Datenklassifizierung verwenden

NetApp Data Classification

NetApp
February 11, 2026

Inhalt

Datenklassifizierung verwenden

Mit NetApp Data Classification Governance-Details zu den in Ihrem Unternehmen gespeicherten Daten anzeigen

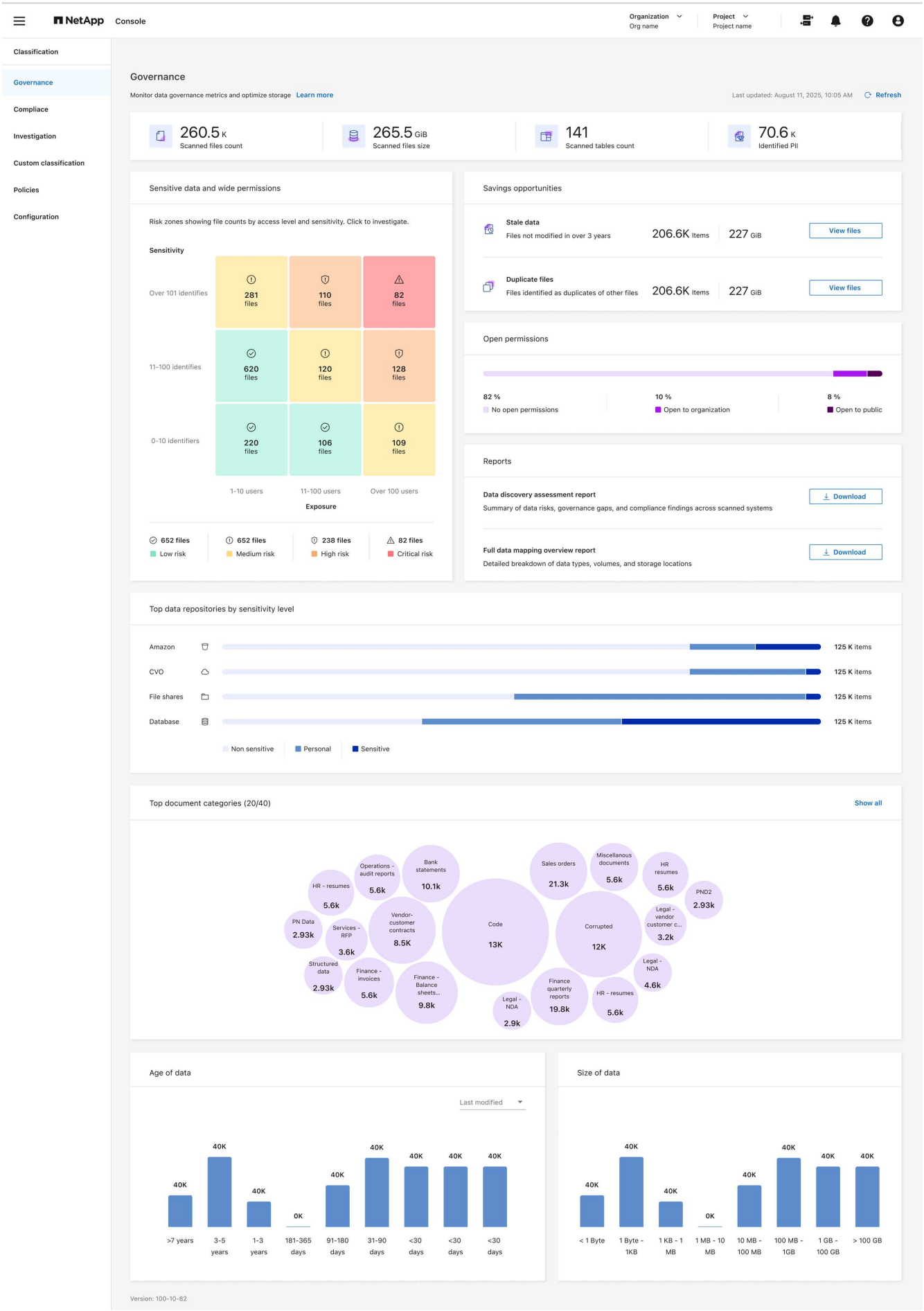
Behalten Sie die Kontrolle über die Kosten im Zusammenhang mit den Daten auf den Speicherressourcen Ihres Unternehmens. NetApp Data Classification ermittelt die Menge veralteter Daten, doppelter Dateien und sehr großer Dateien in Ihren Systemen, sodass Sie entscheiden können, ob Sie einige Dateien entfernen oder in einen kostengünstigeren Objektspeicher verschieben möchten.

Hier sollten Sie mit Ihrer Recherche beginnen. Im Governance-Dashboard können Sie einen Bereich für weitere Untersuchungen auswählen.

Wenn Sie außerdem planen, Daten von lokalen Standorten in die Cloud zu migrieren, können Sie vor dem Verschieben die Größe der Daten anzeigen und feststellen, ob die Daten vertrauliche Informationen enthalten.

Überprüfen des Governance-Dashboards

Das Governance-Dashboard bietet Informationen, mit denen Sie die Effizienz steigern und die Kosten im Zusammenhang mit den auf Ihren Speicherressourcen gespeicherten Daten kontrollieren können.


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

Schritte

1. Wählen Sie im NetApp Console **Governance > Klassifizierung** aus.
2. Wählen Sie **Governance** aus.

   Das Governance-Dashboard wird angezeigt.

Sparmöglichkeiten prüfen

Die Komponente „Einsparmöglichkeiten“ zeigt Daten an, die Sie löschen oder in einen kostengünstigeren Objektspeicher verschieben können. Die Daten in *Sparmöglichkeiten* werden alle 2 Stunden aktualisiert. Sie können die Daten auch manuell aktualisieren.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Governance“ aus.
2. Wählen Sie in jeder Kachel „Einsparmöglichkeiten“ des Governance-Dashboards **Speicher optimieren** aus, um die gefilterten Ergebnisse auf der Untersuchungsseite anzuzeigen. Um herauszufinden, welche Daten Sie löschen oder auf günstigeren Speicher verschieben sollten, untersuchen Sie die *Sparmöglichkeiten*.
   - **Veraltete Daten** - Standardmäßig gelten Daten als veraltet, wenn sie zuletzt vor mehr als 3 Jahren geändert wurden. Sie können die Definition von veralteten Daten anpassen (task-stale-data.html).
   - **Doppelte Dateien** – Dateien, die an anderen Speicherorten in den von Ihnen gescannten Datenquellen dupliziert sind. "Sehen Sie, welche Arten von doppelten Dateien angezeigt werden" .

Wenn eine Ihrer Datenquellen Daten-Tiering implementiert, können alte Daten, die sich bereits im Objektspeicher befinden, in der Kategorie „Veraltete Daten“ identifiziert werden.

Erstellen des Data Discovery-Bewertungsberichts

Der Bewertungsbericht zur Datenermittlung bietet eine umfassende Analyse der gescannten Umgebung, um Problembereiche und mögliche Abhilfemaßnahmen aufzuzeigen. Die Ergebnisse basieren sowohl auf der Zuordnung als auch auf der Klassifizierung Ihrer Daten. Das Ziel dieses Berichts besteht darin, das Bewusstsein für drei wichtige Aspekte Ihres Datensatzes zu schärfen:

Funktion	Beschreibung
Bedenken hinsichtlich der Datenverwaltung	Ein detailliertes Bild aller Daten, die Sie besitzen, und Bereiche, in denen Sie möglicherweise die Datenmenge reduzieren können, um Kosten zu sparen.
Datensicherheitsrisiken	Bereiche, in denen Ihre Daten aufgrund umfassender Zugriffsberechtigungen internen oder externen Angriffen ausgesetzt sind.
Lücken in der Datenkonformität	Wo sich Ihre persönlichen oder sensiblen persönlichen Daten befinden, sowohl aus Sicherheitsgründen als auch für DSARs (Anfragen zur Auskunftserteilung durch betroffene Personen).

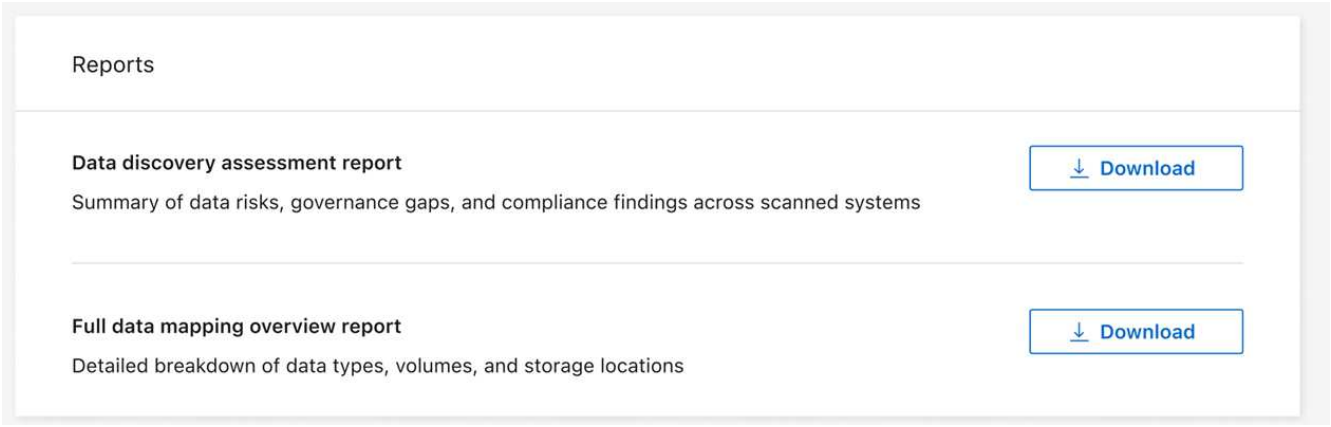
Mit dem Bericht können Sie folgende Aktionen ausführen:

- Reduzieren Sie die Speicherkosten, indem Sie Ihre Aufbewahrungsrichtlinie ändern oder bestimmte Daten (veraltete oder doppelte Daten) verschieben oder löschen.
- Schützen Sie Ihre Daten mit umfassenden Berechtigungen, indem Sie die globalen Gruppenverwaltungsrichtlinien überarbeiten.

- Schützen Sie Ihre Daten, die persönliche oder sensible persönliche Informationen enthalten, indem Sie PII in sicherere Datenspeicher verschieben.

Schritte

1. Wählen Sie unter „Datenklassifizierung“ **Governance** aus.
2. Wählen Sie in der Berichtskachel **Data Discovery Assessment Report** aus.



Ergebnis

Die Datenklassifizierung generiert einen PDF-Bericht, den Sie überprüfen und weitergeben können.

Erstellen des Datenzuordnungsübersichtsberichts

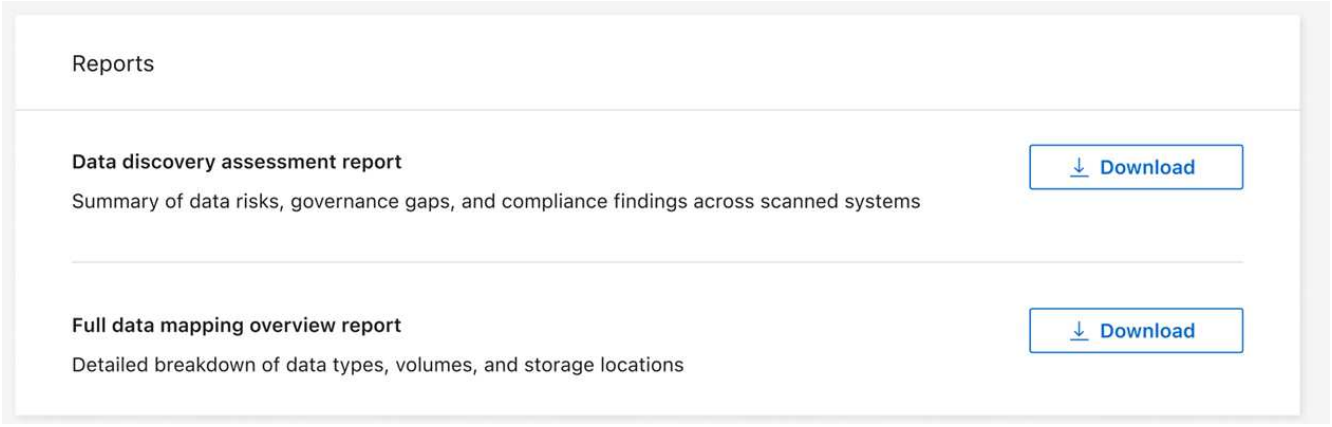
Der Übersichtsbericht zur Datenzuordnung bietet einen Überblick über die in Ihren Unternehmensdatenquellen gespeicherten Daten und unterstützt Sie bei Entscheidungen zu Migrations-, Sicherungs-, Sicherheits- und Compliance-Prozessen. Der Bericht fasst alle Systeme und Datenquellen zusammen. Es bietet auch eine Analyse für jedes System.

Der Bericht enthält die folgenden Informationen:

Kategorie	Beschreibung
Nutzungskapazität	Für alle Systeme: Listet die Anzahl der Dateien und die verwendete Kapazität für jedes System auf. Für Einzelsysteme: Listet die Dateien auf, die die meiste Kapazität beanspruchen.
Zeitalter der Daten	Bietet drei Diagramme und Grafiken zum Zeitpunkt der Erstellung, der letzten Änderung oder des letzten Zugriffs auf Dateien. Listet die Anzahl der Dateien und ihre verwendete Kapazität basierend auf bestimmten Datumsbereichen auf.
Datengröße	Listet die Anzahl der Dateien auf, die in Ihren Systemen innerhalb bestimmter Größenbereiche vorhanden sind.

Schritte

1. Wählen Sie unter „Datenklassifizierung“ **Governance** aus.
2. Wählen Sie in der Berichtskachel **Vollständiger Übersichtsbericht zur Datenzuordnung** aus.



Ergebnis

Die Datenklassifizierung generiert einen PDF-Bericht, den Sie überprüfen und bei Bedarf an andere Gruppen senden können.

Wenn der Bericht größer als 1 MB ist, wird die PDF-Datei in der Datenklassifizierungsinstanz gespeichert und Sie sehen eine Popup-Meldung mit dem genauen Speicherort. Wenn Data Classification auf einem Linux-Computer bei Ihnen vor Ort oder auf einem Linux-Computer installiert ist, den Sie in der Cloud bereitgestellt haben, können Sie direkt zur PDF-Datei navigieren. Wenn die Datenklassifizierung in der Cloud bereitgestellt wird, müssen Sie sich per SSH bei der Datenklassifizierungsinstanz autorisieren, um die PDF-Datei herunterzuladen.

Überprüfen Sie die wichtigsten Datenspeicher nach Datensensibilität

Im Bereich „Top-Datenrepositorys nach Vertraulichkeitsstufe“ des Berichts „Datenzuordnungsübersicht“ werden die vier wichtigsten Datenrepositorys (Systeme und Datenquellen) aufgelistet, die die sensibelsten Elemente enthalten. Das Balkendiagramm für jedes System ist unterteilt in:

- Nicht sensible Daten
- personenbezogene Daten
- Sensible personenbezogene Daten

Diese Daten werden alle zwei Stunden aktualisiert und können manuell aktualisiert werden.

Schritte

1. Um die Gesamtzahl der Elemente in jeder Kategorie anzuzeigen, positionieren Sie den Cursor über jedem Abschnitt der Leiste.
2. Um die Ergebnisse zu filtern, die auf der Untersuchungsseite angezeigt werden, wählen Sie jeden Bereich in der Leiste aus und untersuchen Sie ihn weiter.

Überprüfen Sie vertrauliche Daten und umfassende Berechtigungen

Der Bereich „Sensible Daten und umfassende Berechtigungen“ des Governance-Dashboards zeigt die Anzahl der Dateien an, die vertrauliche Daten enthalten und über umfassende Berechtigungen verfügen. Die Tabelle zeigt die folgenden Berechtigungstypen:

- Von den restriktivsten Berechtigungen bis zu den freizügigsten Einschränkungen auf der horizontalen Achse.
- Von den am wenigsten sensiblen Daten zu den sensibelsten Daten auf der vertikalen Achse.

Schritte

1. Um die Gesamtzahl der Dateien in jeder Kategorie anzuzeigen, positionieren Sie den Cursor über jedem Kästchen.
2. Um die Ergebnisse zu filtern, die auf der Untersuchungsseite angezeigt werden, wählen Sie ein Kästchen aus und untersuchen Sie die Ergebnisse weiter.

Überprüfen Sie die nach Arten offener Berechtigungen aufgelisteten Daten

Der Bereich „Offene Berechtigungen“ des Berichts „Datenzuordnungsübersicht“ zeigt den Prozentsatz für jeden Berechtigungstyp an, der für alle gescannten Dateien vorhanden ist. Das Diagramm zeigt die folgenden Berechtigungstypen:

- Keine offenen Berechtigungen
- Offen für Organisation
- Für die Öffentlichkeit zugänglich
- Unbekannter Zugriff

Schritte

1. Um die Gesamtzahl der Dateien in jeder Kategorie anzuzeigen, positionieren Sie den Cursor über jedem Kästchen.
2. Um die Ergebnisse zu filtern, die auf der Untersuchungsseite angezeigt werden, wählen Sie ein Kästchen aus und untersuchen Sie die Ergebnisse weiter.

Überprüfen Sie das Alter und die Größe der Daten

Sie können die Elemente in den Diagrammen „Alter“ und „Größe“ des Berichts „Datenzuordnungsübersicht“ untersuchen, um festzustellen, ob es Daten gibt, die Sie löschen oder in einen weniger teuren Objektspeicher verschieben sollten.

Schritte

1. Um im Diagramm „Alter der Daten“ Details zum Alter der Daten anzuzeigen, positionieren Sie den Cursor über einem Punkt im Diagramm.
2. Um nach einem Alters- oder Größenbereich zu filtern, wählen Sie dieses Alter oder diese Größe aus.
    - **Datenalter-Diagramm** – Kategorisiert Daten basierend auf dem Zeitpunkt ihrer Erstellung, dem letzten Zugriff oder der letzten Änderung.
    - **Größe des Datendiagramms** – Kategorisiert Daten basierend auf der Größe.

Wenn eine Ihrer Datenquellen Daten-Tiering implementiert, werden alte Daten, die sich bereits im Objektspeicher befinden, möglicherweise im Diagramm „Alter der Daten“ identifiziert.

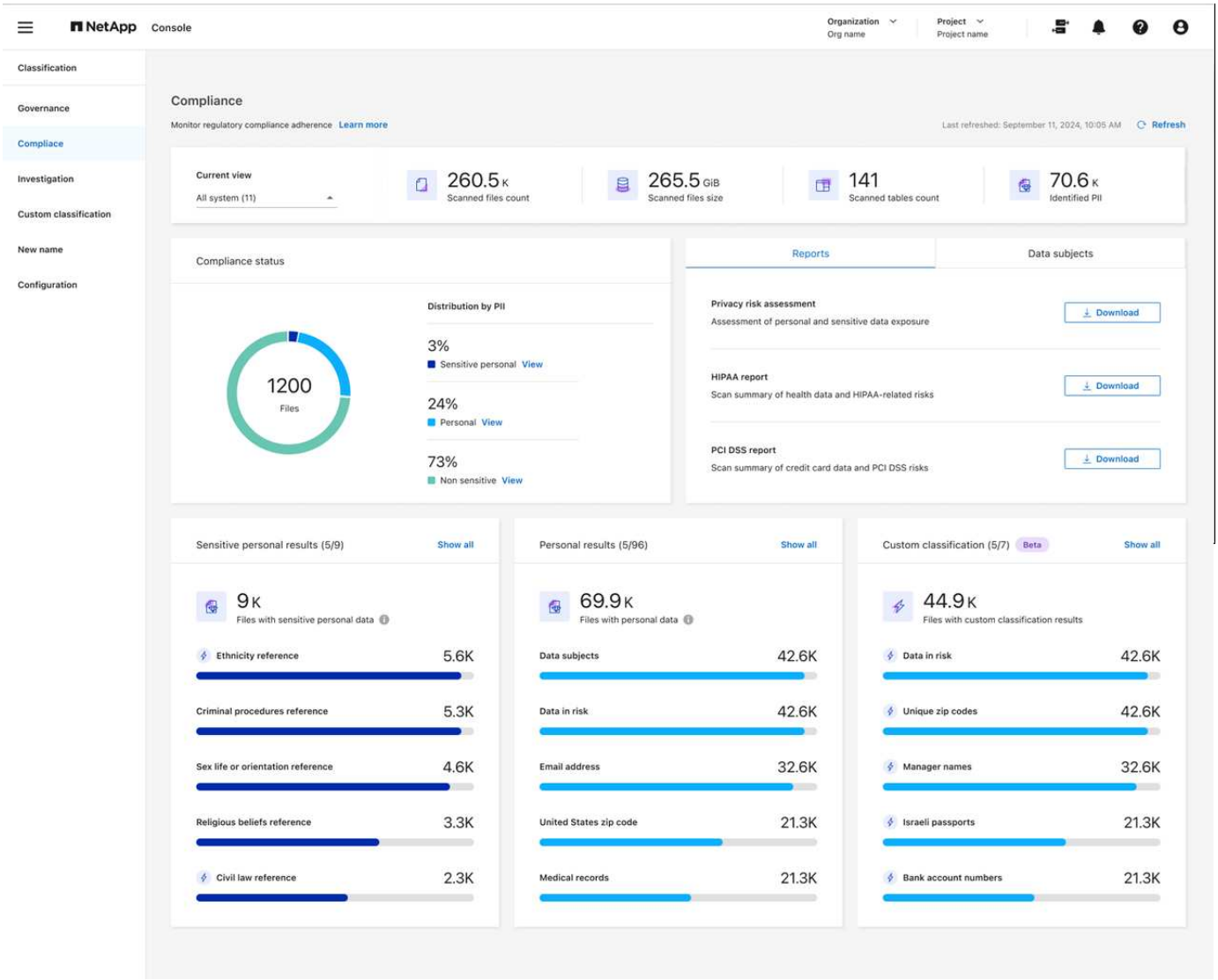
Mit NetApp Data Classification können Sie Compliance-Details zu den in Ihrem Unternehmen gespeicherten privaten Daten einsehen.

