il report alle prime 10.000 righe ed è limitata al formato **CSV**. Se selezioni **Locale** non è necessario compilare altri campi.

5. Seleziona **Scarica report**.



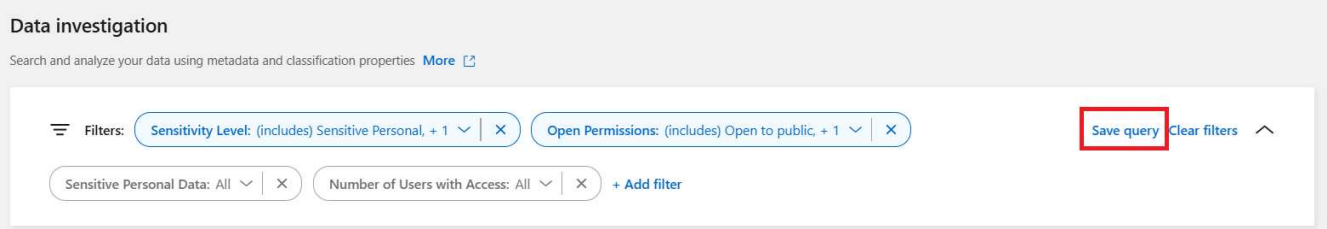
Risultato

Una finestra di dialogo visualizza un messaggio che indica che i report sono in fase di download.

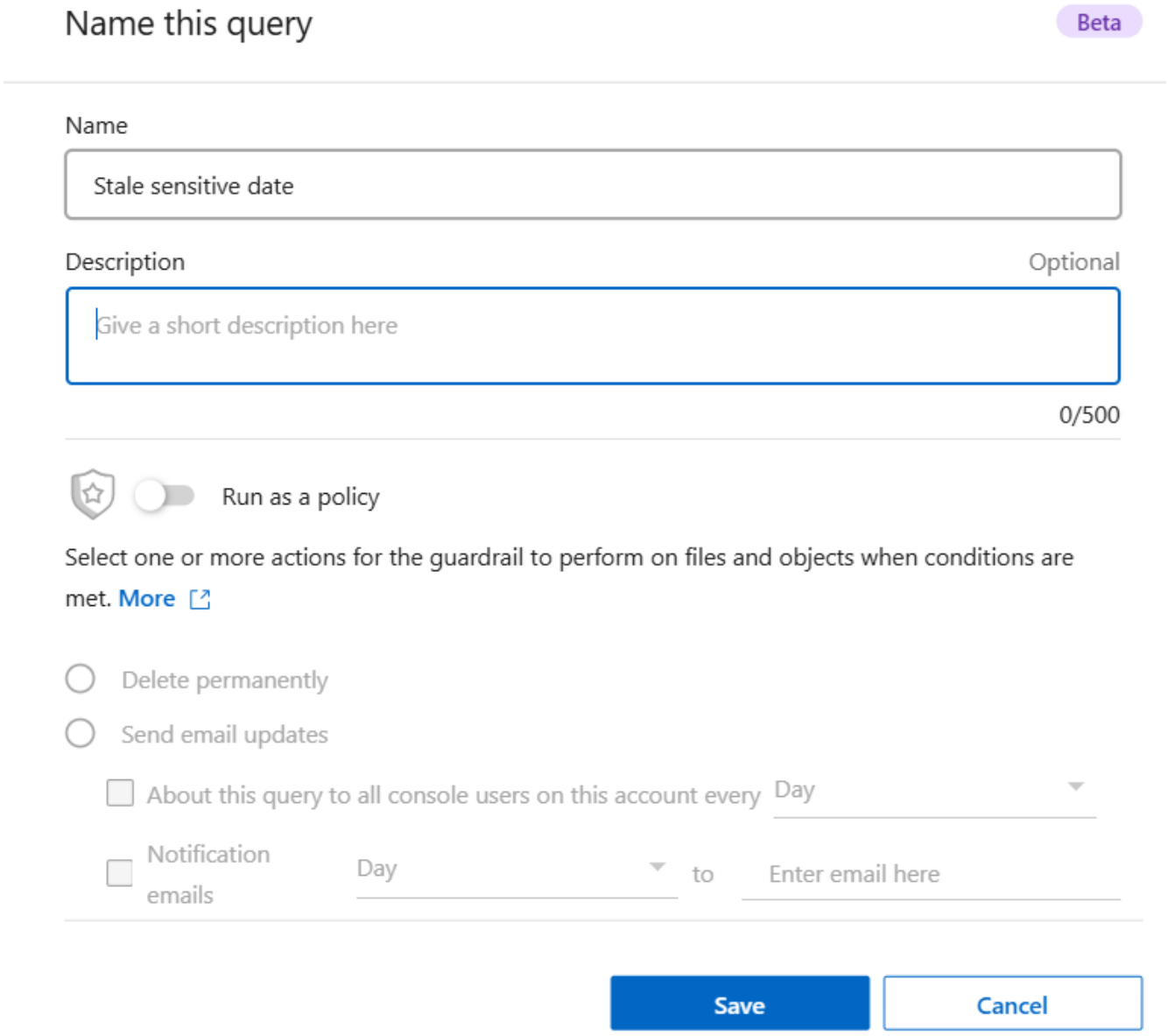
Crea una query salvata in base ai filtri selezionati

Passi

1. Nella scheda Indagine, definisci una ricerca selezionando i filtri che desideri utilizzare. Vedere"Filtraggio dei dati nella pagina Indagine" per i dettagli.
2. Dopo aver impostato tutte le caratteristiche del filtro come preferisci, seleziona **Salva query**.



3. Assegna un nome alla query salvata e aggiungi una descrizione. Il nome deve essere univoco.
4. Facoltativamente, puoi salvare la query come criterio:
   a. Per salvare la query come criterio, attivare l'opzione **Esegui come criterio**.
   b. Scegli se **Eliminare definitivamente** o **Inviare aggiornamenti via email**. Se scegli gli aggiornamenti via e-mail, puoi inviare via e-mail i risultati della query a *tutti* gli utenti della Console con cadenza giornaliera, settimanale o mensile. In alternativa, è possibile inviare la notifica a un indirizzo e-mail specifico con le stesse frequenze.
5. Seleziona **Salva**.



Dopo aver creato la ricerca o la policy, puoi visualizzarla nella scheda **Query salvate**.

Potrebbero essere necessari fino a 15 minuti prima che i risultati vengano visualizzati nella pagina Query salvate.

Gestisci le query salvate con NetApp Data Classification

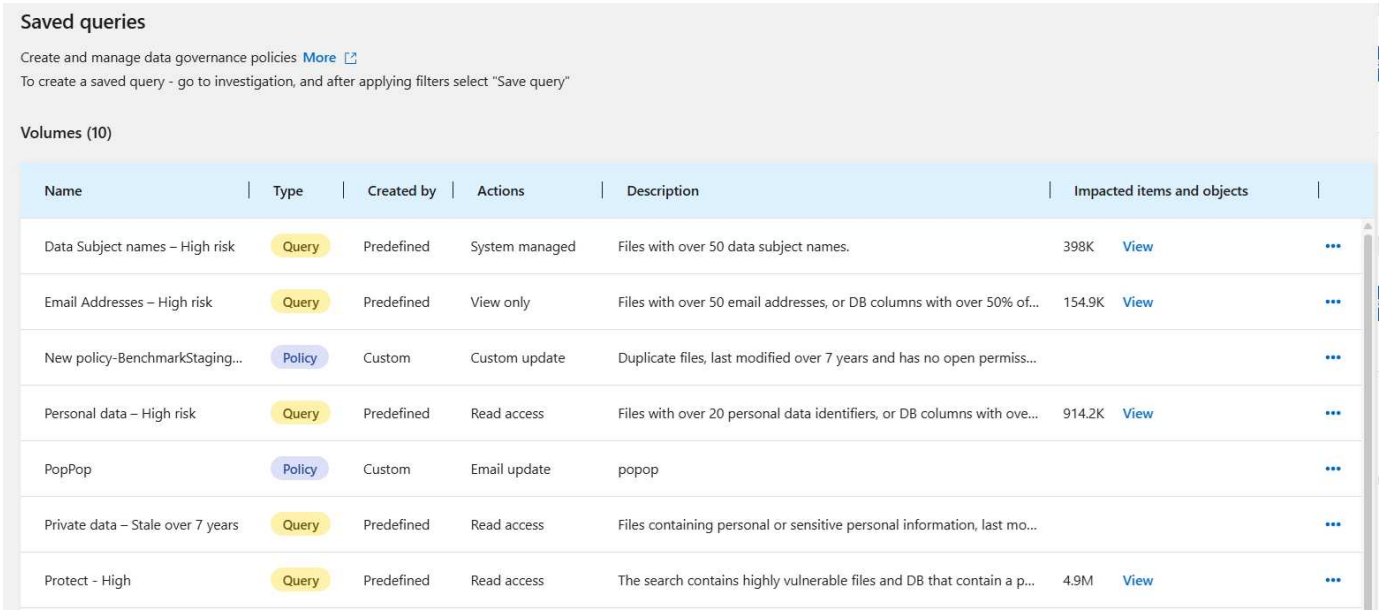
NetaApp Data Classification supporta il salvataggio delle query di ricerca. Con una query salvata, puoi creare filtri personalizzati per ordinare le query frequenti nella pagina di indagine sui dati. La classificazione dei dati include anche query salvate predefinite basate su richieste comuni.

La scheda **Query salvate** nella dashboard Conformità elenca tutte le query salvate predefinite e

personalizzate disponibili in questa istanza di Classificazione dati.

Le query salvate possono essere salvate anche come **policy**. Mentre le query filtrano i dati, i criteri consentono di agire sui dati. Con una policy: puoi eliminare i dati rilevati o inviare aggiornamenti via email sui dati rilevati.

Le query salvate vengono visualizzate anche nell'elenco dei filtri nella pagina Indagine.



Visualizza i risultati delle query salvate nella pagina Indagine

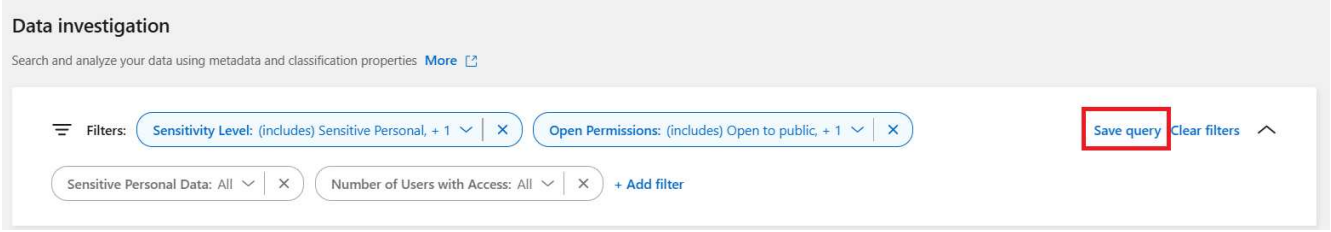
Per visualizzare i risultati di una query salvata nella pagina Indagine, selezionare pulsante per una ricerca specifica, quindi seleziona **Esamina risultati**.

Crea query e policy salvate

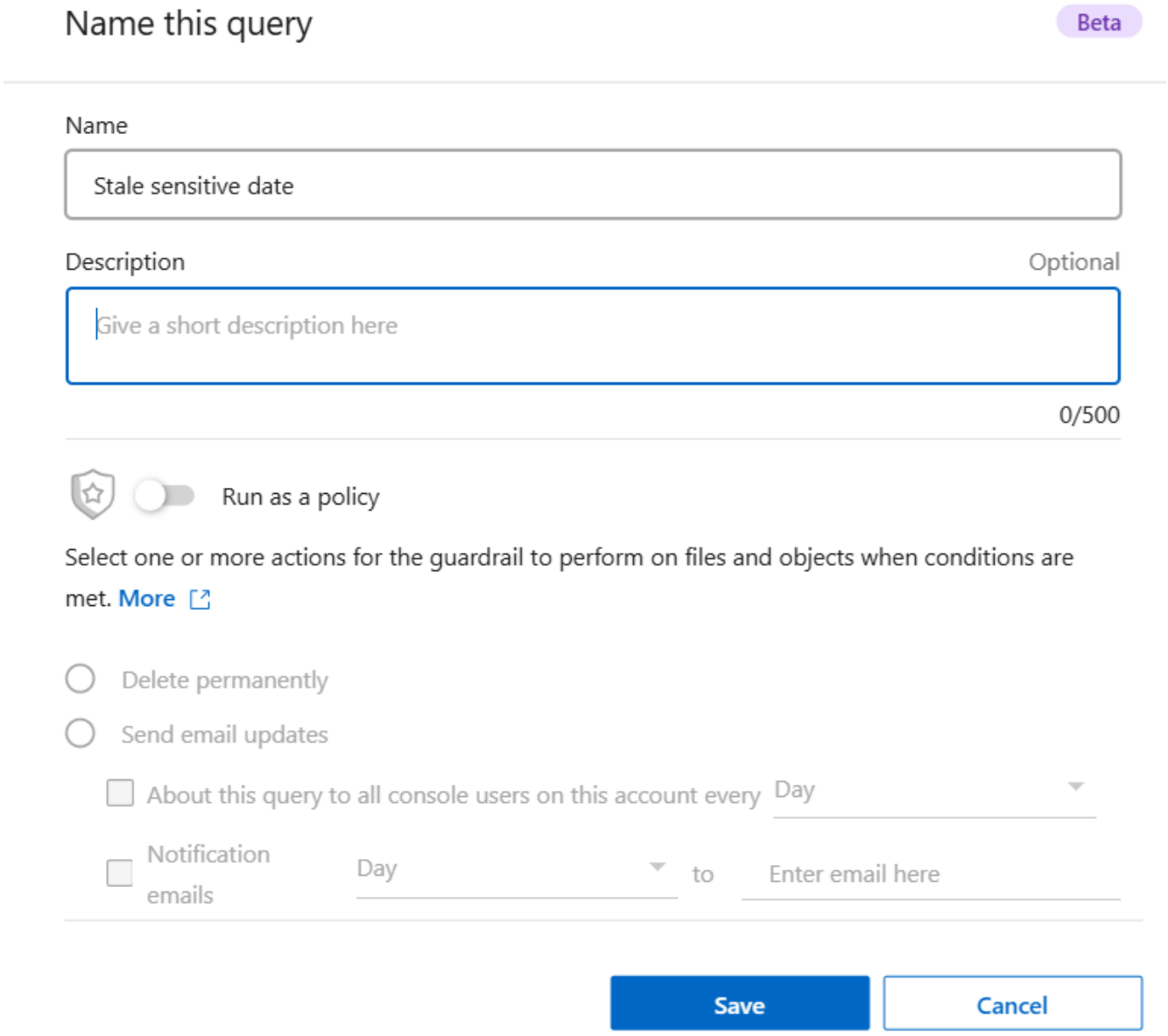
Puoi creare query salvate personalizzate che forniscono risultati per query specifiche della tua organizzazione. Vengono restituiti risultati per tutti i file e le directory (condivisioni e cartelle) che corrispondono ai criteri di ricerca.

Passi

1. Nella scheda Indagine, definisci una ricerca selezionando i filtri che desideri utilizzare. Vedere"Filtraggio dei dati nella pagina Indagine" per i dettagli.
2. Dopo aver impostato tutte le caratteristiche del filtro come preferisci, seleziona **Salva query**.



3. Assegna un nome alla query salvata e aggiungi una descrizione. Il nome deve essere univoco.
4. Facoltativamente, puoi salvare la query come criterio:
   a. Per salvare la query come criterio, attivare l'opzione **Esegui come criterio**.
   b. Scegli se **Eliminare definitivamente** o **Inviare aggiornamenti via email**. Se scegli gli aggiornamenti via e-mail, puoi inviare via e-mail i risultati della query a *tutti* gli utenti della Console con cadenza giornaliera, settimanale o mensile. In alternativa, è possibile inviare la notifica a un indirizzo e-mail specifico con le stesse frequenze.
5. Seleziona **Salva**.



Dopo aver creato la ricerca o la policy, puoi visualizzarla nella scheda **Query salvate**.

Modifica query o policy salvate

È possibile modificare il nome e la descrizione di una query salvata. È anche possibile convertire una query in una policy e viceversa.

Non è possibile modificare le query salvate predefinite. Non è possibile modificare i filtri di una query salvata. In alternativa, è possibile visualizzare i risultati dell'indagine di una query salvata, modificare o alterare i filtri, quindi salvarla come nuova query o criterio.

Passi

1. Dalla pagina Query salvate, seleziona **Modifica ricerca** per la ricerca che desideri modificare.

2. Apportare le modifiche ai campi nome e descrizione. Per modificare solo i campi nome e descrizione.

   Facoltativamente, è possibile convertire la query in una policy oppure convertire la policy in una query salvata. Attivare l'opzione **Esegui come criterio** secondo necessità. .. Se stai convertendo la query in un criterio, scegli **Elimina definitivamente** o **Invia aggiornamenti via email**. Se scegli gli aggiornamenti via e-mail, puoi inviare via e-mail i risultati della query a *tutti* gli utenti della Console con cadenza giornaliera, settimanale o mensile. In alternativa, è possibile inviare la notifica a un indirizzo e-mail specifico con le stesse frequenze.

