Utilizzare la classificazione dei dati

NetApp Data Classification

NetApp
February 11, 2026

Sommario

Utilizzare la classificazione dei dati . . . 1
Visualizza i dettagli di governance sui dati archiviati nella tua organizzazione con NetApp Data Classification . . . 1
Esaminare la dashboard di governance . . . 1
Creare il report di valutazione della scoperta dei dati . . . 3
Creare il report di panoramica della mappatura dei dati . . . 4
Visualizza i dettagli di conformità sui dati privati archiviati nella tua organizzazione con NetApp Data Classification . . . 6
Visualizza i file che contengono dati personali . . . 7
Visualizza i file che contengono dati personali sensibili . . . 10
Categorie di dati privati nella NetApp Data Classification . . . 13
Tipi di dati personali . . . 13
Tipi di dati personali sensibili . . . 17
Tipi di categorie . . . 18
Tipi di file . . . 19
Accuratezza delle informazioni trovate . . . 19
Crea una classificazione personalizzata in NetApp Data Classification . . . 20
Crea un identificatore personale personalizzato . . . 20
Crea una categoria personalizzata . . . 24
Modifica un classificatore personalizzato . . . 25
Elimina un classificatore personalizzato . . . 26
Prossimi passi . . . 26
Esamina i dati archiviati nella tua organizzazione con NetApp Data Classification . . . 26
Struttura dell’indagine sui dati . . . 26
Filtri dati . . . 26
Visualizza i metadati del file . . . 29
Visualizza i permessi utente per file e directory . . . 31
Controlla i file duplicati nei tuoi sistemi di archiviazione . . . 31
Scarica il tuo report . . . 32
Crea una query salvata in base ai filtri selezionati . . . 35
Gestisci le query salvate con NetApp Data Classification . . . 37
Visualizza i risultati delle query salvate nella pagina Indagine . . . 38
Crea query e policy salvate . . . 38
Modifica query o policy salvate . . . 40
Elimina le query salvate . . . 41
Query predefinite . . . 41
Modifica le impostazioni di scansione NetApp Data Classification per i tuoi repository . . . 42
Visualizza lo stato della scansione per i tuoi repository . . . 42
Cambia il tipo di scansione per un repository . . . 43
Dare priorità alle scansioni . . . 44
Interrompere la scansione per un repository . . . 45
Metti in pausa e riprendi la scansione di un repository . . . 46
Visualizza i report sulla conformità NetApp Data Classification . . . 46

Seleziona i sistemi per i report . . . 47
Segnalazione della richiesta di accesso ai dati dell'interessato . . . 48
Rapporto sulla legge sulla portabilità e responsabilità dell'assicurazione sanitaria (HIPAA) . . . 50
Rapporto sullo standard di sicurezza dei dati del settore delle carte di pagamento (PCI DSS) . . . 51
Rapporto di valutazione del rischio per la privacy . . . 52
Monitora lo stato di integrità NetApp Data Classification . . . 54
Approfondimenti di Health Monitor . . . 54
Accedi alla dashboard di Health Monitor . . . 55

Utilizzare la classificazione dei dati

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

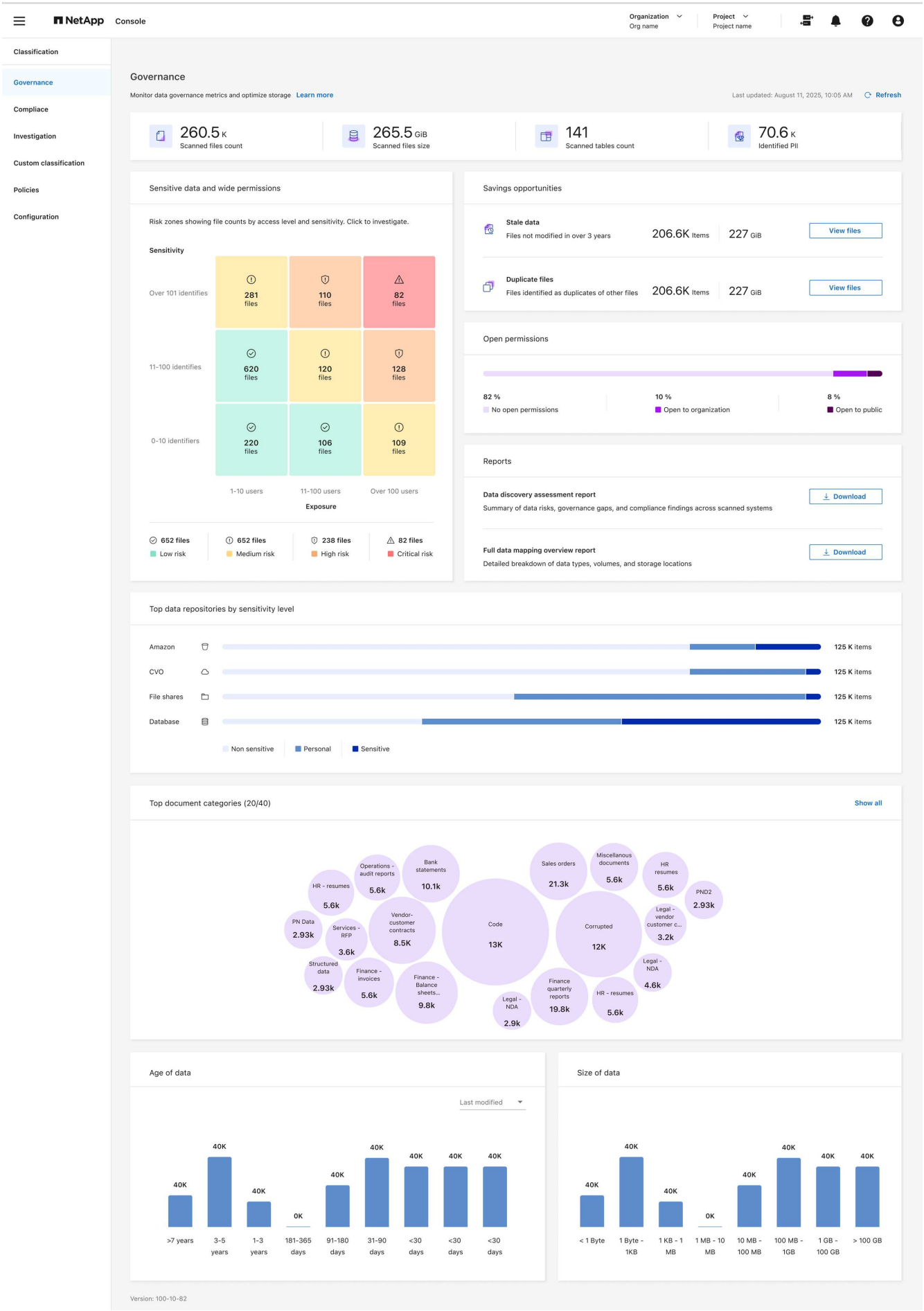
Ottieni il controllo dei costi relativi ai dati sulle risorse di archiviazione della tua organizzazione. NetApp Data Classification identifica la quantità di dati obsoleti, file duplicati e file di grandi dimensioni presenti nei tuoi sistemi, così puoi decidere se rimuovere o spostare alcuni file in 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** - Per impostazione predefinita, i dati vengono considerati obsoleti se l'ultima modifica risale a più di 3 anni fa. È possibile [personalizzare la definizione di dati obsoleti](task-stale-data.html).
   - **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:

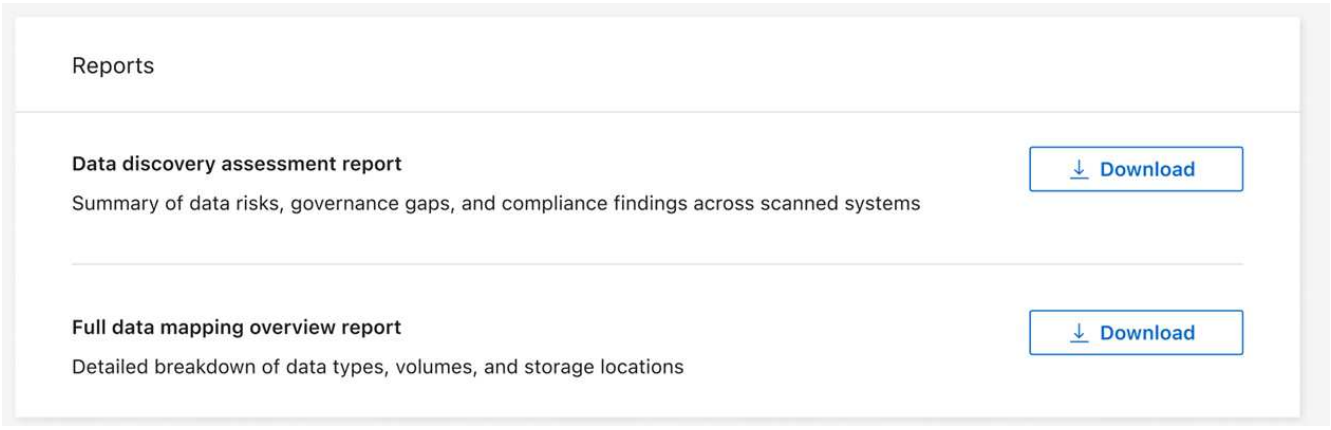
Caratteristica	Descrizione
Preoccupazioni sulla governance dei dati	Un quadro dettagliato di tutti i dati in tuo possesso e delle aree in cui potresti ridurre la quantità di dati per risparmiare sui costi.
Esposizioni alla sicurezza dei dati	Aree in cui i tuoi dati sono accessibili ad attacchi interni 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

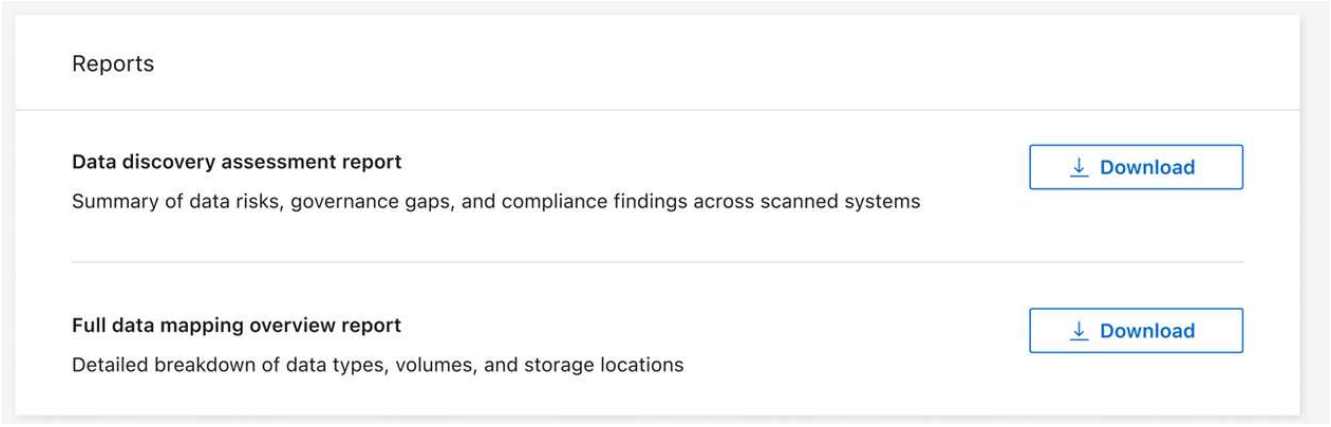
Il report di panoramica sulla mappatura dei dati fornisce una panoramica dei dati archiviati nelle fonti dati aziendali per assisterti nelle decisioni relative ai processi di migrazione, backup, sicurezza e conformità. Il rapporto riassume tutti i sistemi e le fonti di dati. Fornisce inoltre un'analisi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

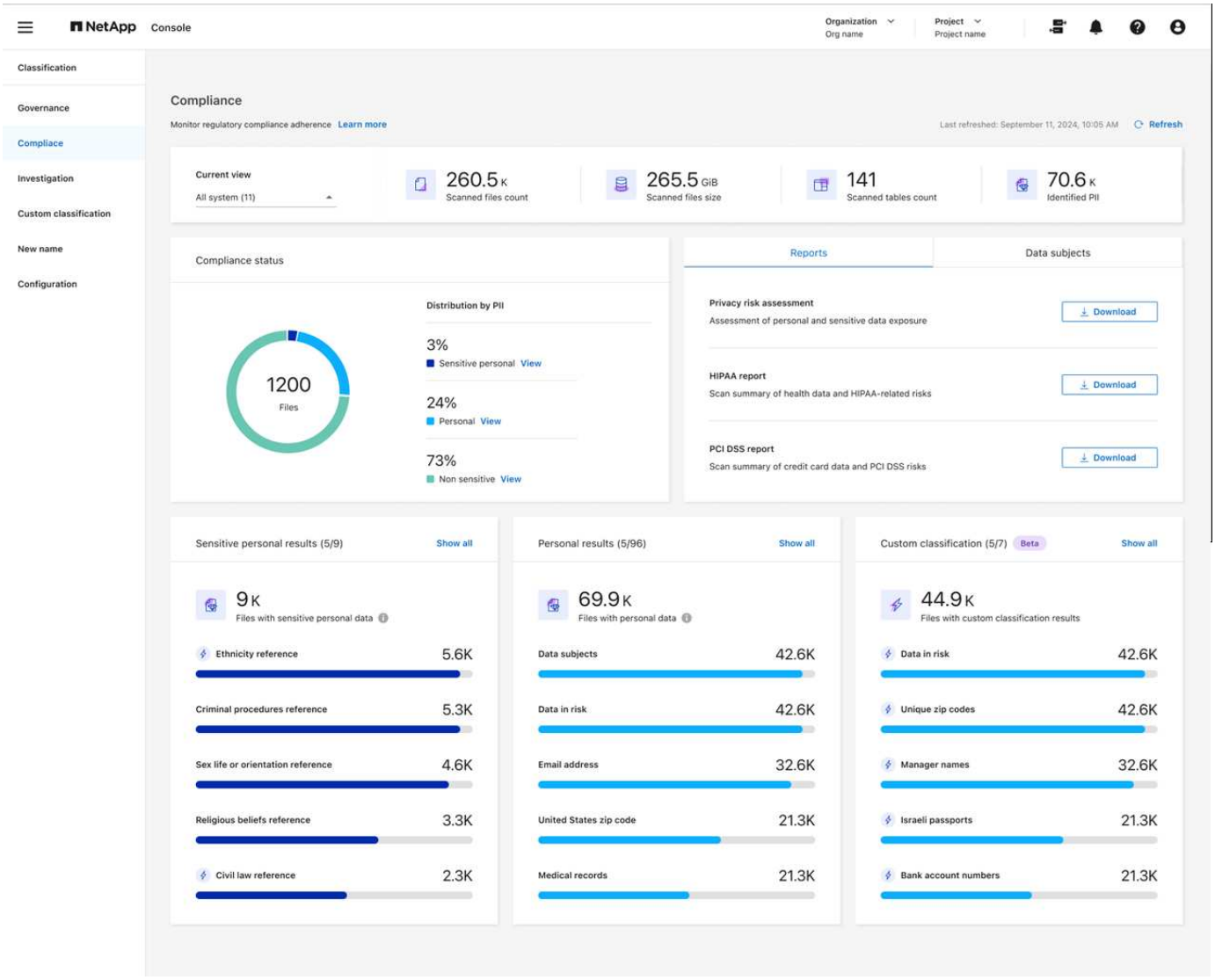
Se una qualsiasi delle tue origini dati implementa la suddivisione in livelli dei dati, i vecchi dati già presenti nell'archiviazione degli oggetti potrebbero essere identificati nel grafico *Age of Data*.