Übernehmen Sie die Kontrolle über Ihre privaten Daten, indem Sie Details zu den personenbezogenen Daten (PII) und sensiblen personenbezogenen Daten (SPII) in Ihrem Unternehmen anzeigen. Sie können außerdem Transparenz gewinnen, indem Sie

die Kategorien und Dateitypen überprüfen, die NetApp Data Classification in Ihren Daten gefunden hat.

Konformitätsdetails auf Dateiebene sind nur verfügbar, wenn Sie einen vollständigen Klassifizierungsscan durchführen. Reine Mapping-Scans liefern keine Details auf Dateiebene.

Standardmäßig zeigt das Dashboard „Datenklassifizierung“ Compliance-Daten für alle Systeme und Datenbanken an. Um nur für einige der Systeme Daten anzuzeigen, wählen Sie diese aus.



Sie können die Ergebnisse auf der Seite „Datenuntersuchung“ filtern und einen Ergebnisbericht als CSV-Datei herunterladen. Sehen"Filtern von Daten auf der Seite „Datenuntersuchung“" für Details.

Anzeigen von Dateien, die personenbezogene Daten enthalten

Die Datenklassifizierung identifiziert automatisch bestimmte Wörter, Zeichenfolgen und Muster (Regex) in den Daten. "Zum Beispiel Kreditkartennummern, Sozialversicherungsnummern, Bankkontonummern, Passwörter und mehr."Die Datenklassifizierung identifiziert diese Art von Informationen in einzelnen Dateien, in Dateien innerhalb von Verzeichnissen (Freigaben und Ordnern) und in Datenbanktabellen.

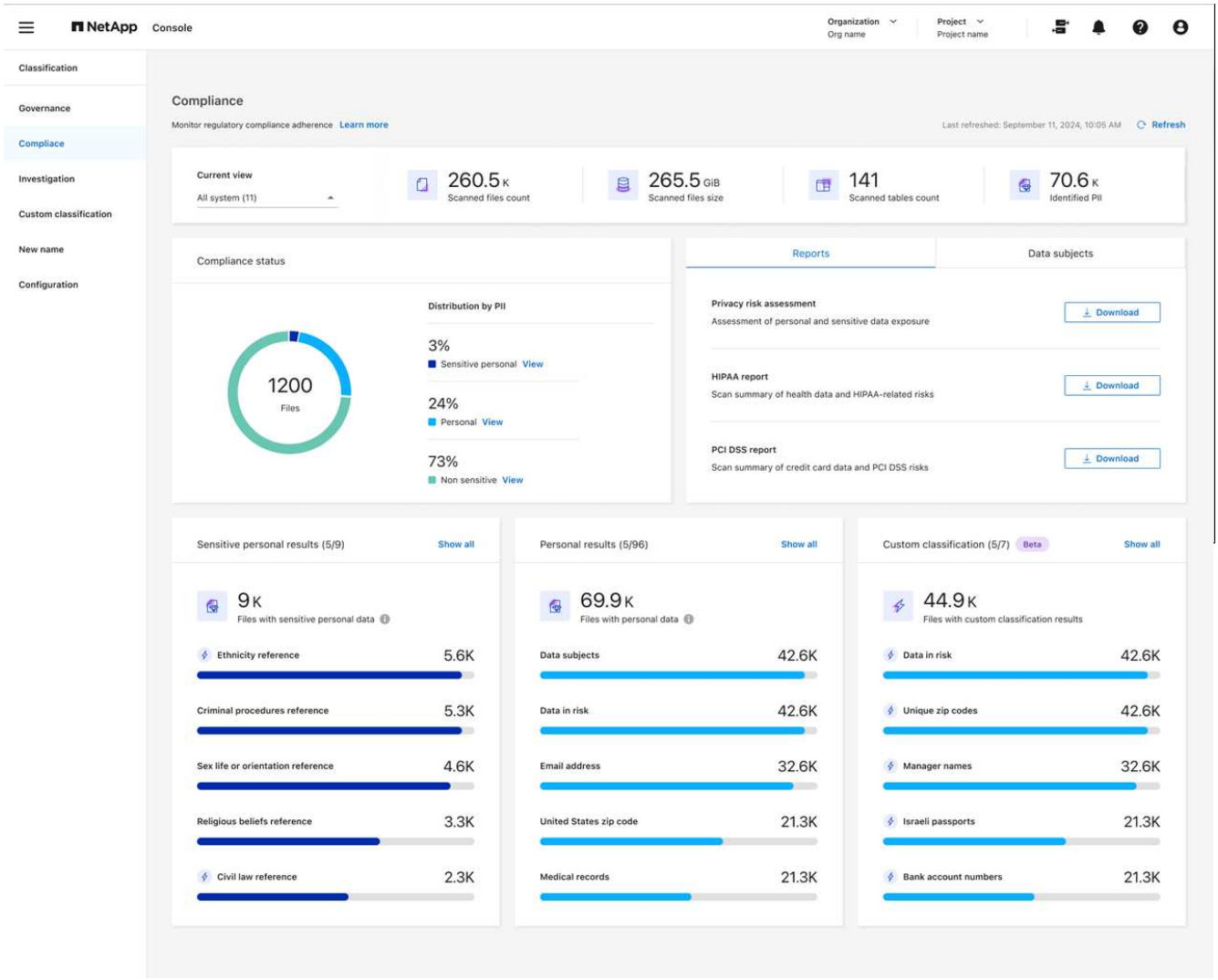
Sie können auch benutzerdefinierte Suchbegriffe erstellen, um personenbezogene Daten zu identifizieren, die

für Ihre Organisation spezifisch sind. Weitere Informationen finden Sie unter "Erstellen einer benutzerdefinierten Klassifizierung" .

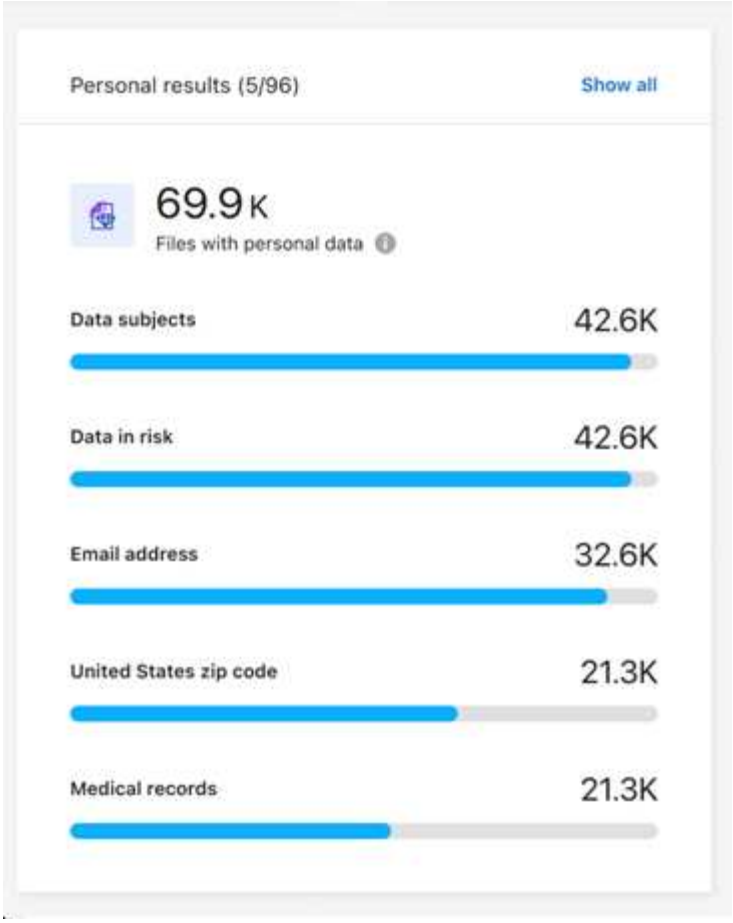
Für einige Arten personenbezogener Daten verwendet die Datenklassifizierung eine Näherungsvalidierung, um ihre Ergebnisse zu validieren. Die Validierung erfolgt durch die Suche nach einem oder mehreren vordefinierten Schlüsselwörtern in der Nähe der gefundenen personenbezogenen Daten. Beispielsweise identifiziert die Datenklassifizierung eine US-Sozialversicherungsnummer (SSN) als SSN, wenn sie daneben ein Näherungswort sieht, beispielsweise *SSN* oder *Sozialversicherung*. "Die Tabelle der personenbezogenen Daten" zeigt an, wann die Datenklassifizierung eine Näherungsvalidierung verwendet.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Registerkarte „Compliance“ aus.
2. Um die Details aller personenbezogenen Daten zu untersuchen, wählen Sie das Symbol neben dem Prozentsatz der personenbezogenen Daten aus.

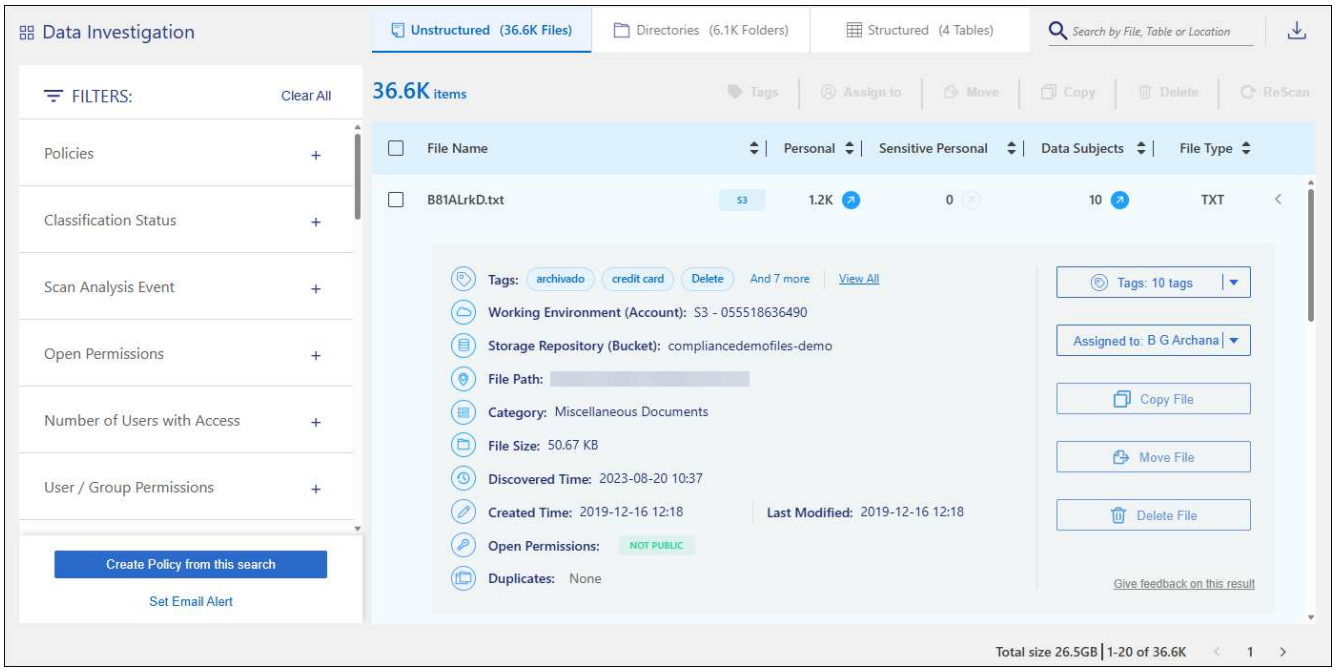


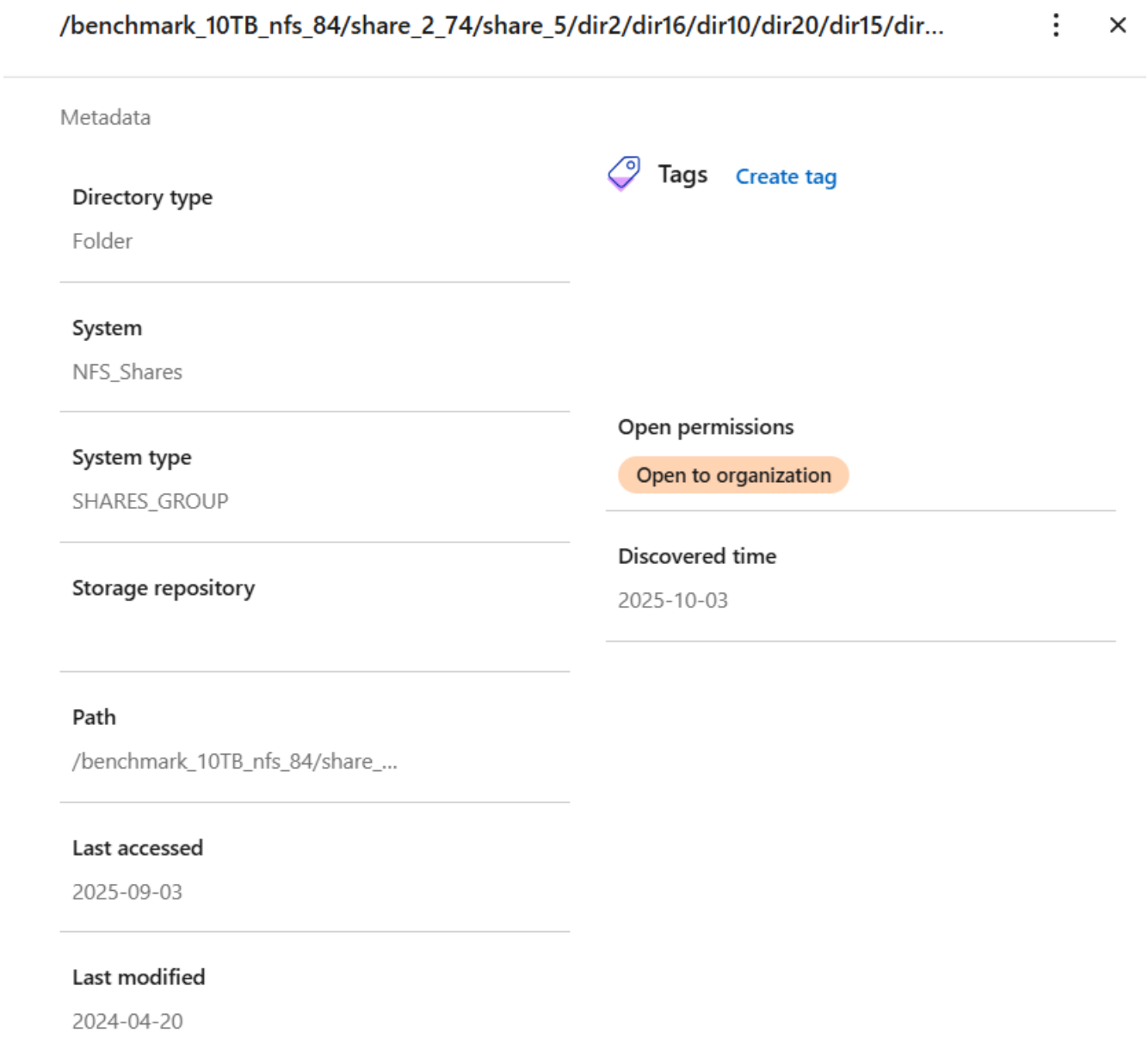
3. Um die Details für einen bestimmten Typ personenbezogener Daten zu untersuchen, wählen Sie **Alle anzeigen** und dann das Pfeilsymbol **Ergebnisse untersuchen** für einen bestimmten Typ personenbezogener Daten, beispielsweise E-Mail-Adressen.



4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sie sortieren, Details erweitern, den Pfeil **Ergebnisse untersuchen** auswählen, um maskierte Informationen anzuzeigen, oder indem Sie die Dateiliste herunterladen.

   Die folgenden Bilder zeigen persönliche Daten, die in einem Verzeichnis (Freigaben und Ordner) gefunden wurden. Im Reiter **Strukturiert** können Sie in Datenbanken gefundene personenbezogene Daten einsehen. Auf der Registerkarte **Unstrukturiert** können Sie Daten auf Dateiebene anzeigen.


Data Investigation
Unstructured (36.6K Files)
Directories (6.1K Folders)
Structured (4 Tables)
Search by File, Table or Location
FILTERS:
Clear All
Policies
Classification Status
Scan Analysis Event
Open Permissions
Number of Users with Access
User / Group Permissions
Create Policy from this search
Set Email Alert
36.6K items
Tags
Assign to
Move
Copy
Delete
ReScan
File Name
Personal
Sensitive Personal
Data Subjects
File Type
B81ALrkD.txt
S3
1.2K
0
10
TXT
Tags: archivado credit card Delete And 7 more View All
Working Environment (Account): S3 - 055518636490
Storage Repository (Bucket): compliancedemofiles-demo
File Path:
Category: Miscellaneous Documents
File Size: 50.67 KB
Discovered Time: 2023-08-20 10:37
Created Time: 2019-12-16 12:18
Last Modified: 2019-12-16 12:18
Open Permissions: NOT PUBLIC
Duplicates: None
Tags: 10 tags
Assigned to: B G Archana
Copy File
Move File
Delete File
Give feedback on this result
Total size 26.5GB | 1-20 of 36.6K
1



Anzeigen von Dateien, die vertrauliche personenbezogene Daten enthalten

Die Datenklassifizierung identifiziert automatisch spezielle Arten sensibler personenbezogener Daten, wie sie in Datenschutzbestimmungen definiert sind, wie z. B. "Artikel 9 und 10 der DSGVO" . Beispielsweise Informationen zum Gesundheitszustand, zur ethnischen Herkunft oder zur sexuellen Orientierung einer Person. "Vollständige Liste anzeigen" . Die Datenklassifizierung identifiziert diese Art von Informationen in einzelnen Dateien, in Dateien innerhalb von Verzeichnissen (Freigaben und Ordnern) und in Datenbanktabellen.

Bei der Datenklassifizierung werden KI, natürliche Sprachverarbeitung (NLP), maschinelles Lernen (ML) und kognitives Computing (CC) verwendet, um die Bedeutung der gescannten Inhalte zu verstehen, Entitäten zu extrahieren und sie entsprechend zu kategorisieren.