3. Selezionare **Salva** per completare le modifiche.

Elimina le query salvate

Puoi eliminare qualsiasi query o criterio personalizzato salvato se non ti serve più. Non è possibile eliminare le query salvate di default.

Per eliminare una query salvata, selezionare pulsante per una ricerca specifica, seleziona **Elimina query**, quindi seleziona nuovamente **Elimina query** nella finestra di dialogo di conferma.

Query predefinite

La classificazione dei dati fornisce le seguenti query di ricerca definite dal sistema:

- **Nomi degli interessati - Rischio elevato**

  File con più di 50 nomi di interessati

- **Indirizzi email - Rischio elevato**

  File con più di 50 indirizzi e-mail o colonne di database con più del 50% delle righe contenenti indirizzi e-mail

- **Dati personali - Rischio elevato**

  File con più di 20 identificatori di dati personali o colonne di database con più del 50% delle loro righe contenenti identificatori di dati personali

- **Dati privati - Non aggiornati da oltre 7 anni**

  File contenenti informazioni personali o sensibili, modificati l'ultima volta più di 7 anni fa

- **Protezione - Alta**

  File o colonne di database che contengono una password, informazioni sulla carta di credito, numero IBAN o codice fiscale

- **Protezione - Basso**

  File a cui non si è avuto accesso per più di 3 anni

- **Protezione - Media**

  File che contengono file o colonne di database con identificatori di dati personali, tra cui numeri di identificazione, numeri di identificazione fiscale, numeri di patente di guida, ID medicinali o numeri di passaporto

- **Dati personali sensibili - Rischio elevato**

  File con più di 20 identificatori di dati personali sensibili o colonne di database con più del 50% delle loro righe contenenti dati personali sensibili

Modifica le impostazioni di scansione NetApp Data Classification per i tuoi repository

Puoi gestire il modo in cui i tuoi dati vengono scansionati in ciascuno dei tuoi sistemi e fonti di dati. È possibile apportare modifiche su base "repository", ovvero è possibile apportare modifiche per ciascun volume, schema, utente, ecc. a seconda del tipo di origine dati che si sta analizzando.

Alcune delle cose che puoi modificare sono se un repository viene scansionato o meno e se NetApp Data Classification sta eseguendo un"scansione di mappatura o scansione di mappatura e classificazione" . È anche possibile mettere in pausa e riprendere la scansione, ad esempio se è necessario interrompere la scansione di un volume per un periodo di tempo.

Visualizza lo stato della scansione per i tuoi repository

È possibile visualizzare i singoli repository sottoposti a scansione da NetApp Data Classification (volumi, bucket, ecc.) per ciascun sistema e origine dati. Puoi anche vedere quanti sono stati "Mappati" e quanti sono stati "Classificati". La classificazione richiede più tempo perché l'identificazione completa dell'IA viene eseguita su tutti i dati.

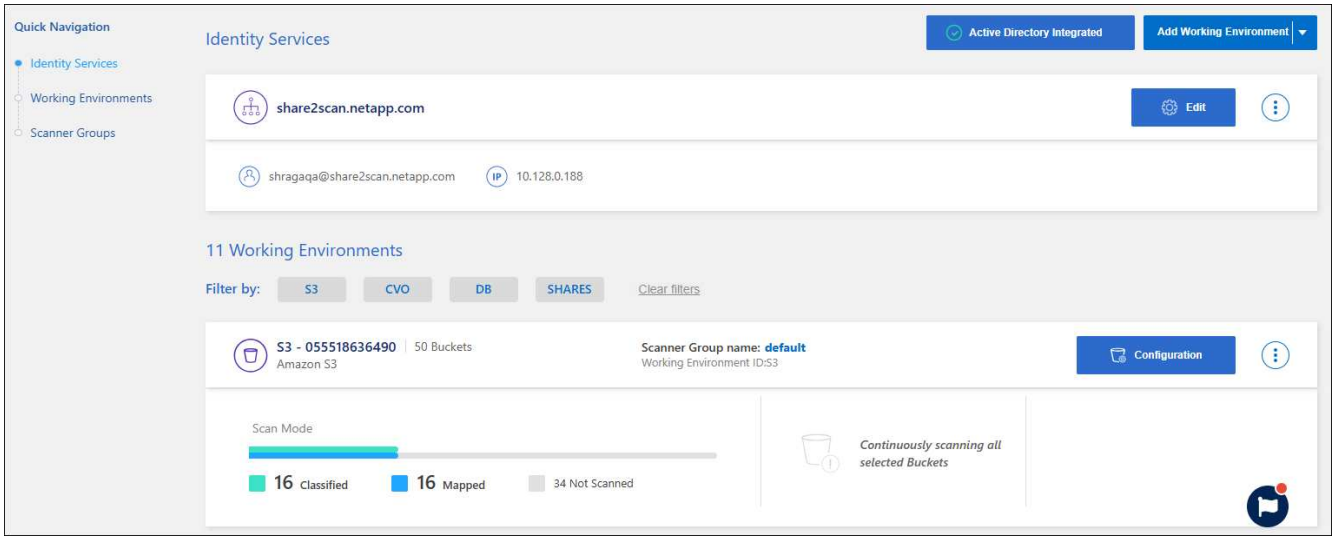
È possibile visualizzare lo stato di scansione di ciascun ambiente di lavoro nella pagina Configurazione:

- **Inizializzazione** (punto azzurro): la configurazione della mappa o della classificazione è attivata. Appare per alcuni secondi prima di avviare lo stato di "coda in attesa".
- **Coda in attesa** (punto arancione): l'attività di scansione è in attesa di essere elencata nella coda di scansione.
- **In coda** (punto arancione): l'attività è stata aggiunta correttamente alla coda di scansione. Il sistema inizierà a mappare o classificare il volume quando arriverà il suo turno nella coda.
- **In esecuzione** (punto verde): l'attività di scansione, che era in coda, è in corso sul repository di archiviazione selezionato.
- **Finito** (punto verde): la scansione del repository di archiviazione è completa.
- **In pausa** (punto grigio): hai selezionato l'opzione "Pausa" per mettere in pausa la scansione. Sebbene le modifiche al volume non vengano visualizzate nel sistema, le informazioni acquisite tramite scansione vengono comunque visualizzate.
- **Errore** (punto rosso): la scansione non può essere completata perché si sono verificati dei problemi. Se è necessario completare un'azione, l'errore viene visualizzato nella descrizione comandi nella colonna "Azione richiesta". In caso contrario, il sistema visualizza lo stato di "errore" e tenta di ripristinare. Una volta terminato, lo stato cambia.

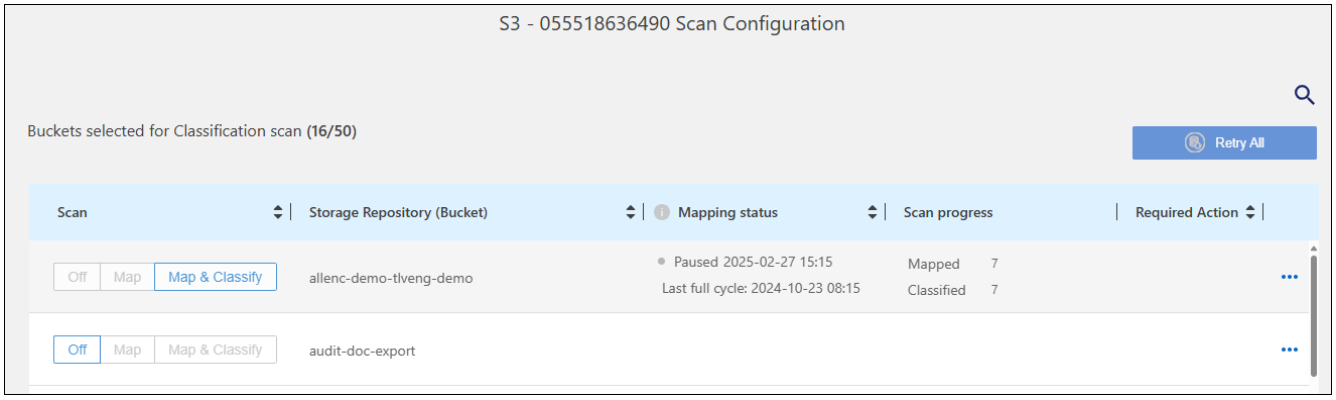
- **Non in scansione**: è stata selezionata la configurazione del volume su "Off" e il sistema non sta eseguendo la scansione del volume.

Passi

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



2. Dalla scheda Configurazione, selezionare il pulsante **Configurazione** per il sistema.
3. Nella pagina Configurazione scansione, visualizza le impostazioni di scansione per tutti i repository.



4. Passa il cursore sul grafico nella colonna *Stato di mappatura* per visualizzare il numero di file che devono ancora essere mappati o classificati in ciascun repository (bucket in questo esempio).

Cambia il tipo di scansione per un repository

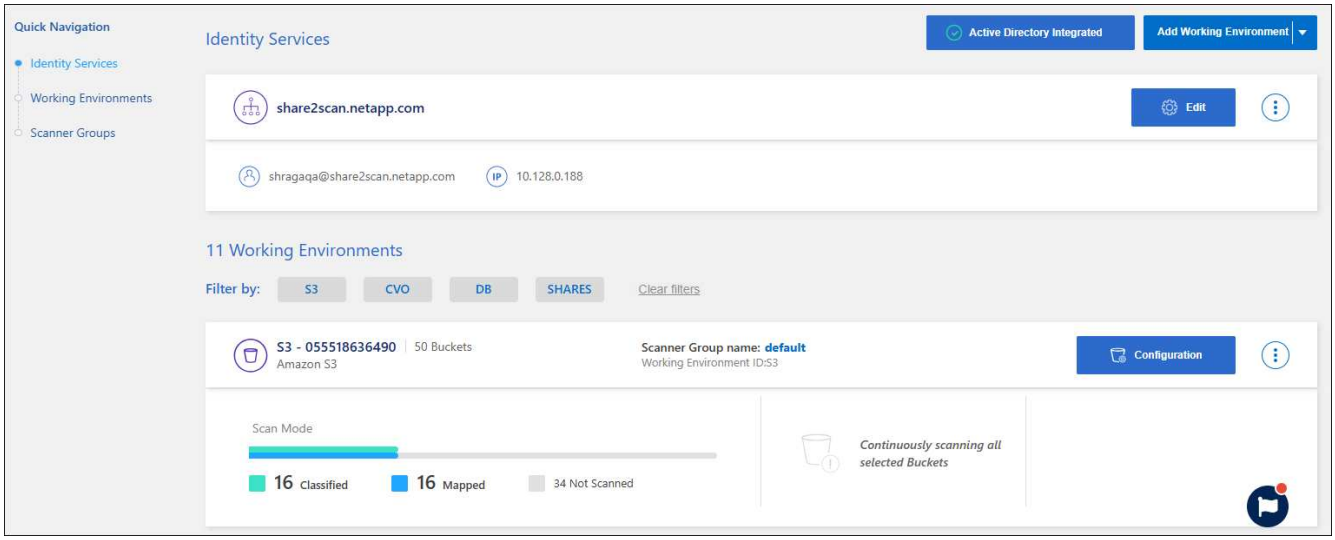
È possibile avviare o interrompere in qualsiasi momento le scansioni di sola mappatura o le scansioni di mappatura e classificazione in un sistema dalla pagina Configurazione. È anche possibile passare da scansioni di sola mappatura a scansioni di mappatura e classificazione e viceversa.

I database non possono essere impostati per scansioni di sola mappatura. La scansione del database può essere disattivata o attivata; dove attivata equivale a mappare e classificare.

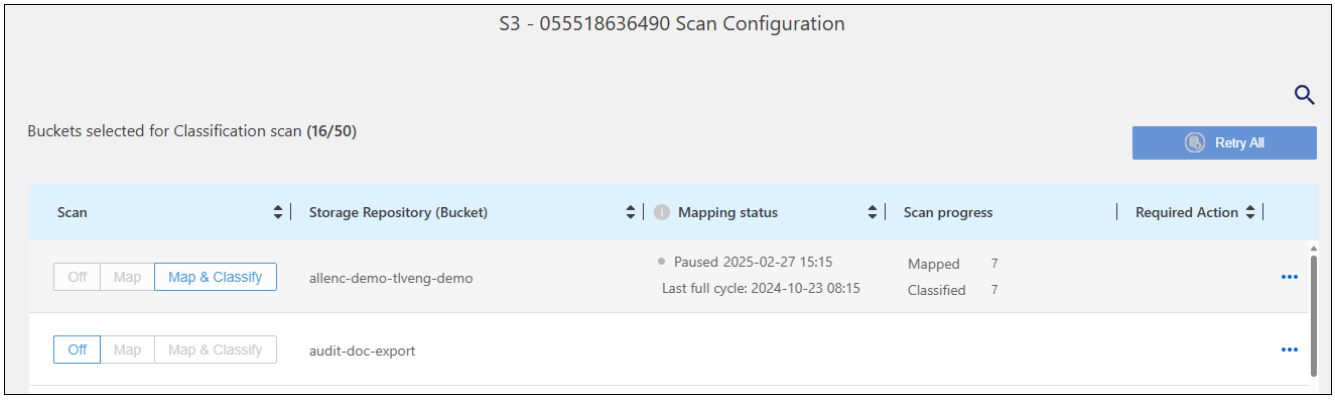
Passi

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

2. Dalla scheda Configurazione, selezionare il pulsante **Configurazione** per il sistema.

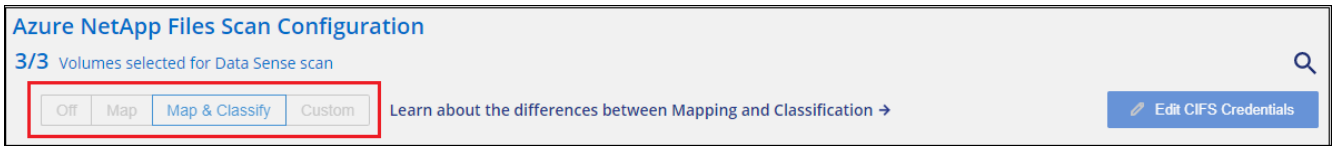


3. Nella pagina Configurazione scansione, modifica uno qualsiasi dei repository (bucket in questo esempio) per eseguire scansioni **Mappa** o **Mappa e classifica**.



Alcuni tipi di sistemi consentono di modificare il tipo di scansione a livello globale per tutti i repository utilizzando una barra dei pulsanti nella parte superiore della pagina. Ciò è valido per i sistemi Cloud Volumes ONTAP, ONTAP locale, Azure NetApp Files e Amazon FSx per ONTAP .

L'esempio seguente mostra questa barra dei pulsanti per un sistema Azure NetApp Files .



Dare priorità alle scansioni

È possibile dare priorità alle scansioni più importanti di sola mappatura oppure alle scansioni di mappatura e classificazione per garantire che le scansioni ad alta priorità vengano completate per prime.

Per impostazione predefinita, le scansioni vengono messe in coda in base all'ordine in cui vengono avviate. Grazie alla possibilità di dare priorità alle scansioni, è possibile spostarle in cima alla coda. È possibile dare priorità a più scansioni. La priorità viene assegnata in base all'ordine "first-in, first-out", ovvero la prima scansione a cui si dà priorità viene spostata in cima alla coda; la seconda scansione a cui si dà priorità diventa

la seconda nella coda e così via.

La priorità viene concessa una sola volta. Le nuove scansioni automatiche dei dati di mappatura avvengono nell'ordine predefinito.

Passi

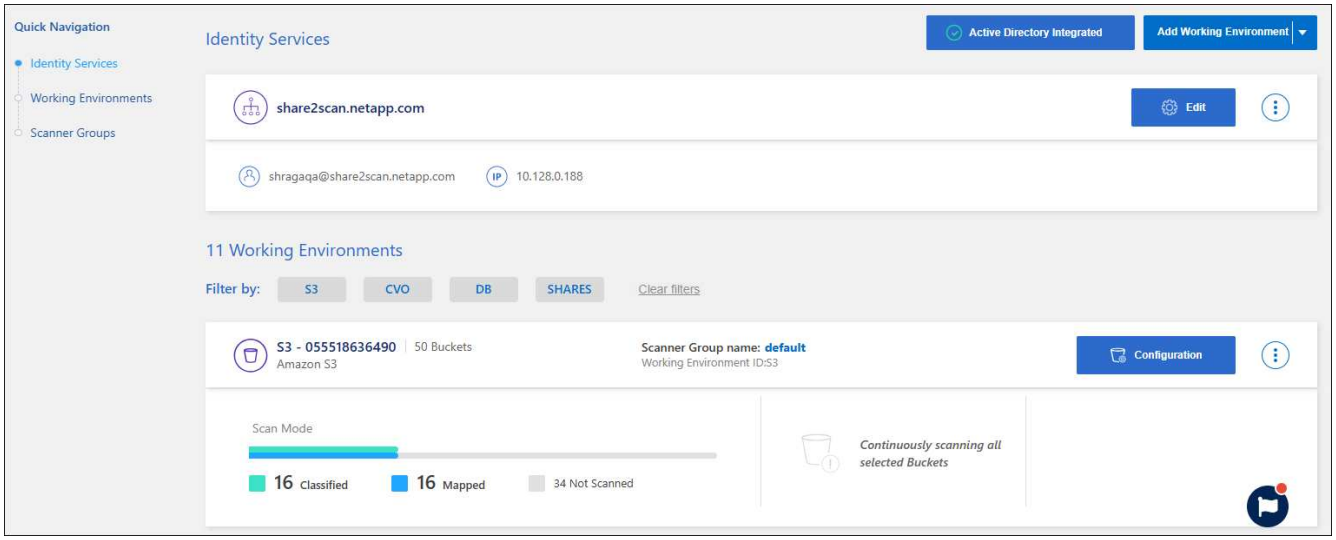
1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Seleziona le risorse a cui vuoi dare priorità.
3. Dalle azioni … opzione, seleziona **Dai priorità alla scansione**.