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

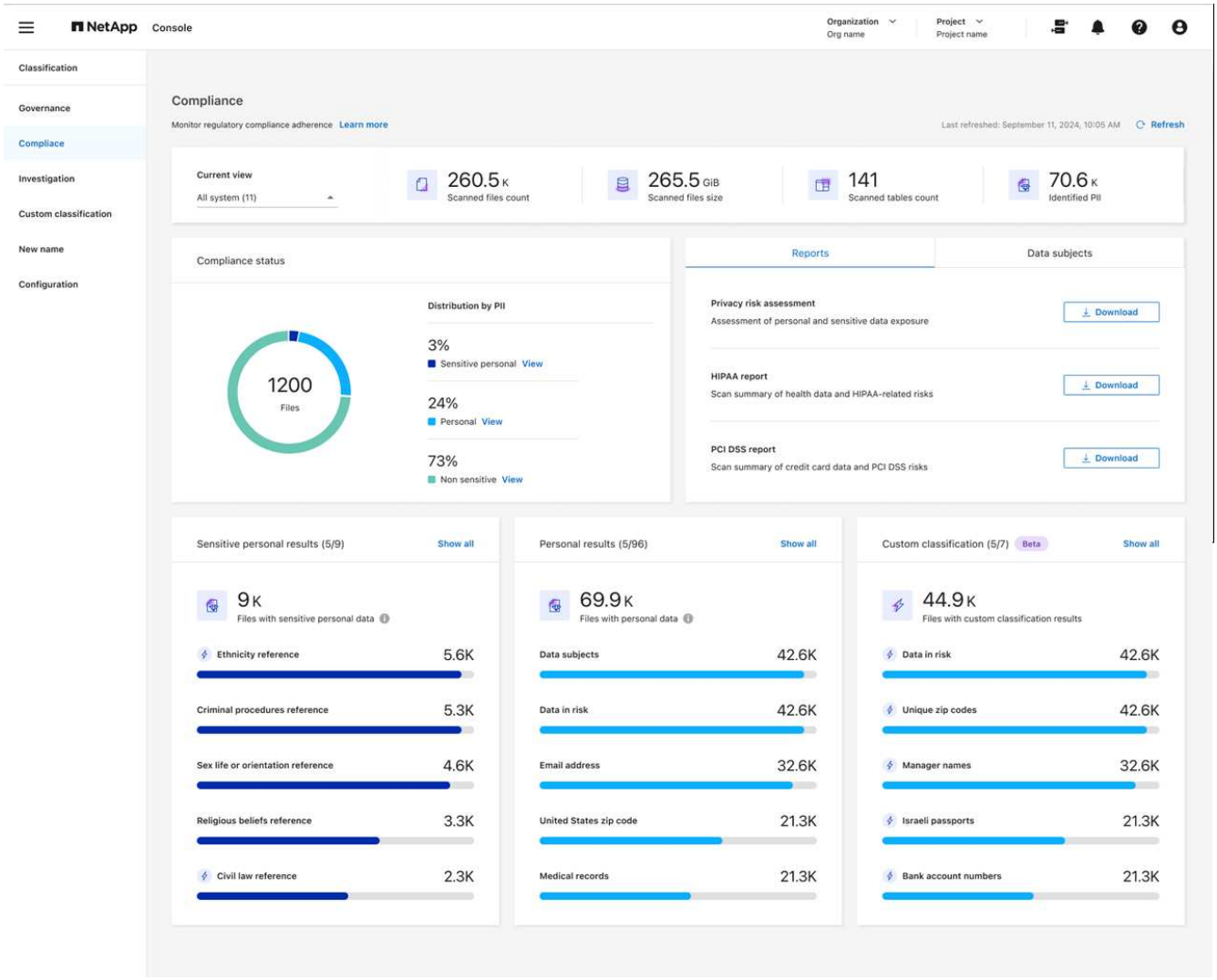
La classificazione dei dati identifica automaticamente parole, stringhe e modelli specifici (Regex) all'interno dei dati. "Ad esempio, numeri di carte di credito, numeri di previdenza sociale, numeri di conti bancari, password e altro ancora."La classificazione dei dati identifica questo tipo di informazioni 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" .

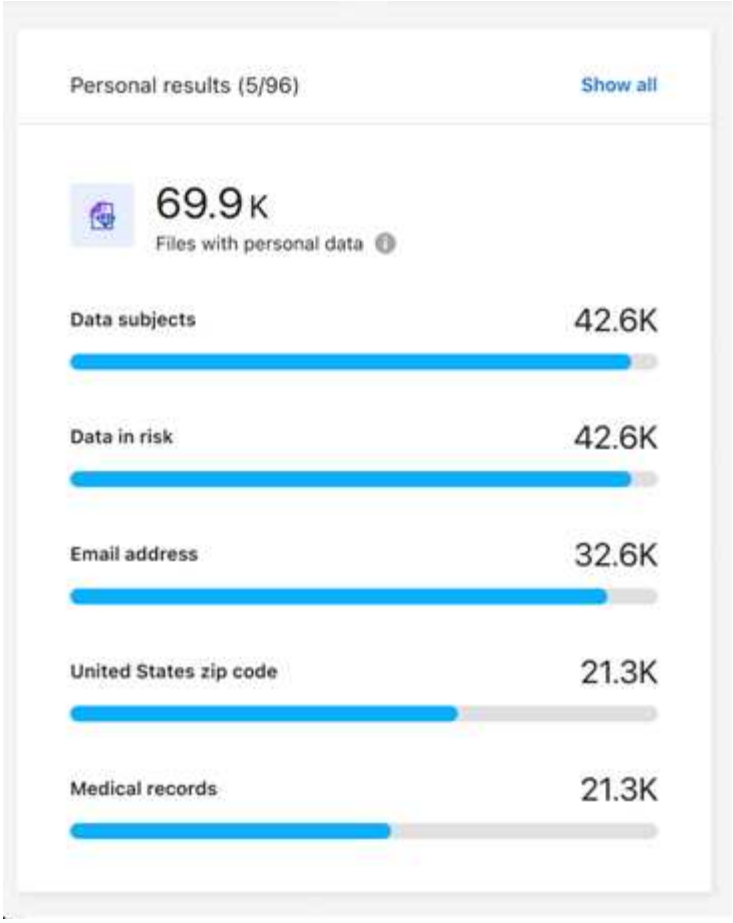
Per alcuni tipi di dati personali, la classificazione dei dati utilizza la *validazione di prossimità* per convalidare i propri risultati. La validazione avviene ricercando una o più parole chiave predefinite in prossimità dei dati personali trovati. Ad esempio, la classificazione dei dati identifica 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.

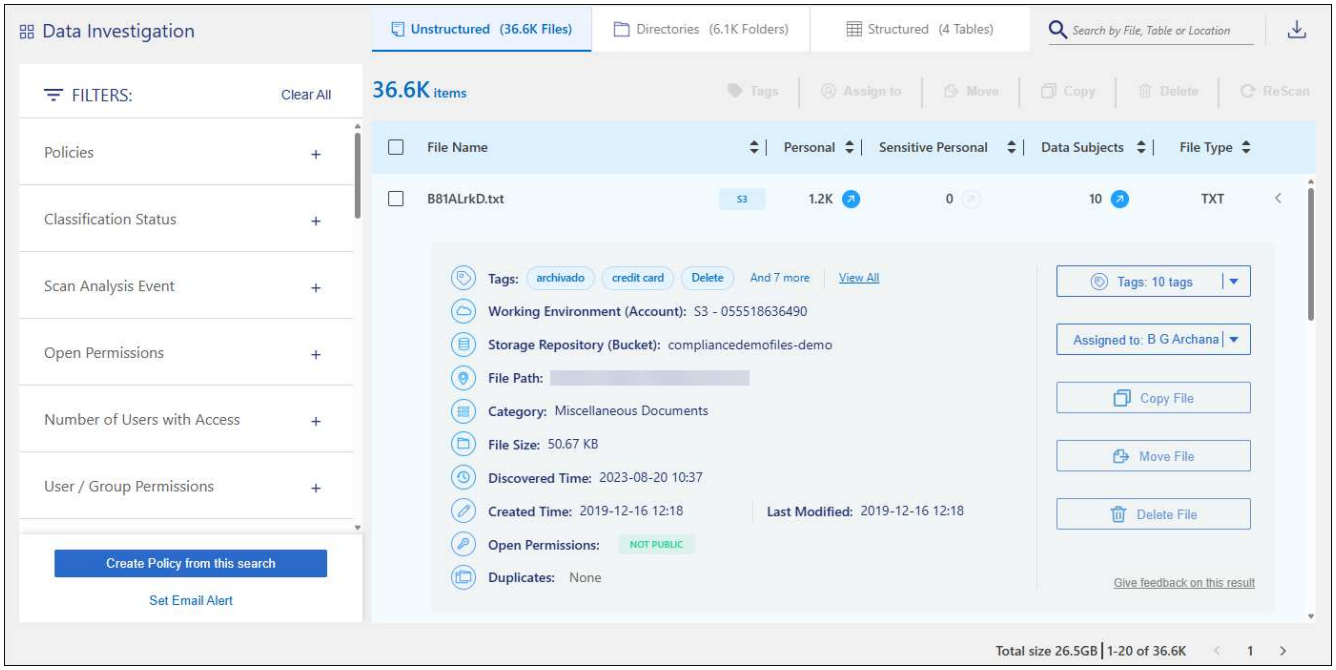


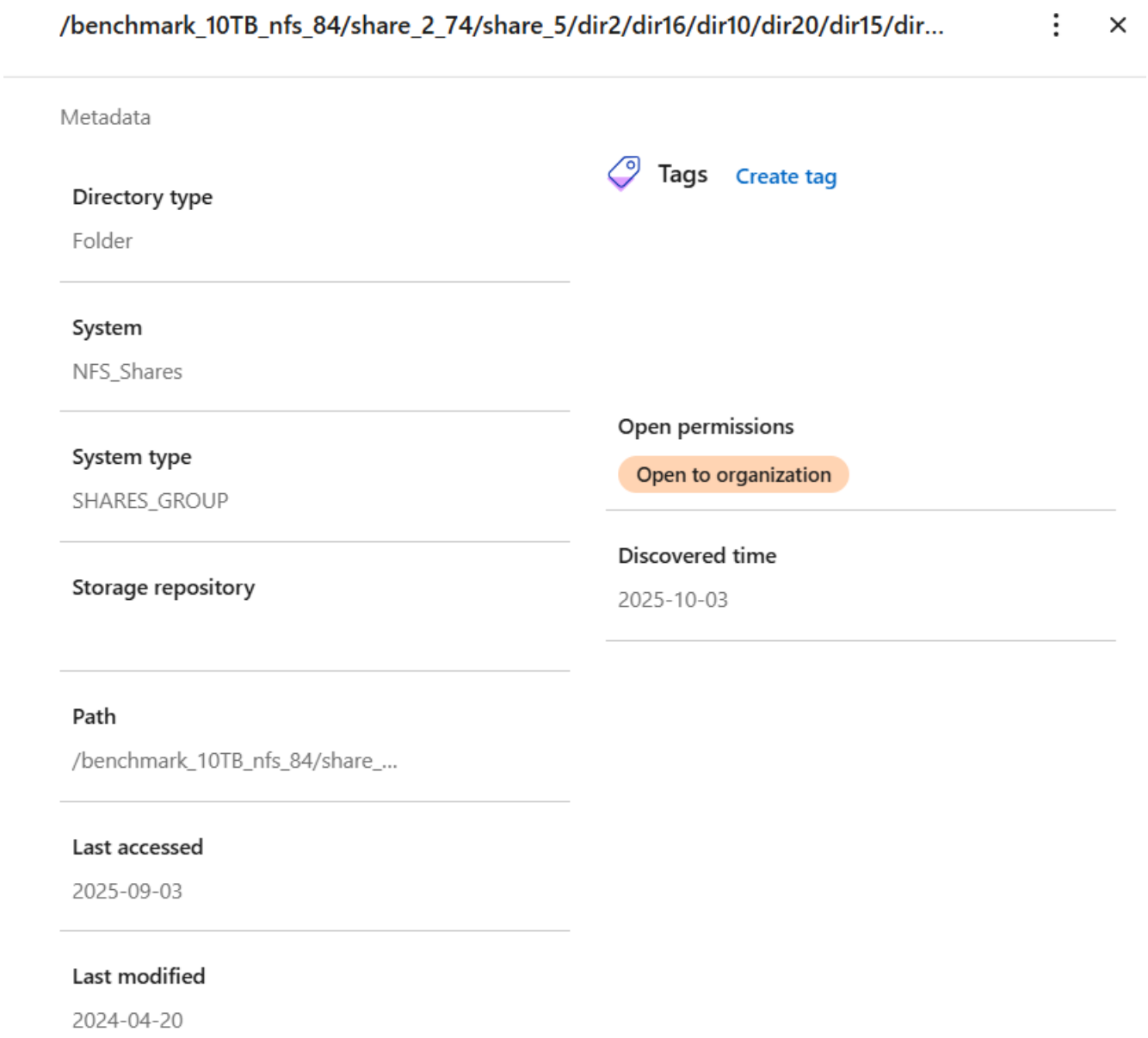
3. Per esaminare i dettagli di un tipo specifico di dati personali, seleziona **Visualizza tutto** e poi seleziona l'icona a freccia **Esamina risultati** per un tipo specifico di dati personali, ad esempio indirizzi e-mail.



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.