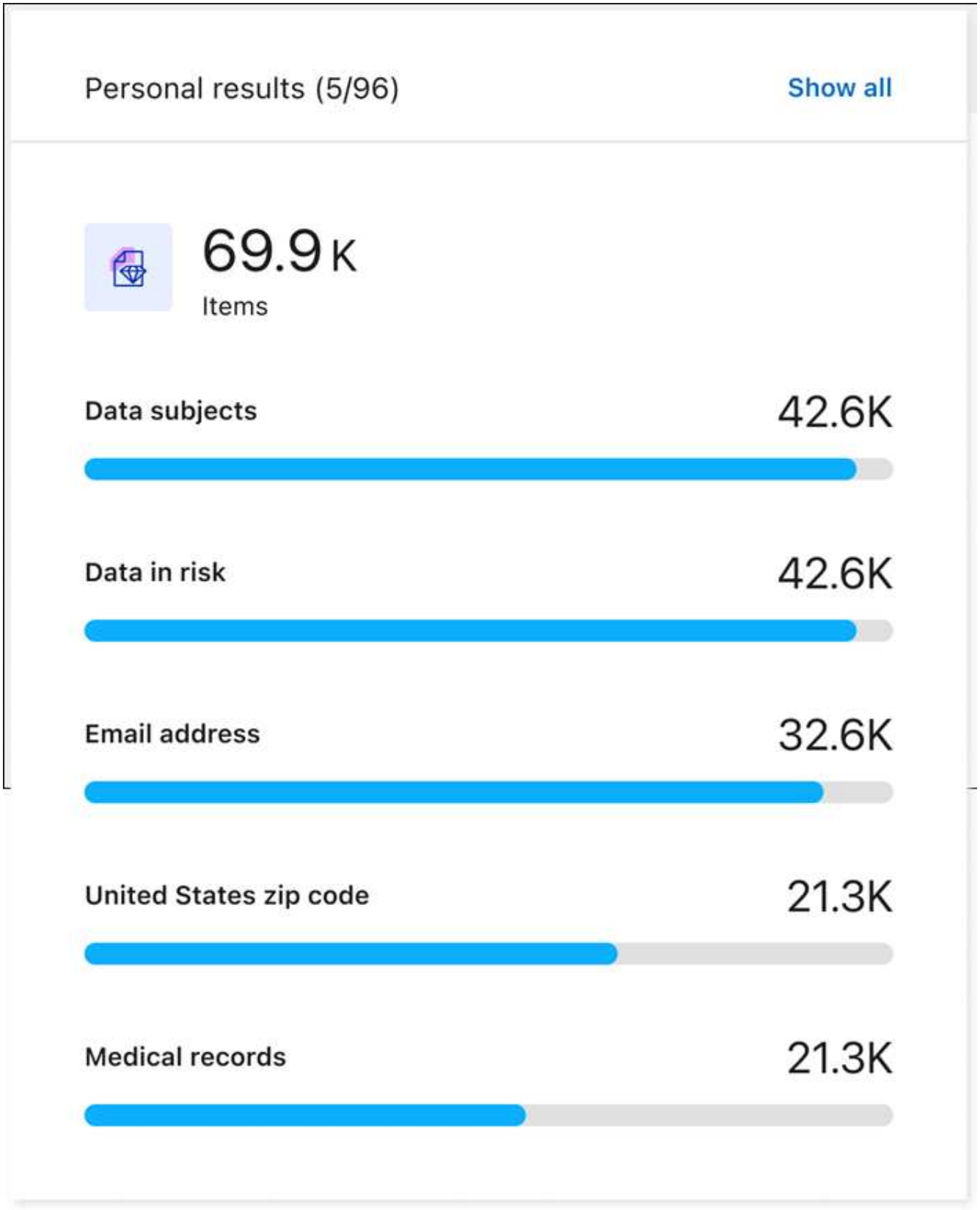
Eine sensible Datenkategorie der DSGVO ist beispielsweise die ethnische Herkunft. Aufgrund seiner NLP-Fähigkeiten kann die Datenklassifizierung den Unterschied zwischen einem Satz erkennen, der lautet: „George ist Mexikaner“ (was auf sensible Daten gemäß Artikel 9 der DSGVO hinweist) und „George isst mexikanisches

Essen“.

Beim Scannen nach sensiblen personenbezogenen Daten wird nur Englisch unterstützt. Die Unterstützung für weitere Sprachen wird später hinzugefügt.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Compliance“ aus.
2. Um die Details aller sensiblen personenbezogenen Daten zu untersuchen, suchen Sie die Karte **Sensible personenbezogene Ergebnisse** und wählen Sie dann **Alle anzeigen**.



.

3. Um die Details für einen bestimmten Typ sensibler personenbezogener Daten zu untersuchen, wählen Sie **Alle anzeigen** und dann das Pfeilsymbol **Ergebnisse untersuchen** für einen bestimmten Typ sensibler personenbezogener Daten.
4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sie sortieren, Details

erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder indem Sie die Dateiliste herunterladen.

Kategorien privater Daten in der NetApp Data Classification

Es gibt viele Arten privater Daten, die NetApp Data Classification in Ihren Volumes und Datenbanken identifizieren kann.

Bei der Datenklassifizierung werden zwei Arten personenbezogener Daten unterschieden:

- **Persönlich identifizierbare Informationen (PII)**
- **Sensible personenbezogene Daten (SPII)**

Wenn Sie eine Datenklassifizierung benötigen, um andere private Datentypen zu identifizieren, z. B. zusätzliche nationale ID-Nummern oder Gesundheitskennungen, wenden Sie sich an Ihren Kundenbetreuer.

Arten personenbezogener Daten

Bei den in Dateien enthaltenen personenbezogenen Daten oder persönlich identifizierbaren Informationen (PII) kann es sich um allgemeine personenbezogene Daten oder nationale Kennungen handeln. Die dritte Spalte in der folgenden Tabelle gibt an, ob die Datenklassifizierung"Näherungsvalidierung" um seine Ergebnisse für die Kennung zu validieren.

Die Sprachen, in denen diese Elemente erkannt werden können, sind in der Tabelle angegeben.

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	japanisch
Allgemein	Kreditkartennummer	Ja	✓	✓	✓		✓
	Betroffene Personen	Nein	✓	✓	✓		
	E-Mail-Adresse	Nein	✓	✓	✓		✓
	IBAN-Nummer (International Bank Account Number)	Nein	✓	✓	✓		✓
	IP-Adresse	Nein	✓	✓	✓		✓
	Passwort	Ja	✓	✓	✓		✓

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	japanisch
Nationale Kennungen							

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	japanisch

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	japanisch

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	japanisch
	Nummer des National Health Service (NHS)	Ja	✓	✓	✓		
	Neuseeländisches Bankkonto	Ja	✓	✓	✓		
	Neuseeländischer Führerschein	Ja	✓	✓	✓		
	Neuseeländische IRD-Nummer (Steuernummer)	Ja	✓	✓	✓		
	Neuseeländische NHI-Nummer (National Health Index)	Ja	✓	✓	✓		
	Neuseeländische Reisepassnummer	Ja	✓	✓	✓		
	Polnischer Personalausweis (PESEL)	Ja	✓	✓	✓		
	Portugiesische Steueridentifikationsnummer (NIF)	Ja	✓	✓	✓		
	Rumänischer Personalausweis (CNP)	Ja	✓	✓	✓		
	Nationaler Registrierungsausweis von Singapur (NRIC)	Ja	✓	✓	✓		
	Slowenischer Ausweis (EMSO)	Ja	✓	✓	✓		
	Südafrikanischer Ausweis	Ja	✓	✓	✓		
	Spanische Steueridentifikationsnummer	Ja	✓	✓	✓		
	Schwedischer Ausweis	Ja	✓	✓	✓		
	Britischer Ausweis (NINO)	Ja	✓	✓	✓		
	USA Kalifornien Führerschein	Ja	✓	✓	✓		
	USA Indiana Führerschein	Ja	✓	✓	✓		
	USA New York Führerschein	Ja	✓	✓	✓		
	USA Texas Führerschein	Ja	✓	✓	✓		
	Sozialversicherungsnummer der USA (SSN)	Ja	✓	✓	✓		

Arten sensibler personenbezogener Daten

Die Datenklassifizierung kann die folgenden sensiblen persönlichen Informationen (SPII) in Dateien finden.

Die folgenden SPII können derzeit nur in englischer Sprache erkannt werden:

- **Strafprozessuale Referenz**: Daten zu strafrechtlichen Verurteilungen und Straftaten einer natürlichen Person.
- **Ethnizitätsreferenz**: Daten zur rassischen oder ethnischen Herkunft einer natürlichen Person.
- **Gesundheitsbezug**: Daten zur Gesundheit einer natürlichen Person.
- **ICD-9-CM-Medizincodes**: In der Medizin- und Gesundheitsbranche verwendete Codes.
- **ICD-10-CM-Medizincodes**: In der Medizin- und Gesundheitsbranche verwendete Codes.
- **Referenz zu philosophischen Überzeugungen**: Daten zu den philosophischen Überzeugungen einer natürlichen Person.
- **Referenz zu politischen Meinungen**: Daten zu den politischen Meinungen einer natürlichen Person.

- **Referenz zu religiösen Überzeugungen**: Daten zu den religiösen Überzeugungen einer natürlichen Person.
- **Referenz zum Sexualleben oder zur sexuellen Orientierung**: Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

Kategorientypen

Die Datenklassifizierung kategorisiert Ihre Daten wie folgt.

Die meisten dieser Kategorien sind auf Englisch, Deutsch und Spanisch erkennbar.

Kategorie	Typ	Englisch	Deutsch	Spanisch
Finanzen	Bilanzen	✓	✓	✓
	Bestellungen	✓	✓	✓
	Rechnungen	✓	✓	✓
	Quartalsberichte	✓	✓	✓
Personalwesen	Hintergrundüberprüfungen	✓		✓
	Vergütungspläne	✓	✓	✓
	Arbeitsverträge	✓		✓
	Mitarbeiterbewertungen	✓		✓
	Systemzustand	✓		✓
	Lebensläufe	✓	✓	✓
Rechtliches	Geheimhaltungsvereinbarungen	✓	✓	✓
	Lieferanten-Kunden-Verträge	✓	✓	✓
Marketing	Kampagnen	✓	✓	✓
	Konferenzen	✓	✓	✓
Operationen	Prüfberichte	✓	✓	✓
Verkäufe	Verkaufsaufträge	✓	✓	
Leistungen	RFI	✓		✓
	RFP	✓		✓
	SAU	✓	✓	✓
	Training	✓	✓	✓
Support	Beschwerden und Tickets	✓	✓	✓

Die folgenden Metadaten werden ebenfalls in denselben unterstützten Sprachen kategorisiert und identifiziert:

- Anwendungsdaten
- Archivdateien

- Audio
- Breadcrumbs aus der Datenklassifizierung von Geschäftsanwendungsdaten
- CAD-Dateien
- Code
- Beschädigt
- Datenbank- und Indexdateien
- Designdateien
- E-Mail-Anwendungsdaten
- Verschlüsselt (Dateien mit einem hohen Entropiewert)
- Ausführbare Dateien
- Finanzielle Anwendungsdaten
- Gesundheitsanwendungsdaten
- Bilder
- Protokolle
- Verschiedene Dokumente
- Verschiedene Präsentationen
- Verschiedene Tabellenkalkulationen
- Sonstiges "Unbekannt"
- Passwortgeschützte Dateien
- Strukturierte Daten
- Videos
- Null-Byte-Dateien

Dateitypen

Die Datenklassifizierung durchsucht alle Dateien nach Kategorien und Metadaten und zeigt alle Dateitypen im Abschnitt „Dateitypen“ des Dashboards an. Wenn die Datenklassifizierung personenbezogene Daten (PII) erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt:

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

Genauigkeit der gefundenen Informationen

NetApp kann keine 100-prozentige Genauigkeit der durch die Datenklassifizierung identifizierten personenbezogenen Daten und sensiblen personenbezogenen Daten garantieren. Sie sollten die Informationen immer durch Überprüfung der Daten validieren.

Basierend auf unseren Tests zeigt die folgende Tabelle die Genauigkeit der von der Datenklassifizierung gefundenen Informationen. Wir unterteilen es nach *Präzision* und *Rückruf*:

Präzision

Die Wahrscheinlichkeit, dass das, was die Datenklassifizierung findet, richtig identifiziert wurde. Beispielsweise bedeutet eine Genauigkeitsrate von 90 % für personenbezogene Daten, dass 9 von 10

Dateien, die als personenbezogene Daten identifiziert wurden, tatsächlich personenbezogene Daten enthalten. 1 von 10 Dateien wäre ein falsch positives Ergebnis.

Abrufen

Die Wahrscheinlichkeit, dass die Datenklassifizierung das findet, was sie finden soll. Beispielsweise bedeutet eine Rückrufrate von 70 % für personenbezogene Daten, dass die Datenklassifizierung 7 von 10 Dateien identifizieren kann, die tatsächlich personenbezogene Daten in Ihrem Unternehmen enthalten. Bei der Datenklassifizierung würden 30 % der Daten fehlen und diese würden nicht im Dashboard angezeigt.

Wir verbessern ständig die Genauigkeit unserer Ergebnisse. Diese Verbesserungen werden in zukünftigen Versionen der Datenklassifizierung automatisch verfügbar sein.

Typ	Präzision	Abrufen
Personenbezogene Daten - Allgemein	90 % – 95 %	60 % – 80 %
Personenbezogene Daten - Länderkennungen	30 % – 60 %	40 % – 60 %
Sensible personenbezogene Daten	80 % – 95 %	20 % – 30 %
Kategorien	90 % – 97 %	60 % – 80 %

Erstellen Sie eine benutzerdefinierte Klassifizierung in NetApp Data Classification

Mit NetApp Data Classification können Sie benutzerdefinierte Kategorien oder persönliche Kennungen erstellen, um Daten zu identifizieren, die den regulatorischen und Compliance-Anforderungen Ihrer Organisation entsprechen.

Die Datenklassifizierung unterstützt zwei Arten von benutzerdefinierten Klassifikatoren: Kategorien und persönliche Kennungen. Benutzerdefinierte Kategorien werden auf Basis einer Reihe von Dateien erstellt, die Sie hochladen. Aus diesen Dateien erstellt die Datenklassifizierung ein KI-Modell, um ähnliche Daten in Ihrer Organisation zu identifizieren (beispielsweise könnte ein Unternehmen für Gesundheitsforschung eine Kategorie für klinische Analysen erstellen). Individuelle Kennungen werden mithilfe von Stichwortlisten oder regulären Ausdrücken (Regex) erstellt, um Informationen zu identifizieren, die spezifisch für Ihre Organisation sind und ein Compliance-Risiko darstellen können.

Alle benutzerdefinierten Klassifizierungen sind im Dashboard „Benutzerdefinierte Klassifizierung“ verfügbar.

Erstellen Sie eine benutzerdefinierte persönliche Kennung

Die Datenklassifizierung ermöglicht es Ihnen, mithilfe von Kontext-Schlüsselwörtern oder einem regulären Ausdruck eine benutzerdefinierte persönliche Kennung zu erstellen, um Daten zu identifizieren, die für Ihre Organisation eindeutig sind.

Anforderungen an Schlüsselwörter

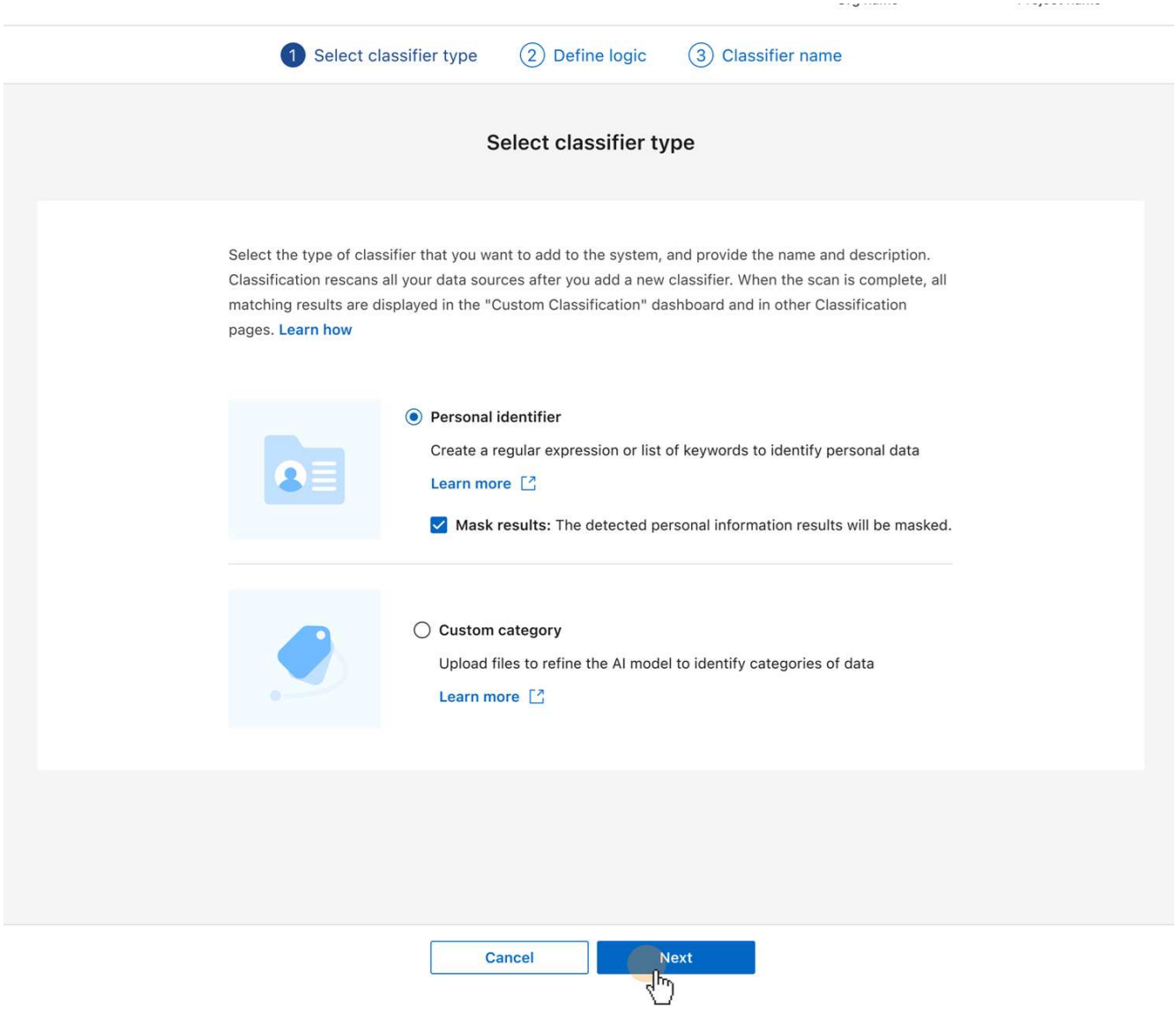
Wenn Sie Ihre persönliche Kennung mithilfe einer Stichwortliste erstellen, muss die Liste folgende Anforderungen erfüllen:

- Bei der Eingabe von Schlüsselwörtern wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- Schlüsselwörter müssen mindestens drei Zeichen lang sein. Wörter mit weniger als drei Zeichen werden ignoriert.