Interrompere la scansione per un repository

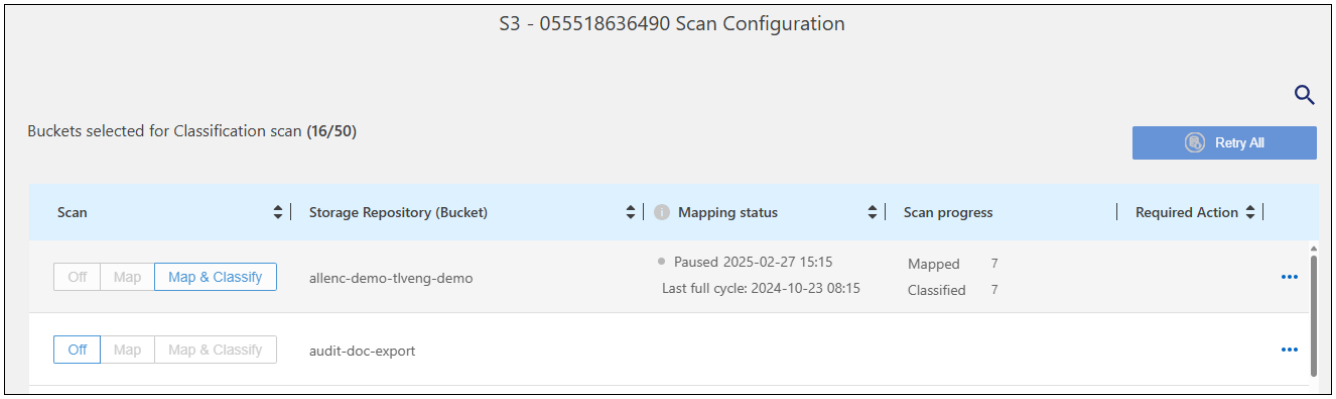
È possibile interrompere la scansione di un repository (ad esempio, un volume) se non è più necessario monitorarne la conformità. Per farlo, è necessario disattivare la scansione. Quando la scansione è disattivata, tutta l'indicizzazione e le informazioni relative a quel volume vengono rimosse dal sistema e la tariffazione per la scansione dei dati viene interrotta.

Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Dalla scheda Configurazione, selezionare il pulsante **Configurazione** per il sistema.



3. Nella pagina Configurazione scansione selezionare **Off** per interrompere la scansione di un bucket specifico.



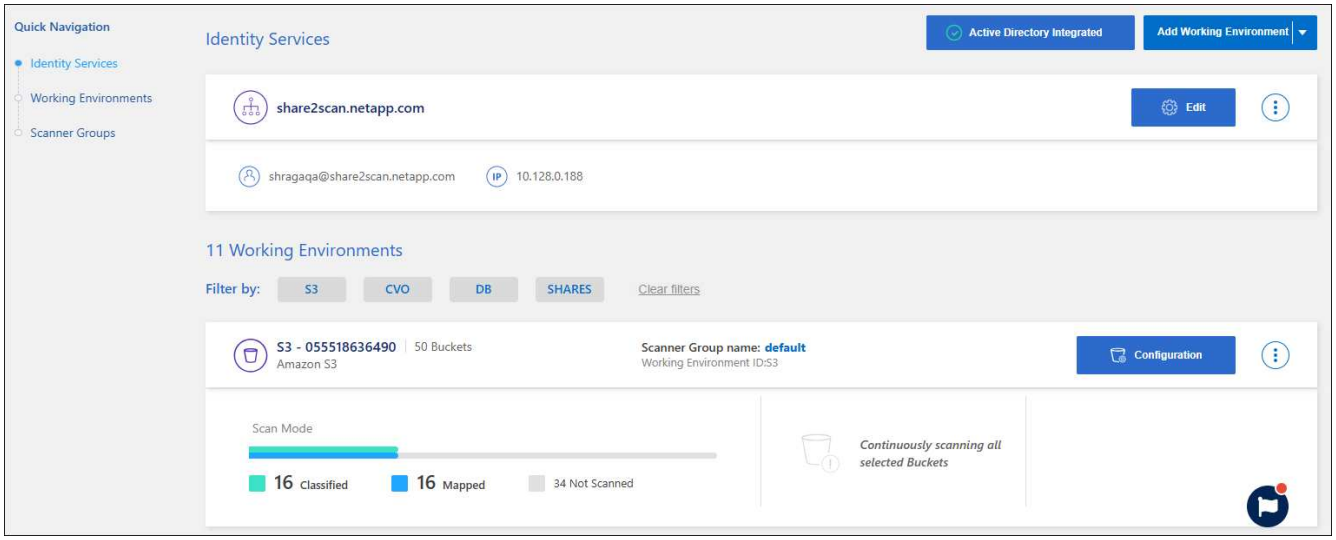
Metti in pausa e riprendi la scansione di un repository

È possibile "mettere in pausa" la scansione di un repository se si desidera interrompere temporaneamente la scansione di determinati contenuti. Sospendere la scansione significa che Data Classification non eseguirà più scansioni future per rilevare modifiche o aggiunte al repository, ma tutti i risultati correnti continueranno a essere visualizzati nel sistema. La sospensione della scansione non interrompe l'addebito dei dati scansionati, perché i dati esistono ancora.

È possibile "riprendere" la scansione in qualsiasi momento.

Passi

1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Dalla scheda Configurazione, selezionare il pulsante **Configurazione** per il sistema.



3. Nella pagina Configurazione scansione, seleziona Azioni ••• icona.
4. Selezionare **Pausa** per mettere in pausa la scansione di un volume oppure selezionare **Riprendi** per riprendere la scansione di un volume che era stata precedentemente messa in pausa.

Visualizza i report sulla conformità NetApp Data Classification

NetApp Data Classification fornisce report che puoi utilizzare per comprendere meglio lo stato del programma di privacy dei dati della tua organizzazione.

Per impostazione predefinita, i dashboard di classificazione dei dati visualizzano i dati di conformità e governance per tutti i sistemi, database e origini dati. Se si desidera visualizzare report che contengono dati solo per alcuni sistemi, è possibile filtrare per visualizzarli solo.

- I report di conformità sono disponibili solo se si esegue una scansione completa della classificazione sulle origini dati. Le fonti dati che hanno eseguito una scansione di sola mappatura possono generare solo il report di mappatura dei dati.
- NetApp non può garantire l'accuratezza al 100% dei dati personali e dei dati personali sensibili identificati dalla classificazione dei dati. Dovresti sempre convalidare le informazioni esaminando i dati.

Per la classificazione dei dati sono disponibili i seguenti report:

- **Rapporto di valutazione della scoperta dei dati**: fornisce un'analisi di alto livello dell'ambiente scansionato per evidenziare i risultati del sistema e mostrare le aree problematiche e i potenziali passaggi di correzione. Questo report è disponibile nella dashboard Governance.
- **Report completo sulla mappatura dei dati**: fornisce informazioni sulle dimensioni e sul numero di file presenti nei sistemi. Ciò include la capacità di utilizzo, l'età dei dati, la dimensione dei dati e i tipi di file. Questo report è disponibile nella dashboard Governance.
- **Rapporto sulla richiesta di accesso ai dati dell'interessato**: consente di estrarre un rapporto di tutti i file che contengono informazioni riguardanti il nome specifico o l'identificatore personale di un interessato. Questo report è disponibile nella dashboard Conformità.
- **Rapporto HIPAA**: ti aiuta a identificare la distribuzione delle informazioni sanitarie nei tuoi file. Questo report è disponibile nella dashboard Conformità.
- **Rapporto PCI DSS**: ti aiuta a identificare la distribuzione delle informazioni sulle carte di credito nei tuoi file. Questo report è disponibile nella dashboard Conformità.
- **Rapporto di valutazione del rischio per la privacy**: fornisce informazioni sulla privacy dei tuoi dati e un punteggio di rischio per la privacy. Questo report è disponibile nella dashboard Conformità.
- **Report su un tipo di informazione specifico**: sono disponibili report che includono dettagli sui file identificati che contengono dati personali e dati personali sensibili. È anche possibile visualizzare i file suddivisi per categoria e tipo di file.

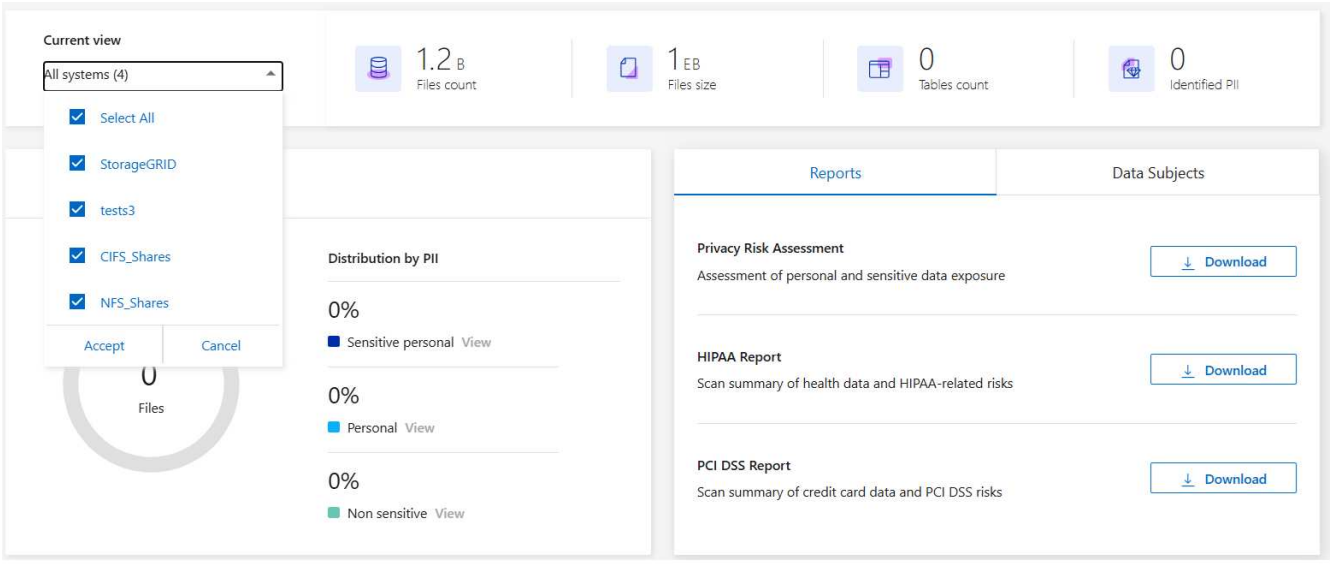
Seleziona i sistemi per i report

È possibile filtrare il contenuto della dashboard Conformità alla classificazione dei dati per visualizzare i dati di conformità per tutti i sistemi e database oppure solo per sistemi specifici.

Quando si filtra la dashboard, la classificazione dei dati limita i dati e i report sulla conformità solo ai sistemi selezionati.

Passi

1. Dal menu Classificazione dati, selezionare **Conformità**.
2. Selezionare il filtro dei sistemi dal menu a discesa, quindi selezionare i sistemi.
3. Seleziona **Accetta** per confermare la selezione.



Segnalazione della richiesta di accesso ai dati dell'interessato

Le normative sulla privacy, come il GDPR europeo, garantiscono agli interessati (come clienti o dipendenti) il diritto di accedere ai propri dati personali. Quando un soggetto interessato richiede queste informazioni, si parla di DSAR (richiesta di accesso ai dati). Le organizzazioni sono tenute a rispondere a tali richieste "senza indebito ritardo" e al più tardi entro un mese dal ricevimento.

È possibile rispondere a una DSAR cercando il nome completo di un soggetto o un identificativo noto (ad esempio un indirizzo e-mail) e quindi scaricando un rapporto. Il report è stato ideato per aiutare la tua organizzazione a conformarsi al GDPR o a leggi simili sulla privacy dei dati.

In che modo la classificazione dei dati può aiutarti a rispondere a una DSAR?

Quando si esegue una ricerca di un soggetto interessato, la classificazione dei dati trova tutti i file che contengono il nome o l'identificativo di quella persona. La classificazione dei dati verifica i dati preindicizzati più recenti per il nome o l'identificatore. Non avvia una nuova scansione.

Una volta completata la ricerca, è possibile scaricare l'elenco dei file per un report sulla richiesta di accesso ai dati personali. Il report aggrega le informazioni ricavate dai dati e le traduce in termini legali, così da poterle inviare alla persona interessata.

La ricerca degli interessati non è attualmente supportata nei database.

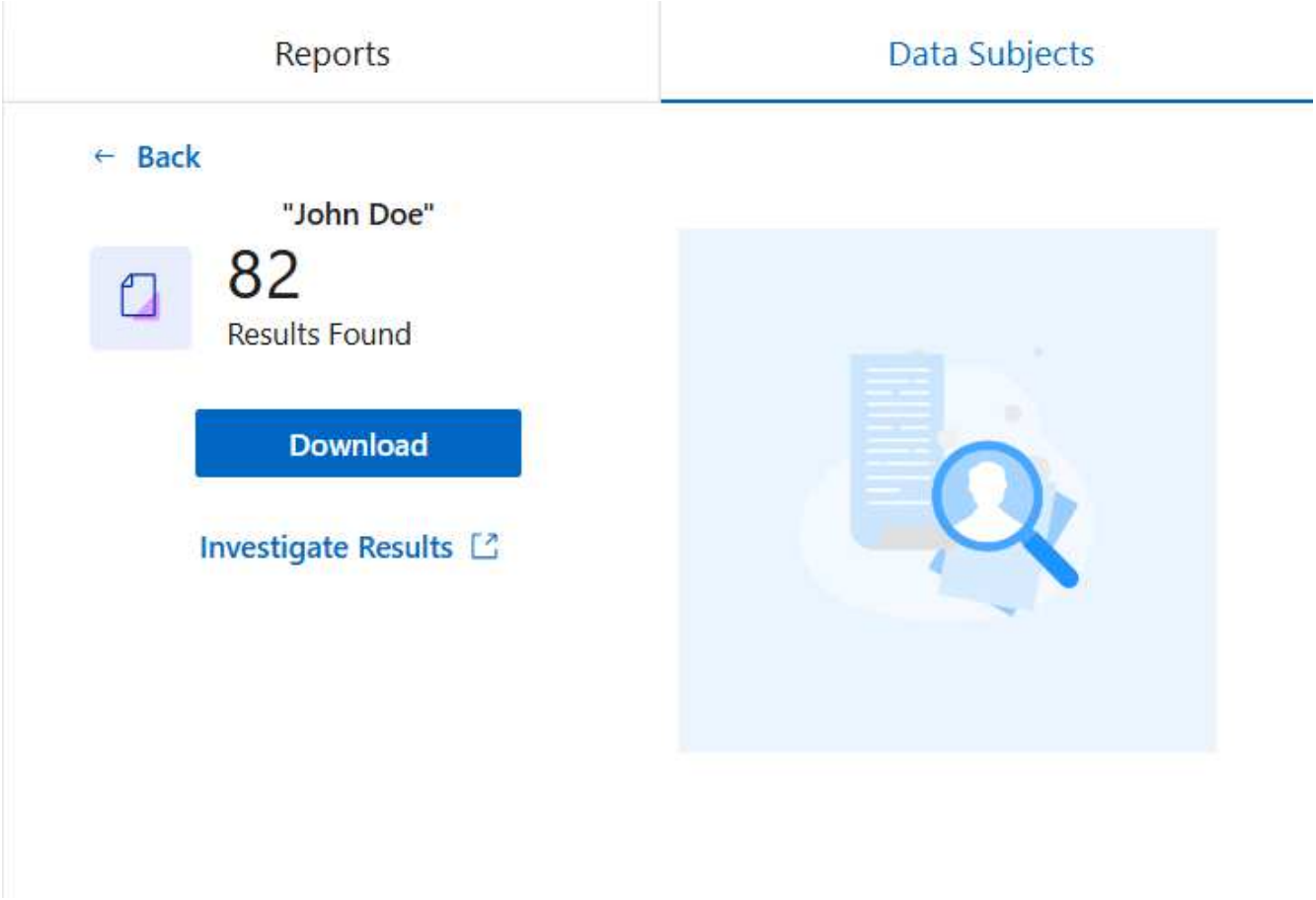
Cerca gli interessati e scarica i report

Cerca il nome completo o l'identificativo noto dell'interessato e poi scarica un report con l'elenco dei file o un report DSAR. Puoi cercare per"qualsiasi tipo di informazione personale" .

Per la ricerca dei nomi degli interessati sono supportate le lingue inglese, tedesco, giapponese e spagnolo. In seguito verrà aggiunto il supporto per altre lingue.