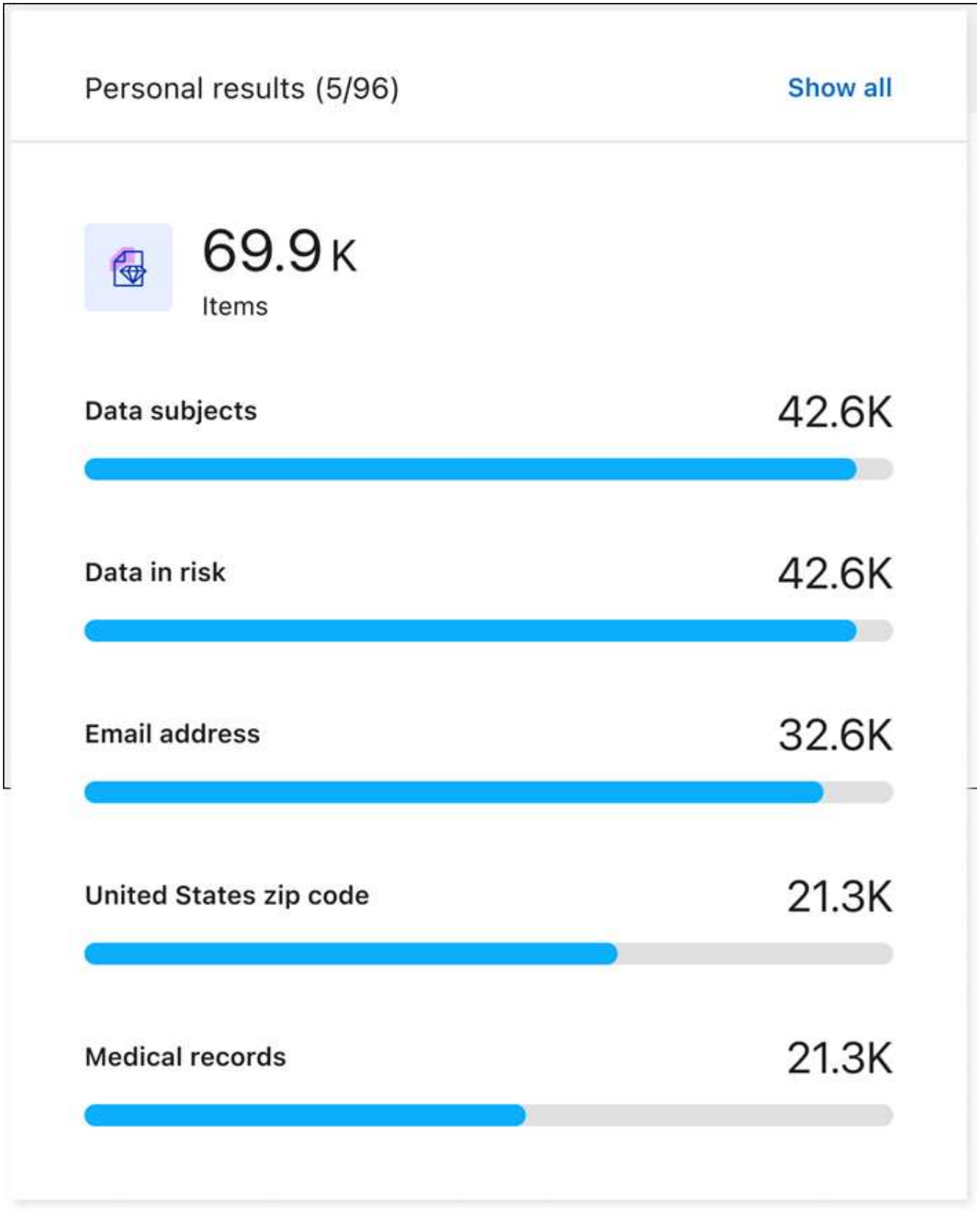
La classificazione dei dati utilizza l'intelligenza artificiale, l'elaborazione del linguaggio naturale (NLP), l'apprendimento automatico (ML) e il cognitive computing (CC) per comprendere il significato del contenuto analizzato, al fine di estrarre entità e categorizzarle di conseguenza.

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

NetApp Data Classification consente di creare categorie personalizzate o identificatori personali per identificare dati specifici in base ai requisiti normativi e di conformità della tua organizzazione.

Data Classification supporta due tipi di classificatori personalizzati: categorie e identificatori personali. Le categorie personalizzate vengono create in base a un set di file caricati, da cui Data Classification crea un modello di intelligenza artificiale per identificare dati simili nella tua organizzazione (ad esempio, un'azienda di ricerca sanitaria potrebbe creare una categoria di analisi clinica). Gli identificatori personali personalizzati vengono creati utilizzando elenchi di parole chiave o un'espressione regolare (regex) per identificare informazioni specifiche della tua organizzazione che possono rappresentare un rischio per la conformità.

Tutte le classificazioni personalizzate sono disponibili nella dashboard Classificazione personalizzata.

Crea un identificatore personale personalizzato

La classificazione dei dati consente di creare un identificatore personale personalizzato utilizzando parole chiave contestuali o un'espressione regolare per identificare i dati univoci della tua organizzazione.

Requisiti per le parole chiave

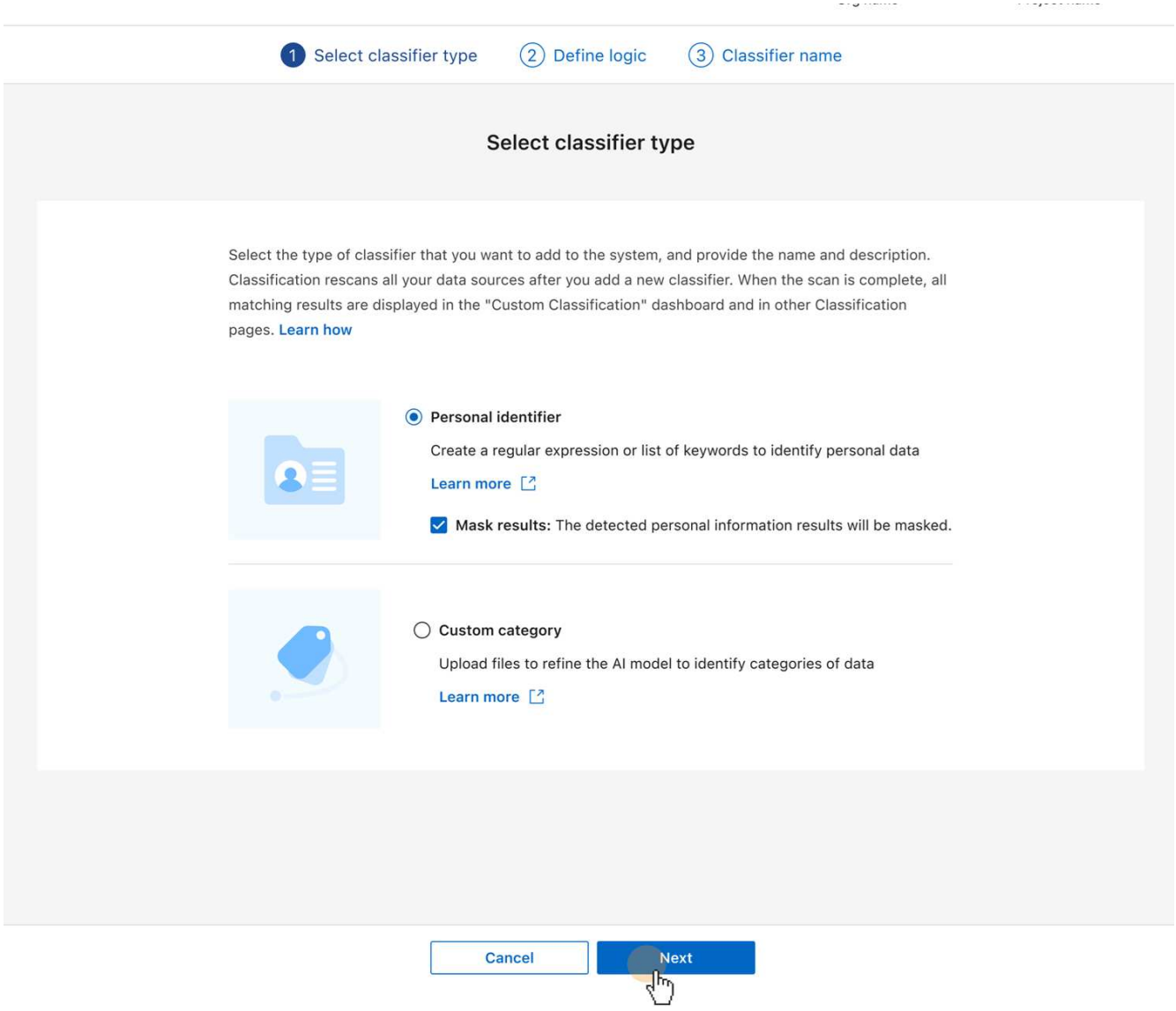
Se stai creando il tuo identificatore personale con un elenco di parole chiave, l'elenco deve soddisfare i seguenti requisiti:

- Le voci delle parole chiave non fanno distinzione tra maiuscole e minuscole.
- Le parole chiave devono essere composte da almeno tre caratteri. Tutte le parole più corte di tre caratteri verranno ignorate.

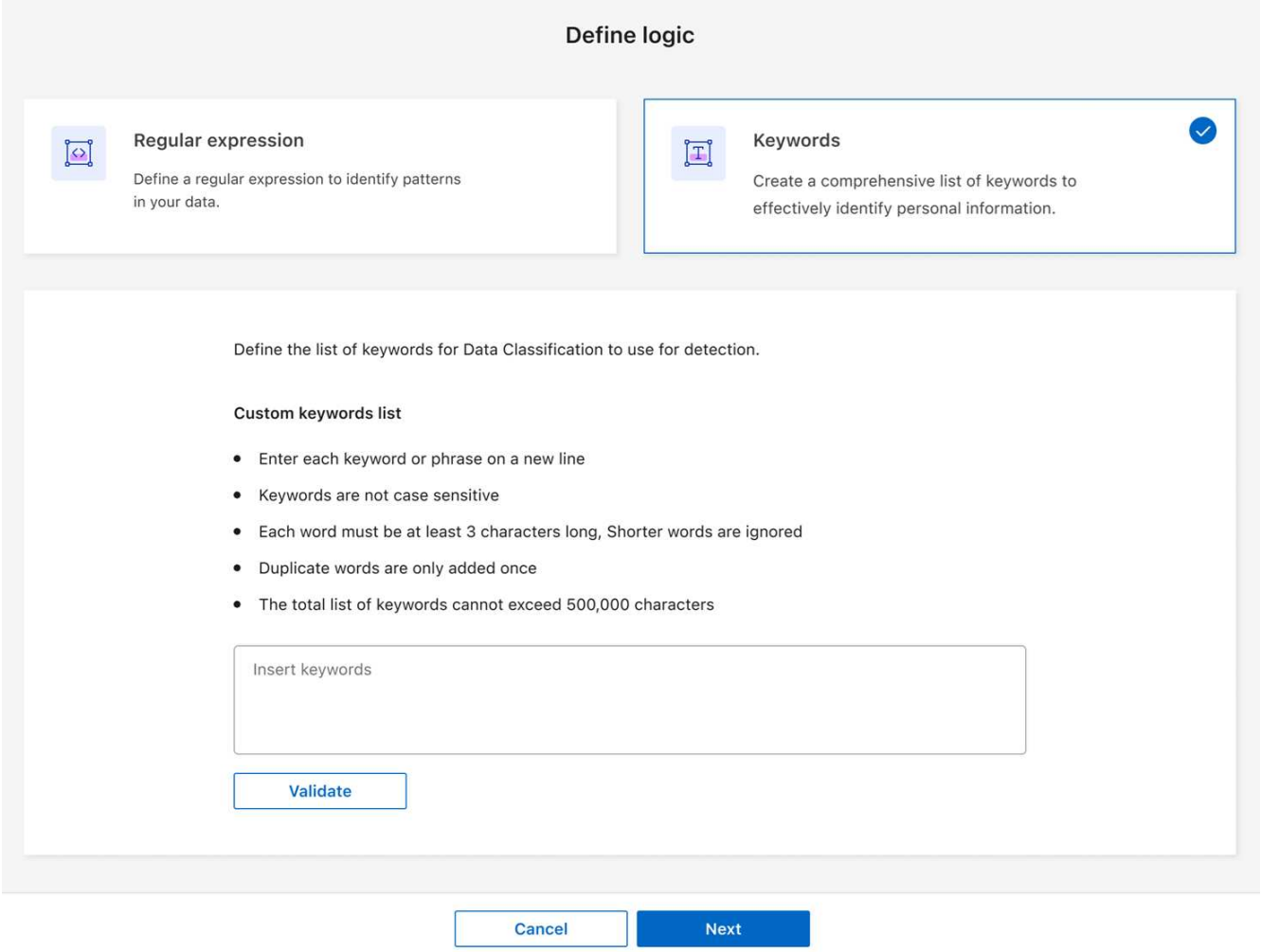
- Le parole duplicate vengono aggiunte una sola volta.
- L'elenco totale delle parole chiave non può superare i 500.000 caratteri. L'elenco deve includere almeno una parola chiave.

Passi

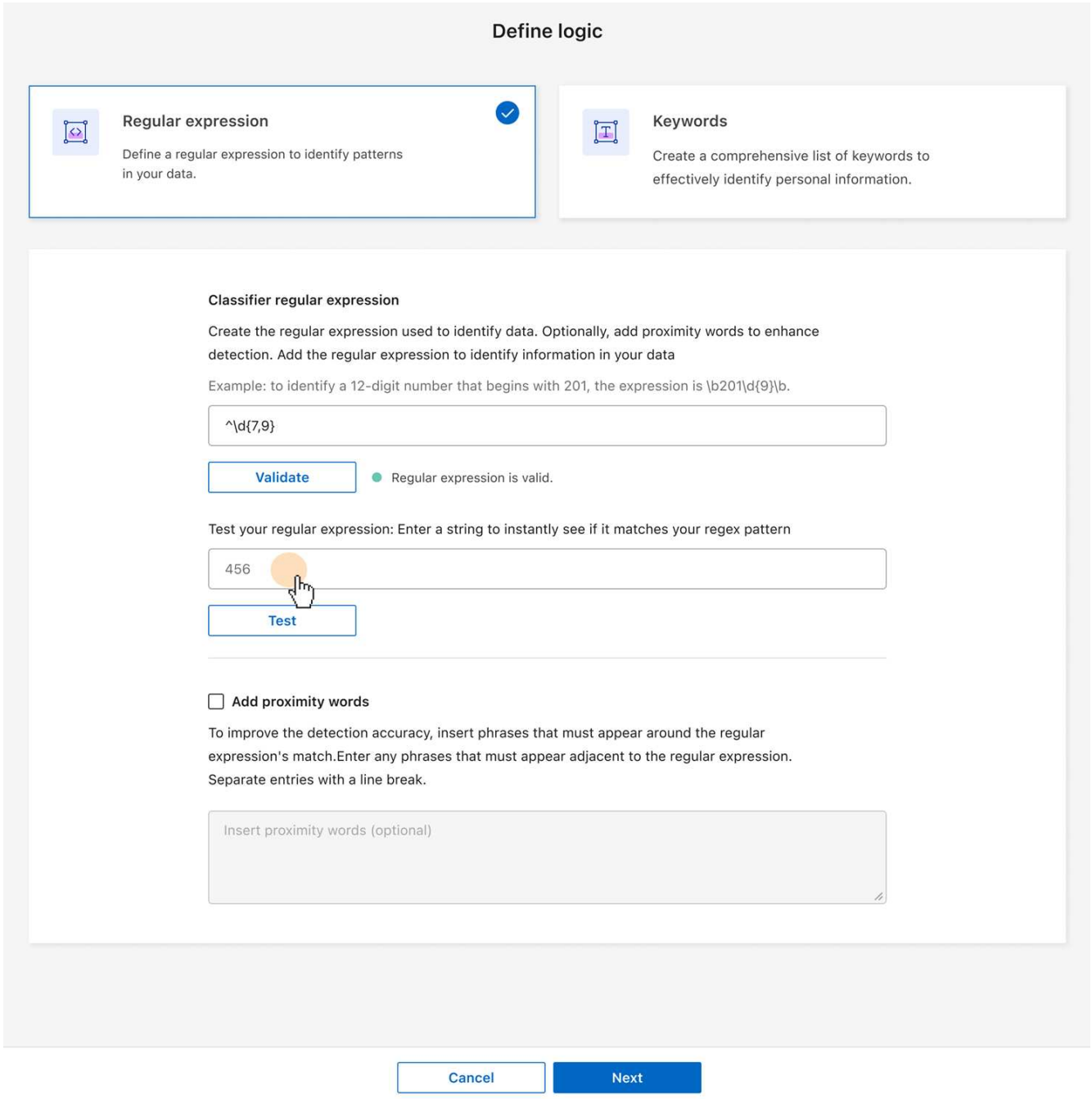
1. Selezionare la scheda **Classificazione personalizzata**.
2. Selezionare **+ Nuovo classificatore** per creare il classificatore personalizzato.
3. Selezionare **Identificatore personale**. Facoltativamente, seleziona **Maschera risultati** per mascherare i dati personali rilevati.
4. Selezionare **Avanti**.