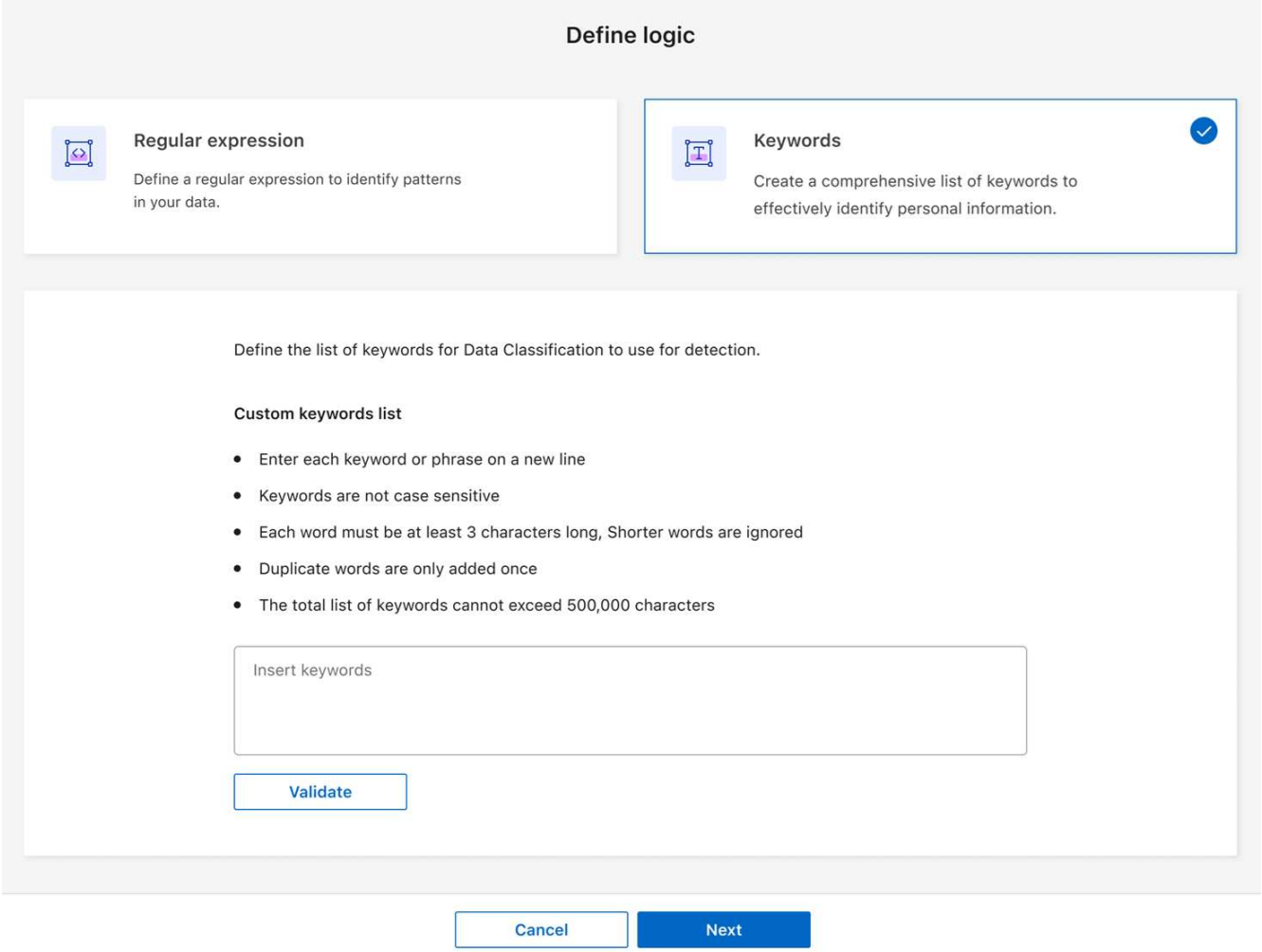
- Doppelte Wörter werden nur einmal hinzugefügt.
- Die Gesamtliste der Schlüsselwörter darf 500.000 Zeichen nicht überschreiten. Die Liste muss mindestens ein Schlüsselwort enthalten.

Schritte

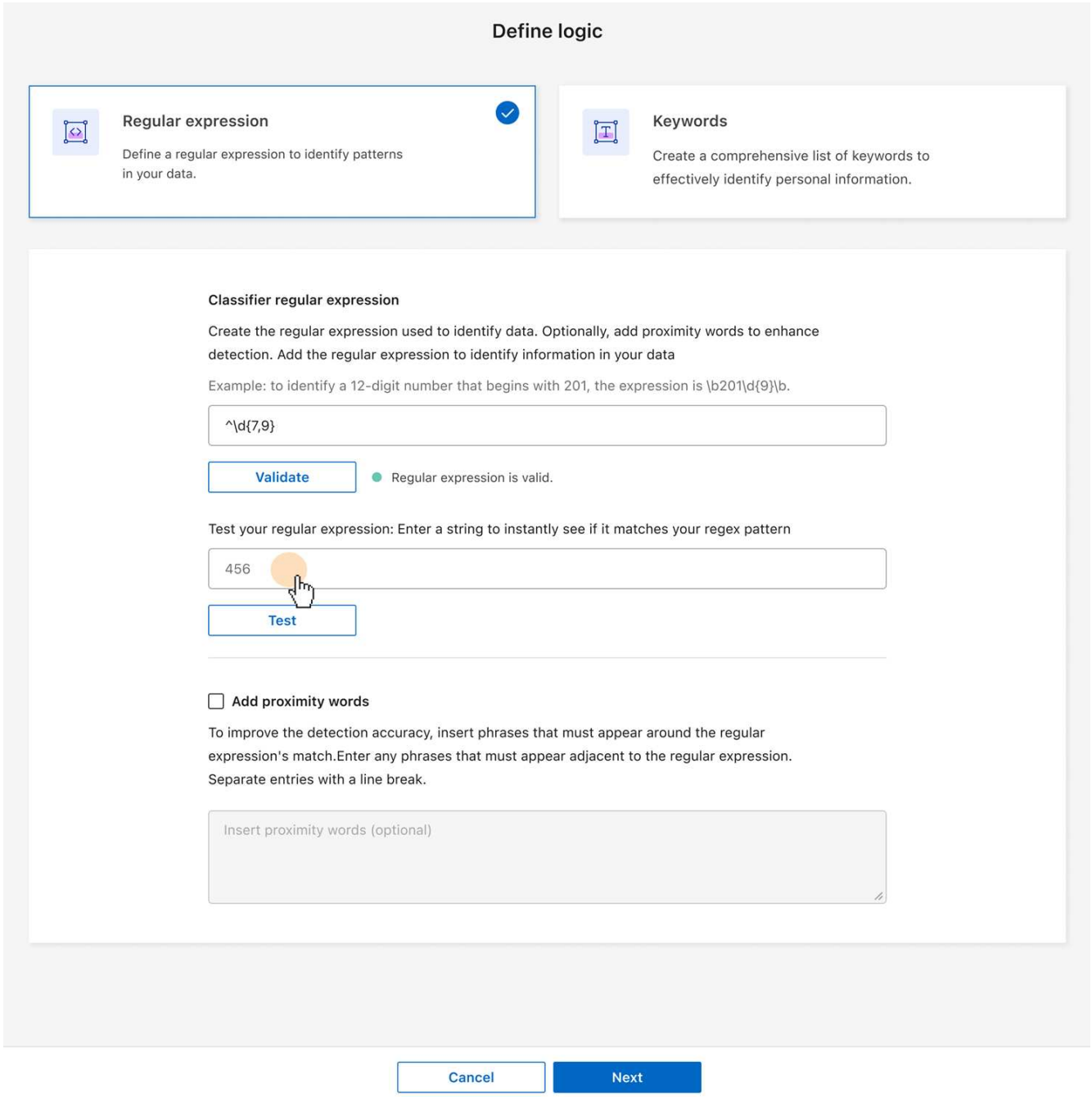
1. Wählen Sie die Registerkarte **Benutzerdefinierte Klassifizierung**.
2. Wählen Sie **+ Neuer Klassifikator**, um den benutzerdefinierten Klassifikator zu erstellen.
3. Wählen Sie **Persönliche Kennung**. Optional können Sie **Ergebnisse maskieren**, um erkannte personenbezogene Daten zu maskieren.
4. Wählen Sie **Weiter**.



5. Um den Klassifikator mit Schlüsselwörtern hinzuzufügen, wählen Sie **Schlüsselwörter** aus. Geben Sie eine Liste von Schlüsselwörtern ein, wobei jeder Eintrag in einer separaten Zeile stehen soll. Stellen Sie sicher, dass die Schlüsselwörter den Anforderungen entsprechen.



Um den Klassifikator als regulären Ausdruck hinzuzufügen, wählen Sie **Regulärer Ausdruck** und fügen Sie dann ein Muster hinzu, um die spezifischen Informationen Ihrer Daten zu erkennen. Wählen Sie **Validieren**, um die Syntax Ihrer Eingabe zu bestätigen.



a. Optional können Sie eine Beispielzeichenfolge eingeben, die Ihrem regulären Ausdrucksmuster entsprechen soll, und dann **Testen** auswählen, um dies zu überprüfen.

b. Optional können Sie Wörter hinzufügen, die die Nähe zueinander beschreiben. Wenn Sie Nähewörter hinzufügen, markiert die Datenklassifizierung das Regex-Muster nur dann, wenn die Nähewörter direkt an die übereinstimmende Zeichenkette angrenzen.

6. Wählen Sie **Weiter**.
7. Geben Sie einen **Klassifikatornamen** und eine **Beschreibung** ein, um die benutzerdefinierte Kategorie in Ihrem Dashboard zu identifizieren.
8. Wählen Sie **Speichern**, um die benutzerdefinierte persönliche Kennung zu erstellen.

Nachdem Sie eine benutzerdefinierte persönliche Kennung erstellt haben, werden deren Ergebnisse beim nächsten geplanten Scan erfasst. Um schneller Ergebnisse zu erhalten, führen Sie einen Scan auf Abruf

durch. Um die Ergebnisse anzuzeigen, siehe Erstellen von Compliance-BerichtenDie

Erstellen Sie eine benutzerdefinierte Kategorie

Mit benutzerdefinierten Kategorien können Sie Daten speziell für Ihre Organisation kategorisieren. Es werden benutzerdefinierte Kategorien auf Basis von Textdateien erstellt, die Sie hochladen. Aus diesen Dateien erstellt die Datenklassifizierung ein KI-Modell, um ähnliche Informationen in anderen Dateien zu identifizieren.

Anforderungen an Trainingsdaten

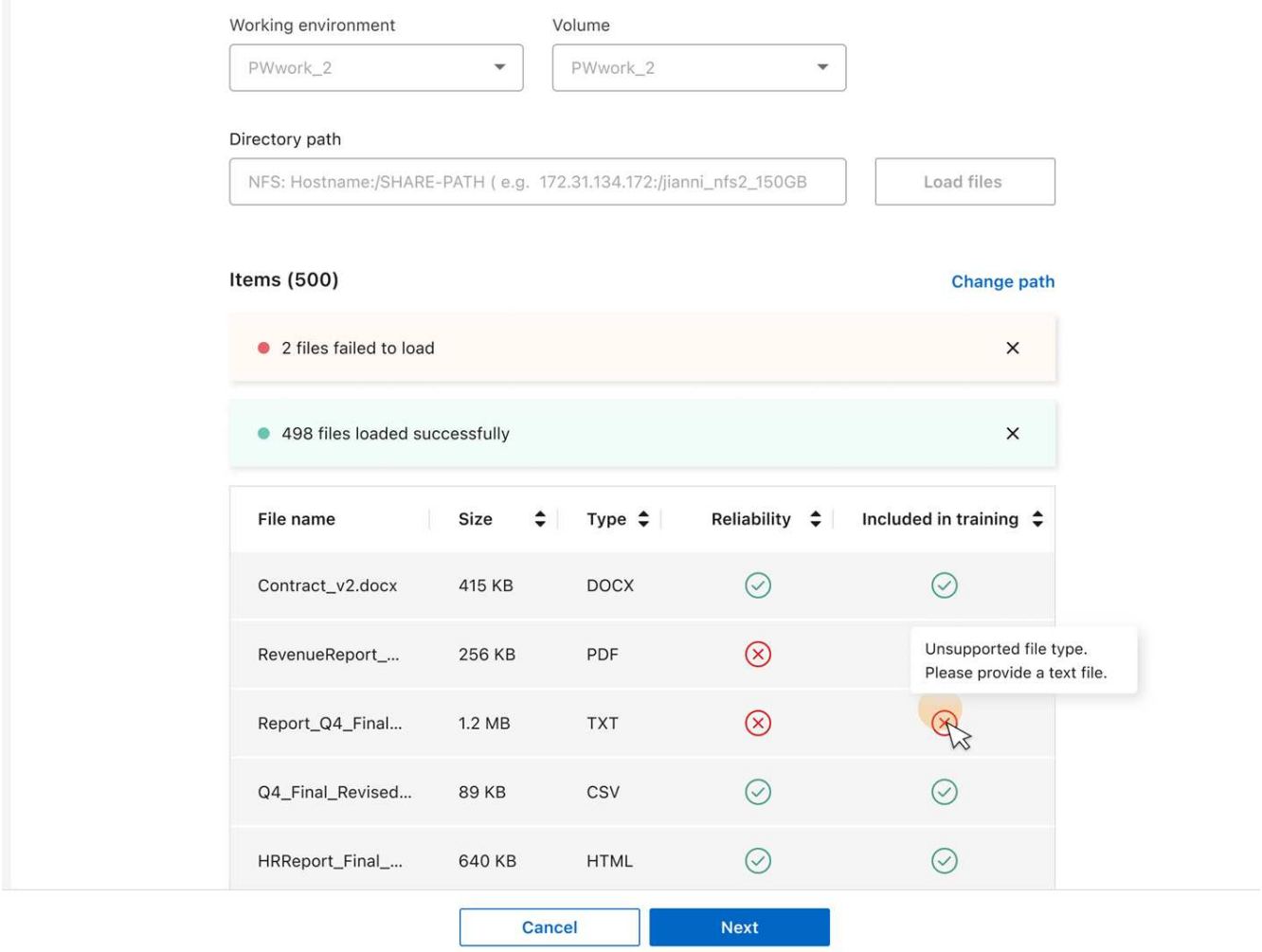
- Der Trainingsdatensatz muss mindestens 25 Dateien enthalten. Die maximale Dateianzahl beträgt 1.000.
- Alle Dateien müssen sich direkt im von Ihnen angegebenen Dateipfad befinden.
- Alle Dateien müssen größer als 100 Byte sein.
- Die Trainingsdaten für die Datenklassifizierung müssen in einem der folgenden Dateitypen vorliegen: CSV, DOCX, DOC, GZ, JSON, PDF, PPTX, TXT, RTT, XLS oder XLSX. Sie können eine Kombination aller unterstützten Dateitypen hochladen.

Schritte

1. Wählen Sie in NetApp Data Classification die Option **Benutzerdefinierte Klassifizierung**.
2. **+ Neuer Klassifikator** auswählen.
3. Wählen Sie als Klassifizierungstyp **Benutzerdefinierte Kategorie** und klicken Sie dann auf **Weiter**.
4. Definieren Sie die Logik für Ihre benutzerdefinierte Kategorie mithilfe einer Sammlung textbasierter Dateien. Geben Sie die IP-Adresse der **Arbeitsadresse** ein und wählen Sie dann das **Volume** aus dem Dropdown-Menü aus.

   Geben Sie den **Verzeichnispfad** für das Verzeichnis ein, das die Trainingsdaten enthält.

5. Wählen Sie für die Datenklassifizierung **Dateien laden**, um eine Überprüfung der Dateien durchzuführen. Sie können die Zusammenfassung der Dateien einsehen, in der Dateiname, Größe, Typ und Hinweise aufgeführt sind, falls die Datei für Schulungszwecke als geeignet eingestuft wurde.



Data Classification zeigt die voraussichtliche Abschlusszeit für das Datentraining an. .. Um den Dateipfad zu ändern oder Dateien erneut hochzuladen, wählen Sie **Change path**, geben Sie die Daten ein und laden Sie die Dateien erneut.

6. Wenn Sie mit den hochgeladenen Dateien zufrieden sind, wählen Sie **Weiter**.
7. Geben Sie einen **Klassifikatornamen** und eine **Beschreibung** ein, um die benutzerdefinierte Kategorie in Ihrem Dashboard zu identifizieren.
8. Wählen Sie **Speichern**, um die benutzerdefinierte Kategorie zu erstellen.

Ergebnis

Nachdem Sie eine benutzerdefinierte Kategorie erstellt haben, werden deren Ergebnisse beim nächsten geplanten Scan erfasst. Um schneller Ergebnisse zu erhalten, starten Sie den Scan manuell.

Bearbeiten Sie einen benutzerdefinierten Klassifikator

Sie können die Logik einer persönlichen Kennung auch nach deren Erstellung ändern. Sie können weder den Typ der persönlichen Kennung noch den Logiktyp ändern; beispielsweise können Sie eine benutzerdefinierte Kategorie nicht in eine benutzerdefinierte persönliche Kennung ändern. Außerdem können Sie einen auf Schlüsselwörtern basierenden benutzerdefinierten Bezeichner nicht in einen auf regulären Ausdrücken basierenden benutzerdefinierten Bezeichner ändern.

Schritte

1. Wählen Sie in NetApp Data Classification die Option **Benutzerdefinierte Klassifizierung**.
2. Identifizieren Sie den Klassifikator, den Sie löschen möchten, und wählen Sie dann das Aktionsmenü aus. … am Ende seiner Reihe.
3. Wählen Sie **Logik bearbeiten**.
4. Wenn Sie Schlüsselwörter ändern, fügen Sie die entsprechenden Schlüsselwörter hinzu, löschen oder bearbeiten Sie sie. Wenn Sie einen regulären Ausdruck ändern, geben Sie den neuen regulären Ausdruck ein und überprüfen Sie ihn. Optional können Sie Nähe-Keywords hinzufügen.
5. Wählen Sie **Speichern**, um die Änderungen zu übernehmen.

Einen benutzerdefinierten Klassifikator löschen

1. Wählen Sie in NetApp Data Classification die Option **Benutzerdefinierte Klassifizierung**.
2. Identifizieren Sie den Klassifikator, den Sie löschen möchten, und wählen Sie dann das Aktionsmenü aus. … am Ende seiner Reihe.
3. Wählen Sie **Klassifikator löschen**.

Nächste Schritte

- Erstellen von Compliance-Berichten

Untersuchen Sie die in Ihrem Unternehmen gespeicherten Daten mit NetApp Data Classification

Das Data Investigation-Dashboard bietet Einblicke in Ihre Daten auf Datei- und Verzeichnisebene und ermöglicht Ihnen das Sortieren und Filtern der Ergebnisse. Die Seite „Datenuntersuchung“ bietet Einblicke in Datei- und Verzeichnismetadaten und -berechtigungen und identifiziert doppelte Dateien. Mit Einblicken auf Datei-, Verzeichnis- und Datenbankebene können Sie Maßnahmen ergreifen, um die Compliance Ihres Unternehmens zu verbessern und Speicherplatz zu sparen. Die Seite „Datenuntersuchung“ unterstützt auch das Verschieben, Kopieren und Löschen von Dateien.

Um Erkenntnisse aus der Untersuchungsseite zu gewinnen, müssen Sie einen vollständigen Klassifizierungsscan Ihrer Datenquellen durchführen. Datenquellen, bei denen nur ein Mapping-Scan durchgeführt wurde, zeigen keine Details auf Dateiebene an.

Struktur der Datenuntersuchung

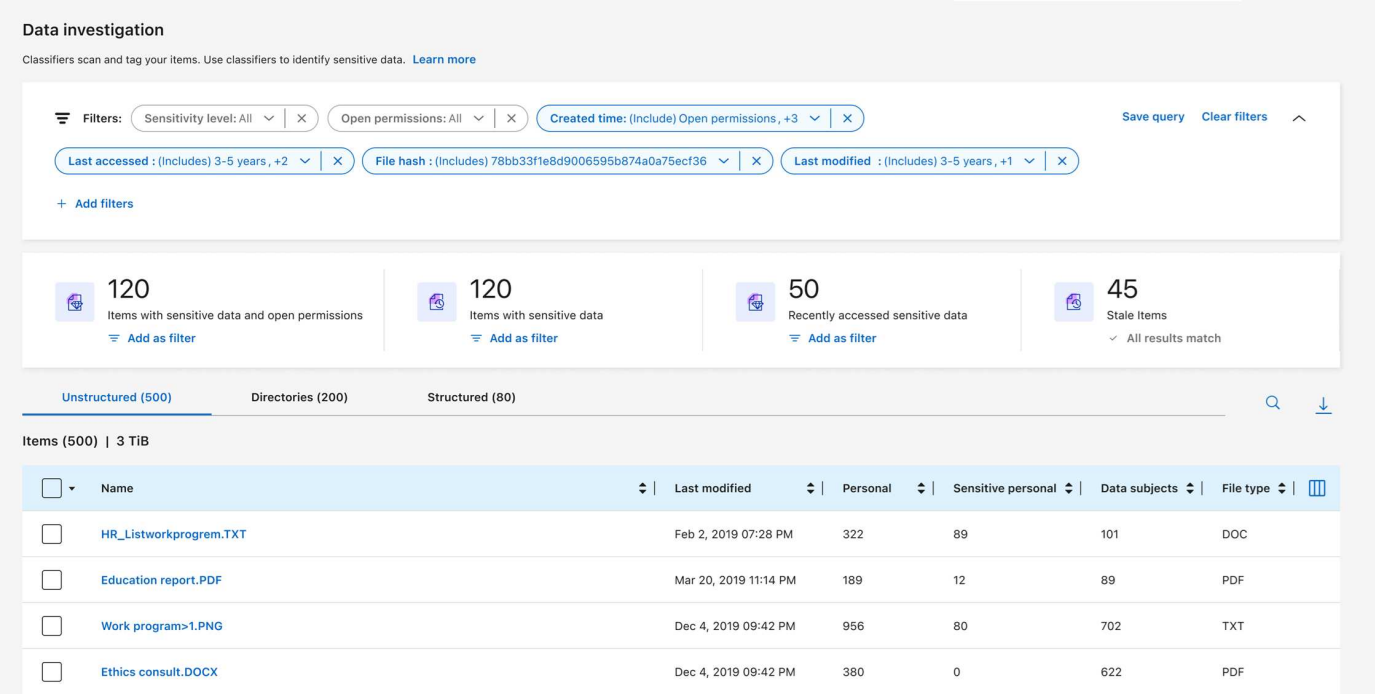
Auf der Seite „Datenuntersuchung“ werden die Daten in drei Registerkarten sortiert:

- **Unstrukturierte Daten**: Dateidaten
- **Verzeichnisse**: Ordner und Dateifreigaben
- **Strukturiert**: Datenbank

Datenfilter

Die Seite „Datenuntersuchung“ bietet zahlreiche Filter zum Sortieren Ihrer Daten, damit Sie das finden, was Sie benötigen. Sie können mehrere Filter gleichzeitig verwenden.