Passi

1. Dal menu Classificazione dati, selezionare **Conformità**.
2. Nella pagina Conformità, individuare la scheda **Interessati**.
3. Nella sezione **Interessati**, inserisci un nome o un identificativo noto, quindi seleziona **Cerca**.
4. Una volta completata la ricerca, seleziona **Scarica** per accedere alla risposta alla richiesta di accesso ai dati dell'interessato. Selezionare **Indaga sui risultati** per visualizzare maggiori informazioni nella pagina Indagine sui
dati.



5. Esamina i risultati in Classificazione dati o scaricali come report selezionando l'icona di download.

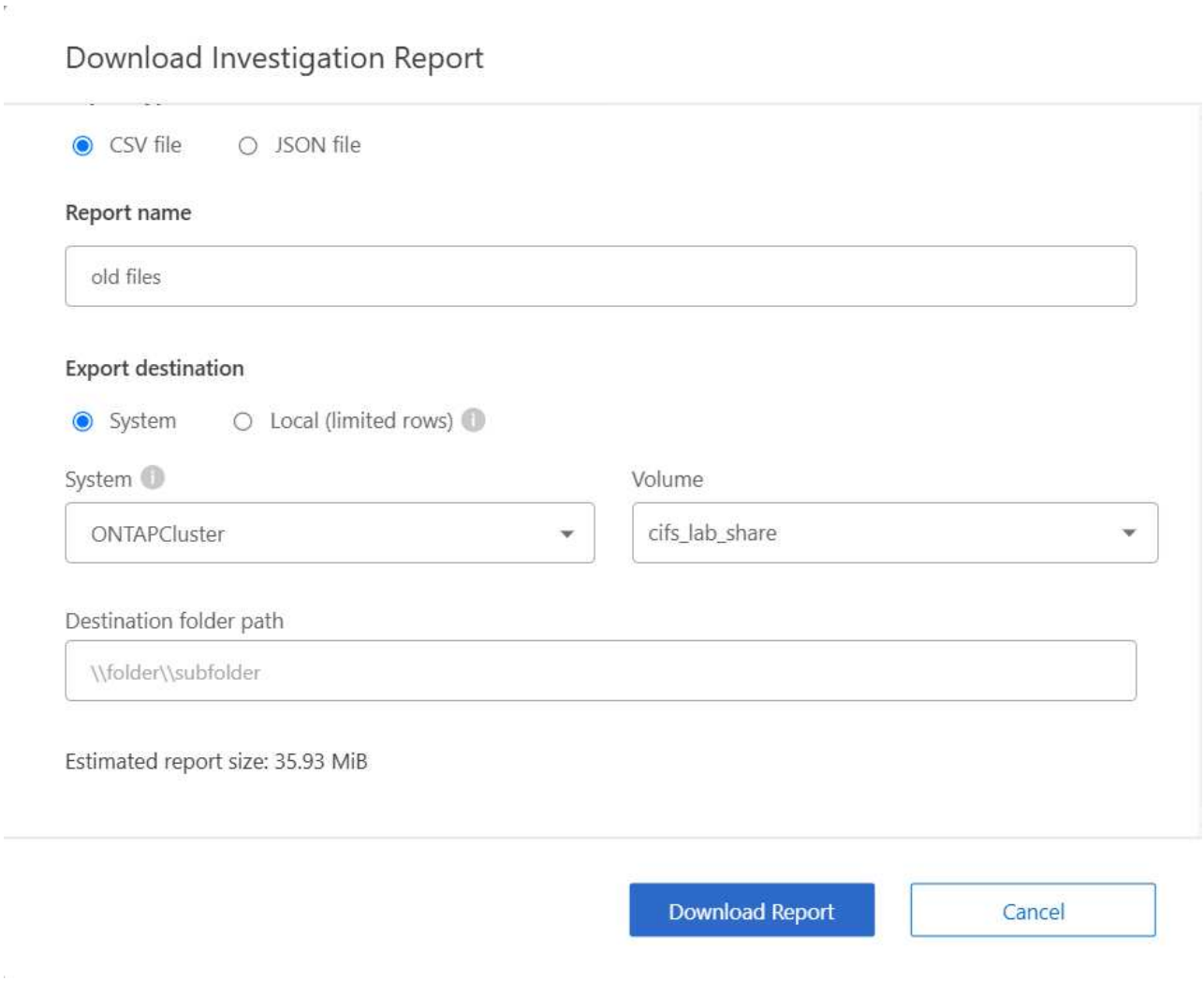
   a. Quando selezioni l'icona di download, configura le impostazioni di download:

      - Scegli il formato del film: CSV o JSON
      - Inserisci un **Nome del report**
      - Scegli la destinazione di esportazione: **Sistema** o la tua macchina **Locale**.

        Se si sceglie il sistema, tutti i dati vengono scaricati. È necessario selezionare anche **Sistema**, **Volume** e **Percorso della cartella di destinazione**.

Se si sceglie **Locale**, il report viene limitato alle prime 10.000 righe di dati non strutturati, 5.000 righe di dati non strutturati e 1.000 righe di dati strutturati.

   a. Selezionare **Scarica report** per avviare il download.



Rapporto sulla legge sulla portabilità e responsabilità dell'assicurazione sanitaria (HIPAA)

Il rapporto HIPAA (Health Insurance Portability and Accountability Act) può aiutarti a identificare i file contenenti informazioni sanitarie. È progettato per aiutare la tua organizzazione a rispettare i requisiti di conformità alle leggi sulla privacy dei dati HIPAA. Le informazioni ricercate dalla classificazione dei dati includono:

- Modello di riferimento sanitario
- Codice medico ICD-10-CM
- Codice medico ICD-9-CM
- Risorse umane - Categoria Salute
- Categoria Dati delle applicazioni sanitarie

Il rapporto include le seguenti informazioni:

- Panoramica: quanti file contengono informazioni sanitarie e in quali sistemi.
- Crittografia: percentuale di file contenenti informazioni sanitarie che si trovano su sistemi crittografati o non crittografati. Queste informazioni sono specifiche per Cloud Volumes ONTAP.
- Protezione ransomware: percentuale di file contenenti informazioni sanitarie presenti su sistemi con o senza protezione ransomware abilitata. Queste informazioni sono specifiche per Cloud Volumes ONTAP.

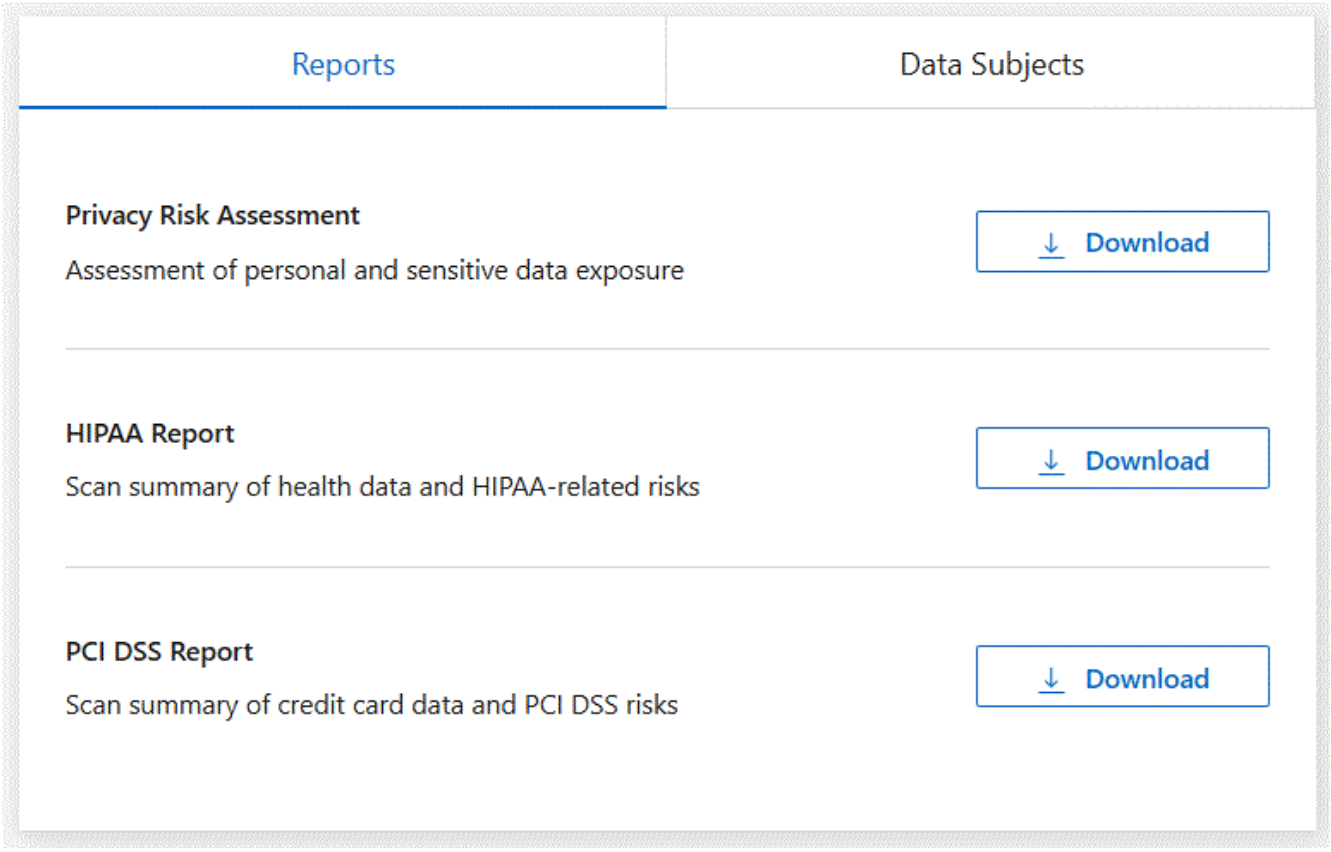
- Conservazione: intervallo di tempo in cui i file sono stati modificati l'ultima volta. Questo è utile perché non dovresti conservare le informazioni sanitarie più a lungo del necessario per elaborarle.
- Distribuzione delle informazioni sanitarie: i sistemi in cui sono state trovate le informazioni sanitarie e se sono abilitate la crittografia e la protezione dal ransomware.

Genera il rapporto HIPAA

Vai alla scheda Conformità per generare il report.

Passi

1. Dal menu Classificazione dati, selezionare **Conformità**.
2. Individuare il **riquadro Report**. Selezionare l'icona di download accanto a **Rapporto HIPAA**.



Risultato

La classificazione dei dati genera un report in formato PDF.

Rapporto sullo standard di sicurezza dei dati del settore delle carte di pagamento (PCI DSS)

Il report PCI DSS (Payment Card Industry Data Security Standard) può aiutarti a identificare la distribuzione delle informazioni sulle carte di credito nei tuoi file.

Il rapporto include le seguenti informazioni:

- Panoramica: quanti file contengono informazioni sulle carte di credito e in quali sistemi.
- Crittografia: percentuale di file contenenti informazioni sulla carta di credito che si trovano su sistemi

crittografati o non crittografati. Queste informazioni sono specifiche per Cloud Volumes ONTAP.

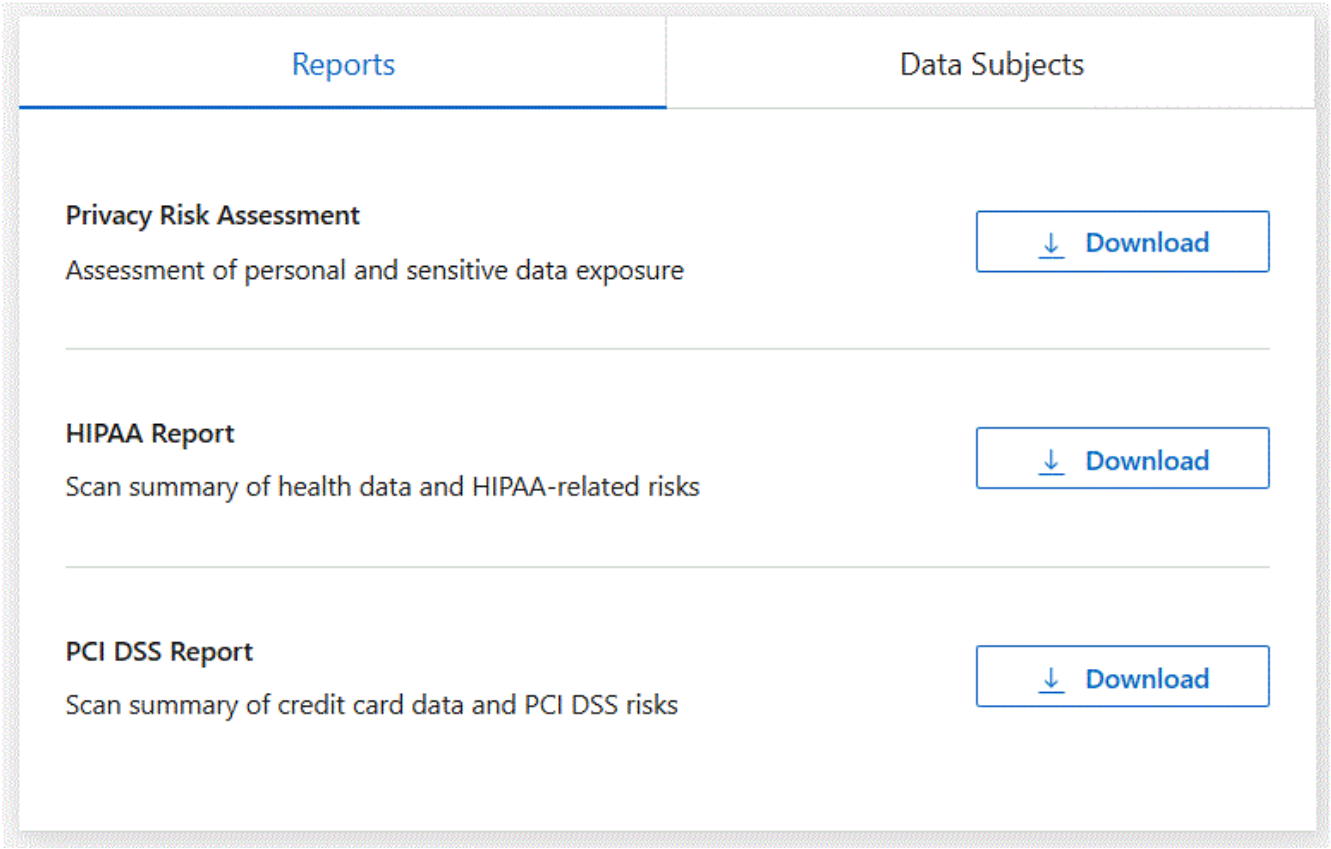
- Protezione ransomware: percentuale di file contenenti informazioni sulla carta di credito presenti su sistemi con o senza protezione ransomware abilitata. Queste informazioni sono specifiche per Cloud Volumes ONTAP.
- Conservazione: intervallo di tempo in cui i file sono stati modificati l'ultima volta. Questo è utile perché non dovresti conservare i dati della tua carta di credito più a lungo del necessario per elaborarli.
- Distribuzione delle informazioni sulla carta di credito: i sistemi in cui sono state trovate le informazioni sulla carta di credito e se sono abilitate la crittografia e la protezione anti-ransomware.

Generare il rapporto PCI DSS

Vai alla scheda Conformità per generare il report.

Passi

1. Dal menu Classificazione dati, selezionare **Conformità**.
2. Individuare il **riquadro Report**. Selezionare l'icona di download accanto a **Rapporto PCI DSS**.



Risultato

La classificazione dei dati genera un report PDF che puoi rivedere e inviare ad altri gruppi, se necessario.

Rapporto di valutazione del rischio per la privacy

Il rapporto sulla valutazione del rischio per la privacy fornisce una panoramica dello stato del rischio per la privacy della tua organizzazione, come richiesto dalle normative sulla privacy quali GDPR e CCPA.