5. Per aggiungere il classificatore con parole chiave, seleziona **Parole chiave**. Inserisci un elenco di parole chiave, inserendo ogni voce su una riga separata. Assicurarsi che le parole chiave siano conformi ai requisiti.



Per aggiungere il classificatore come espressione regolare, seleziona **Espressione regolare**, quindi aggiungi un modello per rilevare le informazioni specifiche dei tuoi dati. Selezionare **Convalida** per confermare la sintassi della voce.



a. Facoltativamente, inserisci una stringa di esempio che corrisponda al tuo modello regex, quindi seleziona **Test** per verificarla.

b. Facoltativamente, aggiungere parole di prossimità. Se si aggiungono parole di prossimità, la classificazione dei dati contrassegna il modello regex solo se le parole di prossimità sono adiacenti alla stringa corrispondente.

6. Selezionare **Avanti**.
7. Inserisci un **Nome classificatore** e una **Descrizione** per identificare la categoria personalizzata nella dashboard.
8. Selezionare **Salva** per creare l'identificatore personale personalizzato.

Dopo aver creato un identificatore personale personalizzato, i suoi risultati vengono acquisiti nella successiva scansione pianificata. Per ottenere risultati più rapidamente, esegui una scansione su richiesta. Per

visualizzare i risultati, vedere Generare report di conformità.

Crea una categoria personalizzata

Grazie alle categorie personalizzate puoi categorizzare i dati specifici della tua organizzazione. Le categorie personalizzate vengono create in base ai file di testo caricati, dai quali Data Classification crea un modello di intelligenza artificiale per identificare informazioni simili in altri file.

Requisiti dei dati di formazione

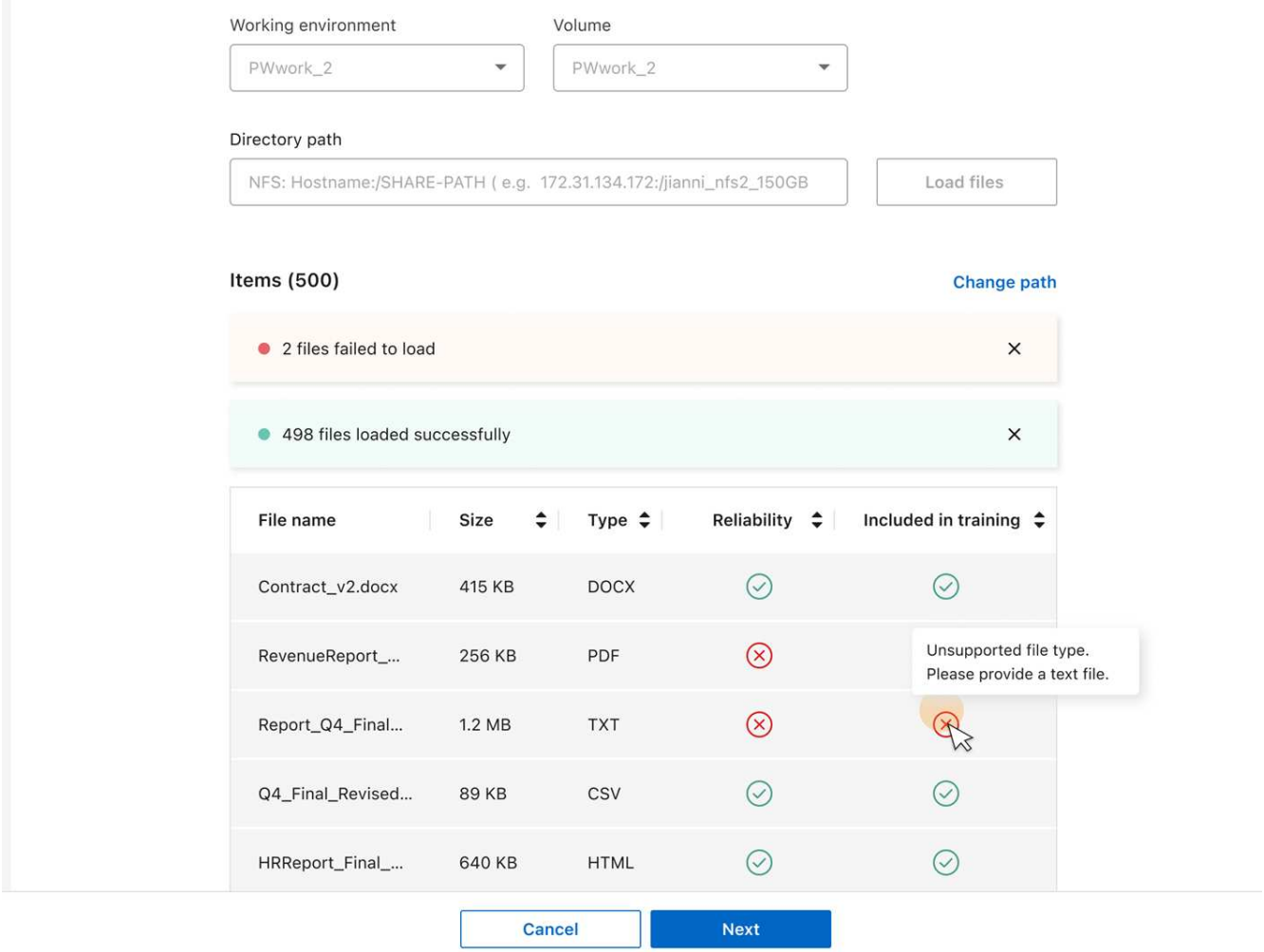
- Il set di dati di addestramento deve contenere almeno 25 file. Il numero massimo di file è 1.000.
- Tutti i file devono trovarsi direttamente nel percorso file fornito.
- Tutti i file devono essere più grandi di 100 byte.
- I dati di addestramento per la classificazione dei dati devono essere uno dei seguenti tipi di file: CSV, DOCX, DOC, GZ, JSON, PDF, PPTX, TXT, RTT, XLS o XLSX. È possibile caricare una combinazione di tutti i tipi di file supportati.

Passi

1. In NetApp Data Classification, seleziona **Classificazione personalizzata**.
2. Seleziona **+ Nuovo classificatore**.
3. Seleziona **Categoria personalizzata** come tipo di classificatore, quindi **Avanti**.
4. Definisci la logica per la tua categoria personalizzata con una raccolta di file basati su testo. Fornire l'indirizzo IP dell'**Indirizzo di lavoro**, quindi selezionare il **Volume** dal menu a discesa.

   Immettere il **Percorso directory** per la directory che contiene i dati di formazione.

5. Selezionare **Carica file** per la classificazione dei dati per eseguire un controllo dei file. È possibile rivedere il riepilogo dei file, che elenca il nome del file, la dimensione, il tipo e le note se il file è stato ritenuto accettabile per la formazione.



La classificazione dei dati visualizza il tempo di completamento stimato per l'addestramento dei dati. .. Per modificare il percorso del file o ricaricare i file, selezionare **Cambia percorso** quindi immettere i dati e caricare nuovamente i file.

6. Quando sei soddisfatto dei file caricati, seleziona **Avanti**.
7. Inserisci un **Nome classificatore** e una **Descrizione** per identificare la categoria personalizzata nella dashboard.
8. Selezionare **Salva** per creare la categoria personalizzata.

Risultato

Dopo aver creato una categoria personalizzata, i suoi risultati vengono acquisiti nella successiva scansione pianificata. Per ottenere risultati più rapidamente, avviare manualmente la scansione.

Modifica un classificatore personalizzato

È possibile modificare la logica di un identificatore personale dopo averlo creato. Non è possibile modificare il tipo di identificatore personale o il tipo logico; ad esempio, non è possibile modificare una categoria personalizzata in un identificatore personale personalizzato. Non è inoltre possibile modificare un identificatore personalizzato basato su parole chiave in un identificatore personalizzato basato su espressioni regolari.

Passi

1. In NetApp Data Classification, seleziona **Classificazione personalizzata**.

2. Identifica il classificatore che vuoi eliminare, quindi seleziona il menu Azione … alla fine della sua fila.
3. Selezionare **Modifica logica**.
4. Se stai modificando le parole chiave, aggiungi, elimina o modifica le parole chiave appropriate. Se stai modificando un'espressione regolare, inserisci la nuova espressione regolare e convalidala. Facoltativamente, aggiungi parole chiave di prossimità.
5. Selezionare **Salva** per applicare le modifiche.

Elimina un classificatore personalizzato

1. In NetApp Data Classification, seleziona **Classificazione personalizzata**.
2. Identifica il classificatore che vuoi eliminare, quindi seleziona il menu Azione … alla fine della sua fila.
3. Seleziona **Elimina classificatore**.

Prossimi passi

- Generare 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

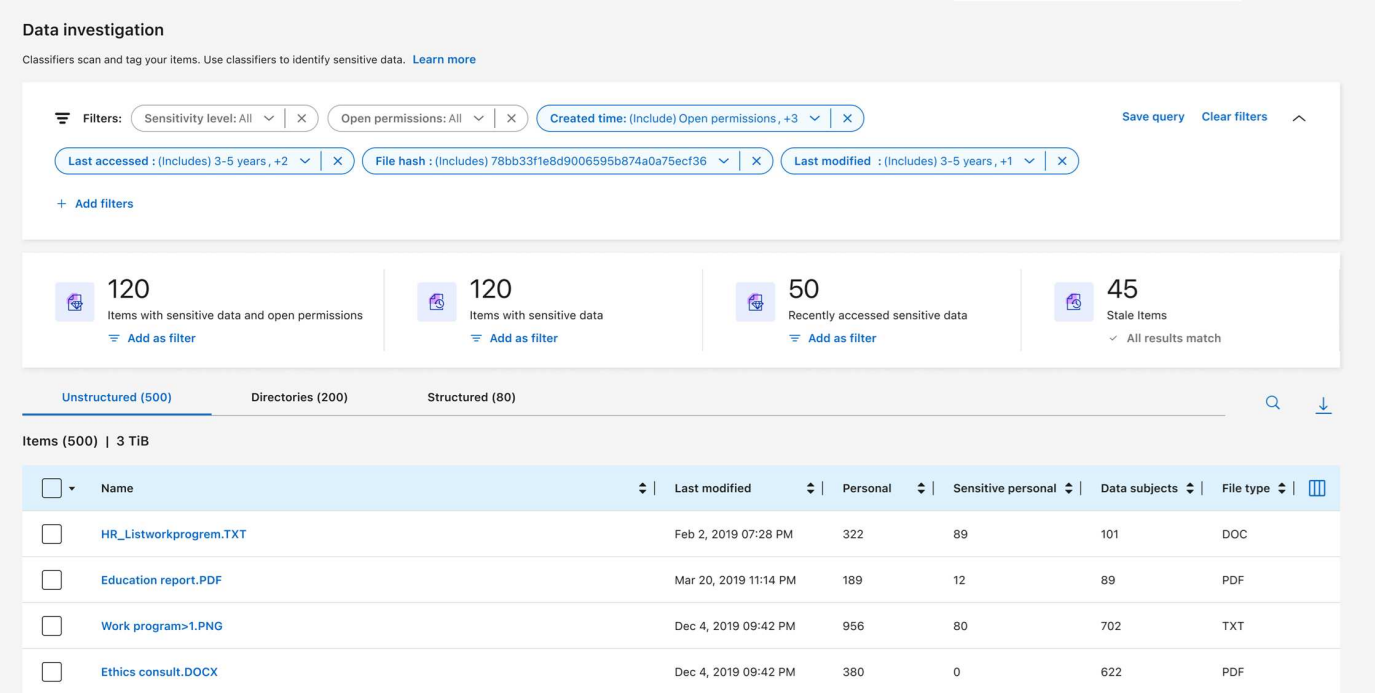
La pagina Indagine sui dati ordina i dati in tre schede:

- **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.
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.

Filtro	Dettagli
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.
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

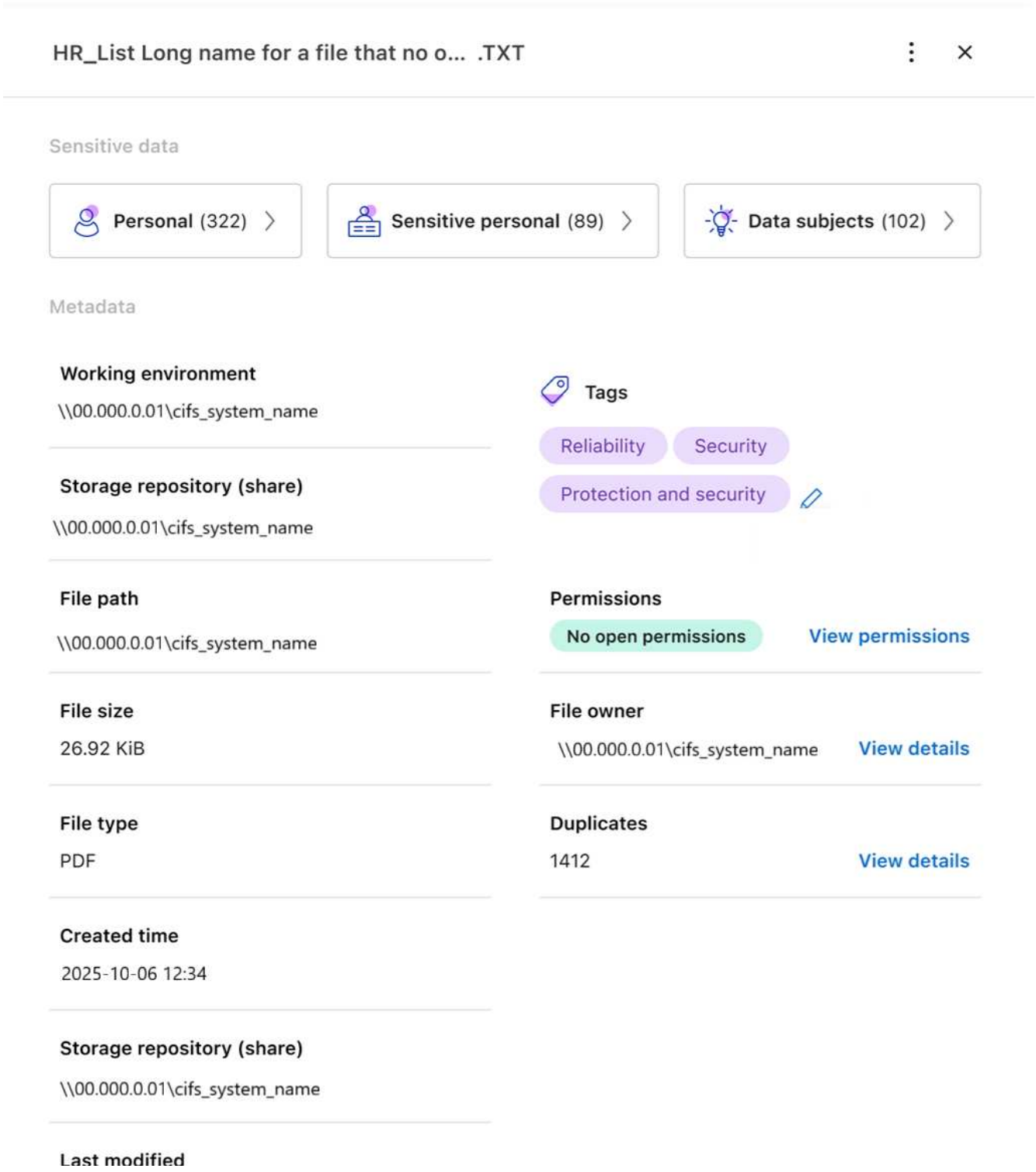
Oltre a mostrare il sistema e il volume in cui risiede il file, i metadati mostrano molte altre informazioni, tra cui le autorizzazioni del file, il proprietario del file e se sono presenti duplicati di questo file. Questa informazione è utile se stai pianificando di"creare query salvate" perché puoi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