Um einen Filter hinzuzufügen, wählen Sie die Schaltfläche **Filter hinzufügen**.



Filterempfindlichkeit und Inhalt

Verwenden Sie die folgenden Filter, um anzuzeigen, wie viele vertrauliche Informationen Ihre Daten enthalten.

Filter	Details
Kategorie	Wählen Sie die"Arten von Kategorien" .
Empfindlichkeitsstufe	Wählen Sie die Empfindlichkeitsstufe: Persönlich, Persönlich sensibel oder Nicht sensibel.
Anzahl der Kennungen	Wählen Sie den Bereich der erkannten vertraulichen Kennungen pro Datei aus. Umfasst personenbezogene Daten und sensible personenbezogene Daten. Beim Filtern in Verzeichnissen summiert die Datenklassifizierung die Übereinstimmungen aller Dateien in jedem Ordner (und Unterordnern). HINWEIS: In der Version vom Dezember 2023 (Version 1.26.6) wurde die Option zum Berechnen der Anzahl personenbezogener Daten (PII) nach Verzeichnissen entfernt.
Personenbezogene Daten	Wählen Sie die"Arten personenbezogener Daten" .
Sensible personenbezogene Daten	Wählen Sie die"Arten sensibler personenbezogener Daten" .
Betroffener	Geben Sie den vollständigen Namen oder eine bekannte Kennung einer betroffenen Person ein. "Erfahren Sie hier mehr über betroffene Personen" .

Benutzereigentümer und Benutzerberechtigungen filtern

Verwenden Sie die folgenden Filter, um Dateieigentümer und Berechtigungen für den Zugriff auf Ihre Daten anzuzeigen.

Filter	Details
Berechtigungen öffnen	Wählen Sie die Art der Berechtigungen innerhalb der Daten und innerhalb von Ordnern/Freigaben aus.
Benutzer-/Gruppenberechtigungen	Wählen Sie einen oder mehrere Benutzernamen und/oder Gruppennamen aus oder geben Sie einen Teilnamen ein.
Dateieigentümer	Geben Sie den Namen des Dateieigentümers ein.
Anzahl der Benutzer mit Zugriff	Wählen Sie einen oder mehrere Kategoriebereiche aus, um anzuzeigen, welche Dateien und Ordner für eine bestimmte Anzahl von Benutzern geöffnet sind.

Chronologisch filtern

Verwenden Sie die folgenden Filter, um Daten basierend auf Zeitkriterien anzuzeigen.

Filter	Details
Erstellungszeit	Wählen Sie einen Zeitraum aus, in dem die Datei erstellt wurde. Sie können auch einen benutzerdefinierten Zeitraum angeben, um die Suchergebnisse weiter zu verfeinern.
Entdeckte Zeit	Wählen Sie einen Zeitraum aus, in dem die Datenklassifizierung die Datei entdeckt hat. Sie können auch einen benutzerdefinierten Zeitraum angeben, um die Suchergebnisse weiter zu verfeinern.
Zuletzt geändert	Wählen Sie einen Zeitraum aus, in dem die Datei zuletzt geändert wurde. Sie können auch einen benutzerdefinierten Zeitraum angeben, um die Suchergebnisse weiter zu verfeinern.
Letzter Zugriff	Wählen Sie einen Zeitraum aus, in dem zuletzt auf die Datei oder das Verzeichnis* zugegriffen wurde. Sie können auch einen benutzerdefinierten Zeitraum angeben, um die Suchergebnisse weiter zu verfeinern. Bei den Dateitypen, die von Data Classification gescannt werden, ist dies der letzte Zeitpunkt, zu dem Data Classification die Datei gescannt hat.

* Die letzte Zugriffszeit für ein Verzeichnis ist nur für NFS- oder CIFS-Freigaben verfügbar.

Metadaten filtern

Verwenden Sie die folgenden Filter, um Daten basierend auf Standort, Größe und Verzeichnis oder Dateityp anzuzeigen.

Filter	Details
Dateipfad	Geben Sie bis zu 20 Teil- oder Vollpfade ein, die Sie in die Abfrage einschließen oder aus ihr ausschließen möchten. Wenn Sie sowohl Einschlusspfade als auch Ausschlusspfade eingeben, sucht die Datenklassifizierung zuerst nach allen Dateien in den eingeschlossenen Pfaden, entfernt dann Dateien aus ausgeschlossenen Pfaden und zeigt anschließend die Ergebnisse an. Beachten Sie, dass die Verwendung von „*“ in diesem Filter keine Wirkung hat und dass Sie bestimmte Ordner nicht vom Scan ausschließen können – alle Verzeichnisse und Dateien unter einer konfigurierten Freigabe werden gescannt.
Verzeichnistyp	Wählen Sie den Verzeichnistyp aus: entweder „Freigeben“ oder „Ordner“.
Dateityp	Wählen Sie die"Dateitypen" .
Dateigröße	Wählen Sie den Dateigrößenbereich aus.
Datei-Hash	Geben Sie den Hash der Datei ein, um eine bestimmte Datei zu finden, auch wenn der Name anders ist.

Filterspeichertyp

Verwenden Sie die folgenden Filter, um Daten nach Speichertyp anzuzeigen.

Filter	Details
Systemtyp	Wählen Sie den Systemtyp aus.
Name der Systemumgebung	Wählen Sie bestimmte Systeme aus.
Speicher-Repository	Wählen Sie das Speicherrepository aus, beispielsweise ein Volume oder ein Schema.

Filterabfrage

Verwenden Sie den folgenden Filter, um Daten nach gespeicherten Abfragen anzuzeigen.

Filter	Details
Gespeicherte Abfrage	Wählen Sie eine oder mehrere gespeicherte Abfragen aus. Gehen Sie zum"Registerkarte „Gespeicherte Abfragen“" , um die Liste der vorhandenen gespeicherten Abfragen anzuzeigen und neue zu erstellen.
Schlagwörter	Wählen"das Tag oder die Tags" die Ihren Dateien zugewiesen sind.

Filteranalysestatus

Verwenden Sie den folgenden Filter, um Daten nach dem Scanstatus der Datenklassifizierung anzuzeigen.

Filter	Details
Analysestatus	Wählen Sie eine Option aus, um die Liste der Dateien anzuzeigen, deren erster Scan aussteht, deren Scan abgeschlossen ist, deren erneuter Scan aussteht oder deren Scan fehlgeschlagen ist.

Filter	Details
Scan-Analyse-Ereignis	Wählen Sie aus, ob Sie Dateien anzeigen möchten, die nicht klassifiziert wurden, weil die Datenklassifizierung den letzten Zugriffszeitpunkt nicht wiederherstellen konnte, oder Dateien, die klassifiziert wurden, obwohl die Datenklassifizierung den letzten Zugriffszeitpunkt nicht wiederherstellen konnte.

"Details zum Zeitstempel „Letzter Zugriff“ anzeigen"Weitere Informationen zu den Elementen, die auf der Untersuchungsseite angezeigt werden, wenn Sie mithilfe des Scan-Analyse-Ereignisses filtern.

Daten nach Duplikaten filtern

Verwenden Sie den folgenden Filter, um Dateien anzuzeigen, die in Ihrem Speicher dupliziert sind.

Filter	Details
Duplikate	Wählen Sie aus, ob die Datei in den Repositories dupliziert wird.

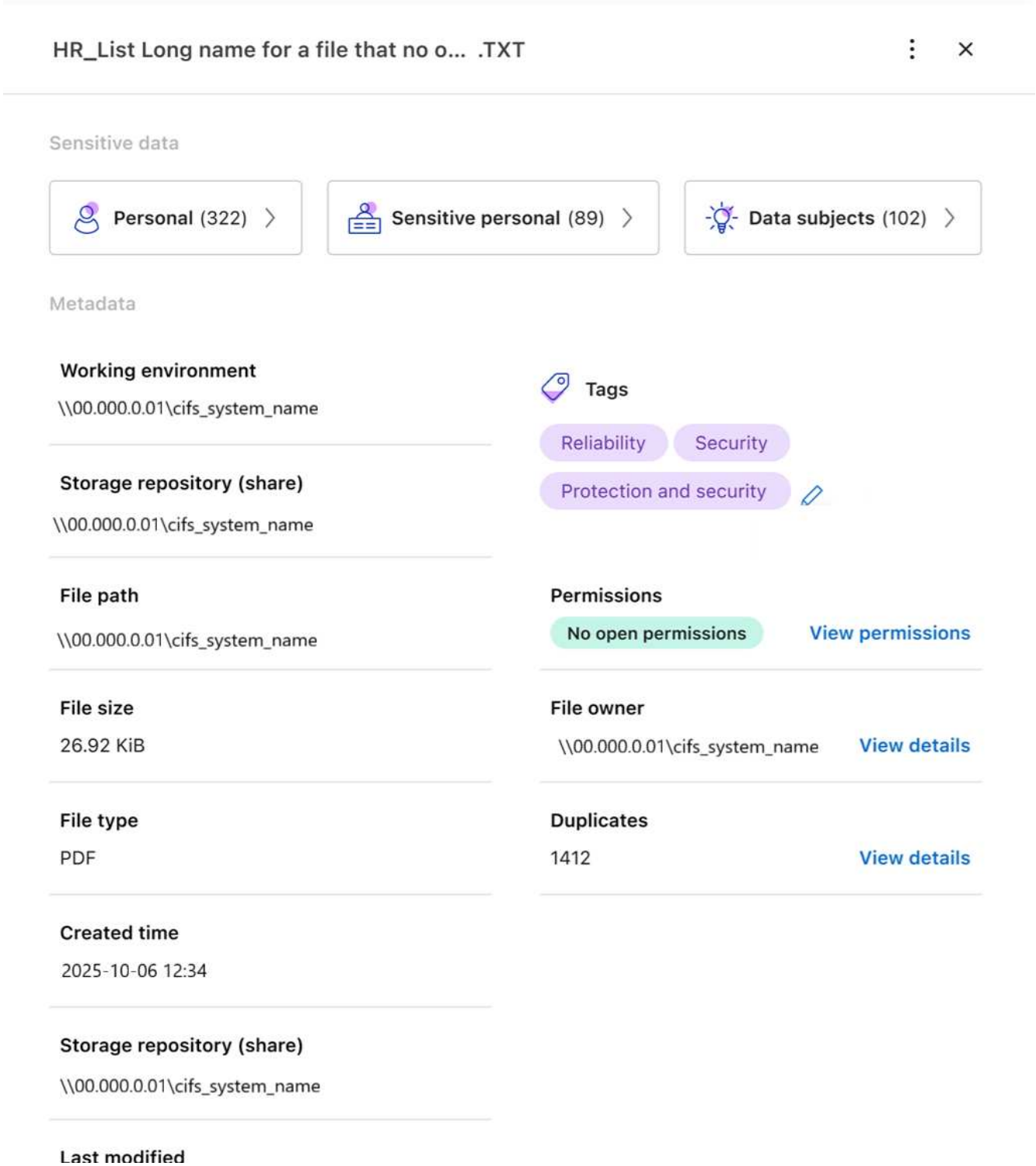
Dateimetadaten anzeigen

Die Metadaten zeigen Ihnen nicht nur das System und das Volume an, auf dem sich die Datei befindet, sondern enthalten auch viele weitere Informationen, darunter die Dateiberechtigungen, den Dateieigentümer und ob es Duplikate dieser Datei gibt. Diese Informationen sind nützlich, wenn Sie planen,"Erstellen gespeicherter Abfragen" weil Sie alle Informationen sehen, die Sie zum Filtern Ihrer Daten verwenden können.

Die Verfügbarkeit von Informationen hängt von der Datenquelle ab. Beispielsweise werden Volumename und Berechtigungen für Datenbankdateien nicht freigegeben.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Untersuchung“ aus.
2. Wählen Sie in der Liste „Datenuntersuchung“ auf der rechten Seite das Abwärtspfeilzeichen rechts für jede einzelne Datei, um die Dateimetadaten anzuzeigen.



3. Optional können Sie mit der Schaltfläche **Tag erstellen** ein Tag erstellen oder der Datei hinzufügen. Wählen Sie ein vorhandenes Tag aus dem Dropdown-Menü aus oder fügen Sie mit der Schaltfläche **+ Hinzufügen** ein neues Tag hinzu. Tags können zum Filtern von Daten verwendet werden.

Benutzerberechtigungen für Dateien und Verzeichnisse anzeigen

Um eine Liste aller Benutzer oder Gruppen anzuzeigen, die Zugriff auf eine Datei oder ein Verzeichnis haben, sowie die Art ihrer Berechtigungen, wählen Sie **Alle Berechtigungen anzeigen**. Diese Option ist nur für Daten in CIFS-Freigaben verfügbar.

Wenn Sie Sicherheitskennungen (SIDs) anstelle von Benutzer- und Gruppennamen verwenden, sollten Sie Ihr Active Directory in die Datenklassifizierung integrieren. Weitere Informationen finden Sie unter "Active Directory zur Datenklassifizierung hinzufügen" .

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Untersuchung“ aus.
2. Wählen Sie in der Liste „Datenuntersuchung“ auf der rechten Seite das Abwärtspfeilzeichen rechts für jede einzelne Datei, um die Dateimetadaten anzuzeigen.
3. Um eine Liste aller Benutzer oder Gruppen anzuzeigen, die Zugriff auf eine Datei oder ein Verzeichnis haben, sowie die Art ihrer Berechtigungen, wählen Sie im Feld „Öffnen Sie Berechtigungen“ die Option „Alle Berechtigungen anzeigen“ aus.

   Die Datenklassifizierung zeigt bis zu 100 Benutzer in der Liste an.

4. Wählen Sie das Abwärtspfeilzeichen Klicken Sie für jede Gruppe auf die Schaltfläche, um die Liste der Benutzer anzuzeigen, die Teil der Gruppe sind.

   Sie können eine Ebene der Gruppe erweitern, um die Benutzer anzuzeigen, die Teil der Gruppe sind.

5. Wählen Sie den Namen eines Benutzers oder einer Gruppe aus, um die Untersuchungsseite zu aktualisieren, sodass Sie alle Dateien und Verzeichnisse sehen können, auf die der Benutzer oder die Gruppe Zugriff hat.

Suchen Sie in Ihren Speichersystemen nach doppelten Dateien

Sie können überprüfen, ob in Ihren Speichersystemen doppelte Dateien gespeichert werden. Dies ist nützlich, wenn Sie Bereiche identifizieren möchten, in denen Sie Speicherplatz sparen können. Außerdem sollten Sie sicherstellen, dass bestimmte Dateien mit speziellen Berechtigungen oder vertraulichen Informationen nicht unnötig in Ihren Speichersystemen dupliziert werden.

Die Datenklassifizierung vergleicht alle Dateien (mit Ausnahme von Datenbanken) auf Duplikate, falls diese:

- 1 MB oder mehr
- Oder enthalten persönliche oder sensible persönliche Informationen

Bei der Datenklassifizierung wird Hashing-Technologie verwendet, um doppelte Dateien zu ermitteln. Wenn zwei Dateien denselben Hash-Code haben, handelt es sich um exakte Duplikate, selbst wenn die Dateinamen unterschiedlich sind.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Untersuchung“ aus.
2. Wählen Sie im Filterbereich „Dateigröße“ zusammen mit „Duplikate“ („Hat Duplikate“) aus, um zu sehen, welche Dateien eines bestimmten Größenbereichs in Ihrer Umgebung dupliziert sind.
3. Laden Sie optional die Liste der doppelten Dateien herunter und senden Sie sie an Ihren Speicheradministrator, damit dieser entscheiden kann, welche Dateien ggf. gelöscht werden können.
4. Optional können Sie die doppelten Dateien löschen, markieren oder verschieben. Wählen Sie die Dateien aus, für die Sie eine Aktion ausführen möchten, und wählen Sie dann die entsprechende Aktion aus.

Anzeigen, ob eine bestimmte Datei dupliziert ist

Sie können sehen, ob eine einzelne Datei Duplikate enthält.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Untersuchung“ aus.
2. Wählen Sie in der Liste „Datenuntersuchung“ rechts für jede einzelne Datei, um die Dateimetadaten anzuzeigen.

   Wenn für eine Datei Duplikate vorhanden sind, wird diese Information neben dem Feld *Duplikate* angezeigt.

3. Um die Liste der doppelten Dateien und ihren Speicherort anzuzeigen, wählen Sie **Details anzeigen**.
4. Wählen Sie auf der nächsten Seite **Duplikate anzeigen** aus, um die Dateien auf der Untersuchungsseite anzuzeigen.
5. Optional können Sie die doppelten Dateien löschen, markieren oder verschieben. Wählen Sie die Dateien aus, für die Sie eine Aktion ausführen möchten, und wählen Sie dann die entsprechende Aktion aus.

Sie können den auf dieser Seite bereitgestellten „Datei-Hash“-Wert verwenden und ihn jederzeit direkt auf der Untersuchungsseite eingeben, um nach einer bestimmten doppelten Datei zu suchen – oder Sie können ihn in einer gespeicherten Abfrage verwenden.

Laden Sie Ihren Bericht herunter

Sie können Ihre gefilterten Ergebnisse im CSV- oder JSON-Format herunterladen.

Es können bis zu drei Berichtsdateien heruntergeladen werden, wenn die Datenklassifizierung Dateien (unstrukturierte Daten), Verzeichnisse (Ordner und Dateifreigaben) und Datenbanken (strukturierte Daten) scannt.

Die Dateien werden in Dateien mit einer festen Anzahl von Zeilen oder Datensätzen aufgeteilt:

- JSON: 100.000 Datensätze pro Bericht, dessen Generierung etwa 5 Minuten dauert
- CSV: 200.000 Datensätze pro Bericht, dessen Generierung etwa 4 Minuten dauert

Sie können eine Version der CSV-Datei herunterladen und in diesem Browser anzeigen. Diese Version ist auf 10.000 Datensätze beschränkt.

Was ist im herunterladbaren Bericht enthalten?

Der **Datenbericht zu unstrukturierten Dateien** enthält die folgenden Informationen zu Ihren Dateien:

- Dateiname
- Standorttyp
- Systemname
- Speicherrepository (z. B. ein Volume, Bucket, Freigaben)
- Repository-Typ
- Dateipfad
- Dateityp
- Dateigröße (in MB)

- Erstellungszeit
- Zuletzt geändert
- Letzter Zugriff
- Dateieigentümer
  - Zu den Dateieigentümerdaten gehören Kontoname, SAM-Kontoname und E-Mail-Adresse, wenn Active Directory konfiguriert ist.
- Kategorie
- Persönliche Informationen
- Sensible persönliche Informationen
- Berechtigungen öffnen
- Scan-Analysefehler
- Datum der Löschungserkennung

  Das Löscherkennungsdatum gibt das Datum an, an dem die Datei gelöscht oder verschoben wurde. Auf diese Weise können Sie erkennen, wann vertrauliche Dateien verschoben wurden. Gelöschte Dateien werden nicht zur Anzahl der Dateien gezählt, die im Dashboard oder auf der Untersuchungsseite angezeigt werden. Die Dateien erscheinen nur in den CSV-Berichten.