Il rapporto include le seguenti informazioni:

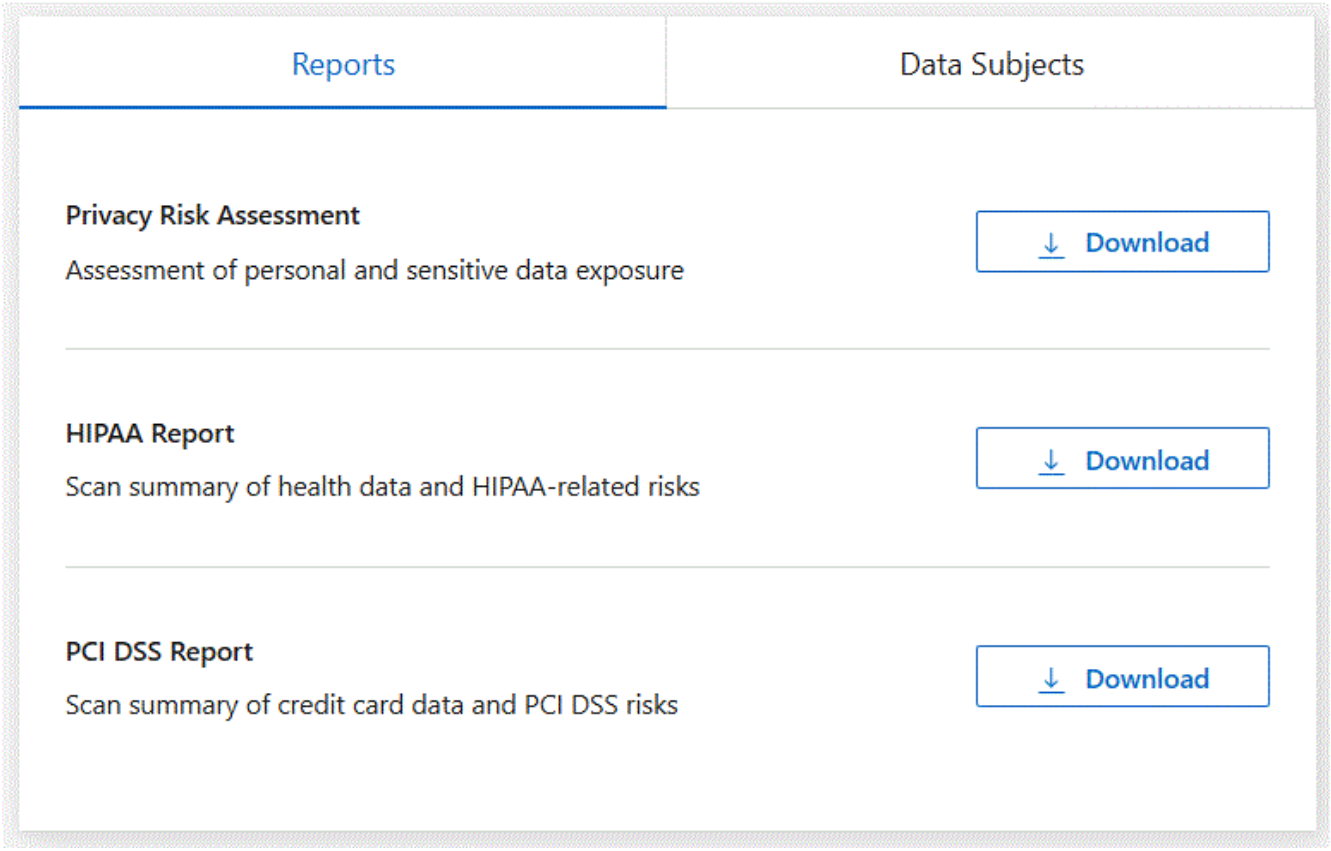
- Stato di conformità: punteggio di gravità e distribuzione dei dati, siano essi non sensibili, personali o sensibili personali.
- Panoramica della valutazione: una ripartizione dei tipi di dati personali rilevati, nonché delle categorie di dati.
- Soggetti interessati in questa valutazione: numero di persone, per posizione, per le quali sono stati trovati identificatori nazionali.

Generare il rapporto di valutazione del rischio per la privacy

Vai alla scheda Conformità per generare il report.

Passi

1. Dal menu Classificazione dati, selezionare **Conformità**.
2. Individuare il **riquadro Report**. Selezionare l'icona di download accanto a **Rapporto di valutazione del rischio per la privacy**.



Risultato

La classificazione dei dati genera un report PDF che puoi rivedere e inviare ad altri gruppi, se necessario.

Punteggio di gravità

La classificazione dei dati calcola il punteggio di gravità per il rapporto di valutazione del rischio per la privacy sulla base di tre variabili:

- La percentuale di dati personali rispetto a tutti i dati.
- La percentuale di dati personali sensibili rispetto a tutti i dati.

- La percentuale di file che includono soggetti interessati, determinata da identificatori nazionali quali documenti d'identità nazionali, numeri di previdenza sociale e numeri di identificazione fiscale.

La logica utilizzata per determinare il punteggio è la seguente:

Punteggio di gravità	Logica
0	Tutte e tre le variabili sono esattamente 0%
1	Una delle variabili è maggiore dello 0%
2	Una delle variabili è maggiore del 3%
3	Due delle variabili sono maggiori del 3%
4	Tre delle variabili sono maggiori del 3%
5	Una delle variabili è maggiore del 6%
6	Due delle variabili sono maggiori del 6%
7	Tre delle variabili sono maggiori del 6%
8	Una delle variabili è maggiore del 15%
9	Due delle variabili sono maggiori del 15%
10	Tre delle variabili sono maggiori del 15%

Gestire la classificazione dei dati

Escludere directory specifiche dalle scansioni NetApp Data Classification

Se si desidera che NetApp Data Classification escluda directory specifiche dalle scansioni, è possibile aggiungere i nomi di queste directory a un file di configurazione. Dopo aver applicato questa modifica, il motore di classificazione dei dati esclude tali directory dalle scansioni.

Per impostazione predefinita, le scansioni di classificazione dei dati escludono i dati degli snapshot del volume, che sono identici alla loro origine nel volume.

Fonti dati supportate

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

- ONTAP in sede
- Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Condivisioni di file generali

Definisci le directory da escludere dalla scansione

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

Considerazioni

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

Passi

1. Nel sistema di classificazione dei dati, vai su "/opt/netapp/config/custom_configuration" quindi apri il file `data_provider.yaml` .
2. Nella sezione "data_providers", sotto la riga "exclude:", immettere i percorsi delle directory da escludere. Per esempio:

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

Non modificare nient'altro in questo file.

3. Salvare le modifiche al file.
4. Vai su "/opt/netapp/Datasense/tools/customer_configuration/data_providers" ed esegui il seguente script:

```
update_data_providers_from_config_file.sh
```

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

Risultato

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

È possibile aggiungere, modificare o eliminare elementi dall'elenco di esclusione seguendo gli stessi passaggi. L'elenco delle esclusioni rivisto verrà aggiornato dopo aver eseguito lo script per confermare le modifiche.

Esempi

Configurazione 1:

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

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

Risultati previsti per i percorsi che verranno esclusi:

- /CVO1/cartella1
- /CVO1/nomecartella1
- /CVO1/cartella10
- /CVO1/*cartella1
- /CVO1/+nomecartella1
- /CVO1/noncartella10
- /CVO22/cartella1
- /CVO22/nomecartella1
- /CVO22/cartella10

Esempi di percorsi che non verranno esclusi:

- /CVO1/*cartella
- /CVO1/nomecartella
- /CVO22/*cartella20

Configurazione 2:

Verranno escluse tutte le cartelle che contengono "*folder1" solo all'inizio del nome.

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

Risultati previsti per i percorsi che verranno esclusi:

- /CVO/*cartella1
- /CVO/*nomecartella1
- /CVO/*cartella10

Esempi di percorsi che non verranno esclusi:

- /CVO/cartella1
- /CVO/nomecartella1
- /CVO/non*cartella10

Configurazione 3:

Verrà esclusa ogni cartella nella sorgente dati "CVO22" che contiene "folder1" in qualsiasi punto del nome.

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

Risultati previsti per i percorsi che verranno esclusi:

- /CVO22/cartella1
- /CVO22/nomecartella1
- /CVO22/cartella10

Esempi di percorsi che non verranno esclusi:

- /CVO1/cartella1
- /CVO1/nomecartella1
- /CVO1/cartella10

Escape dei caratteri speciali nei nomi delle cartelle

Se il nome di una cartella contiene uno dei seguenti caratteri speciali e si desidera escludere dalla scansione i dati in quella cartella, sarà necessario utilizzare la sequenza di escape \\ prima del nome della cartella.

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

Percorso nella sorgente: `/project/*not_to_scan`

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

Visualizza l’elenco delle esclusioni corrente

È possibile che il contenuto del `data_provider.yaml` file di configurazione diverso da quello effettivamente commesso dopo l’esecuzione del `update_data_providers_from_config_file.sh` sceneggiatura. Per visualizzare l’elenco corrente delle directory escluse dalla scansione di Data Classification, eseguire il seguente comando da "/opt/netapp/Datasense/tools/customer_configuration/data_providers":

```
get_data_providers_configuration.sh
```

Definisci ID di gruppo aggiuntivi come aperti all’organizzazione in NetApp Data Classification

Quando gli ID di gruppo (GID) vengono allegati a file o cartelle in condivisioni file NFS, definiscono le autorizzazioni per il file o la cartella, ad esempio se sono "aperti all’organizzazione". Se alcuni GID non sono inizialmente configurati con il livello di autorizzazione "Aperto all’organizzazione", è possibile aggiungere tale autorizzazione al GID in modo che tutti i file e le cartelle a cui è associato tale GID vengano considerati "aperti all’organizzazione".

Dopo aver apportato questa modifica e aver eseguito una nuova scansione dei file e delle cartelle da NetApp Data Classification , tutti i file e le cartelle a cui sono associati questi ID gruppo mostreranno questa autorizzazione nella pagina Dettagli indagine e appariranno anche nei report in cui vengono visualizzate le autorizzazioni dei file.

Per attivare questa funzionalità, è necessario accedere al sistema di classificazione dei dati in modo da poter modificare un file di configurazione ed eseguire uno script. Scopri come"accedi al sistema di classificazione dei dati" a seconda che il software sia stato installato manualmente su una macchina Linux o che l’istanza sia stata distribuita nel cloud.

Aggiungere l’autorizzazione "apri all’organizzazione" agli ID di gruppo

Prima di iniziare questa attività è necessario disporre dei numeri ID del gruppo (GID).

Passi

1. Nel sistema di classificazione dei dati, vai su "/opt/netapp/config/custom_configuration" e apri il file `data_provider.yaml` .
2. Nella riga "organization_group_ids: []" aggiungere gli ID del gruppo. Per esempio:

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

   Non modificare nient’altro in questo file.
3. Salvare le modifiche al file.
4. Vai su "/opt/netapp/Datasense/tools/customer_configuration/data_providers" ed esegui il seguente script:

```
update_data_providers_from_config_file.sh
```

Questo comando invia le autorizzazioni dell'ID gruppo riviste al motore di classificazione.

Risultato

Tutte le scansioni successive dei dati identificheranno i file o le cartelle a cui sono associati questi ID di gruppo come "aperti all'organizzazione".

Puoi modificare l'elenco degli ID gruppo ed eliminare tutti gli ID gruppo aggiunti in passato seguendo gli stessi passaggi. L'elenco rivisto degli ID gruppo verrà aggiornato dopo aver eseguito lo script per confermare le modifiche.

Visualizza l'elenco corrente degli ID gruppo

È possibile che il contenuto del `data_provider.yaml` file di configurazione per differire da ciò che è stato effettivamente commesso dopo l'esecuzione del `update_data_providers_from_config_file.sh` sceneggiatura. Per visualizzare l'elenco corrente degli ID gruppo aggiunti a Data Classification, eseguire il seguente comando da "/opt/netapp/Datasense/tools/customer_configuration/data_providers":

```
get_data_providers_configuration.sh
```

Rimuovere le origini dati da NetApp Data Classification

Se necessario, è possibile impedire a NetApp Data Classification di analizzare uno o più sistemi, database o gruppi di condivisione file.

Disattivare le scansioni per un sistema

Quando si disattivano le scansioni, Data Classification non esegue più la scansione dei dati sul sistema e rimuove le informazioni indicizzate dall'istanza di Data Classification. I dati del sistema stesso non vengono eliminati.

1. Dalla pagina *Configurazione*, seleziona pulsante nella riga per il sistema, quindi **Disattiva classificazione dati**.

È anche possibile disattivare le scansioni per un sistema dal pannello Servizi quando si seleziona il sistema.

Rimuovere un database dalla classificazione dei dati

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

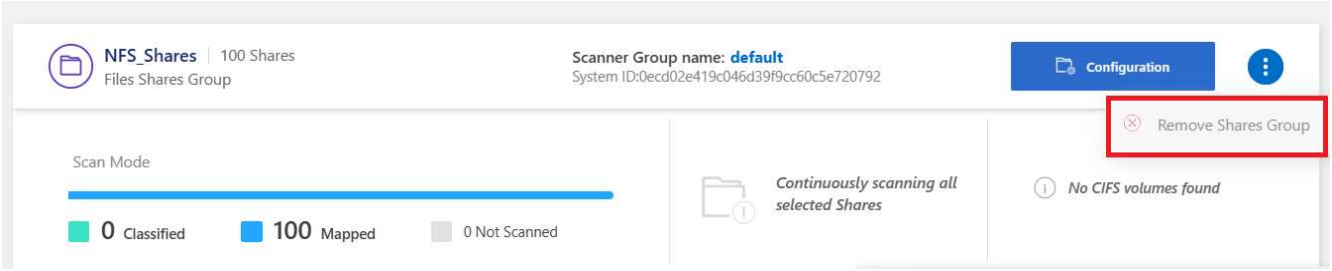
1. Dalla pagina *Configurazione*, seleziona pulsante nella riga per il database, quindi **Rimuovi server DB**.

Rimuovere un gruppo di condivisioni file dalla classificazione dei dati

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

Passi

1. Dalla pagina *Configurazione*, seleziona pulsante nella riga per il Gruppo Condivisioni File, quindi **Rimuovi Gruppo Condivisioni File**.



2. Selezionare **Elimina gruppo di condivisioni** dalla finestra di dialogo di conferma.

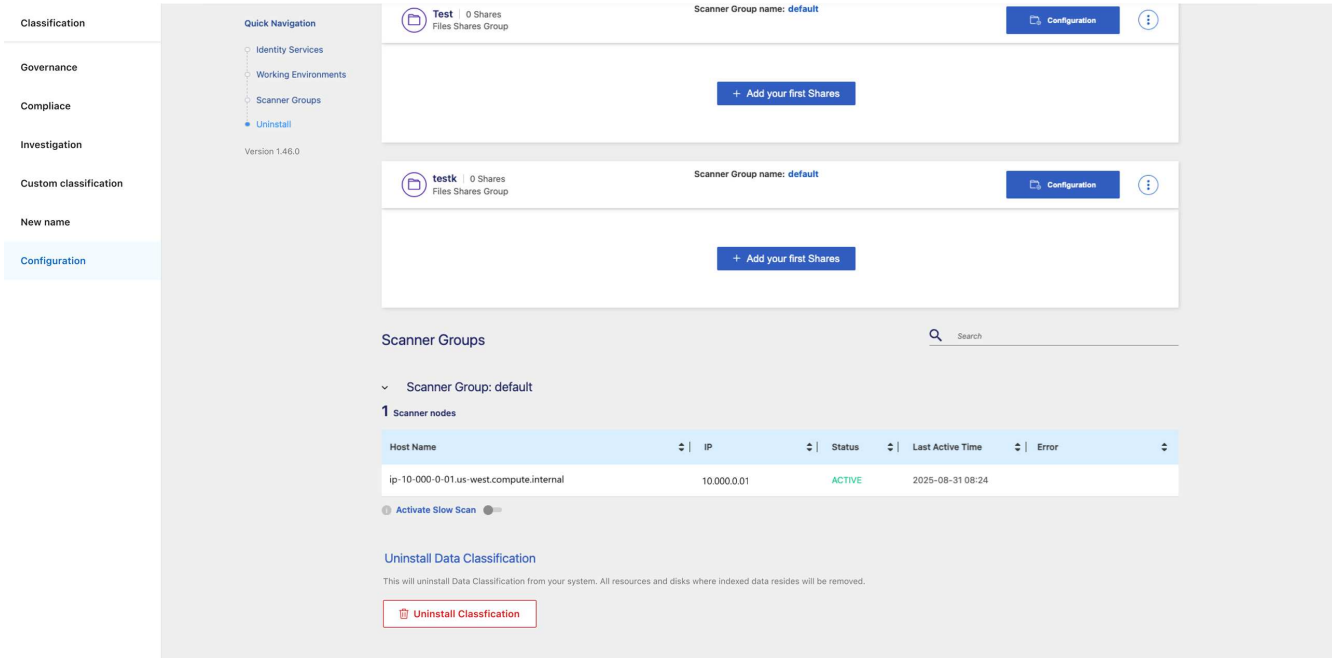
Disinstallare NetApp Data Classification

È possibile disinstallare NetApp Data Classification per risolvere eventuali problemi o per rimuovere definitivamente il software dall'host. L'eliminazione dell'istanza comporta anche l'eliminazione dei dischi associati in cui risiedono i dati indicizzati, il che significa che tutte le informazioni analizzate da Data Classification verranno eliminate definitivamente.

I passaggi da seguire variano a seconda che Data Classification sia stato distribuito nel cloud o su un host locale.