La classificazione dei dati confronta tutti i file (esclusi i database) per individuare eventuali duplicati se sono:

- 1 MB o più
- Oppure contengono informazioni personali o sensibili

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, 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)

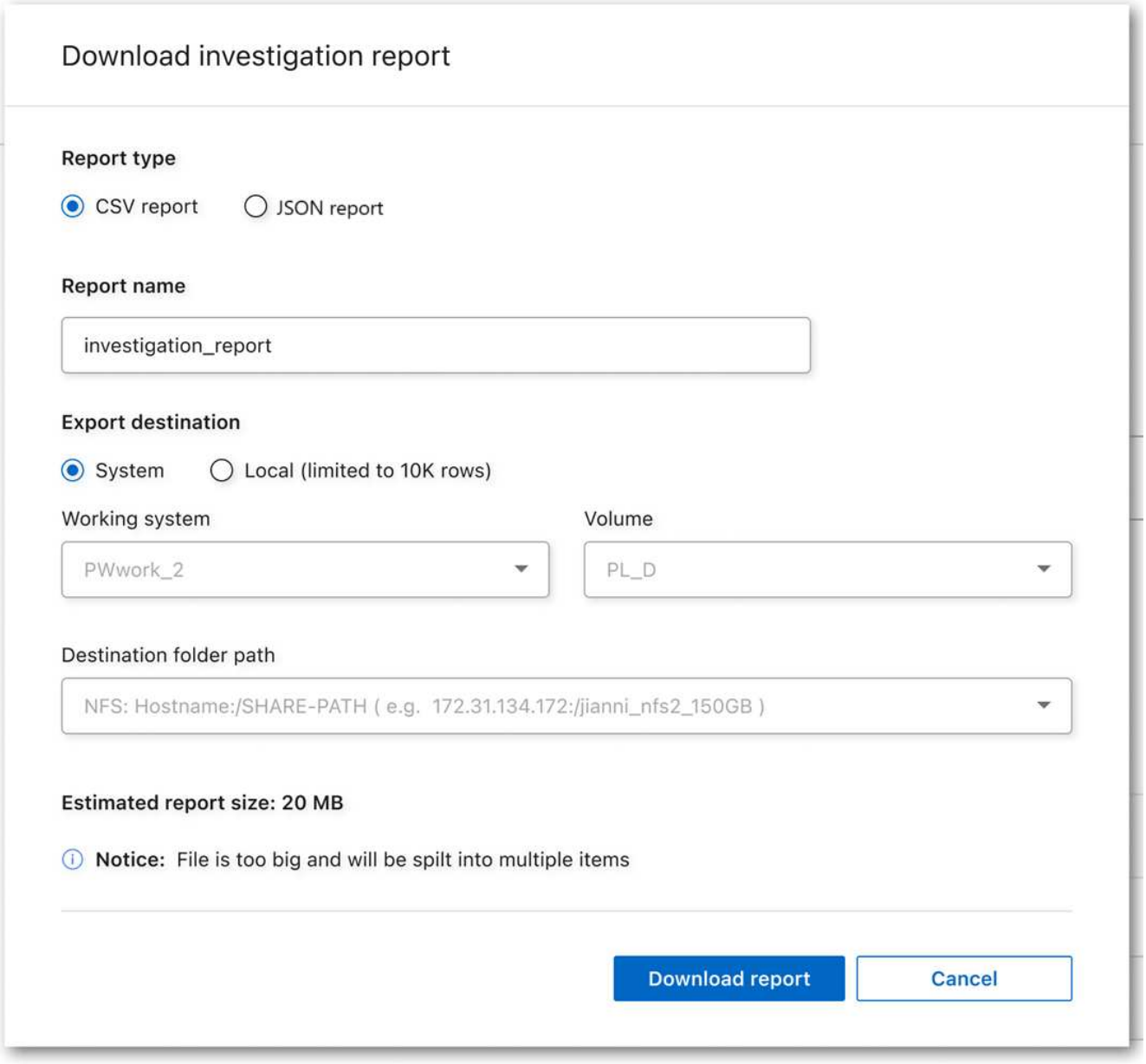
- Numero di colonne
- Conteggio delle righe
- Informazioni personali
- Informazioni personali sensibili

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**.



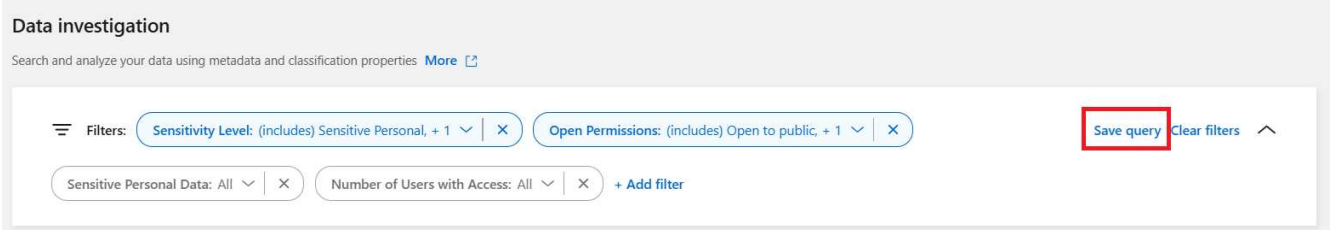
Risultato

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

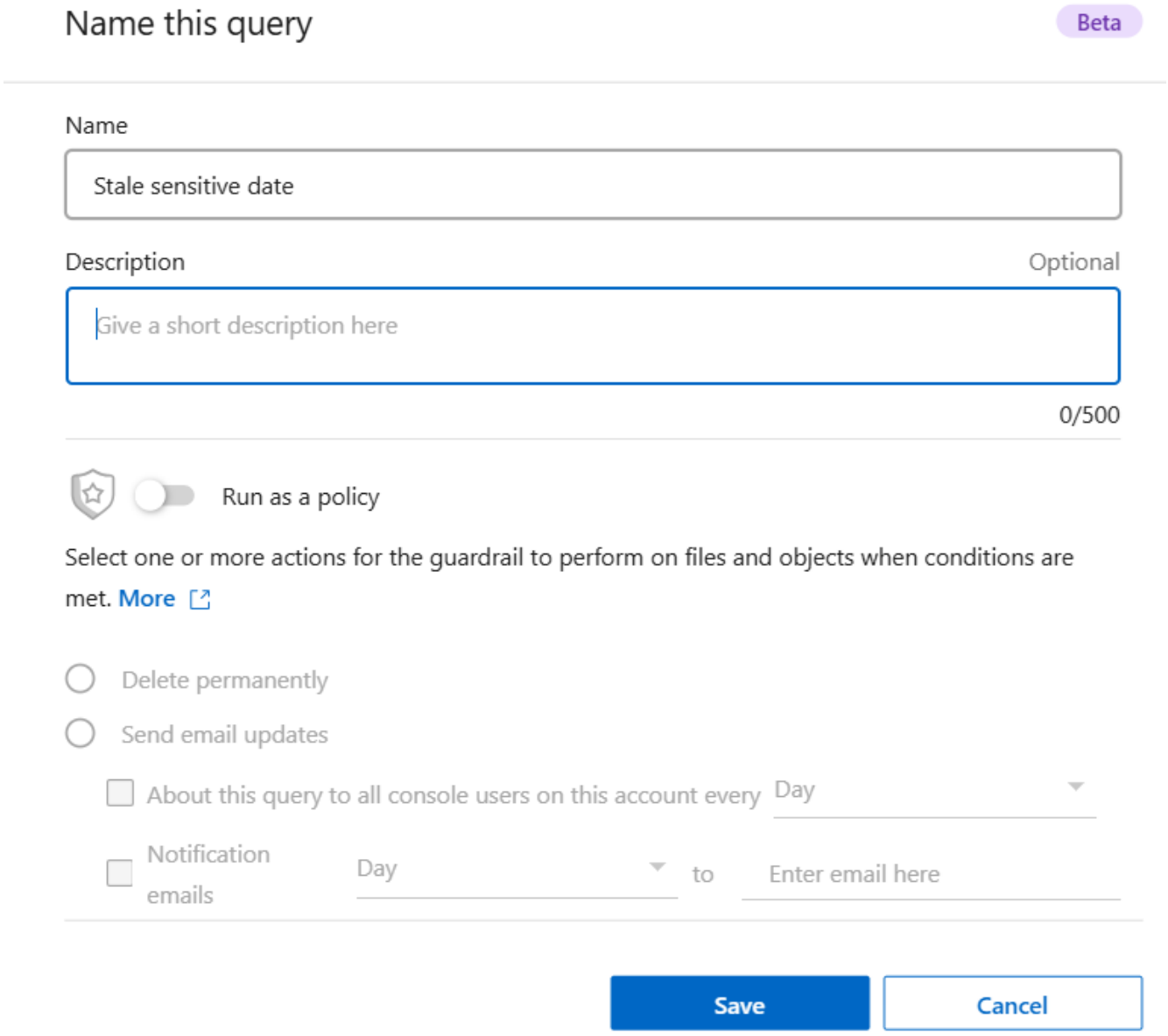
Crea una query salvata in base ai filtri selezionati

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

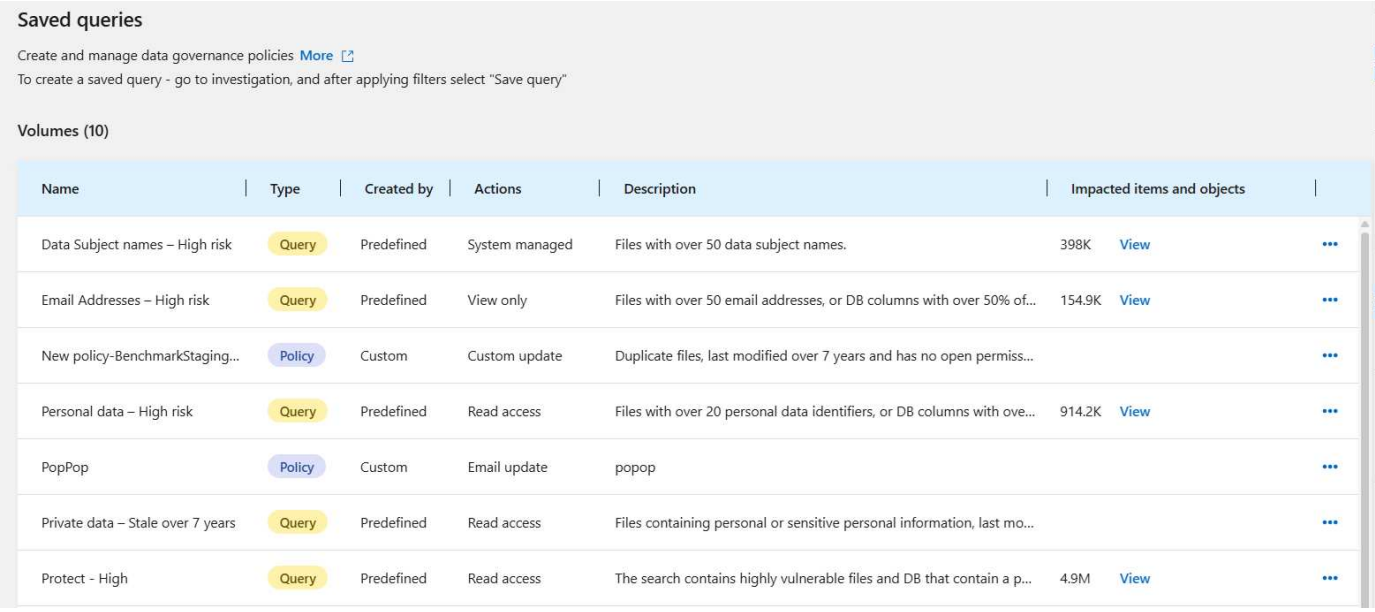
NetaApp Data Classification supporta il salvataggio delle query di ricerca. Con una query salvata, puoi creare filtri personalizzati per ordinare le query frequenti nella pagina di indagine sui dati. La classificazione dei dati include anche query salvate predefinite basate su richieste comuni.

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

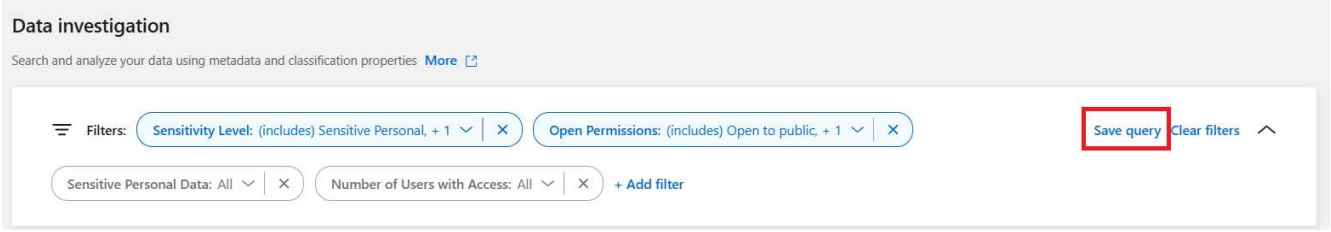
Per visualizzare i risultati di una query salvata nella pagina Indagine, selezionare pulsante per una ricerca specifica, quindi seleziona **Esamina risultati**.