Der **Bericht zu unstrukturierten Verzeichnisdaten** enthält die folgenden Informationen zu Ihren Ordnern und Dateifreigaben:

- Systemtyp
- Systemname
- Verzeichnisname
- Speicherrepository (z. B. ein Ordner oder Dateifreigaben)
- Verzeichnisbesitzer
- Erstellungszeit
- Entdeckte Zeit
- Zuletzt geändert
- Letzter Zugriff
- Berechtigungen öffnen
- Verzeichnistyp

Der **Strukturierter Datenbericht** enthält die folgenden Informationen zu Ihren Datenbanktabellen:

- DB-Tabellenname
- Standorttyp
- Systemname
- Speicherrepository (z. B. ein Schema)
- Spaltenanzahl
- Zeilenanzahl
- Persönliche Informationen

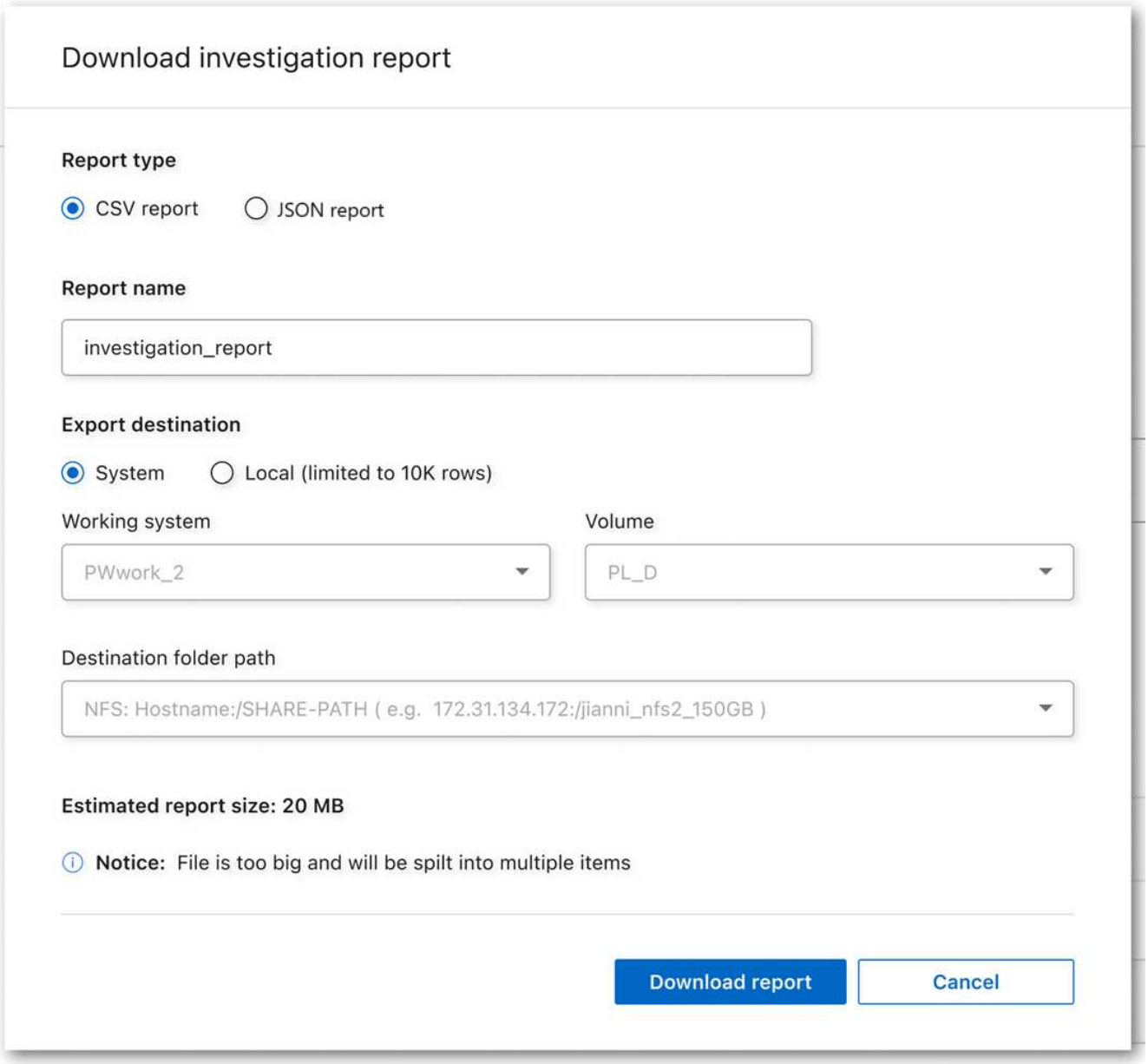
- Sensible persönliche Informationen

Schritte zum Erstellen des Berichts

1. Wählen Sie auf der Seite „Datenuntersuchung“ die Schaltfläche oben rechts auf der Seite.
2. Wählen Sie den Berichtstyp: CSV oder JSON.
3. Geben Sie einen **Berichtsnamen** ein.
4. Um den vollständigen Bericht herunterzuladen, wählen Sie **System** und dann **System** und **Lautstärke** aus den jeweiligen Dropdown-Menüs. Geben Sie einen **Zielordnerpfad** an.

   Um den Bericht im Browser herunterzuladen, wählen Sie **Lokal** aus. Beachten Sie, dass diese Option den Bericht auf die ersten 10.000 Zeilen beschränkt und auf das **CSV**-Format beschränkt ist. Wenn Sie **Lokal** auswählen, müssen Sie keine weiteren Felder ausfüllen.

5. Wählen Sie **Bericht herunterladen**.



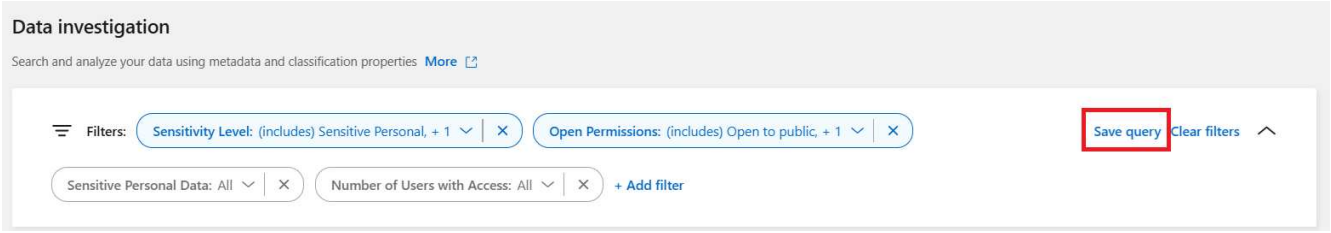
Ergebnis

In einem Dialogfeld wird die Meldung angezeigt, dass die Berichte heruntergeladen werden.

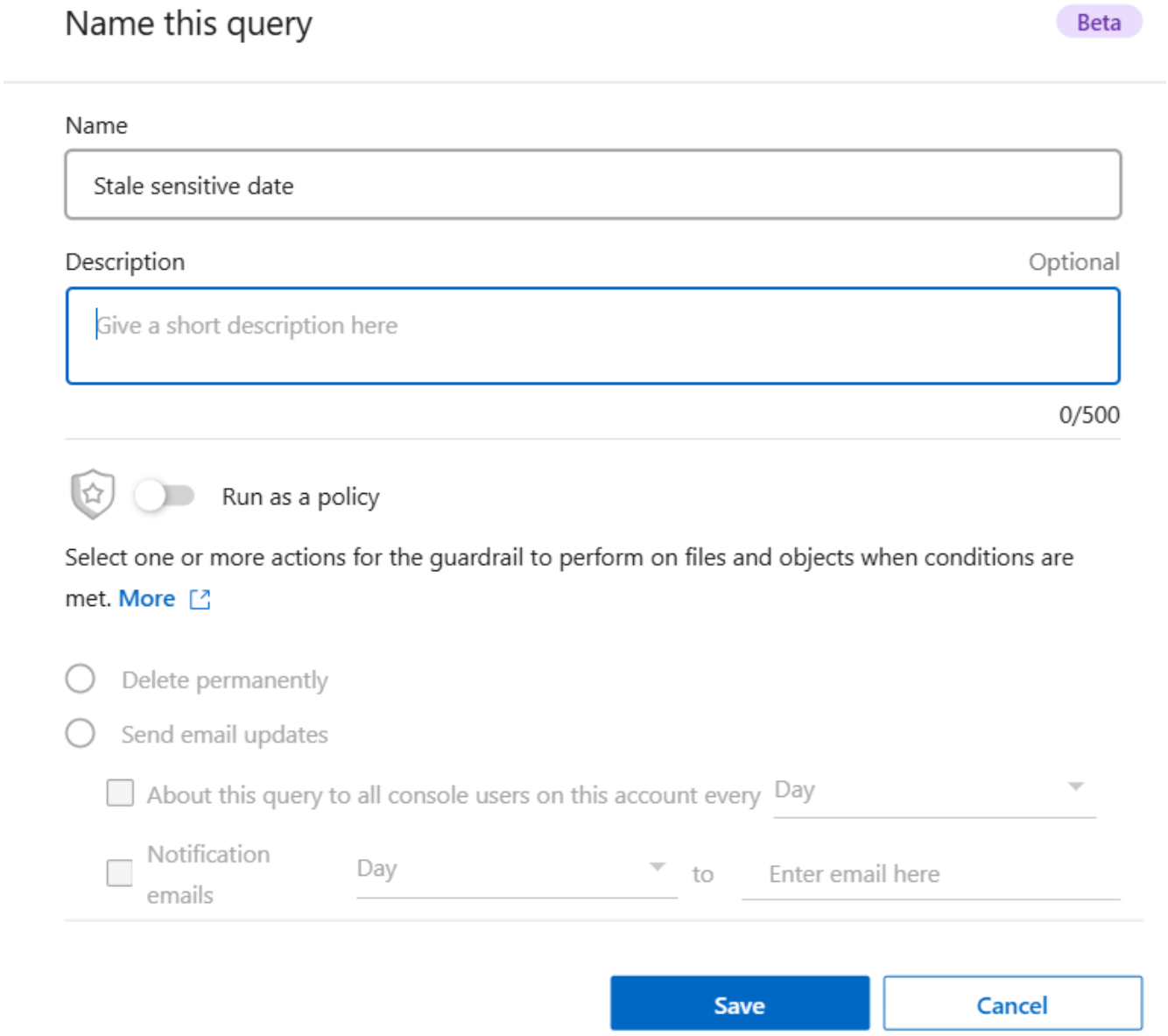
Erstellen Sie eine gespeicherte Abfrage basierend auf ausgewählten Filtern

Schritte

1. Definieren Sie auf der Registerkarte „Untersuchung“ eine Suche, indem Sie die gewünschten Filter auswählen. Sehen"Filtern von Daten auf der Seite „Untersuchung“" für Details.
2. Wenn Sie alle Filtereigenschaften nach Ihren Wünschen eingestellt haben, wählen Sie **Abfrage speichern**.



3. Benennen Sie die gespeicherte Abfrage und fügen Sie eine Beschreibung hinzu. Der Name muss eindeutig sein.
4. Optional können Sie die Abfrage als Richtlinie speichern:
   a. Um die Abfrage als Richtlinie zu speichern, schalten Sie den Schalter **Als Richtlinie ausführen** um.
   b. Wählen Sie **Dauerhaft löschen** oder **E-Mail-Updates senden**. Wenn Sie E-Mail-Updates auswählen, können Sie die Abfrageergebnisse täglich, wöchentlich oder monatlich per E-Mail an *alle* Konsolenbenutzer senden. Alternativ können Sie die Benachrichtigung in der gleichen Häufigkeit an bestimmte E-Mail-Adressen senden.
5. Wählen Sie **Speichern**.



Nachdem Sie die Suche oder Richtlinie erstellt haben, können Sie sie auf der Registerkarte **Gespeicherte Abfragen** anzeigen.

Es kann bis zu 15 Minuten dauern, bis die Ergebnisse auf der Seite „Gespeicherte Abfragen“ angezeigt werden.

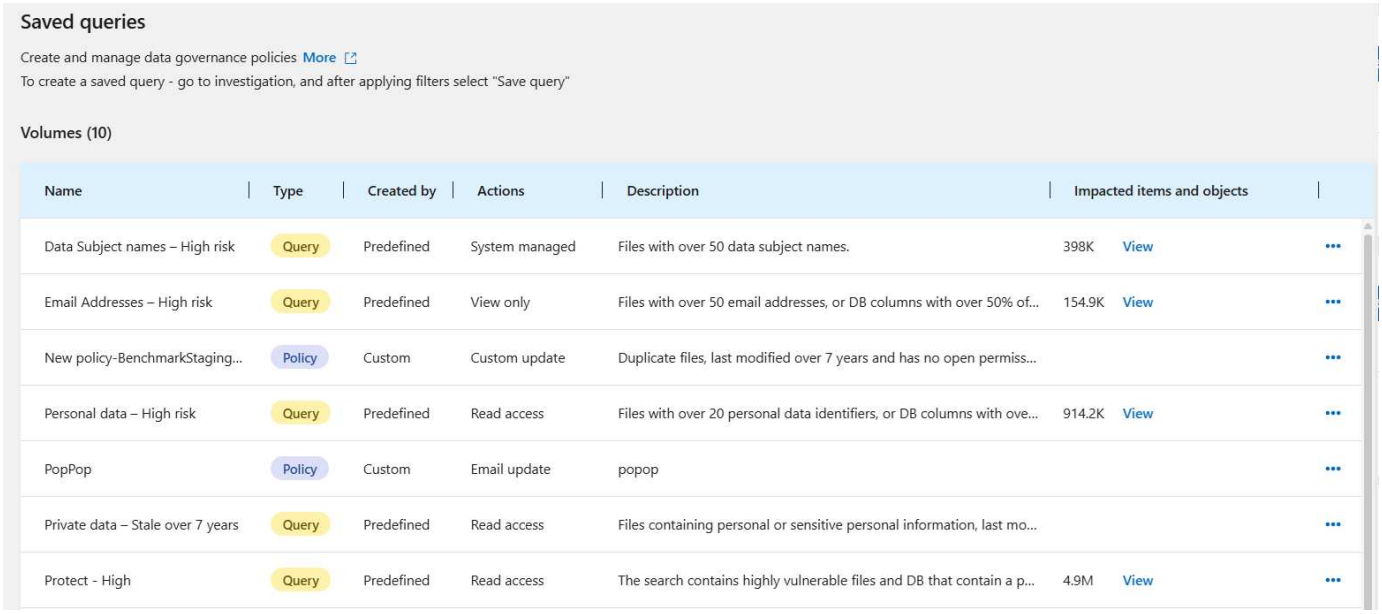
Verwalten gespeicherter Abfragen mit NetApp Data Classification

NetaApp Data Classification unterstützt das Speichern Ihrer Suchanfragen. Mit einer gespeicherten Abfrage können Sie benutzerdefinierte Filter erstellen, um häufige Abfragen Ihrer Datenuntersuchungsseite zu sortieren. Die Datenklassifizierung umfasst auch vordefinierte gespeicherte Abfragen basierend auf häufigen Anfragen.

Die Registerkarte **Gespeicherte Abfragen** im Compliance-Dashboard listet alle vordefinierten und benutzerdefinierten gespeicherten Abfragen auf, die für diese Instanz der Datenklassifizierung verfügbar sind.

Gespeicherte Abfragen können auch als **Richtlinien** gespeichert werden. Während Abfragen Daten filtern, ermöglichen Richtlinien Ihnen, auf die Daten zu reagieren. Mit einer Richtlinie: Sie können erkannte Daten löschen oder E-Mail-Updates zu den erkannten Daten senden.

Gespeicherte Abfragen werden auch in der Filterliste auf der Untersuchungsseite angezeigt.



Anzeigen der Ergebnisse gespeicherter Abfragen auf der Seite „Untersuchung“

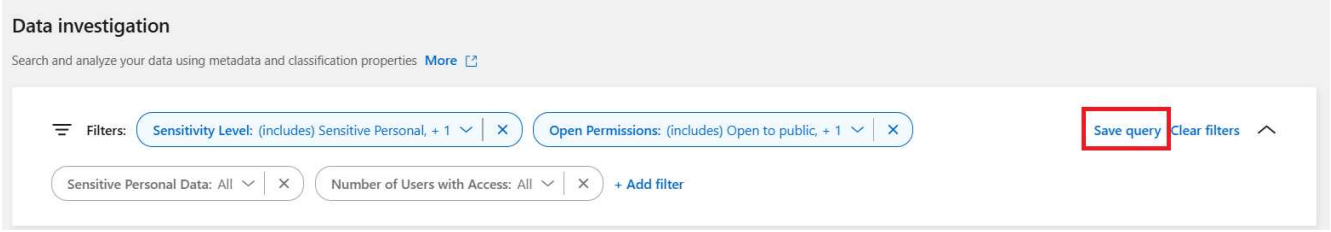
Um die Ergebnisse einer gespeicherten Abfrage auf der Seite „Untersuchung“ anzuzeigen, wählen Sie das Klicken Sie auf die Schaltfläche für eine bestimmte Suche und wählen Sie dann **Ergebnisse untersuchen** aus.

Erstellen gespeicherter Abfragen und Richtlinien

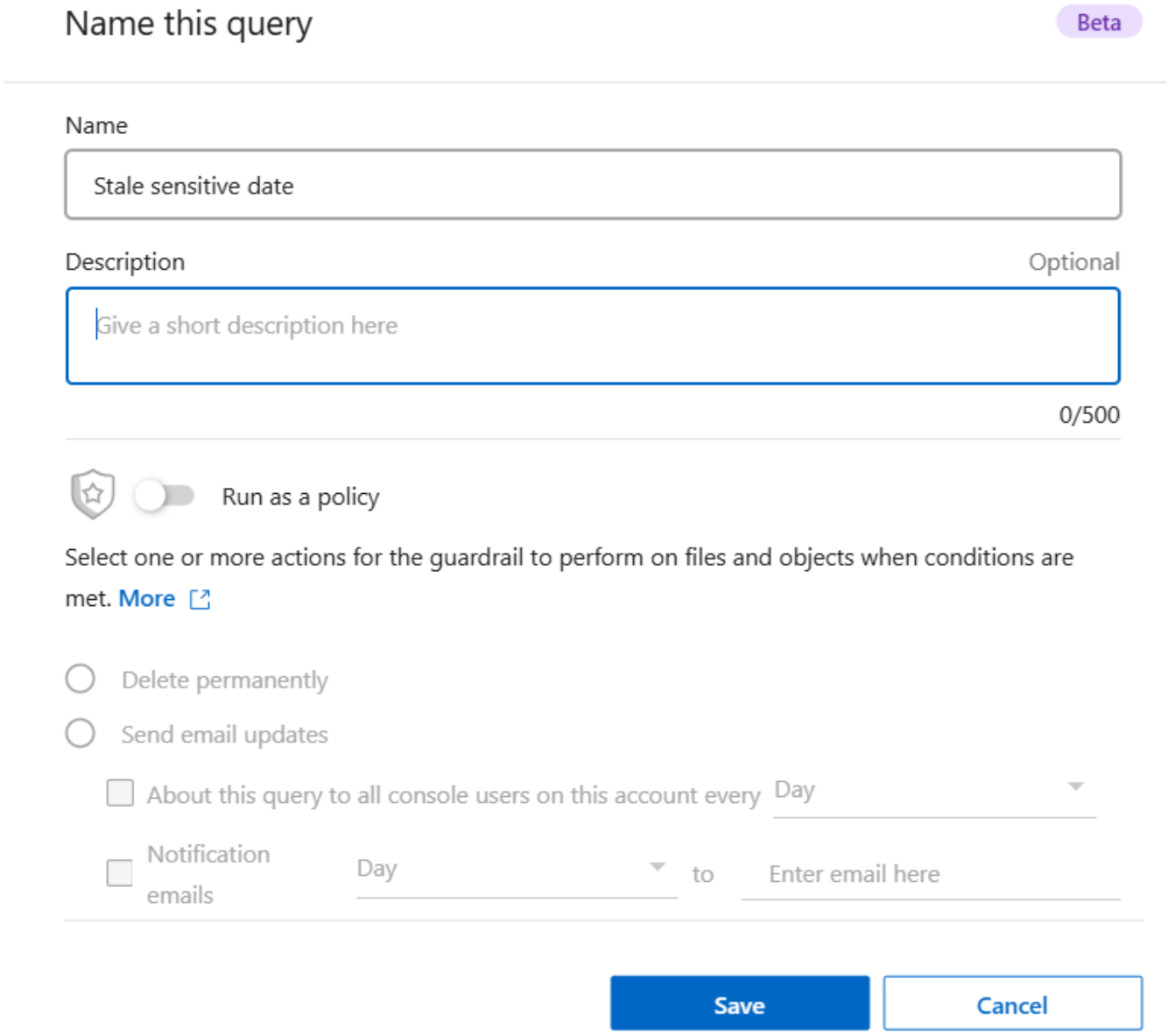
Sie können Ihre eigenen benutzerdefinierten gespeicherten Abfragen erstellen, die Ergebnisse für Abfragen liefern, die für Ihre Organisation spezifisch sind. Es werden Ergebnisse für alle Dateien und Verzeichnisse (Freigaben und Ordner) zurückgegeben, die den Suchkriterien entsprechen.