Disinstallare Data Classification da un provider cloud

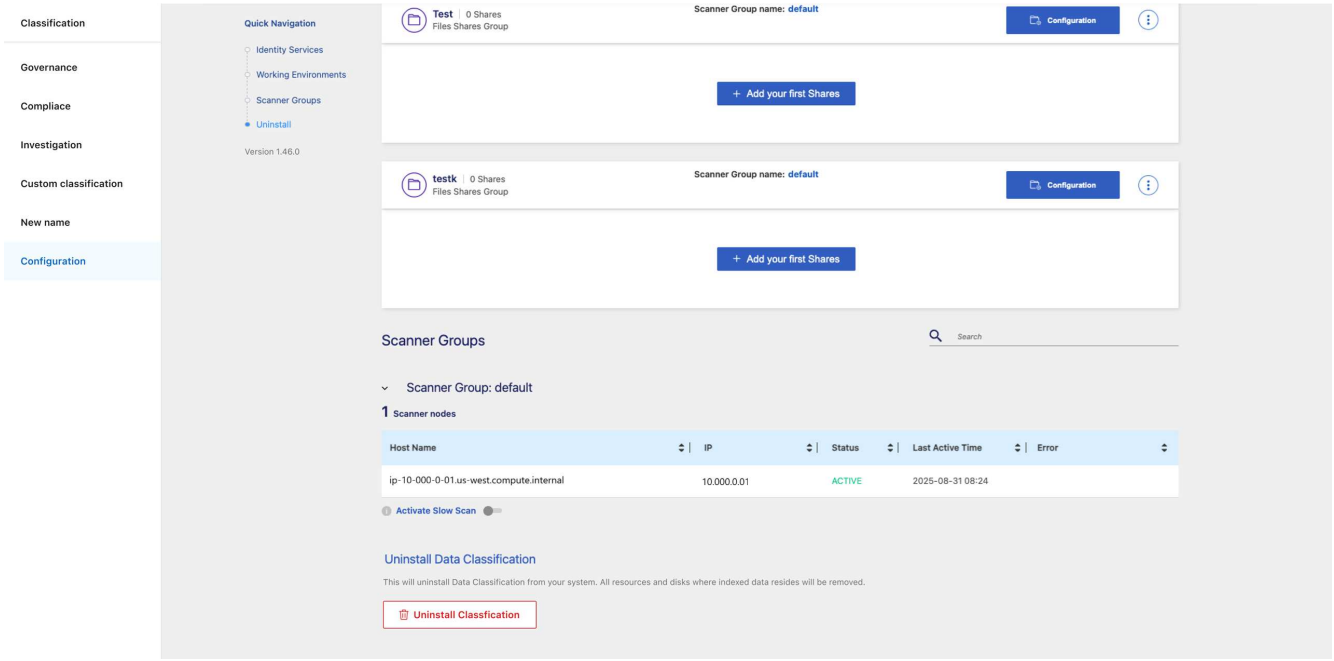
1. Da Classificazione dati, selezionare **Configurazione**.
2. Nella parte inferiore della pagina di configurazione, seleziona **Disinstalla classificazione**.



3. Nella finestra di dialogo, immettere "disinstalla" per procedere con la disconnessione dell'istanza di Data Classification dall'agente Console. Selezionare **Disinstalla** per confermare.
4. Nella finestra di dialogo *Disinstalla classificazione*, digitare **uninstall** per confermare che si desidera disconnettere l'istanza di Data Classification dall'agente Console, quindi selezionare **Disinstalla**.
5. Per completare il processo di disinstallazione, accedi alla console del tuo provider cloud ed elimina l'istanza di Data Classification. L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Disinstallare Data Classification da una distribuzione locale

1. Da Classificazione dati, selezionare **Configurazione**.
2. Nella parte inferiore della pagina di configurazione, seleziona **Disinstalla classificazione**.



3. Nella finestra di dialogo, immettere "disinstalla" per procedere con la disconnessione dell'istanza di Data Classification dall'agente Console. Selezionare **Disinstalla** per confermare.
4. Per disinstallare il software dall'host, eseguire il comando `cleanup.sh` script sulla macchina host di classificazione dei dati, ad esempio:

   ```
   cleanup.sh
   ```

   Lo script si trova nel `/install/light_probe/onprem_installer/cleanup.sh` elenco. Scopri come"accedi alla macchina host di classificazione dei dati" .

Riferimento

Tipi di istanza NetApp Data Classification supportati

Il software NetApp Data Classification deve essere eseguito su un host che soddisfi specifici requisiti del sistema operativo, requisiti RAM, requisiti software e così via. Quando si distribuisce la classificazione dei dati nel cloud, si consiglia di utilizzare un sistema con caratteristiche "large" per una funzionalità completa.

È possibile implementare Data Classification su un sistema con meno CPU e meno RAM, ma ci sono alcune limitazioni quando si utilizzano questi sistemi meno potenti. "Scopri di più su queste limitazioni" .

Nelle tabelle seguenti, se il sistema contrassegnato come "predefinito" non è disponibile nella regione in cui si sta installando Data Classification, verrà distribuito il sistema successivo nella tabella.

Tipi di istanza AWS

Dimensioni del sistema	Specifiche	Tipo di istanza
Extra Large	32 CPU, 128 GB di RAM, 1 TiB gp3 SSD	"m6i.8xlarge"(predefinito)
Grande	16 CPU, 64 GB di RAM, SSD da 500 GiB	"m6i.4xlarge"(predefinito) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Medio	8 CPU, 32 GB di RAM, SSD da 200 GiB	"m6i.2xlarge"(predefinito) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Piccolo	8 CPU, 16 GB di RAM, SSD da 100 GiB	"c6a.2xlarge"(predefinito) c5a.2xlarge c5.2xlarge c4.2xlarge

Tipi di istanza di Azure

Dimensioni del sistema	Specifiche	Tipo di istanza
Extra Large	32 CPU, 128 GB di RAM, disco del sistema operativo (2.048 GiB, velocità di trasmissione minima 250 MB/s) e disco dati (SSD da 1 TiB, velocità di trasmissione minima 750 MB/s)	"Standard_D32_v3"(predefinito)
Grande	16 CPU, 64 GB di RAM, SSD da 500 GiB	"Standard_D16s_v3"(predefinito)

Tipi di istanza GCP

Dimensioni del sistema	Specifiche	Tipo di istanza
Grande	16 CPU, 64 GB di RAM, SSD da 500 GiB	"n2-standard-16"(predefinito) n2d-standard-16 n1-standard-16

Metadati raccolti da fonti di dati in NetApp Data Classification

NetApp Data Classification raccoglie determinati metadati durante l'esecuzione di scansioni di classificazione sui dati provenienti dalle fonti dati e dai sistemi. Data Classification può accedere alla maggior parte dei metadati di cui abbiamo bisogno per classificare i tuoi dati, ma ci sono alcune fonti da cui non siamo in grado di accedere ai dati di cui abbiamo bisogno.

	Metadati	CIFS	Non è vero
Timbri temporali	*Ora di creazione*	Disponibile	Non disponibile (non supportato in Linux)
	Ultimo orario di accesso	Disponibile	Disponibile
	Ora dell'ultima modifica	Disponibile	Disponibile
Autorizzazioni	*Apri permessi*	Se il gruppo "TUTTI" ha accesso al file, questo è considerato "Aperto all'organizzazione"	Se "Altri" ha accesso al file, questo è considerato "Aperto all'organizzazione"
	Accesso utenti/gruppi	Le informazioni sugli utenti e sui gruppi vengono prese da LDAP	Non disponibile (gli utenti NFS sono solitamente gestiti localmente sul server, pertanto lo stesso individuo può avere un UID diverso in ogni server)

- La classificazione dei dati non estrae l'"orario dell'ultimo accesso" dalle fonti dati del database.
- Le versioni precedenti del sistema operativo Windows (ad esempio, Windows 7 e Windows 8) disabilitano per impostazione predefinita la raccolta dell'attributo "ora dell'ultimo accesso" perché può influire sulle prestazioni del sistema. Se questo attributo non viene raccolto, le analisi di classificazione dei dati basate sull'"orario dell'ultimo accesso" saranno interessate. Se necessario, è possibile abilitare la raccolta dell'orario dell'ultimo accesso su questi vecchi sistemi Windows.

Timestamp dell'ultimo accesso

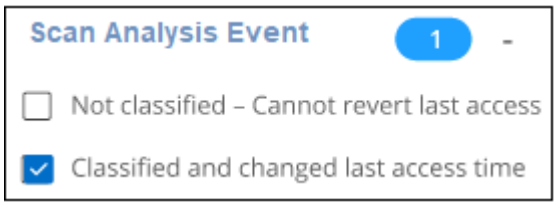
Quando Data Classification estrae dati dalle condivisioni di file, il sistema operativo lo considera come se stesse accedendo ai dati e modifica di conseguenza l'"orario dell'ultimo accesso". Dopo la scansione, la classificazione dei dati tenta di ripristinare l'orario dell'ultimo accesso al timestamp originale. Se Data Classification non dispone di autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS, il sistema non può ripristinare l'orario dell'ultimo accesso al timestamp originale. I volumi ONTAP configurati con SnapLock hanno autorizzazioni di sola lettura e non possono ripristinare l'orario dell'ultimo accesso al timestamp originale.

Per impostazione predefinita, se Data Classification non dispone di queste autorizzazioni, il sistema non analizzerà i file nei volumi perché Data Classification non può ripristinare l'"ultimo orario di accesso" al timestamp originale. Tuttavia, se non ti interessa che l'orario dell'ultimo accesso venga reimpostato sull'orario originale nei tuoi file, puoi selezionare l'opzione **Scansiona quando mancano le autorizzazioni "attributi di**

scrittura" nella parte inferiore della pagina Configurazione, in modo che Data Classification esegua la scansione dei volumi indipendentemente dalle autorizzazioni.

Questa funzionalità è applicabile ai sistemi ONTAP locali, Cloud Volumes ONTAP, Azure NetApp Files, Amazon FSx for NetApp ONTAP e condivisioni file di terze parti.

Nella pagina Indagine è presente un filtro denominato *Evento analisi scansione* che consente di visualizzare i file che non sono stati classificati perché la classificazione dei dati non è riuscita a ripristinare l'orario dell'ultimo accesso oppure i file che sono stati classificati anche se la classificazione dei dati non è riuscita a ripristinare l'orario dell'ultimo accesso.



Le selezioni del filtro sono:

- "Non classificato - Impossibile ripristinare l'ultimo orario di accesso": mostra i file che non sono stati classificati a causa della mancanza di autorizzazioni di scrittura.
- "Ultimo orario di accesso classificato e aggiornato": mostra i file che sono stati classificati e la classificazione dei dati non è riuscita a reimpostare l'ultimo orario di accesso alla data originale. Questo filtro è rilevante solo per gli ambienti in cui è stata attivata l'opzione **Scansione quando mancano le autorizzazioni "attributi di scrittura"**.

Se necessario, è possibile esportare questi risultati in un report, in modo da poter vedere quali file vengono o non vengono analizzati in base alle autorizzazioni. "Scopri di più sui report di Data Investigation".

Accedi al sistema NetApp Data Classification

È necessario accedere al sistema NetApp Data Classification per poter accedere ai file di registro o modificare i file di configurazione.

Quando Data Classification è installato su una macchina Linux in sede o su una macchina Linux distribuita nel cloud, è possibile accedere direttamente al file di configurazione e allo script.

Quando Data Classification viene distribuito nel cloud, è necessario connettersi tramite SSH all'istanza di Data Classification. È possibile accedere al sistema tramite SSH immettendo nome utente e password oppure utilizzando la chiave SSH fornita durante l'installazione dell'agente Console. Il comando SSH è:

```
ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
```

- `<path_to_the_ssh_key>`= posizione delle chiavi di autenticazione ssh
- `<machine_user>:`
  - Per AWS: utilizzare <ec2-user>
  - Per Azure: utilizzare l'utente creato per l'istanza della console
  - Per GCP: utilizzare l'utente creato per l'istanza della console
- `<datasense_ip>`= Indirizzo IP dell'istanza della macchina virtuale

Per accedere al sistema nel cloud è necessario modificare le regole in entrata del gruppo di sicurezza. Per maggiori dettagli, vedere:

- "Regole del gruppo di sicurezza in AWS"
- "Regole del gruppo di sicurezza in Azure"
- "Regole del firewall in Google Cloud"

API NetApp Data Classification

Le funzionalità NetApp Data Classification disponibili tramite l'interfaccia utente Web sono disponibili anche tramite l'API REST.

Nella Classificazione dei dati sono definite quattro categorie che corrispondono alle schede nell'interfaccia utente:

- Indagine
- Conformità
- Governance
- Configurazione

Le API nella documentazione di Swagger consentono di cercare, aggregare dati, monitorare le scansioni ed eseguire azioni tra cui copia, spostamento ed eliminazione.

Panoramica

L'API consente di eseguire le seguenti funzioni:

- Informazioni sull'esportazione
  - Tutto ciò che è disponibile nell'interfaccia utente può essere esportato tramite l'API (ad eccezione dei report)
  - I dati vengono esportati in formato JSON (facile da analizzare e inviare ad applicazioni di terze parti, come Splunk)
- Crea query utilizzando le istruzioni "AND" e "OR", includi ed escludi informazioni e molto altro.

  Ad esempio, è possibile individuare file *senza* informazioni personali identificabili (PII) specifiche (funzionalità non disponibile nell'interfaccia utente). È anche possibile escludere campi specifici dall'operazione di esportazione.

- Eseguire azioni

- Aggiorna le credenziali CIFS
- Visualizza e annulla le azioni
- Ripeti la scansione delle directory
- Esporta dati

L'API è sicura e utilizza lo stesso metodo di autenticazione dell'interfaccia utente. Puoi trovare informazioni sull'autenticazione nel"Documentazione REST API" .

Accesso al riferimento API Swagger

Per accedere a Swagger ti servirà l'indirizzo IP della tua istanza di classificazione dei dati. Nel caso di un'implementazione cloud, utilizzerai l'indirizzo IP pubblico. Quindi dovrai accedere a questo endpoint:

https://<ip_classificazione>/documentazione

Esempio utilizzando le API

L'esempio seguente mostra una chiamata API per copiare i file.

Richiesta API

Inizialmente sarà necessario ottenere tutti i campi e le opzioni rilevanti affinché un sistema possa visualizzare tutti i filtri nella scheda di indagine.

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… " -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients"
```

Risposta

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
      "name": "string",
      "operators": [
        "EQUALS"
      ],
      "optional_values": [
        {}
      ],
      "secondary": {},
      "server_data": false,
      "type": "TEXT"
```

```
    }
  ]
}
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "POLICIES",
      "name": "Policies",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "EXTRACTION_STATUS_RANGE",
      "name": "Scan Analysis Status",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "SCAN_ANALYSIS_ERROR",
      "name": "Scan Analysis Event",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "PUBLIC_ACCESS",
      "name": "Open Permissions",
      "operators": [
        "IN",
```

```
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USERS_PERMISSIONS_COUNT_RANGE",
      "name": "Number of Users with Access",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USER_GROUP_PERMISSIONS",
      "name": "User / Group Permissions",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_OWNER",
      "name": "File Owner",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT_TYPE",
      "name": "system-type",
      "operators": [
```

```
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT",
      "name": "system",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "SCAN_TASK",
      "name": "Storage Repository",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_PATH",
      "name": "File / Directory Path",
      "operators": [
        "MULTI_CONTAINS",
        "MULTI_EXCLUDE"
      ],
      "server_data": true,
      "type": "MULTI_TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
      "field": "CATEGORY",
```

```
    "name": "Category",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "PATTERN_SENSITIVITY_LEVEL",
    "name": "Sensitivity Level",
    "operators": [
      "IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "NUMBER_OF_IDENTIFIERS",
    "name": "Number of identifiers",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "PATTERN_PERSONAL",
    "name": "Personal Data",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
```

```
      "field": "PATTERN_SENSITIVE",
      "name": "Sensitive Personal Data",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DATA_SUBJECT",
      "name": "Data Subject",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "DIRECTORIES",
      "field": "DIRECTORY_TYPE",
      "name": "Directory Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_TYPE",
      "name": "File Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
```

```
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_SIZE_RANGE",
      "name": "File Size",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_CREATION_RANGE_RETENTION",
      "name": "Created Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DISCOVERED_TIME_RANGE",
      "name": "Discovered Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_MODIFICATION_RETENTION",
      "name": "Last Modified",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
```

```
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
      "name": "Last Accessed",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "IS_DUPLICATE",
      "name": "Duplicates",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "FILE_HASH",
      "name": "File Hash",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "USER_DEFINED_STATUS",
      "name": "Tags",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
```

```
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ASSIGNED_TO",
      "name": "Assigned to",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    }
  ]
}
```

Utilizzeremo questa risposta nei parametri della nostra richiesta per filtrare i file desiderati che vogliamo copiare.

È possibile applicare un'azione a più elementi. I tipi di azioni supportati includono: sposta, elimina e copia.