Crea query e policy salvate

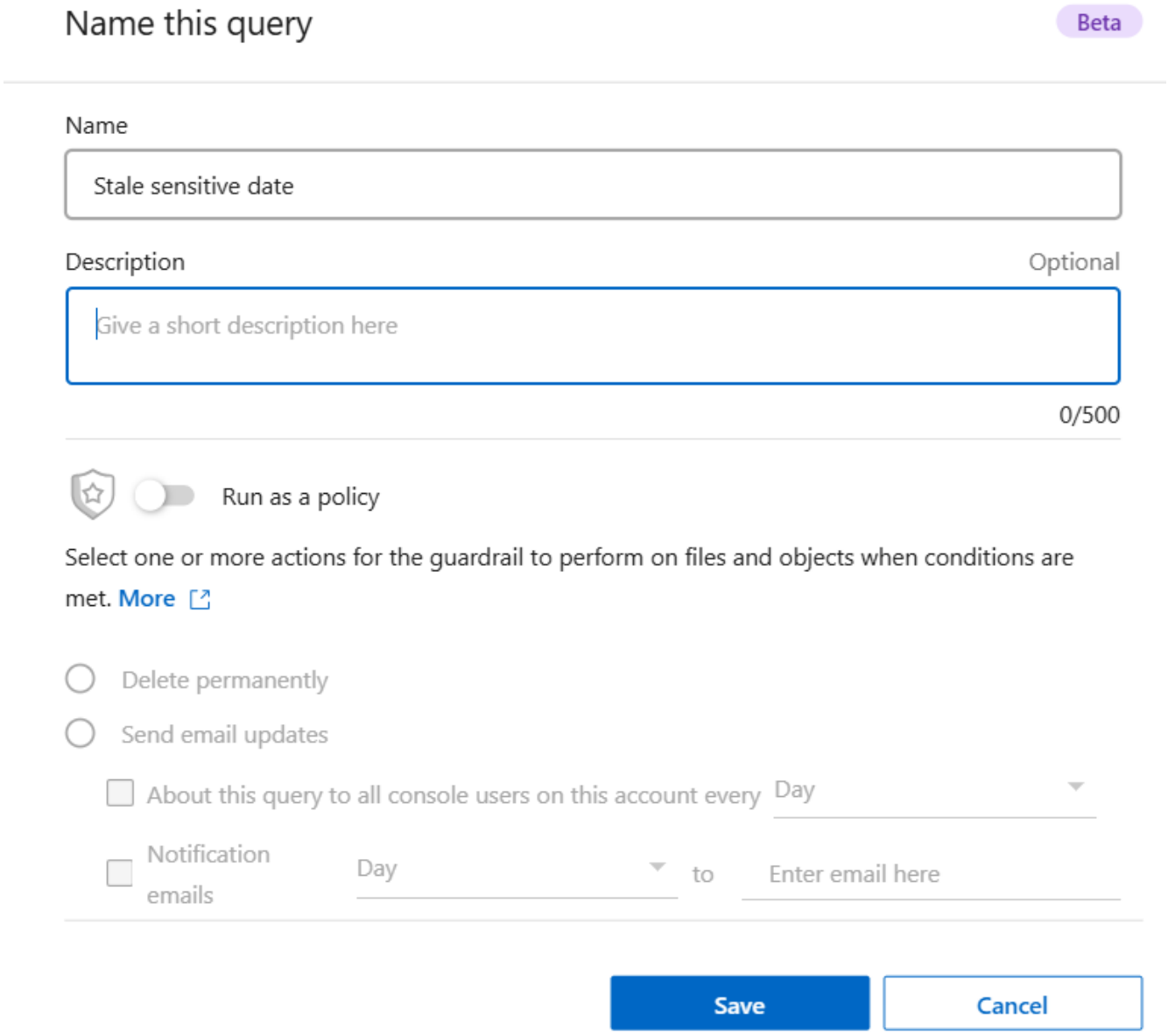
Puoi creare query salvate personalizzate che forniscono risultati per query specifiche della tua organizzazione. Vengono restituiti risultati per tutti i file e le directory (condivisioni e cartelle) che corrispondono ai criteri di ricerca.

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.

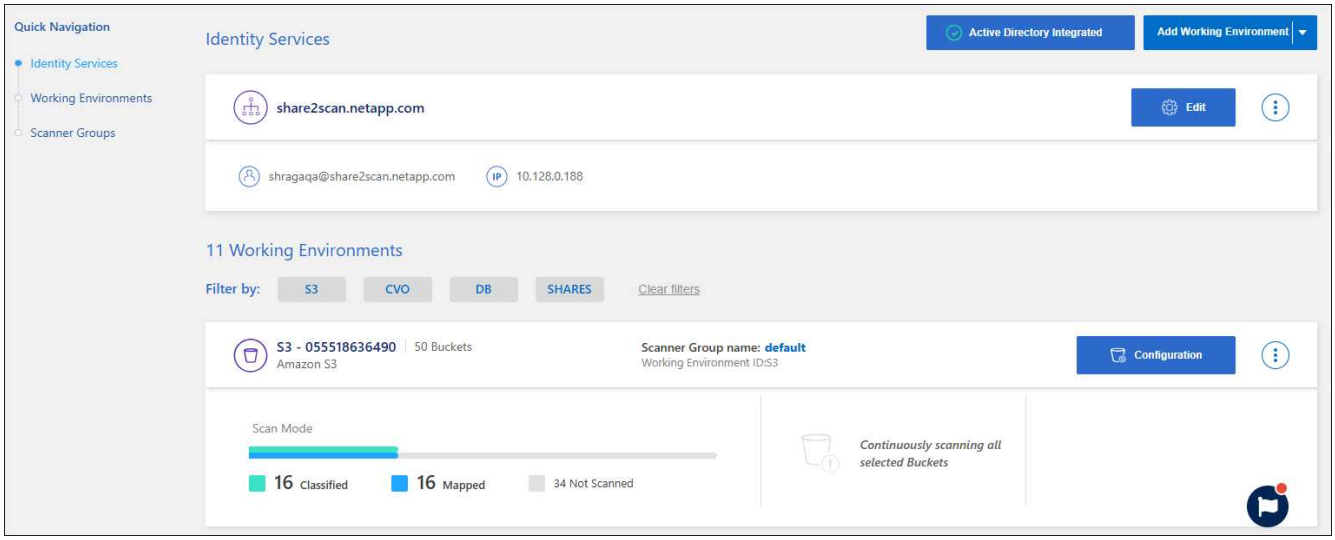
È possibile visualizzare lo stato di scansione di ciascun ambiente di lavoro nella pagina Configurazione:

- **Inizializzazione** (punto azzurro): la configurazione della mappa o della classificazione è attivata. Appare brevemente prima di passare allo stato "coda in sospeso".
- **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 messo in pausa la scansione. Sebbene le modifiche al volume non vengano visualizzate nel sistema, le informazioni acquisite tramite scansione restano disponibili.
- **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.

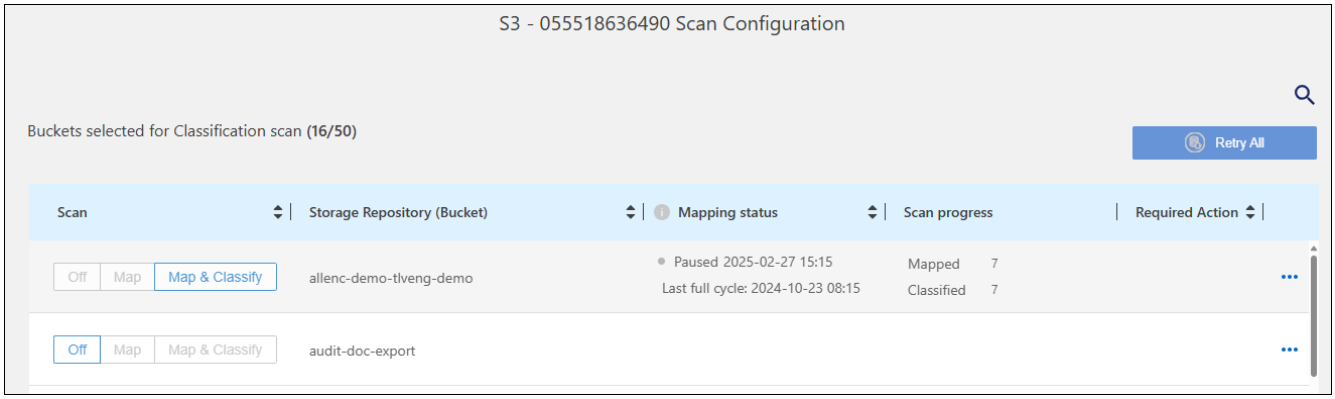
- **Non in scansione**: è stata selezionata la configurazione del volume su "Off" e il sistema non sta eseguendo la scansione del volume.

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. Durante una scansione, passa il cursore sulla barra di avanzamento nella colonna *Stato di mappatura* per visualizzare il numero di file nella coda da mappare o classificare per quel repository.

Cambia il tipo di scansione per un repository

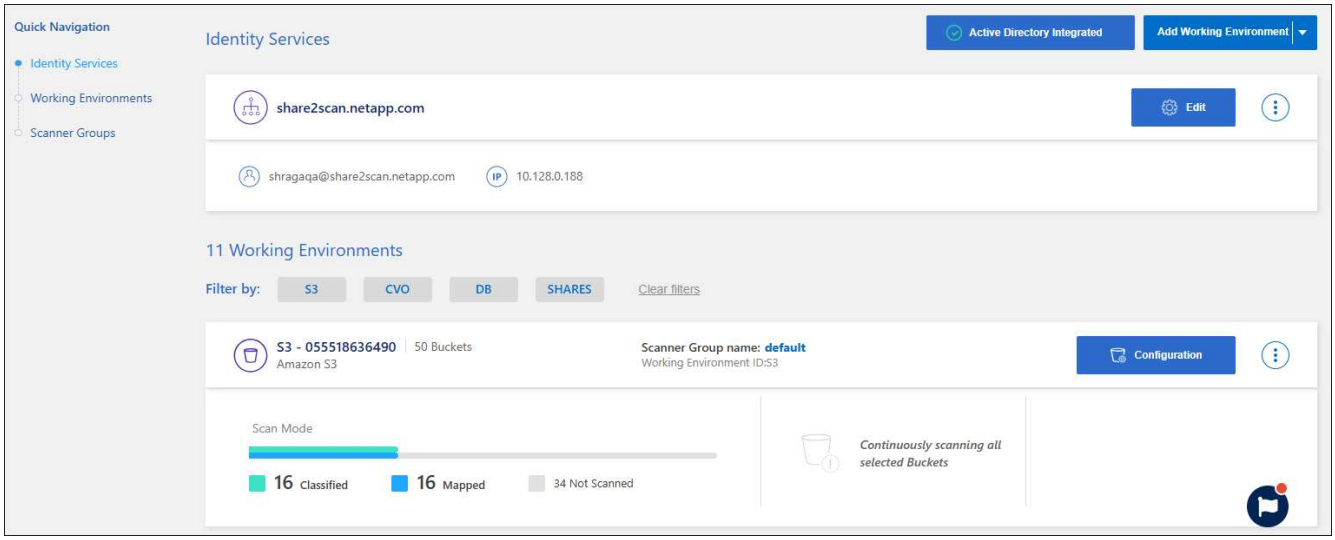
È possibile avviare o interrompere in qualsiasi momento le scansioni di sola mappatura o le scansioni di mappatura e classificazione in un sistema dalla pagina Configurazione. È anche possibile passare da scansioni di sola mappatura a scansioni di mappatura e classificazione e viceversa.

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.

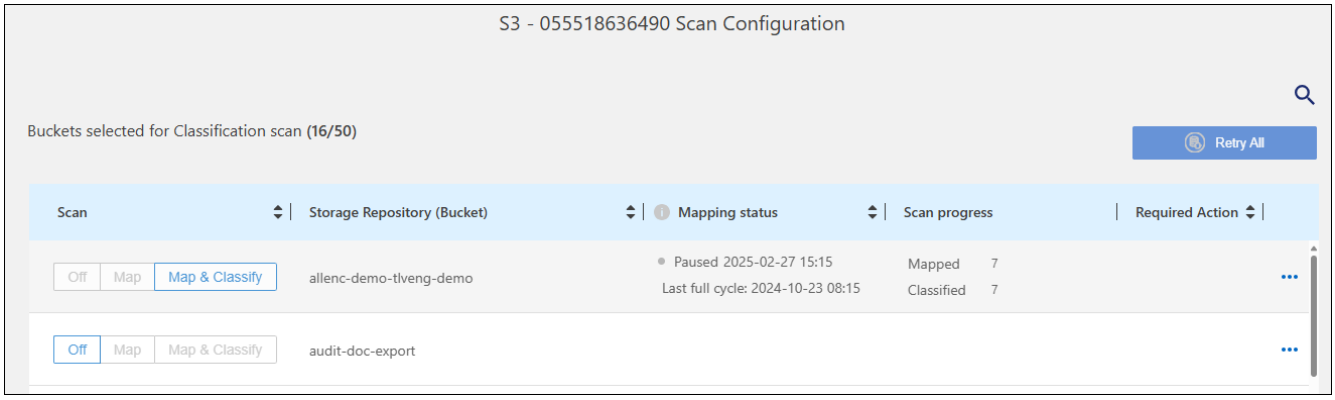
Passi

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

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

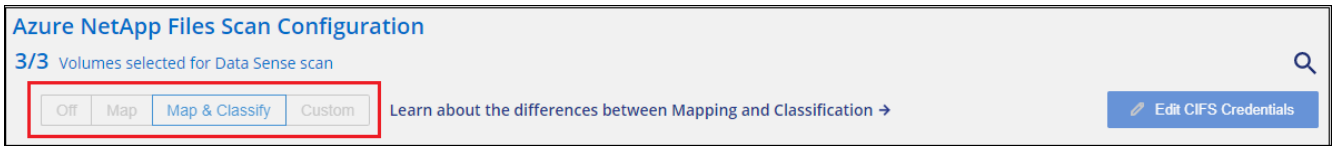


3. Nella pagina Configurazione scansione, modifica uno qualsiasi dei repository (bucket in questo esempio) per eseguire scansioni **Mappa** o **Mappa e classifica**.



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

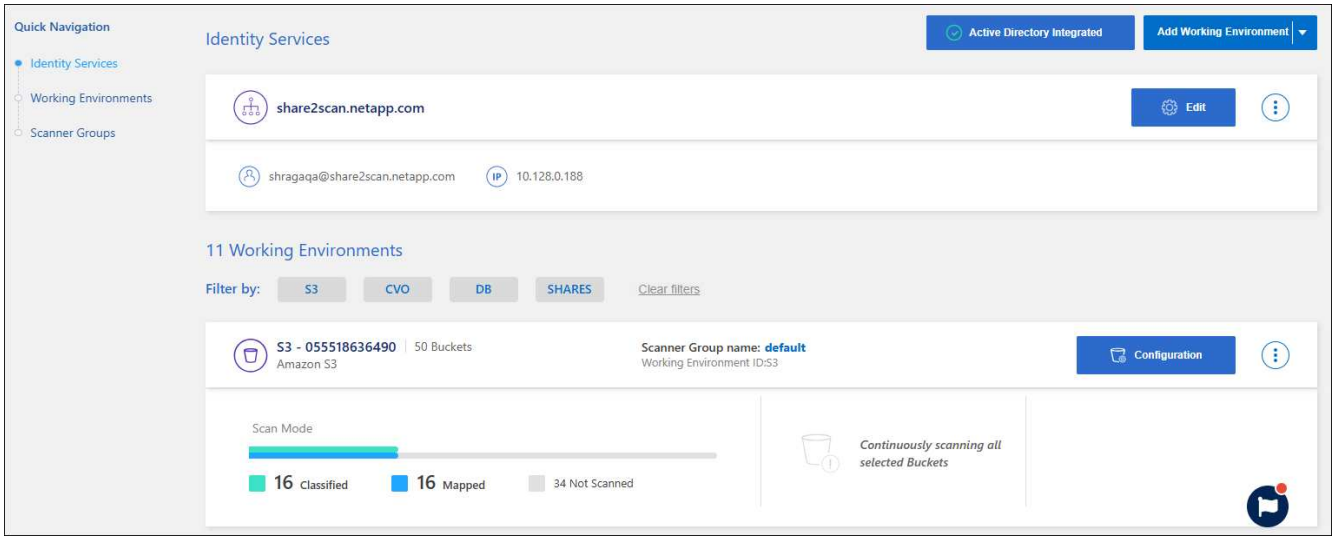
1. Dal menu Classificazione dati, selezionare **Configurazione**.
2. Seleziona le risorse a cui vuoi dare priorità.
3. Dalle azioni … opzione, seleziona **Dai priorità alla scansione**.