Schritte

1. Definieren Sie auf der Registerkarte „Untersuchung“ eine Suche, indem Sie die gewünschten Filter auswählen. Sehen"Filtern von Daten auf der Seite „Untersuchung“" für Details.
2. Wenn Sie alle Filtereigenschaften nach Ihren Wünschen eingestellt haben, wählen Sie **Abfrage speichern**.



3. Benennen Sie die gespeicherte Abfrage und fügen Sie eine Beschreibung hinzu. Der Name muss eindeutig sein.
4. Optional können Sie die Abfrage als Richtlinie speichern:
   a. Um die Abfrage als Richtlinie zu speichern, schalten Sie den Schalter **Als Richtlinie ausführen** um.
   b. Wählen Sie **Dauerhaft löschen** oder **E-Mail-Updates senden**. Wenn Sie E-Mail-Updates auswählen, können Sie die Abfrageergebnisse täglich, wöchentlich oder monatlich per E-Mail an *alle* Konsolenbenutzer senden. Alternativ können Sie die Benachrichtigung in der gleichen Häufigkeit an bestimmte E-Mail-Adressen senden.
5. Wählen Sie **Speichern**.



Nachdem Sie die Suche oder Richtlinie erstellt haben, können Sie sie auf der Registerkarte **Gespeicherte Abfragen** anzeigen.

Bearbeiten gespeicherter Abfragen oder Richtlinien

Sie können den Namen und die Beschreibung einer gespeicherten Abfrage ändern. Sie können eine Abfrage auch in eine Richtlinie umwandeln und umgekehrt.

Sie können standardmäßig gespeicherte Abfragen nicht ändern. Sie können die Filter einer gespeicherten Abfrage nicht ändern. Sie können alternativ die Untersuchungsergebnisse einer gespeicherten Abfrage anzeigen, die Filter ändern oder modifizieren und sie dann als neue Abfrage oder Richtlinie speichern.

Schritte

1. Wählen Sie auf der Seite „Gespeicherte Abfragen“ **Suche bearbeiten** für die Suche aus, die Sie ändern möchten.

2. Nehmen Sie die Änderungen an den Feldern „Name“ und „Beschreibung“ vor. Um nur die Felder Name und Beschreibung zu ändern.

   Sie können die Abfrage optional in eine Richtlinie oder die Richtlinie in eine gespeicherte Abfrage umwandeln. Schalten Sie den Schalter **Als Richtlinie ausführen** nach Bedarf um. .. Wenn Sie die Abfrage in eine Richtlinie umwandeln, wählen Sie **Dauerhaft löschen** oder **E-Mail-Updates senden**. Wenn Sie E-Mail-Updates auswählen, können Sie die Abfrageergebnisse täglich, wöchentlich oder monatlich per E-Mail an *alle* Konsolenbenutzer senden. Alternativ können Sie die Benachrichtigung in der gleichen Häufigkeit an bestimmte E-Mail-Adressen senden.

3. Wählen Sie **Speichern**, um die Änderungen abzuschließen.

Gespeicherte Abfragen löschen

Sie können jede benutzerdefinierte gespeicherte Abfrage oder Richtlinie löschen, wenn Sie sie nicht mehr benötigen. Sie können standardmäßig gespeicherte Abfragen nicht löschen.

Um eine gespeicherte Abfrage zu löschen, wählen Sie das Klicken Sie für eine bestimmte Suche auf die Schaltfläche „Abfrage löschen“, wählen Sie „Abfrage löschen“ und wählen Sie dann im Bestätigungsdialogfeld erneut „Abfrage löschen“.

Standardabfragen

Die Datenklassifizierung bietet die folgenden systemdefinierten Suchanfragen:

- **Namen der betroffenen Personen – Hohes Risiko**

  Dateien mit mehr als 50 Betroffenennamen

- **E-Mail-Adressen – Hohes Risiko**

  Dateien mit mehr als 50 E-Mail-Adressen oder Datenbankspalten, deren Zeilen zu mehr als 50 % aus E-Mail-Adressen bestehen

- **Personenbezogene Daten – Hohes Risiko**

  Dateien mit mehr als 20 personenbezogenen Datenkennungen oder Datenbankspalten, deren Zeilen zu mehr als 50 % personenbezogene Datenkennungen enthalten

- **Private Daten – über 7 Jahre veraltet**

  Dateien mit persönlichen oder sensiblen persönlichen Informationen, die zuletzt vor mehr als 7 Jahren geändert wurden

- **Schutz – Hoch**

  Dateien oder Datenbankspalten, die ein Passwort, Kreditkarteninformationen, eine IBAN-Nummer oder eine Sozialversicherungsnummer enthalten

- **Schutz – Niedrig**

  Dateien, auf die seit mehr als 3 Jahren nicht zugegriffen wurde

- **Schutz - Mittel**

  Dateien, die Dateien oder Datenbankspalten mit personenbezogenen Datenkennungen enthalten, darunter Ausweisnummern, Steueridentifikationsnummern, Führerscheinnummern, medizinische Ausweise oder Passnummern

- **Sensible personenbezogene Daten – Hohes Risiko**

  Dateien mit mehr als 20 Kennungen für sensible personenbezogene Daten oder Datenbankspalten, deren Zeilen zu mehr als 50 % sensible personenbezogene Daten enthalten

Ändern Sie die NetApp Data Classification -Scaneinstellungen für Ihre Repositories

Sie können verwalten, wie Ihre Daten in jedem Ihrer Systeme und Datenquellen gescannt werden. Sie können die Änderungen auf „Repository“-Basis vornehmen. Das bedeutet, dass Sie je nach Art der Datenquelle, die Sie scannen, Änderungen für jedes Volume, Schema, jeden Benutzer usw. vornehmen können.

Sie können unter anderem ändern, ob ein Repository gescannt wird oder nicht und ob NetApp Data Classification eine"Mapping-Scan oder ein Mapping- und Klassifizierungs-Scan" . Sie können den Scanvorgang auch anhalten und fortsetzen, beispielsweise wenn Sie den Scanvorgang eines Volumes für einen bestimmten Zeitraum unterbrechen müssen.

Den Scan-Status für Ihre Repositories anzeigen

Sie können die einzelnen Repositories anzeigen, die NetApp Data Classification für jedes System und jede Datenquelle scannt (Volumes, Buckets usw.). Sie können auch sehen, wie viele „kartiert“ und wie viele „klassifiziert“ wurden. Die Klassifizierung dauert länger, da die vollständige KI-Identifizierung für alle Daten durchgeführt wird.

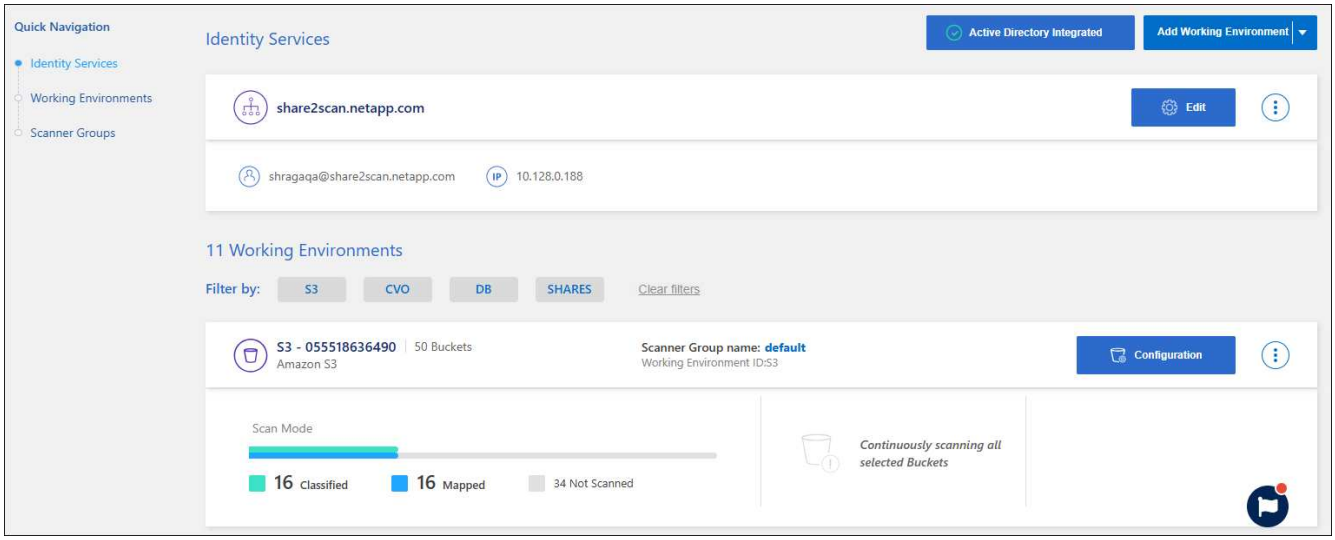
Sie können den Scan-Status jeder Arbeitsumgebung auf der Konfigurationsseite anzeigen:

- **Initialisierung** (hellblauer Punkt): Die Karten- oder Klassifizierungskonfiguration wird aktiviert. Dieser Wert erscheint kurz, bevor er in den Status „in der Warteschlange“ wechselt.
- **Warteschlange ausstehend** (orangefarbener Punkt): Die Scanaufgabe wartet darauf, in die Scan-Warteschlange aufgenommen zu werden.
- **In Warteschlange** (orangefarbener Punkt): Die Aufgabe wurde erfolgreich zur Scan-Warteschlange hinzugefügt. Das System beginnt mit der Zuordnung oder Klassifizierung des Datenträgers, wenn dieser in der Warteschlange an der Reihe ist.
- **Läuft** (grüner Punkt): Die Scanaufgabe, die sich in der Warteschlange befand, wird derzeit aktiv im ausgewählten Speicherrepository ausgeführt.
- **Fertig** (grüner Punkt): Der Scan des Speicherrepositorys ist abgeschlossen.
- **Pausiert** (grauer Punkt): Sie haben den Scanvorgang pausiert. Obwohl die Volumenänderungen im System nicht angezeigt werden, bleiben die gescannten Erkenntnisse verfügbar.

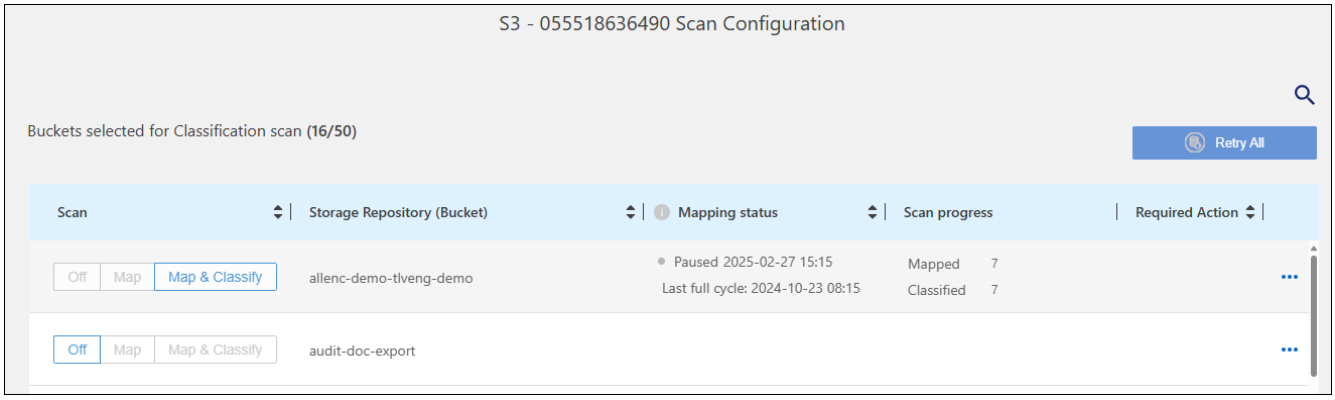
- **Fehler** (roter Punkt): Der Scan kann nicht abgeschlossen werden, da Probleme aufgetreten sind. Wenn Sie eine Aktion abschließen müssen, wird der Fehler im Tooltip unter der Spalte „Erforderliche Aktion“ angezeigt. Andernfalls zeigt das System den Status „Fehler“ an und versucht, die Wiederherstellung durchzuführen. Wenn es fertig ist, ändert sich der Status.
- **Nicht scannen**: Die Volume-Konfiguration wurde auf „Aus“ eingestellt und das System scannt das Volume nicht.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.



2. Wählen Sie auf der Registerkarte „Konfiguration“ die Schaltfläche **Konfiguration** für das System.
3. Zeigen Sie auf der Seite „Scan-Konfiguration“ die Scan-Einstellungen für alle Repositorys an.



4. Bewegen Sie während eines Scans den Mauszeiger über die Fortschrittsanzeige in der Spalte „Zuordnungsstatus“, um die Anzahl der Dateien in der Warteschlange anzuzeigen, die für dieses Repository zugeordnet oder klassifiziert werden sollen.

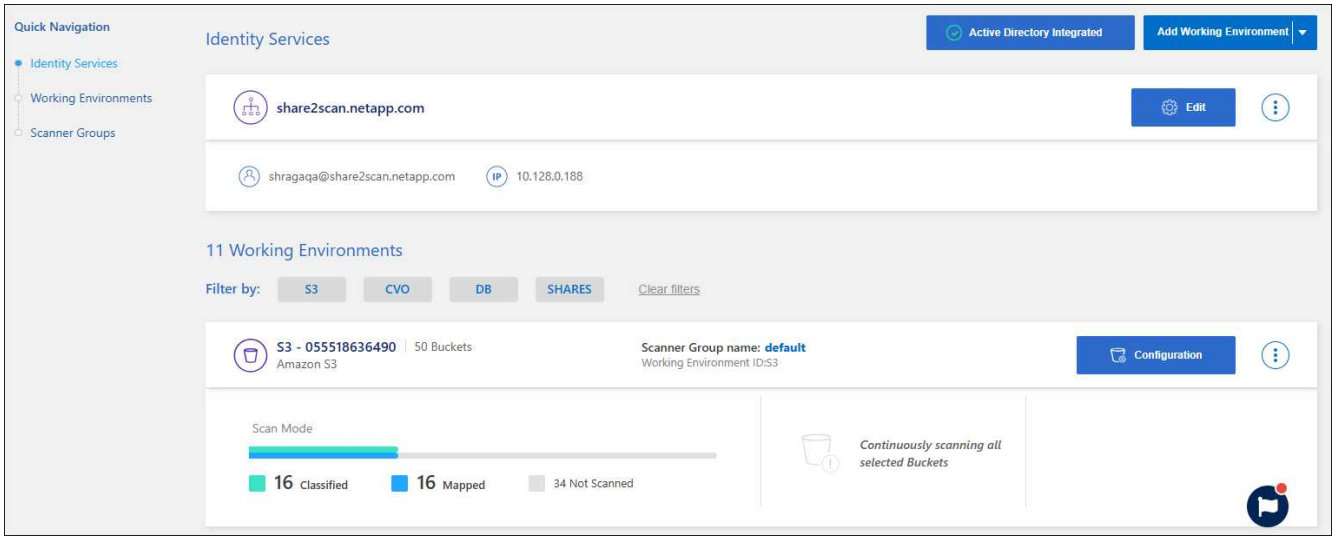
Ändern des Scan-Typs für ein Repository

Sie können reine Mapping-Scans oder Mapping- und Klassifizierungs-Scans in einem System jederzeit über die Konfigurationsseite starten oder stoppen. Sie können auch von reinen Mapping-Scans zu Mapping- und Klassifizierungs-Scans wechseln und umgekehrt.

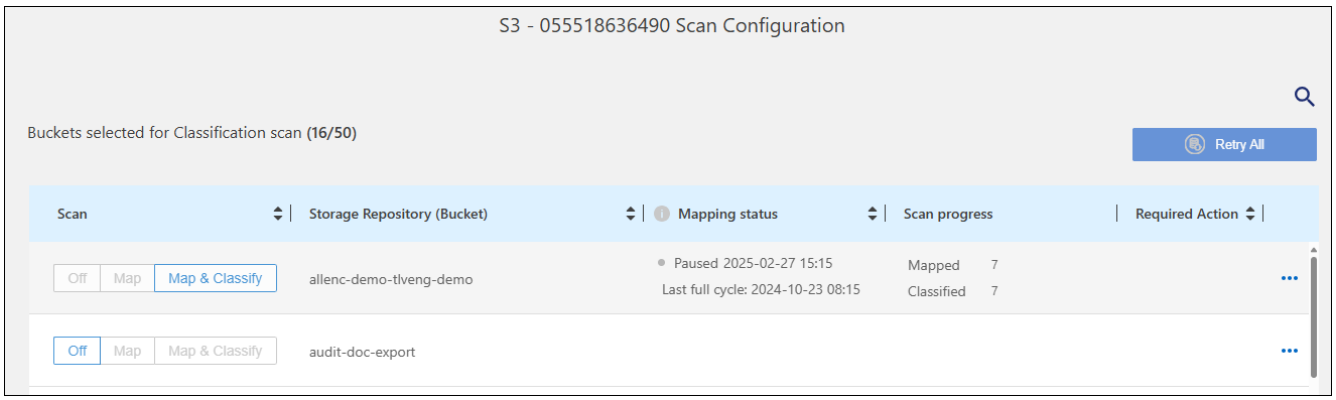
Datenbanken können nicht auf reine Mapping-Scans eingestellt werden. Das Scannen der Datenbank kann aktiviert oder deaktiviert werden, wobei „A“ dem Zuordnen und Klassifizieren entspricht.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Registerkarte „Konfiguration“ die Schaltfläche **Konfiguration** für das System.

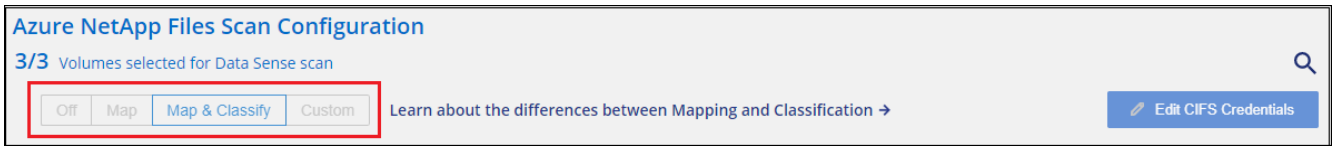


3. Ändern Sie auf der Seite „Scan-Konfiguration“ beliebige Repositories (in diesem Beispiel Buckets), um **Map**- oder **Map & Classify**-Scans durchzuführen.



Bei bestimmten Systemtypen können Sie die Art des Scannens global für alle Repositories ändern, indem Sie eine Schaltflächenleiste oben auf der Seite verwenden. Dies gilt für Cloud Volumes ONTAP, On-Premises ONTAP, Azure NetApp Files und Amazon FSx für ONTAP Systeme.

Das folgende Beispiel zeigt diese Schaltflächenleiste für ein Azure NetApp Files -System.



Priorisieren Sie Scans

Sie können die wichtigsten Nur-Mapping-Scans priorisieren oder Scans zuordnen und klassifizieren, um sicherzustellen, dass Scans mit hoher Priorität zuerst abgeschlossen werden.

Standardmäßig werden Scans in der Reihenfolge ihrer Einleitung in die Warteschlange gestellt. Mit der Möglichkeit, Scans zu priorisieren, können Sie Scans an den Anfang der Warteschlange verschieben. Mehrere Scans können priorisiert werden. Die Priorität wird in der Reihenfolge „First In, First Out“ vergeben. Das bedeutet, dass der erste Scan, den Sie priorisieren, an den Anfang der Warteschlange rückt, der zweite Scan, den Sie priorisieren, an den zweiten in der Warteschlange usw.

Die Priorität wird einmalig gewährt. Automatische erneute Scans der Kartendaten erfolgen in der Standardreihenfolge.