Creeremo l'azione di copia:

Richiesta API

La prossima API è l'API di azione e consente di creare più azioni.

```
curl -X POST "http://
{classification_ip}/api//{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
"{ontap_ip}:/{share_name} " },
\"requested_query\":{"condition":"AND","rules":[{"field":"ENVIRONMENT_TYPE
","operator":"IN","value":["ONPREM"]},{"field":"CATEGORY","operator":"IN",
"value":["21"]}]}}"
```

Risposta

La risposta restituirà l'oggetto azione, quindi è possibile utilizzare le API get ed delete per ottenere lo stato dell'azione o per annullarla.

```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```

Conoscenza e supporto

Registrati per ricevere supporto per NetApp Console

Per ricevere supporto tecnico specifico per NetApp Console e le sue soluzioni di storage e servizi dati è necessaria la registrazione al supporto. La registrazione del supporto è inoltre richiesta per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP .

La registrazione per il supporto non abilita il supporto NetApp per un servizio file del provider cloud. Per assistenza tecnica relativa a un servizio file di un provider cloud, alla sua infrastruttura o a qualsiasi soluzione che utilizzi il servizio, fare riferimento alla sezione "Ottenere assistenza" nella documentazione del prodotto in questione.

- "Amazon FSx per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Panoramica della registrazione del supporto

Per attivare il diritto al sostegno sono previste due modalità di registrazione:

- Registrando il numero di serie del tuo account NetApp Console (il numero di serie di 20 cifre 960xxxxxxxx che si trova nella pagina Risorse di supporto nella Console).

  Questo funge da ID di abbonamento unico per qualsiasi servizio all'interno della Console. Ogni account Console deve essere registrato.

- Registrazione dei numeri di serie di Cloud Volumes ONTAP associati a un abbonamento nel marketplace del tuo provider cloud (si tratta di numeri di serie a 20 cifre 909201xxxxxxxx).

  Questi numeri di serie sono comunemente denominati *numeri di serie PAYGO* e vengono generati dalla NetApp Console al momento della distribuzione Cloud Volumes ONTAP .

La registrazione di entrambi i tipi di numeri di serie consente funzionalità quali l'apertura di ticket di supporto e la generazione automatica di casi. La registrazione viene completata aggiungendo gli account NetApp Support Site (NSS) alla Console come descritto di seguito.

Registra NetApp Console per il supporto NetApp

Per registrarsi per ricevere supporto e attivare il diritto al supporto, un utente del tuo account NetApp Console deve associare un account NetApp Support Site al proprio accesso alla Console. La modalità di registrazione per l'assistenza NetApp varia a seconda che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite la Console.

Passi

1. Selezionare **Amministrazione** > **Credenziali**.

2. Selezionare **Credenziali utente**.
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp (NSS).
4. Per confermare che il processo di registrazione è andato a buon fine, seleziona l'icona Aiuto e poi **Supporto**.

   La pagina **Risorse** dovrebbe mostrare che il tuo account Console è registrato per il supporto.

   Tieni presente che gli altri utenti della Console non vedranno lo stesso stato di registrazione del supporto se non hanno associato un account NetApp Support Site al loro login. Tuttavia, ciò non significa che il tuo account non sia registrato per l'assistenza. Se un utente dell'organizzazione ha seguito questi passaggi, il tuo account è stato registrato.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp esistente con licenze e numeri di serie esistenti ma *nessun* account NSS, devi creare un account NSS e associarlo al tuo accesso alla Console.

Passi

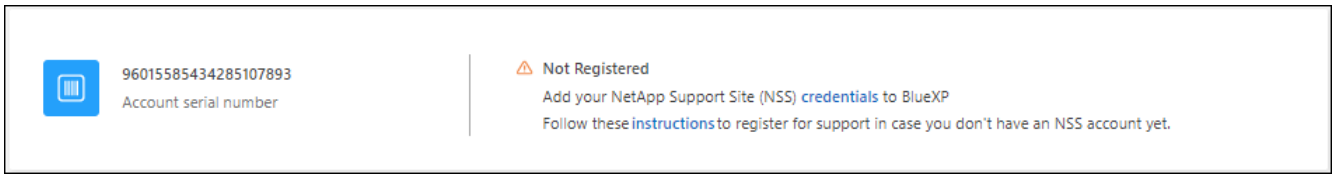
1. Crea un account del sito di supporto NetApp completando il "Modulo di registrazione utente del sito di supporto NetApp"
   a. Assicurati di selezionare il livello utente appropriato, che in genere è **Cliente NetApp /Utente finale**.
   b. Assicurati di copiare il numero di serie dell'account della console (960xxxx) utilizzato sopra per il campo del numero di serie. Ciò velocizzerà l'elaborazione dell'account.
2. Associa il tuo nuovo account NSS al tuo accesso alla Console completando i passaggi indicati di seguitoCliente esistente con un account NSS .

Novità assoluta per NetApp

Se sei un nuovo utente NetApp e non hai un account NSS, segui i passaggi indicati di seguito.

Passi

1. Nell'angolo in alto a destra della Console, seleziona l'icona Aiuto e seleziona **Supporto**.
2. Individua il numero di serie del tuo ID account nella pagina di registrazione del supporto.



3. Vai a "Sito di registrazione del supporto NetApp" e seleziona **Non sono un cliente NetApp registrato**.
4. Compila i campi obbligatori (quelli contrassegnati da asterischi rossi).
5. Nel campo **Linea di prodotti**, seleziona **Cloud Manager** e poi seleziona il tuo fornitore di fatturazione applicabile.
6. Copia il numero di serie del tuo account dal passaggio 2 sopra, completa il controllo di sicurezza e conferma di aver letto l'Informativa globale sulla privacy dei dati di NetApp.

   Per finalizzare questa transazione sicura, verrà inviata immediatamente un'e-mail alla casella di posta indicata. Se l'e-mail di convalida non arriva entro pochi minuti, assicurati di controllare la cartella spam.

7. Conferma l'azione dall'interno dell'e-mail.

   La conferma invia la richiesta a NetApp e ti consiglia di creare un account sul sito di supporto NetApp .

8. Crea un account del sito di supporto NetApp completando il "Modulo di registrazione utente del sito di supporto NetApp"
   a. Assicurati di selezionare il livello utente appropriato, che in genere è **Cliente NetApp /Utente finale**.
   b. Assicurati di copiare il numero di serie dell'account (960xxxx) utilizzato sopra per il campo del numero di serie. Ciò velocizzerà l'elaborazione.

Dopo aver finito

NetApp dovrebbe contattarti durante questo processo. Si tratta di un esercizio di onboarding una tantum per i nuovi utenti.

Una volta ottenuto l'account del sito di supporto NetApp , associalo al tuo accesso alla console completando i passaggi indicati di seguitoCliente esistente con un account NSS .

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

L'associazione delle credenziali del sito di supporto NetApp al tuo account della console è necessaria per abilitare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP:

- Registrazione dei sistemi Cloud Volumes ONTAP a consumo per il supporto

  Per attivare il supporto per il tuo sistema e accedere alle risorse di supporto tecnico NetApp è necessario fornire il tuo account NSS.

- Distribuzione di Cloud Volumes ONTAP quando si utilizza la propria licenza (BYOL)

  È necessario fornire il proprio account NSS affinché la Console possa caricare la chiave di licenza e abilitare l'abbonamento per il periodo acquistato. Ciò include aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP all'ultima versione

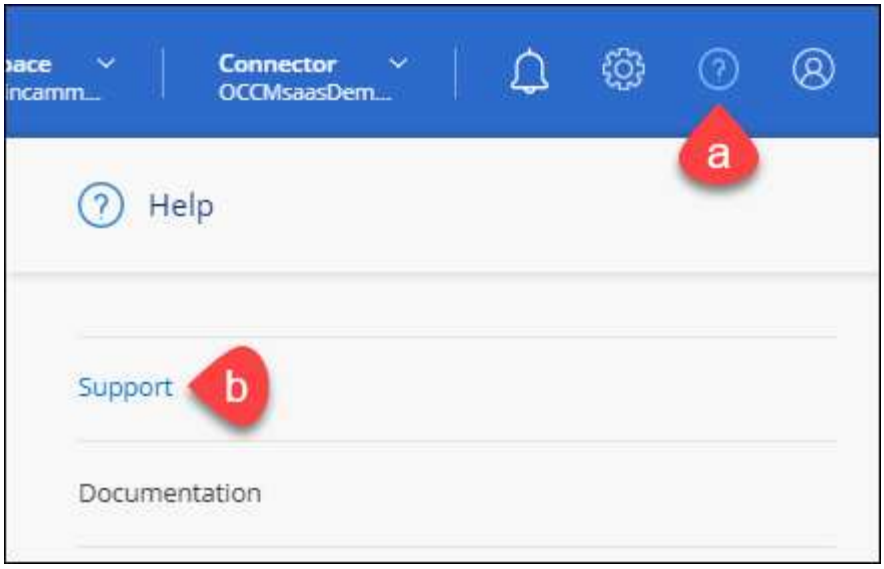
L'associazione delle credenziali NSS al tuo account NetApp Console è diversa dall'associazione dell'account NSS all'accesso utente della Console.

Queste credenziali NSS sono associate al tuo ID account Console specifico. Gli utenti che appartengono all'organizzazione Console possono accedere a queste credenziali da **Supporto > Gestione NSS**.

- Se disponi di un account a livello cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o rivenditore, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

Passi

1. Nell'angolo in alto a destra della Console, seleziona l'icona Aiuto e seleziona **Supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, seleziona **Continua** per essere reindirizzato alla pagina di accesso di Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e le licenze.

4. Nella pagina di accesso, inserisci l'indirizzo email e la password registrati sul sito di supporto NetApp per eseguire il processo di autenticazione.

   Queste azioni consentono alla Console di utilizzare il tuo account NSS per attività quali download di licenze, verifica di aggiornamenti software e future registrazioni di supporto.

   Notare quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account ospite o temporaneo). È possibile avere più account NSS a livello di cliente.
   - Può esserci un solo account NSS se tale account è un account a livello di partner. Se provi ad aggiungere account NSS a livello di cliente ed esiste già un account a livello di partner, riceverai il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account poiché sono già presenti utenti NSS di tipo diverso."

   Lo stesso vale se si dispone di account NSS preesistenti a livello di cliente e si tenta di aggiungere un account a livello di partner.

   - Dopo aver effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che corrisponde al tuo indirizzo email. Nella pagina **Gestione NSS**, puoi visualizzare la tua email da ••• menu.

   - Se hai bisogno di aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Aggiorna credenziali** in ••• menu.

     Utilizzando questa opzione ti verrà richiesto di effettuare nuovamente l'accesso. Si noti che il token per questi account scade dopo 90 giorni. Verrà pubblicata una notifica per avvisarti di ciò.

Ottieni assistenza per la NetApp Data Classification

NetApp fornisce supporto per NetApp Console e i suoi servizi cloud in vari modi. Sono disponibili ampie opzioni di auto-supporto gratuite 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include supporto tecnico remoto tramite ticket web.

Ottieni supporto per un servizio file di un provider cloud

Per il supporto tecnico relativo al servizio file di un provider cloud, alla sua infrastruttura o a qualsiasi soluzione che utilizzi il servizio, fare riferimento alla documentazione del prodotto in questione.

- "Amazon FSx per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Per ricevere supporto tecnico specifico per NetApp e le sue soluzioni di storage e servizi dati, utilizzare le opzioni di supporto descritte di seguito.

Utilizzare opzioni di auto-supporto

Queste opzioni sono disponibili gratuitamente, 24 ore al giorno, 7 giorni alla settimana:

- Documentazione

  La documentazione NetApp Console che stai visualizzando.

- "Base di conoscenza"

  Cerca nella knowledge base NetApp per trovare articoli utili per la risoluzione dei problemi.

- "Comunità"

  Unisciti alla community NetApp Console per seguire le discussioni in corso o crearne di nuove.

Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo aver attivato il supporto.

Prima di iniziare

- Per utilizzare la funzionalità **Crea un caso**, devi prima associare le credenziali del sito di supporto NetApp all'accesso alla console. "Scopri come gestire le credenziali associate al tuo accesso alla Console" .
- Se stai aprendo un caso per un sistema ONTAP che ha un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Passi

1. Nella NetApp Console, seleziona **Guida > Supporto**.
2. Nella pagina **Risorse**, seleziona una delle opzioni disponibili in Supporto tecnico:

a. Seleziona **Chiamaci** se desideri parlare con qualcuno al telefono. Verrai indirizzato a una pagina su netapp.com in cui sono elencati i numeri di telefono che puoi chiamare.

b. Seleziona **Crea un caso** per aprire un ticket con uno specialista del supporto NetApp :

   - **Servizio**: seleziona il servizio a cui è associato il problema. Ad esempio, * NetApp Console* quando si tratta di un problema specifico di supporto tecnico con flussi di lavoro o funzionalità all'interno della Console.
   - **Sistema**: se applicabile all'archiviazione, selezionare * Cloud Volumes ONTAP* o **On-Prem** e quindi l'ambiente di lavoro associato.

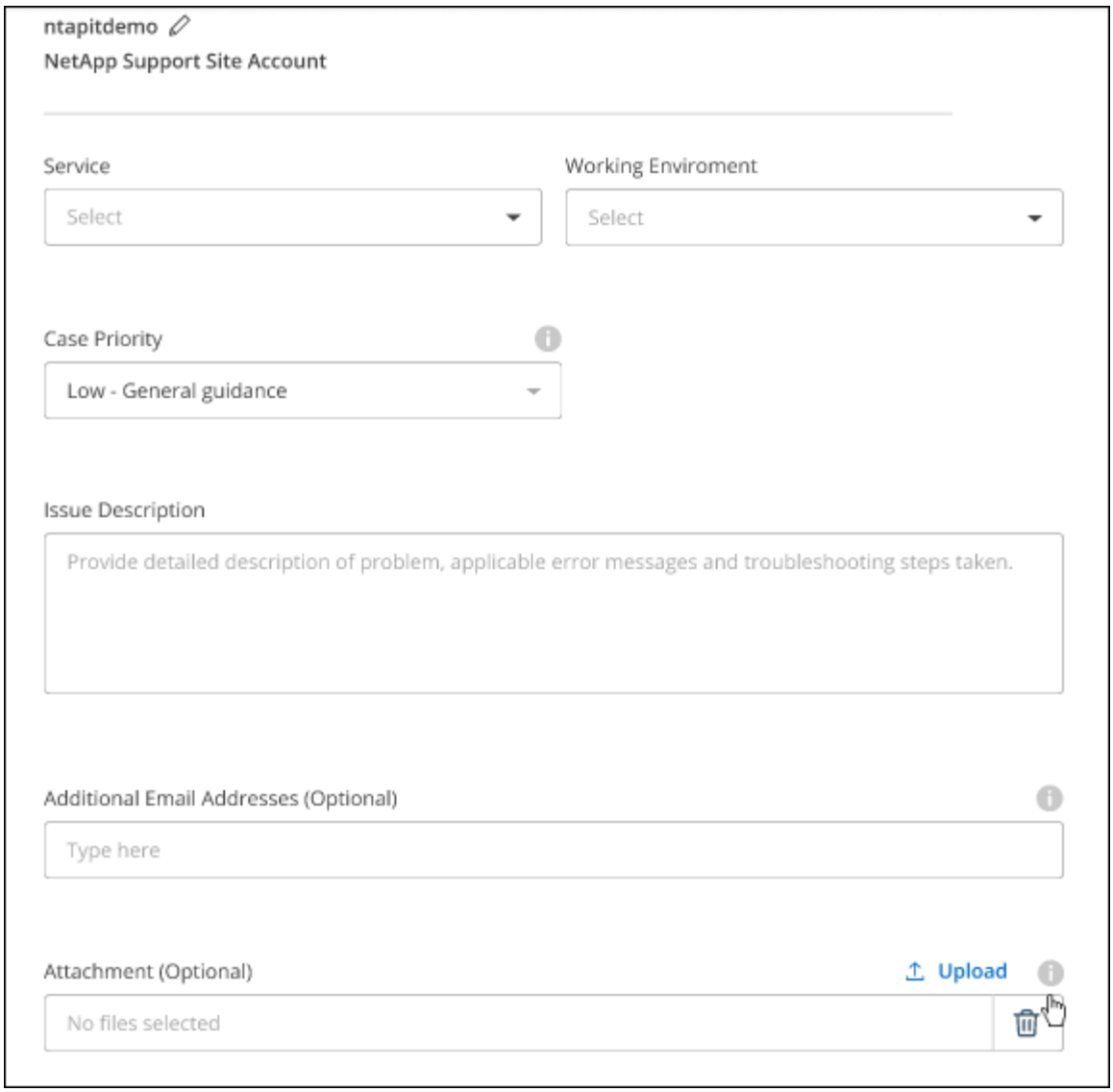
     L'elenco dei sistemi rientra nell'ambito dell'organizzazione della Console e dell'agente della Console selezionato nel banner in alto.

   - **Priorità del caso**: scegli la priorità del caso, che può essere Bassa, Media, Alta o Critica.

     Per saperne di più su queste priorità, passa il mouse sull'icona informativa accanto al nome del campo.

   - **Descrizione del problema**: fornisci una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o passaggi per la risoluzione dei problemi eseguiti.
   - **Indirizzi email aggiuntivi**: inserisci altri indirizzi email se desideri informare qualcun altro di questo problema.
   - **Allegato (facoltativo)**: carica fino a cinque allegati, uno alla volta.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Dopo aver finito

Apparirà una finestra pop-up con il numero del tuo caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei tuoi casi di supporto, puoi selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzarne i dettagli.

È possibile che venga visualizzato il seguente messaggio di errore quando si tenta di creare un caso:

"Non sei autorizzato a creare un caso contro il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società registrata a cui è associato non corrispondono alla stessa società registrata per il numero di serie dell'account NetApp Console (ad esempio 960xxxx) o il numero di serie dell'ambiente di lavoro. Puoi richiedere assistenza utilizzando una delle seguenti opzioni:

- Invia un caso non tecnico a https://mysupport.netapp.com/site/help

Gestisci i tuoi casi di supporto

È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente dalla Console. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

Notare quanto segue:

- La dashboard di gestione dei casi nella parte superiore della pagina offre due visualizzazioni:
  - La vista a sinistra mostra il totale dei casi aperti negli ultimi 3 mesi dall'account NSS utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base al tuo account NSS utente.

  I risultati nella tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come Priorità e Stato. Altre colonne forniscono solo funzionalità di ordinamento.

  Per maggiori dettagli, vedere i passaggi riportati di seguito.
- A livello di singolo caso, offriamo la possibilità di aggiornare le note del caso o di chiudere un caso che non sia già nello stato Chiuso o In attesa di chiusura.

Passi

1. Nella NetApp Console, seleziona **Guida > Supporto**.
2. Seleziona **Gestione casi** e, se richiesto, aggiungi il tuo account NSS alla Console.

   La pagina **Gestione casi** mostra i casi aperti relativi all'account NSS associato al tuo account utente della Console. Si tratta dello stesso account NSS che appare in cima alla pagina **Gestione NSS**.
3. Facoltativamente, modifica le informazioni visualizzate nella tabella:
   - In **Casi dell'organizzazione**, seleziona **Visualizza** per visualizzare tutti i casi associati alla tua azienda.
   - Modifica l'intervallo di date scegliendo un intervallo di date esatto o un intervallo di tempo diverso.
   - Filtra il contenuto delle colonne.
   - Modifica le colonne che appaiono nella tabella selezionando e quindi scegli le colonne che desideri visualizzare.
4. Gestisci un caso esistente selezionando e selezionando una delle opzioni disponibili:
   - **Visualizza caso**: visualizza i dettagli completi su un caso specifico.
   - **Aggiorna note sul caso**: fornisci ulteriori dettagli sul tuo problema o seleziona **Carica file** per allegare fino a un massimo di cinque file.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.
   - **Chiudi caso**: fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.

Domande frequenti sulla NetApp Data Classification

Questa sezione FAQ può aiutarti se stai cercando una risposta rapida a una domanda.

NetApp Data Classification

Le seguenti domande forniscono una comprensione generale della classificazione dei dati.

Come funziona la classificazione dei dati?

La classificazione dei dati implementa un ulteriore livello di intelligenza artificiale insieme al sistema NetApp Console e ai sistemi di storage. Quindi esegue la scansione dei dati su volumi, bucket, database e altri account di archiviazione e indicizza le informazioni sui dati trovate. La classificazione dei dati sfrutta sia l'intelligenza artificiale che l'elaborazione del linguaggio naturale, a differenza delle soluzioni alternative che si basano comunemente su espressioni regolari e pattern matching.

La classificazione dei dati utilizza l'intelligenza artificiale per fornire una comprensione contestuale dei dati, consentendo un rilevamento e una classificazione accurati. È basato sull'intelligenza artificiale perché è progettato per i moderni tipi di dati e per la scalabilità. Comprende inoltre il contesto dei dati per fornire una scoperta e una classificazione solide e accurate.