Interrompere la scansione per un repository

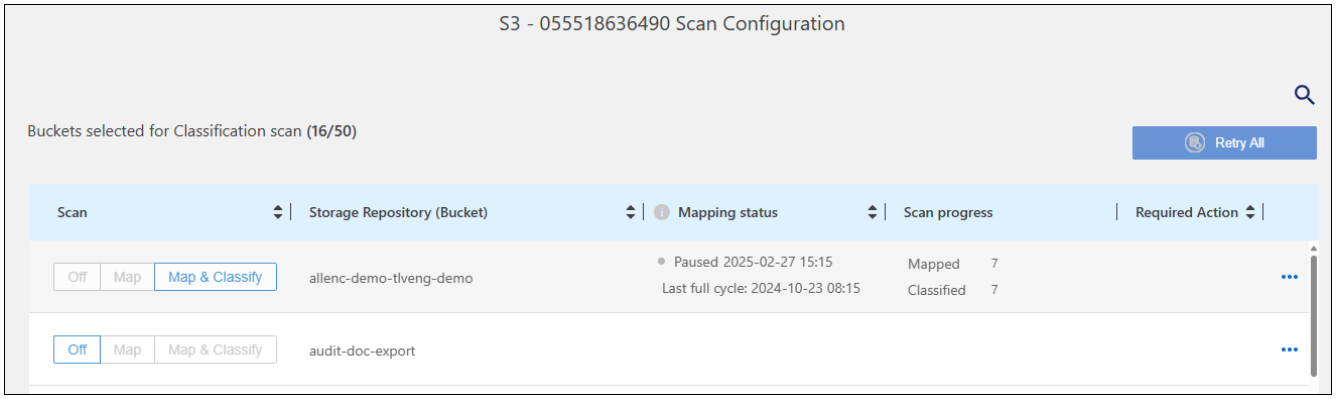
È possibile interrompere la scansione di un repository (ad esempio, un volume) se non è più necessario monitorarne la conformità. Per farlo, è necessario disattivare la scansione. Quando la scansione è disattivata, tutta l'indicizzazione e le informazioni relative a quel volume vengono rimosse dal sistema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

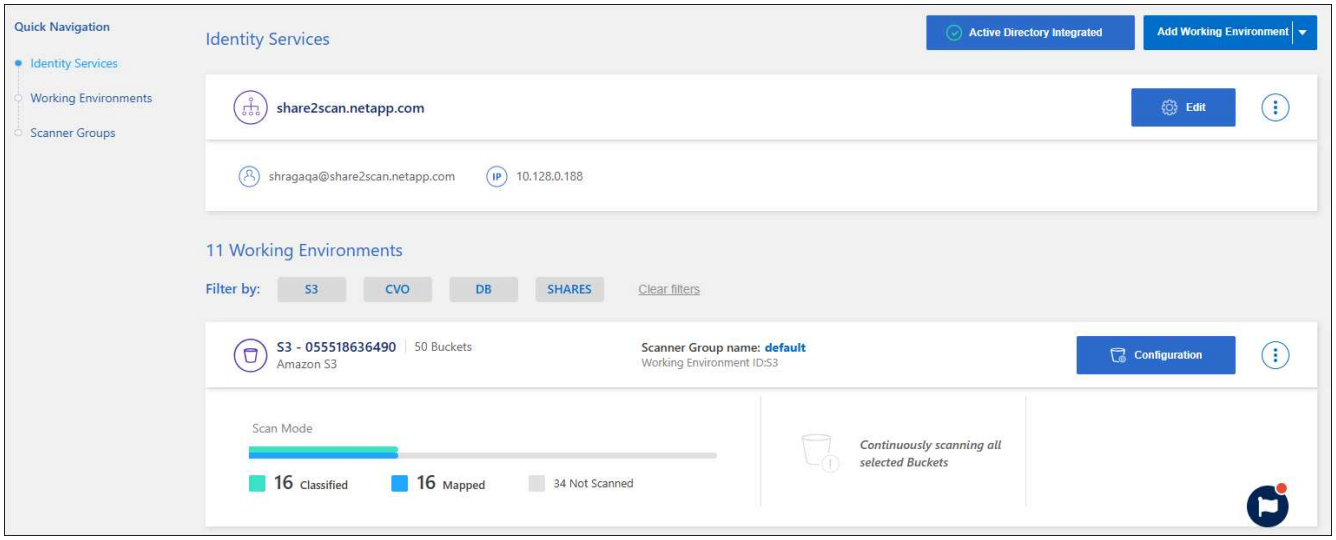
È possibile "mettere in pausa" la scansione di un repository se si desidera interrompere temporaneamente la scansione di determinati contenuti. Sospendendo la scansione, Data Classification non eseguirà più scansioni future per rilevare modifiche o aggiunte al repository. Tutti i risultati della scansione corrente restano accessibili in Classificazione dati.

Se si mettono in pausa le scansioni, gli addebiti non vengono eliminati perché i dati restano nel sistema.

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.

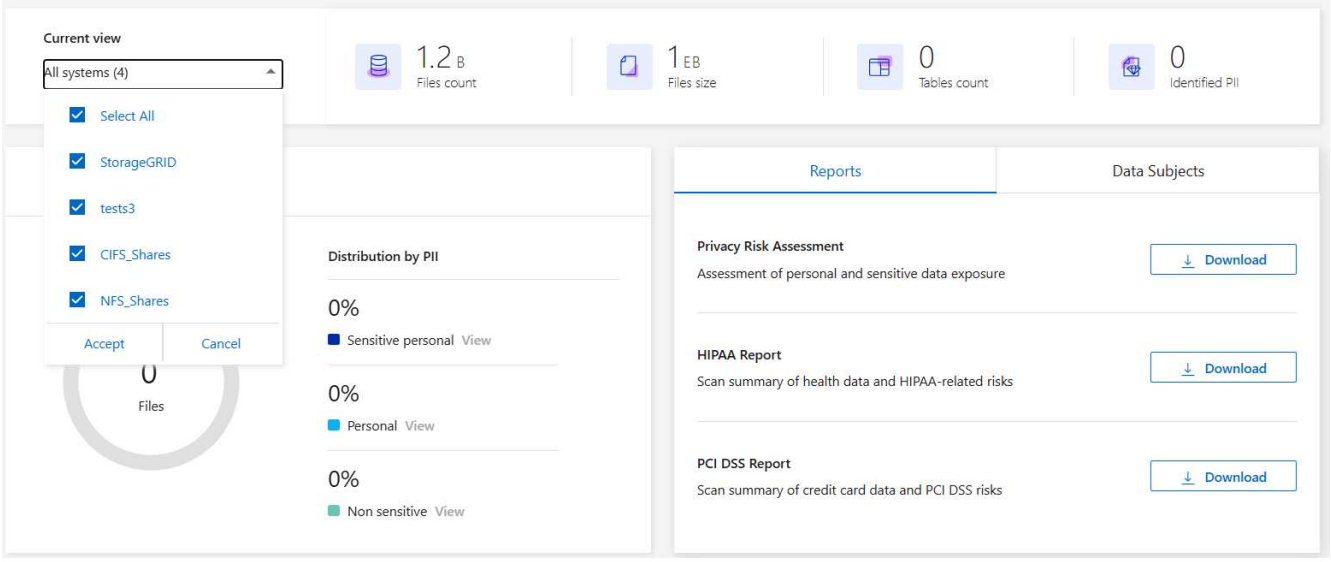
Seleziona i sistemi per i report

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

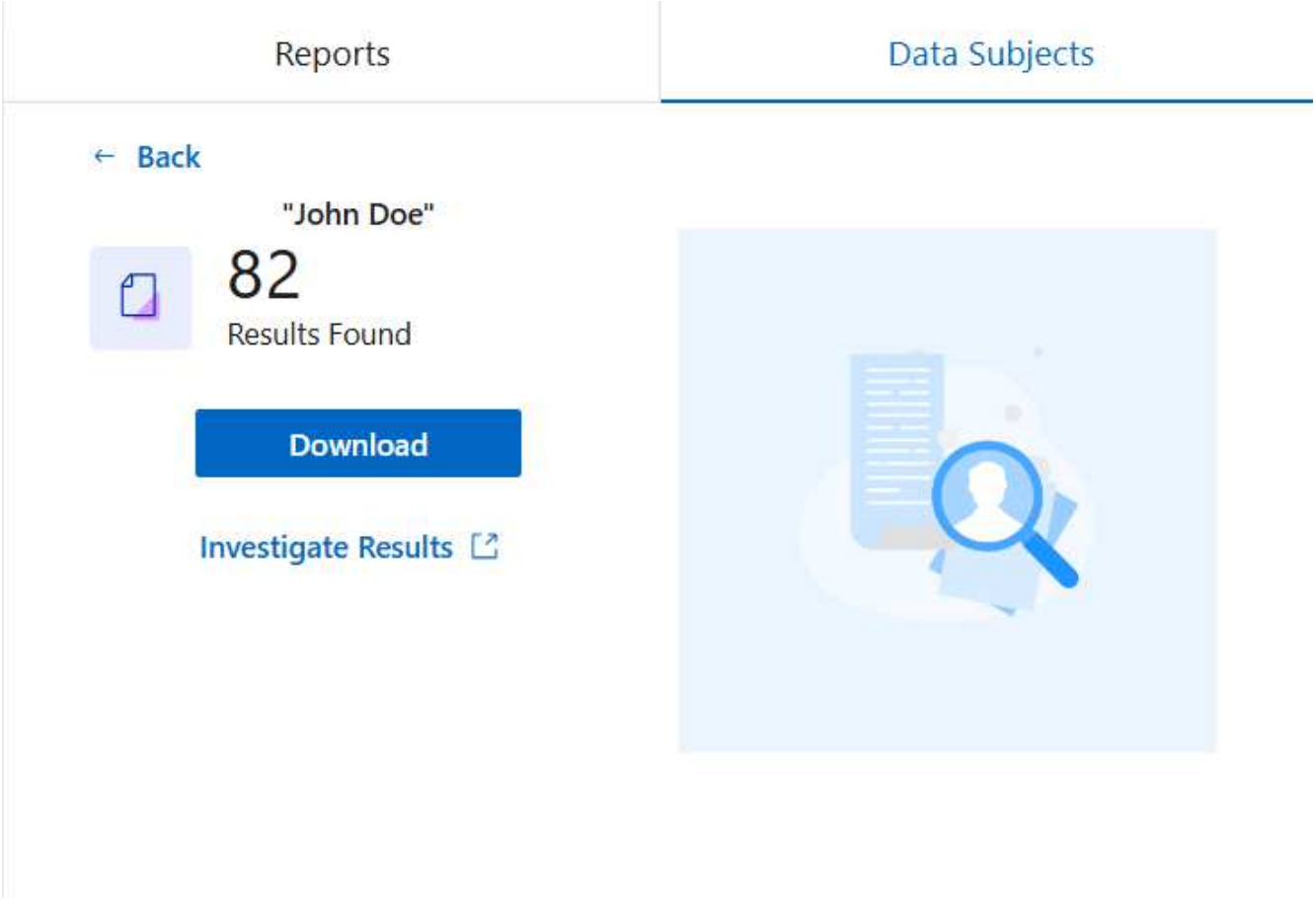
Cerca il nome completo o l'identificativo noto dell'interessato e poi scarica un report con l'elenco dei file o un report DSAR. Puoi cercare per"qualsiasi tipo di informazione personale" .

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.

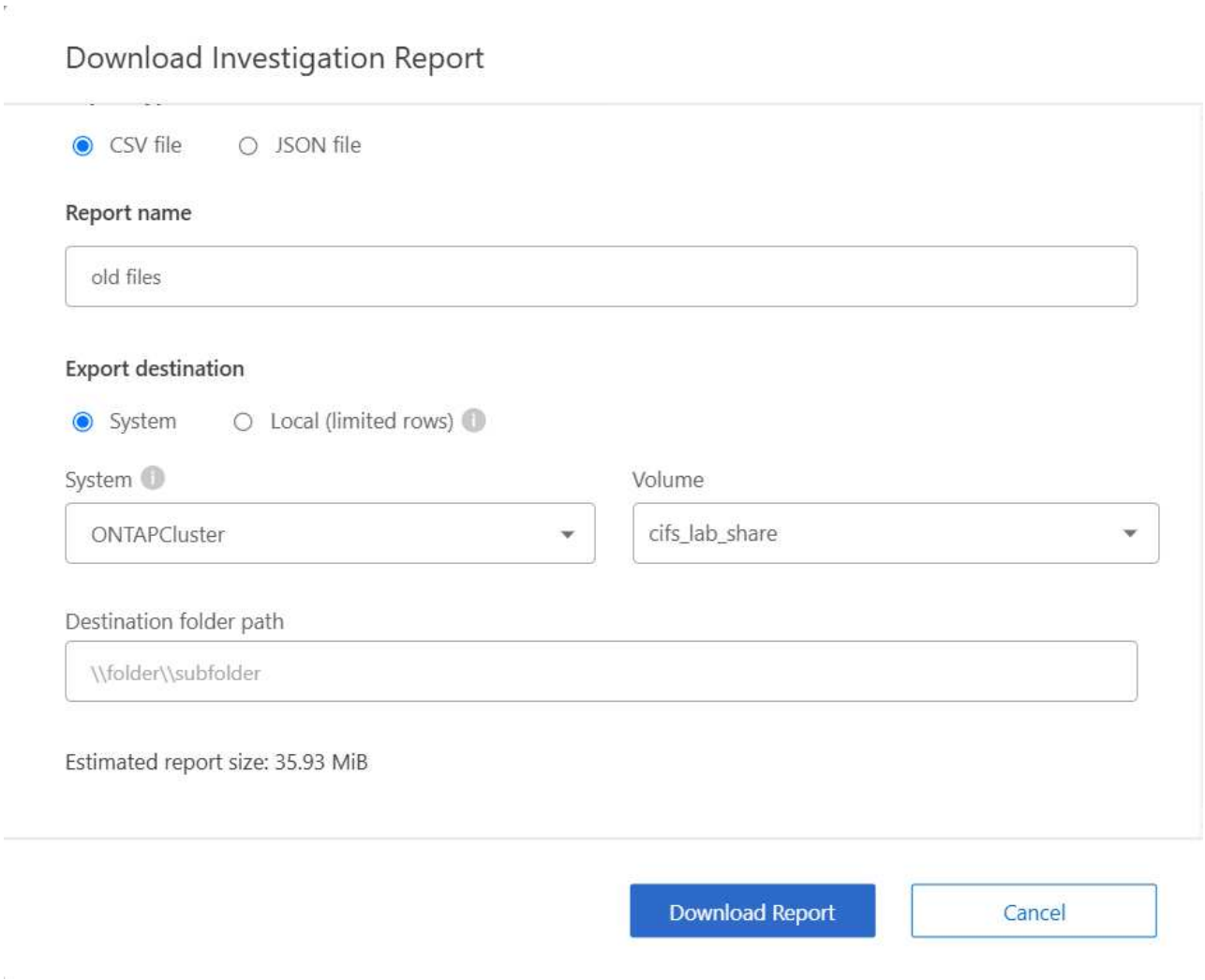
   a. Quando selezioni l'icona di download, configura le impostazioni di download:

      - 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.