"Scopri di più su come funziona la classificazione dei dati" .

Data Classification dispone di un'API REST e funziona con strumenti di terze parti?

Sì, Data Classification dispone di un'API REST per le funzionalità supportate nella versione Data Classification che fa parte della piattaforma core della Console. Vedere "Documentazione API" .

La classificazione dei dati è disponibile tramite i marketplace cloud?

La classificazione dei dati fa parte delle funzionalità principali NetApp Console , quindi non è necessario utilizzare i marketplace per questo servizio.

Scansione e analisi della classificazione dei dati

Le seguenti domande riguardano le prestazioni di scansione e l'analisi della classificazione dei dati.

Con quale frequenza Data Classification analizza i miei dati?

Sebbene la scansione iniziale dei dati possa richiedere un po' di tempo, le scansioni successive esaminano solo le modifiche incrementali, riducendo così i tempi di scansione del sistema. La classificazione dei dati analizza i dati in modo continuo e ciclico, sei repository alla volta, in modo che tutti i dati modificati vengano classificati molto rapidamente.

"Scopri come funzionano le scansioni" .

La classificazione dei dati analizza i database solo una volta al giorno; i database non vengono analizzati continuamente come altre fonti di dati.

Le scansioni dei dati hanno un impatto trascurabile sui sistemi di archiviazione e sui dati.

Le prestazioni della scansione variano?

Le prestazioni della scansione possono variare in base alla larghezza di banda della rete e alla dimensione media dei file nel tuo ambiente. Può dipendere anche dalle caratteristiche dimensionali del sistema host (nel cloud o in locale). Vedere "L'istanza di classificazione dei dati" E "Distribuzione della classificazione dei dati" per maggiori informazioni.

Quando si aggiungono inizialmente nuove fonti di dati, è anche possibile scegliere di eseguire solo una scansione di "mappatura" (Solo mappatura) anziché una scansione di "classificazione" completa (Mappa e classifica). La mappatura delle fonti dati può essere eseguita molto rapidamente perché non è necessario accedere ai file per visualizzare i dati al loro interno. "Scopri la differenza tra una scansione di mappatura e una di classificazione" .

Posso cercare i miei dati utilizzando la classificazione dei dati?

Data Classification offre ampie capacità di ricerca che semplificano la ricerca di un file o di un dato specifico in tutte le fonti connesse. La classificazione dei dati consente agli utenti di effettuare ricerche più approfondite rispetto a quanto riportato nei metadati. Si tratta di un servizio indipendente dal linguaggio, in grado di leggere i file e analizzare una moltitudine di tipi di dati sensibili, come nomi e ID. Ad esempio, gli utenti possono effettuare ricerche sia negli archivi dati strutturati che in quelli non strutturati per trovare dati che potrebbero essere trapelati dai database ai file degli utenti, violando le policy aziendali. Le ricerche possono essere salvate per un secondo momento e si possono creare policy per cercare e intervenire sui risultati con una frequenza stabilita.

Una volta trovati i file di interesse, è possibile elencarne le caratteristiche, tra cui tag, account di sistema, bucket, percorso del file, categoria (dalla classificazione), dimensione del file, ultima modifica, stato delle autorizzazioni, duplicati, livello di sensibilità, dati personali, tipi di dati sensibili all'interno del file, proprietario, tipo di file, dimensione del file, ora di creazione, hash del file, se i dati sono stati assegnati a qualcuno che cercava la loro attenzione e altro ancora. È possibile applicare filtri per escludere le caratteristiche non pertinenti.

La classificazione dei dati prevede anche il controllo degli accessi basato sui ruoli (RBAC) per consentire lo spostamento o l'eliminazione dei file, se sono presenti le autorizzazioni appropriate. Se non sono presenti le autorizzazioni appropriate, le attività possono essere assegnate a qualcuno nell'organizzazione che dispone delle autorizzazioni appropriate.

Gestione della classificazione dei dati e privacy

Le seguenti domande forniscono informazioni su come gestire la classificazione dei dati e le impostazioni sulla privacy.

Come posso abilitare o disabilitare la classificazione dei dati?

Per prima cosa è necessario distribuire un'istanza di Data Classification nella Console o su un sistema locale. Una volta che l'istanza è in esecuzione, è possibile abilitare il servizio su sistemi, database e altre origini dati esistenti dalla scheda **Configurazione** o selezionando un sistema specifico. "Scopri come iniziare" .

> L'attivazione della classificazione dei dati su un'origine dati determina una scansione iniziale immediata. I risultati della scansione vengono visualizzati poco dopo.

È possibile disattivare la classificazione dei dati per impedire la scansione di un singolo sistema, database o gruppo di condivisione file dalla pagina Configurazione classificazione dati. Vedere "Rimuovere le origini dati dalla classificazione dei dati" .

Per rimuovere completamente l'istanza di Data Classification, rimuovila manualmente dal portale del tuo provider cloud o dalla posizione locale.

Il servizio può escludere la scansione dei dati in determinate directory?

Sì. Se si desidera che la classificazione dei dati escluda la scansione dei dati che risiedono in determinate directory di origine dati, è possibile fornire tale elenco al motore di classificazione. Dopo aver applicato la modifica, la classificazione dei dati escluderà la scansione dei dati nelle directory specificate. "Saperne di più" .

Gli snapshot che risiedono sui volumi ONTAP vengono scansionati?

No. La classificazione dei dati non analizza gli snapshot perché il contenuto è identico al contenuto del volume.

Cosa succede se sui volumi ONTAP è abilitato il tiering dei dati?

Quando Data Classification esegue la scansione di volumi che contengono dati inattivi suddivisi in livelli per l'archiviazione di oggetti utilizzando solo scansioni di mappatura, esegue la scansione di tutti i dati: dati presenti sui dischi locali e dati inattivi suddivisi in livelli per l'archiviazione di oggetti. Ciò vale anche per i prodotti non NetApp che implementano la suddivisione in livelli.

La scansione di sola mappatura non surriscalda i dati freddi: questi rimangono freddi e rimangono nell'archivio degli oggetti. D'altro canto, se si esegue la scansione Map & Classify, alcune configurazioni potrebbero surriscaldare i dati inutilizzati.

Tipi di sistemi sorgente e tipi di dati

Le seguenti domande riguardano i tipi di archiviazione che possono essere scansionati e i tipi di dati che vengono scansionati.

Ci sono delle restrizioni quando si opera in una regione governativa?

La classificazione dei dati è supportata quando l'agente della console viene distribuito in una regione governativa (AWS GovCloud, Azure Gov o Azure DoD), nota anche come "modalità limitata".

Quali fonti di dati posso analizzare se installo Data Classification in un sito senza accesso a Internet?

> 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" .

La classificazione dei dati può analizzare solo i dati provenienti da fonti dati locali rispetto al sito locale. Al momento, Data Classification può analizzare le seguenti fonti di dati locali in "Modalità privata", nota anche come sito "dark":

- Sistemi ONTAP on-premise
- Schemi di database
- Object Storage che utilizza il protocollo Simple Storage Service (S3)

Quali tipi di file sono supportati?

La classificazione dei dati analizza tutti i file per ottenere informazioni dettagliate su categorie e metadati e visualizza tutti i tipi di file nella sezione Tipi di file della dashboard.

Quando la classificazione dei dati rileva informazioni personali identificabili (PII) o quando esegue una ricerca DSAR, sono supportati solo i seguenti formati di file:

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

Quali tipi di dati e metadati cattura la classificazione dei dati?

La classificazione dei dati consente di eseguire una scansione di "mappatura" generale o una scansione di "classificazione" completa sulle origini dati. La mappatura fornisce solo una panoramica di alto livello dei dati, mentre la classificazione fornisce una scansione approfondita dei dati. La mappatura delle fonti dati può essere eseguita molto rapidamente perché non è necessario accedere ai file per visualizzare i dati al loro interno.

- **Scansione di mappatura dei dati (scansione solo di mappatura)**: la classificazione dei dati esegue la scansione solo dei metadati. Ciò è utile per la gestione e la governance dei dati complessivi, per una rapida definizione dell'ambito del progetto, per patrimoni molto ampi e per la definizione delle priorità. La mappatura dei dati si basa sui metadati ed è considerata una scansione **veloce**.

  Dopo una scansione rapida, è possibile generare un report di mappatura dei dati. Questo report è una panoramica dei dati archiviati nelle fonti dati aziendali per aiutarti a prendere decisioni sull'utilizzo delle risorse, sulla migrazione, sul backup, sulla sicurezza e sui processi di conformità.

- **Scansione approfondita della classificazione dei dati (scansione mappa e classifica)**: la classificazione dei dati esegue la scansione dei dati utilizzando protocolli standard e autorizzazioni di sola lettura in tutti gli ambienti. Vengono aperti file selezionati e analizzati per rilevare dati aziendali sensibili, informazioni private e problemi correlati al ransomware.

  Dopo una scansione completa, è possibile applicare ai dati numerose funzionalità aggiuntive di classificazione dei dati, come la visualizzazione e la rifinitura dei dati nella pagina Indagine sui dati, la ricerca di nomi all'interno dei file, la copia, lo spostamento e l'eliminazione dei file sorgente e altro ancora.

La classificazione dei dati acquisisce metadati quali: nome del file, autorizzazioni, ora di creazione, ultimo accesso e ultima modifica. Ciò include tutti i metadati che appaiono nella pagina Dettagli indagine dati e nei Report indagine dati.

La classificazione dei dati può identificare molti tipi di dati privati, come le informazioni personali (PII) e le informazioni personali sensibili (SPII). Per i dettagli sui dati privati, fare riferimento aCategorie di dati privati analizzati dalla classificazione dei dati .

Posso limitare le informazioni sulla classificazione dei dati a utenti specifici?

Sì, la classificazione dei dati è completamente integrata con la NetApp Console. Gli utenti NetApp Console possono visualizzare solo le informazioni relative ai sistemi che sono autorizzati a visualizzare in base alle loro autorizzazioni.

Inoltre, se si desidera consentire a determinati utenti di visualizzare solo i risultati della scansione di classificazione dei dati senza avere la possibilità di gestire le impostazioni di classificazione dei dati, è possibile assegnare a tali utenti il ruolo di **Visualizzatore classificazione** (quando si utilizza la NetApp

Console in modalità standard) o il ruolo di **Visualizzatore conformità** (quando si utilizza la NetApp Console in modalità limitata). "Saperne di più" .

Chiunque può accedere ai dati privati inviati tra il mio browser e Data Classification?

No. 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 né terze parti NetApp possono leggerli. Data Classification non condividerà alcun dato o risultato con NetApp a meno che tu non ne richieda e approvi l'accesso.

I dati scansionati rimangono all'interno del tuo ambiente.

Come vengono gestiti i dati sensibili?

NetApp non ha accesso ai dati sensibili e non li visualizza nell'interfaccia utente. I dati sensibili vengono mascherati, ad esempio vengono visualizzate le ultime quattro cifre delle informazioni sulla carta di credito.

Dove vengono archiviati i dati?

I risultati della scansione vengono archiviati in Elasticsearch all'interno dell'istanza di Data Classification.

Come avviene l'accesso ai dati?

La classificazione dei dati accede ai dati archiviati in Elasticsearch tramite chiamate API, che richiedono l'autenticazione e sono crittografate tramite AES-128. Per accedere direttamente a Elasticsearch è necessario l'accesso root.

Licenze e costi

La seguente domanda riguarda la licenza e i costi per l'utilizzo della classificazione dei dati.

Quanto costa la classificazione dei dati?

La classificazione dei dati è una funzionalità fondamentale NetApp Console . Non è caricato.

Distribuzione dell'agente della console

Le seguenti domande riguardano l'agente Console.

Che cos'è l'agente Console?

L'agente Console è un software in esecuzione su un'istanza di elaborazione all'interno del tuo account cloud o in locale, che consente alla NetApp Console di gestire in modo sicuro le risorse cloud. Per utilizzare la classificazione dei dati è necessario distribuire un agente Console.

Dove deve essere installato l'agente Console?

Durante la scansione dei dati, l'agente NetApp Console deve essere installato nei seguenti percorsi:

- Per Cloud Volumes ONTAP in AWS o Amazon FSx per ONTAP: l'agente della console si trova in AWS.
- Per Cloud Volumes ONTAP in Azure o in Azure NetApp Files: l'agente della console si trova in Azure.

- Per Cloud Volumes ONTAP in GCP: l'agente della console si trova in GCP.
- Per i sistemi ONTAP on-premise: l'agente della console è on-premise.

Se hai dati in queste posizioni, potrebbe essere necessario utilizzare "più agenti della console" .

La classificazione dei dati richiede l'accesso alle credenziali?

La classificazione dei dati in sé non recupera le credenziali di archiviazione. Vengono invece archiviati nell'agente Console.

La classificazione dei dati utilizza le credenziali del piano dati, ad esempio le credenziali CIFS, per montare le condivisioni prima della scansione.

La comunicazione tra il servizio e l'agente della console utilizza HTTP?

Sì, Data Classification comunica con l'agente della console tramite HTTP.

Distribuzione della classificazione dei dati

Le seguenti domande riguardano l'istanza separata di Classificazione dei dati.

Quali modelli di distribuzione supporta Data Classification?

La NetApp Console consente all'utente di eseguire scansioni e report sui sistemi praticamente ovunque, inclusi ambienti locali, cloud e ibridi. La classificazione dei dati viene solitamente distribuita utilizzando un modello SaaS, in cui il servizio è abilitato tramite l'interfaccia della console e non richiede alcuna installazione hardware o software. Anche in questa modalità di distribuzione "click-and-run", la gestione dei dati può essere eseguita indipendentemente dal fatto che gli archivi dati si trovino in locale o nel cloud pubblico.

Quale tipo di istanza o VM è richiesta per la classificazione dei dati?

Quando"distribuito nel cloud" :

- In AWS, Data Classification viene eseguito su un'istanza m6i.4xlarge con un disco GP2 da 500 GiB. Durante la distribuzione è possibile selezionare un tipo di istanza più piccolo.
- In Azure, la classificazione dei dati viene eseguita su una macchina virtuale Standard_D16s_v3 con un disco da 500 GiB.
- In GCP, la classificazione dei dati viene eseguita su una VM n2-standard-16 con un disco persistente standard da 500 GiB.

"Scopri di più su come funziona la classificazione dei dati" .

Posso distribuire la classificazione dei dati sul mio host?

Sì. È possibile installare il software di classificazione dei dati su un host Linux dotato di accesso a Internet nella propria rete o nel cloud. Tutto funziona allo stesso modo e puoi continuare a gestire la configurazione e i risultati della scansione tramite la Console. Vedere"Distribuzione della classificazione dei dati in locale" per i requisiti di sistema e i dettagli di installazione.

E per quanto riguarda i siti sicuri senza accesso a Internet?

Sì, anche questo è supportato. Puoi"distribuire la classificazione dei dati in un sito locale che non dispone di accesso a Internet" per siti completamente sicuri.

Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi commerciali, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina Marchi NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politica sulla riservatezza

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp .

- "Avviso per NetApp Console"
- "Avviso per la NetApp Data Classification"

Informazioni sul copyright

Informazioni sul marchio commerciale