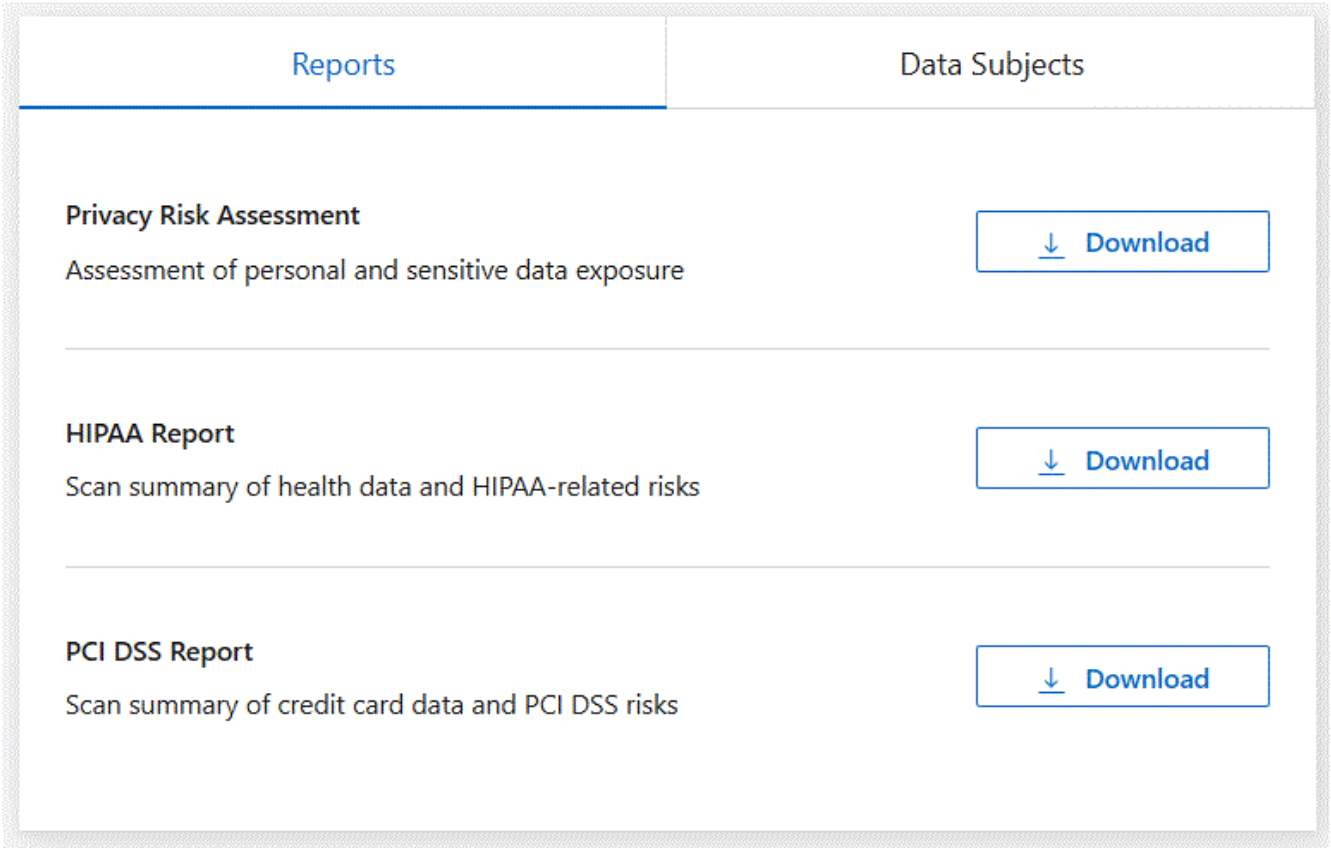
- Conservazione: intervallo di tempo in cui i file sono stati modificati l'ultima volta. Questo è utile perché non dovresti conservare le informazioni sanitarie più a lungo del necessario per elaborarle.
- Distribuzione delle informazioni sanitarie: i sistemi in cui sono state trovate le informazioni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

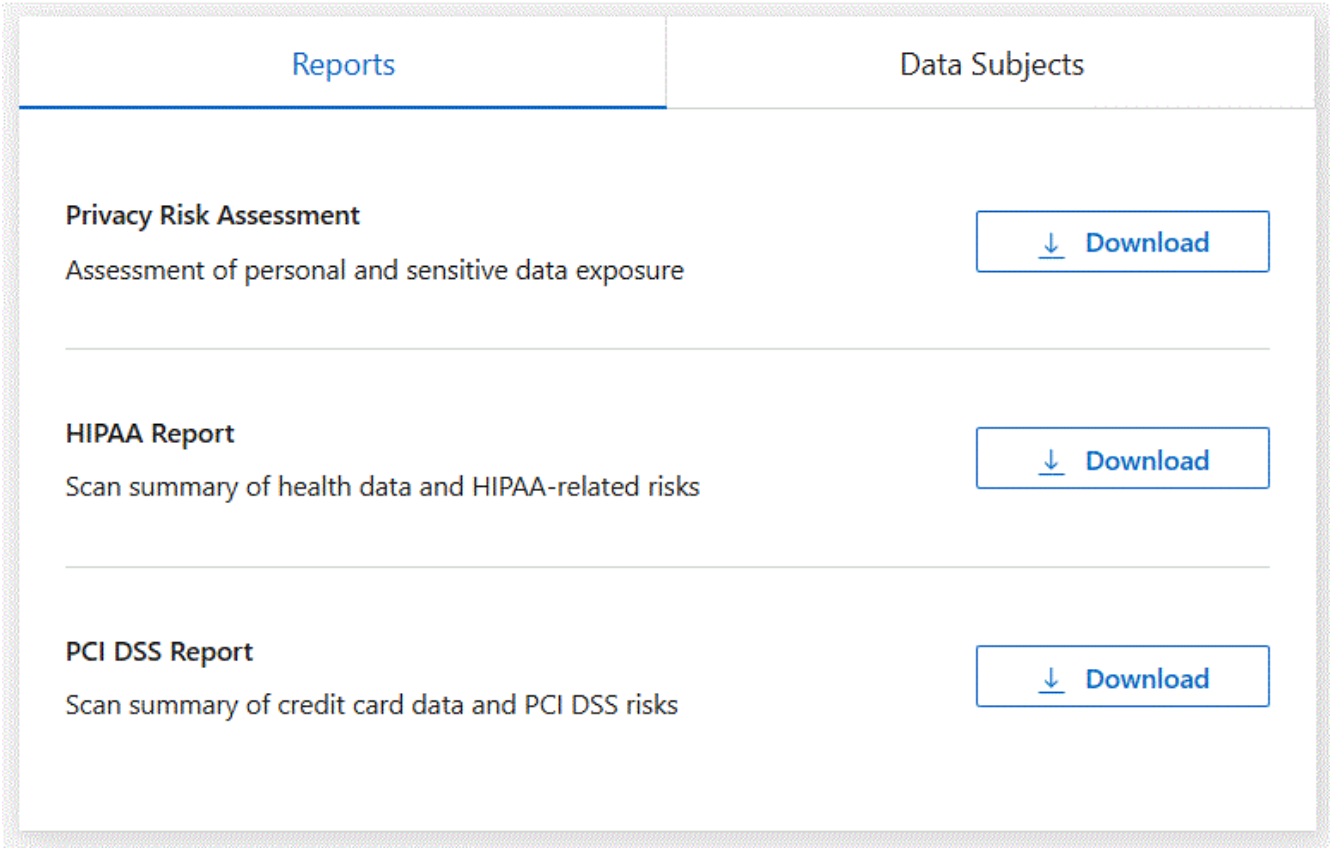
- Protezione ransomware: percentuale di file contenenti informazioni sulla carta di credito presenti su sistemi con o senza protezione ransomware abilitata. Queste informazioni sono specifiche per Cloud Volumes ONTAP.
- Conservazione: intervallo di tempo in cui i file sono stati modificati l'ultima volta. 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:

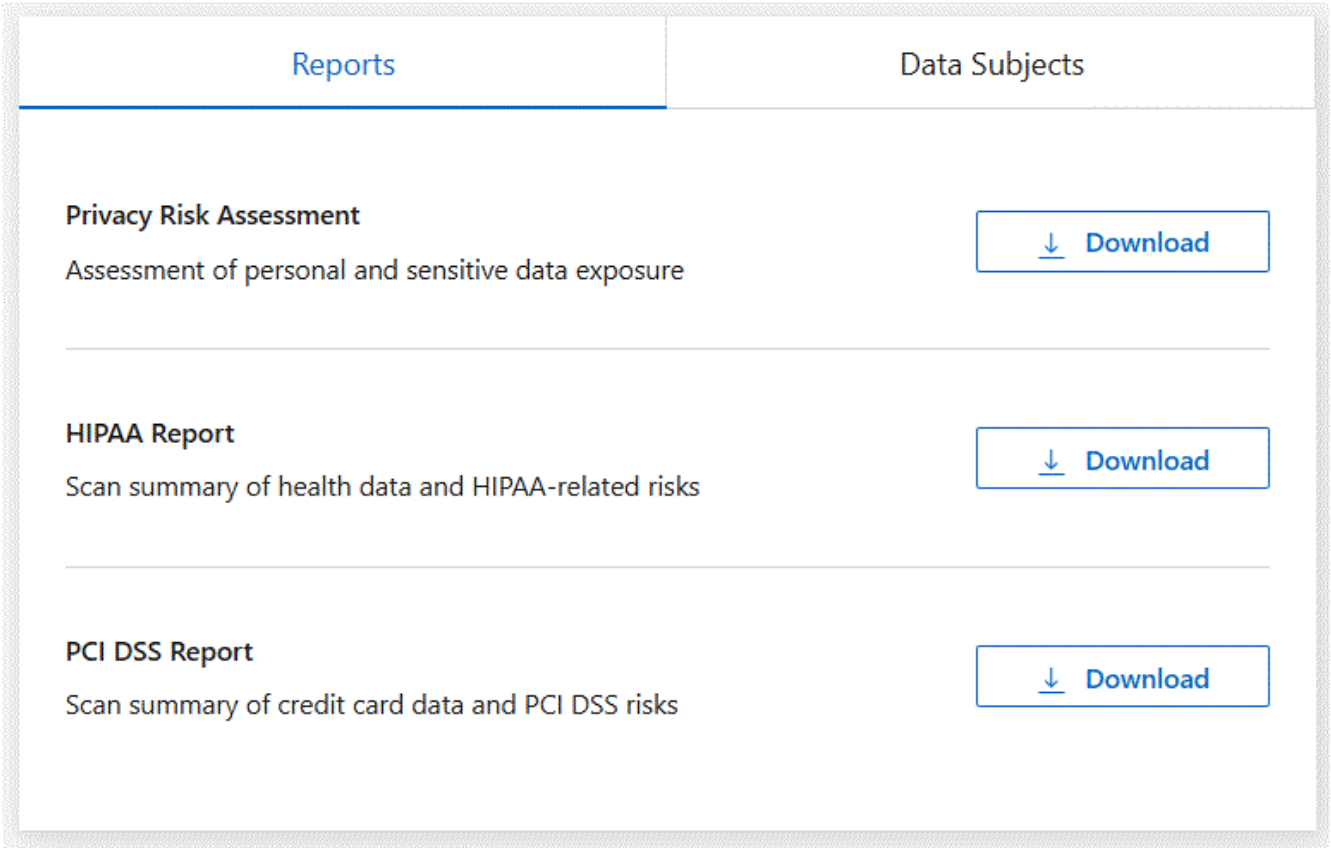
- Stato di conformità: punteggio di gravità e distribuzione dei dati, siano essi non sensibili, personali o sensibili personali.
- Panoramica della valutazione: una ripartizione dei tipi di dati personali rilevati, nonché delle categorie di dati.
- Soggetti interessati in questa valutazione: numero di 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%

Monitora lo stato di integrità NetApp Data Classification

La dashboard NetApp Data Classification Health Monitor fornisce monitoraggio in tempo reale e approfondimenti sulle prestazioni. Health Monitor acquisisce informazioni sull'infrastruttura di classificazione dei dati, sullo stato del sistema, sulle metriche di utilizzo e sui dati di utilizzo, consentendo di identificare e risolvere i problemi.

Approfondimenti di Health Monitor

La dashboard Health Monitor presenta le informazioni in quattro categorie.

- **Stato dell'infrastruttura**

  Visualizza informazioni tra cui lo stato della versione, la stabilità del sistema, il tipo di distribuzione e la scala della macchina.

- **Contenitori problematici**

  Esaminare il campo dei contenitori problematici per informazioni dettagliate sui contenitori che vengono arrestati o riavviati frequentemente. Utilizzare queste informazioni per esaminare i contenitori specifici.

- **Informazioni di sistema**

  Il pannello delle informazioni di sistema acquisisce informazioni critiche sulla NetApp Console e sulla classificazione dei dati, come gli indirizzi IP pubblici e privati, il nome host, il sistema operativo, la versione della console e l'ID della console.

- **Utilizzo e utilizzazione**

Esaminare l'utilizzo della CPU, l'utilizzo del disco, l'utilizzo del disco e l'utilizzo della memoria. Questi valori vengono visualizzati in unità di archiviazione (GB) o in percentuale dell'utilizzo totale. Se in uno dei campi viene visualizzato un avviso, selezionarlo per ottenere informazioni e consigli su come risolvere il problema.

Accedi alla dashboard di Health Monitor

1. In Classificazione dati, seleziona **Configurazione**.
2. Sotto l'intestazione **Configurazione**, seleziona **Monitoraggio dello stato di classificazione dei dati**.
3. Nella dashboard Health Monitor puoi:
   - Esaminare l'utilizzo e l'utilizzazione. Se vengono visualizzati avvisi per le metriche di utilizzo o di utilizzo, selezionare l'avviso per ricevere consigli su come risolvere il problema.
   - Attiva/disattiva il grafico per visualizzare l'utilizzo della CPU, l'utilizzo del disco, l'utilizzo del disco e l'utilizzo della memoria. È possibile modificare l'asse x per visualizzare il contenuto in base alle ore (6, 12 o 24) o ai giorni (2, 7 o 14).
   - Aggiorna la dashboard per visualizzare le metriche dei dati più recenti.