Schritte

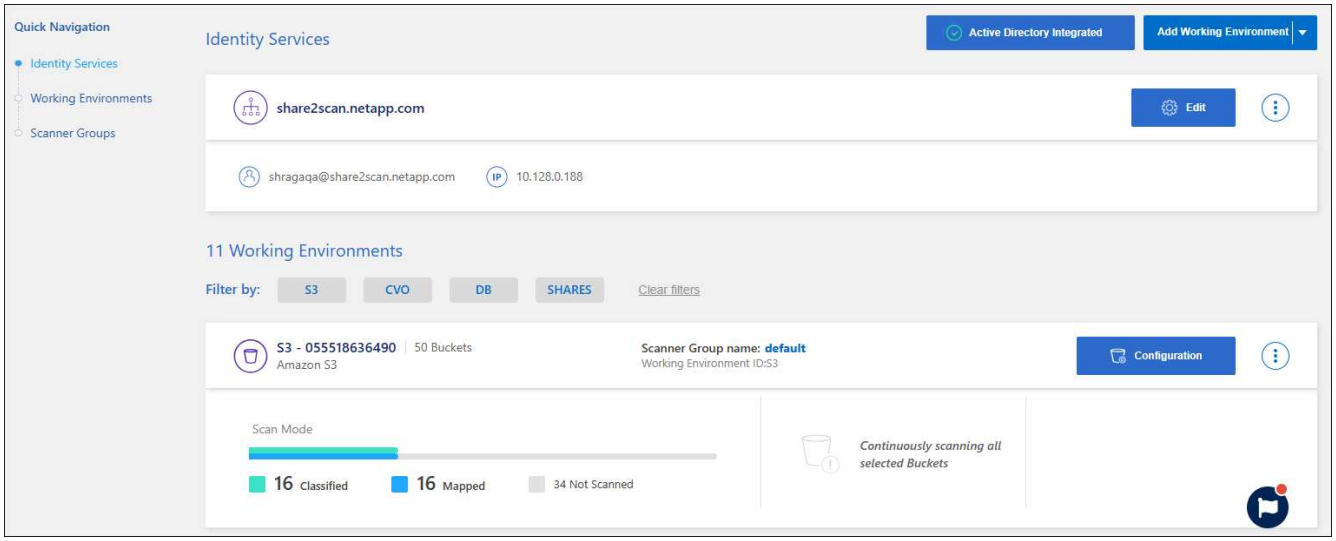
1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie die Ressourcen aus, die Sie priorisieren möchten.
3. Von den Aktionen … Wählen Sie als Option **Scan priorisieren**.

Scannen nach einem Repository beenden

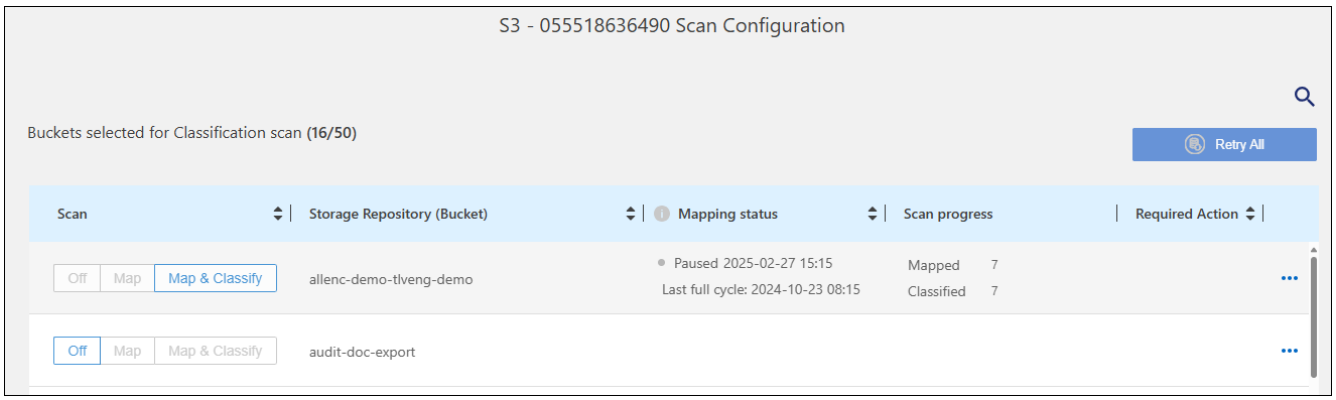
Sie können das Scannen eines Repositorys (z. B. eines Volumes) beenden, wenn Sie es nicht mehr auf Konformität überwachen müssen. Dies erreichen Sie, indem Sie das Scannen „ausschalten“. Wenn das Scannen deaktiviert wird, werden alle Indizes und Informationen zu diesem Datenträger aus dem System entfernt und die Gebühren für das Scannen der Daten werden nicht mehr erhoben.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Registerkarte „Konfiguration“ die Schaltfläche **Konfiguration** für das System.



3. Wählen Sie auf der Seite „Scan-Konfiguration“ **Aus** aus, um das Scannen für einen bestimmten Bucket zu beenden.



Scannen nach einem Repository anhalten und fortsetzen

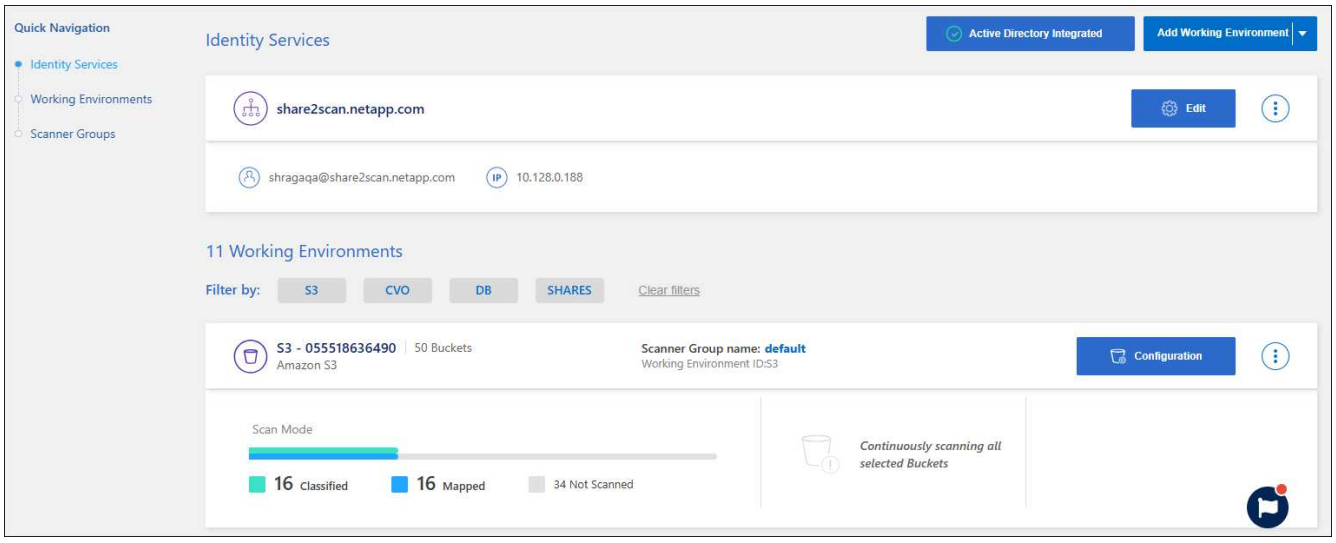
Sie können das Scannen eines Repositorys „anhalten“, wenn Sie das Scannen bestimmter Inhalte vorübergehend beenden möchten. Das Anhalten des Scanvorgangs bedeutet, dass die Datenklassifizierung keine weiteren Scans auf Änderungen oder Ergänzungen im Repository durchführt. Alle aktuellen Scan-Ergebnisse bleiben in der Datenklassifizierung abrufbar.

Wenn Sie Scans pausieren, werden dadurch die Abrechnungsgebühren nicht entfernt, da die Daten weiterhin im System vorhanden sind.

Sie können den Scanvorgang jederzeit fortsetzen.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Registerkarte „Konfiguration“ die Schaltfläche **Konfiguration** für das System.



3. Wählen Sie auf der Seite „Scan-Konfiguration“ die Aktionen ••• Symbol.
4. Wählen Sie **Pause**, um den Scanvorgang für ein Volume anzuhalten, oder wählen Sie **Fortsetzen**, um den Scanvorgang für ein Volume fortzusetzen, der zuvor angehalten wurde.

Compliance-Berichte zur NetApp Data Classification anzeigen

NetApp Data Classification bietet Berichte, mit denen Sie den Status des Datenschutzprogramms Ihres Unternehmens besser verstehen können.

Standardmäßig zeigen die Dashboards zur Datenklassifizierung Compliance- und Governance-Daten für alle Systeme, Datenbanken und Datenquellen an. Wenn Sie Berichte anzeigen möchten, die nur Daten für einige der Systeme enthalten, können Sie filtern, um nur diese anzuzeigen.

- Compliance-Berichte sind nur verfügbar, wenn Sie einen vollständigen Klassifizierungsscan Ihrer Datenquellen durchführen. Datenquellen, bei denen nur ein Mapping-Scan durchgeführt wurde, können nur den Datenmapping-Bericht generieren.
- NetApp kann keine hundertprozentige Genauigkeit der personenbezogenen Daten und sensiblen personenbezogenen Daten garantieren, die durch die Datenklassifizierung identifiziert werden. Sie sollten die Informationen immer durch Überprüfung der Daten validieren.

Für die Datenklassifizierung stehen folgende Berichte zur Verfügung:

- **Bericht zur Bewertung der Datenermittlung**: Bietet eine umfassende Analyse der gescannten Umgebung, um die Ergebnisse des Systems hervorzuheben und Problembereiche sowie mögliche Abhilfemaßnahmen aufzuzeigen. Dieser Bericht ist im Governance-Dashboard verfügbar.
- **Vollständiger Übersichtsbericht zur Datenzuordnung**: Bietet Informationen zur Größe und Anzahl der Dateien in Ihren Systemen. Hierzu zählen Nutzungskapazität, Alter der Daten, Datengröße und Dateitypen. Dieser Bericht ist im Governance-Dashboard verfügbar.
- **Bericht zur Anforderung des Zugriffs auf personenbezogene Daten**: Ermöglicht Ihnen, einen Bericht aller Dateien zu extrahieren, die Informationen zum spezifischen Namen oder zur persönlichen Kennung einer betroffenen Person enthalten. Dieser Bericht ist im Compliance-Dashboard verfügbar.
- **HIPAA-Bericht**: Hilft Ihnen, die Verteilung von Gesundheitsinformationen in Ihren Dateien zu identifizieren. Dieser Bericht ist im Compliance-Dashboard verfügbar.
- **PCI DSS-Bericht**: Hilft Ihnen, die Verteilung von Kreditkarteninformationen in Ihren Dateien zu identifizieren. Dieser Bericht ist im Compliance-Dashboard verfügbar.
- **Bericht zur Bewertung des Datenschutzrisikos**: Bietet Einblicke in den Datenschutz Ihrer Daten und eine Bewertung des Datenschutzrisikos. Dieser Bericht ist im Compliance-Dashboard verfügbar.
- **Berichte zu einem bestimmten Informationstyp**: Es sind Berichte verfügbar, die Details zu den identifizierten Dateien enthalten, die personenbezogene Daten und sensible personenbezogene Daten enthalten. Sie können die Dateien auch nach Kategorie und Dateityp aufgeschlüsselt anzeigen.

Wählen Sie die Systeme für Berichte aus

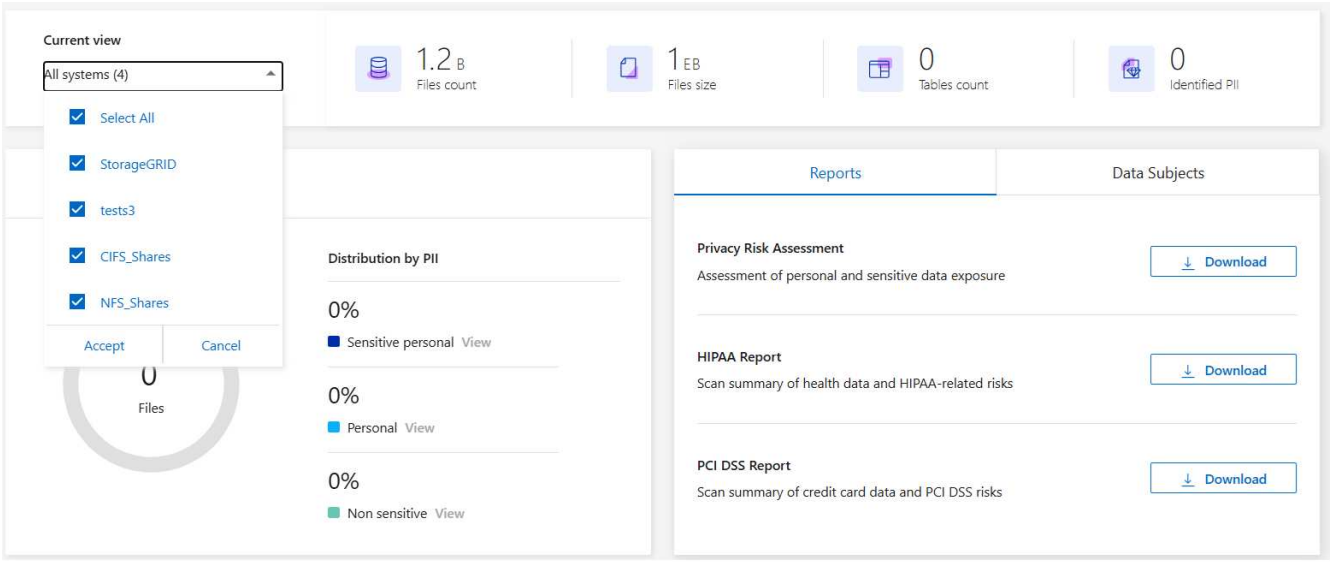
Sie können den Inhalt des Dashboards „Datenklassifizierungs-Compliance“ filtern, um Compliance-Daten für alle Systeme und Datenbanken oder nur für bestimmte Systeme anzuzeigen.

Wenn Sie das Dashboard filtern, beschränkt die Datenklassifizierung die Compliance-Daten und -Berichte auf die von Ihnen ausgewählten Systeme.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Compliance“ aus.

2. Wählen Sie das Dropdown-Menü „Systemfilter“ und dann die Systeme aus.
3. Wählen Sie **Akzeptieren**, um Ihre Auswahl zu bestätigen.



Bericht über die Anforderung des Zugriffs betroffener Personen

Datenschutzbestimmungen wie die europäische DSGVO gewähren betroffenen Personen (wie Kunden oder Mitarbeitern) das Recht auf Zugriff auf ihre personenbezogenen Daten. Wenn eine betroffene Person diese Informationen anfordert, spricht man von einem DSAR (Data Subject Access Request). Die Organisationen sind verpflichtet, auf diese Anfragen „unverzüglich“ und spätestens innerhalb eines Monats nach Erhalt zu antworten.

Sie können auf einen DSAR reagieren, indem Sie nach dem vollständigen Namen oder einer bekannten Kennung (z. B. einer E-Mail-Adresse) einer Person suchen und dann einen Bericht herunterladen. Der Bericht soll Ihr Unternehmen dabei unterstützen, die DSGVO oder ähnliche Datenschutzgesetze einzuhalten.

Wie kann Ihnen die Datenklassifizierung dabei helfen, auf einen DSAR zu reagieren?

Wenn Sie eine Suche nach einer betroffenen Person durchführen, findet die Datenklassifizierung alle Dateien, die den Namen oder die Kennung dieser Person enthalten. Die Datenklassifizierung überprüft die neuesten vorindizierten Daten auf den Namen oder die Kennung. Es wird kein neuer Scan gestartet.

Nachdem die Suche abgeschlossen ist, können Sie die Liste der Dateien für einen Bericht über die Anforderung des Zugriffs betroffener Personen herunterladen. Der Bericht fasst Erkenntnisse aus den Daten zusammen und fasst sie in rechtlichen Begriffen zusammen, die Sie an die Person zurücksenden können.

Die Suche nach betroffenen Personen wird derzeit in Datenbanken nicht unterstützt.

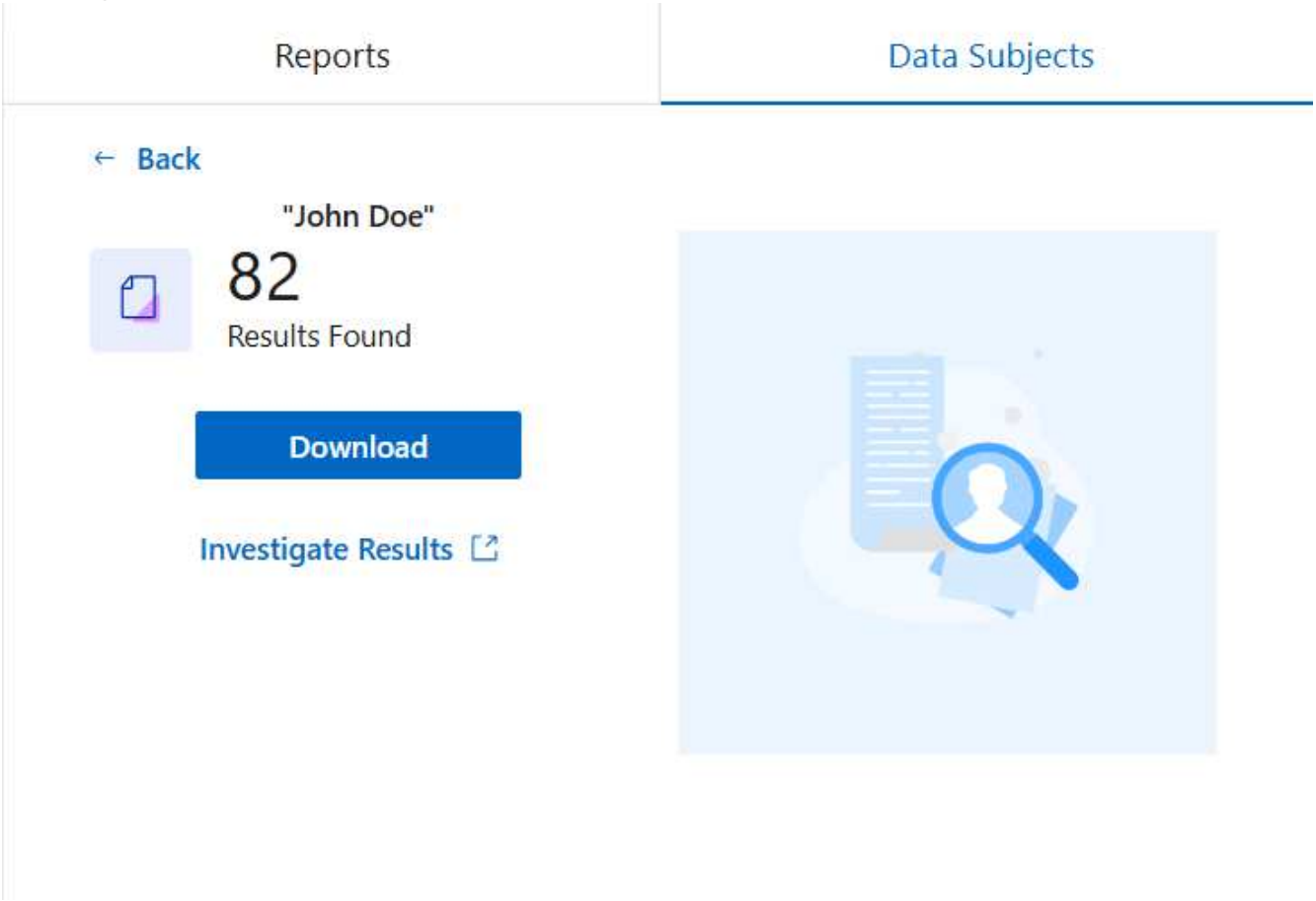
Suche nach betroffenen Personen und Download von Berichten

Suchen Sie nach dem vollständigen Namen oder einer bekannten Kennung der betroffenen Person und laden Sie dann einen Dateilistenbericht oder DSAR-Bericht herunter. Sie können suchen nach"alle Arten persönlicher Informationen" .

Bei der Suche nach den Namen der betroffenen Personen werden Englisch, Deutsch, Japanisch und Spanisch unterstützt. Die Unterstützung für weitere Sprachen wird später hinzugefügt.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Compliance“ aus.
2. Suchen Sie auf der Compliance-Seite die Registerkarte **Datensubjekte**.
3. Geben Sie im Abschnitt **Betroffene Personen** einen Namen oder eine bekannte Kennung ein und wählen Sie dann **Suchen** aus.
4. Wenn die Suche abgeschlossen ist, wählen Sie **Herunterladen**, um auf die Antwort auf die Anfrage zur Datenzugriffsanfrage der betroffenen Person zuzugreifen. Wählen Sie **Ergebnisse untersuchen** aus, um weitere Informationen auf der Seite „Datenuntersuchung“ anzuzeigen.



5. Überprüfen Sie die Ergebnisse in der Datenklassifizierung oder laden Sie sie als Bericht herunter, indem Sie das Download-Symbol auswählen.

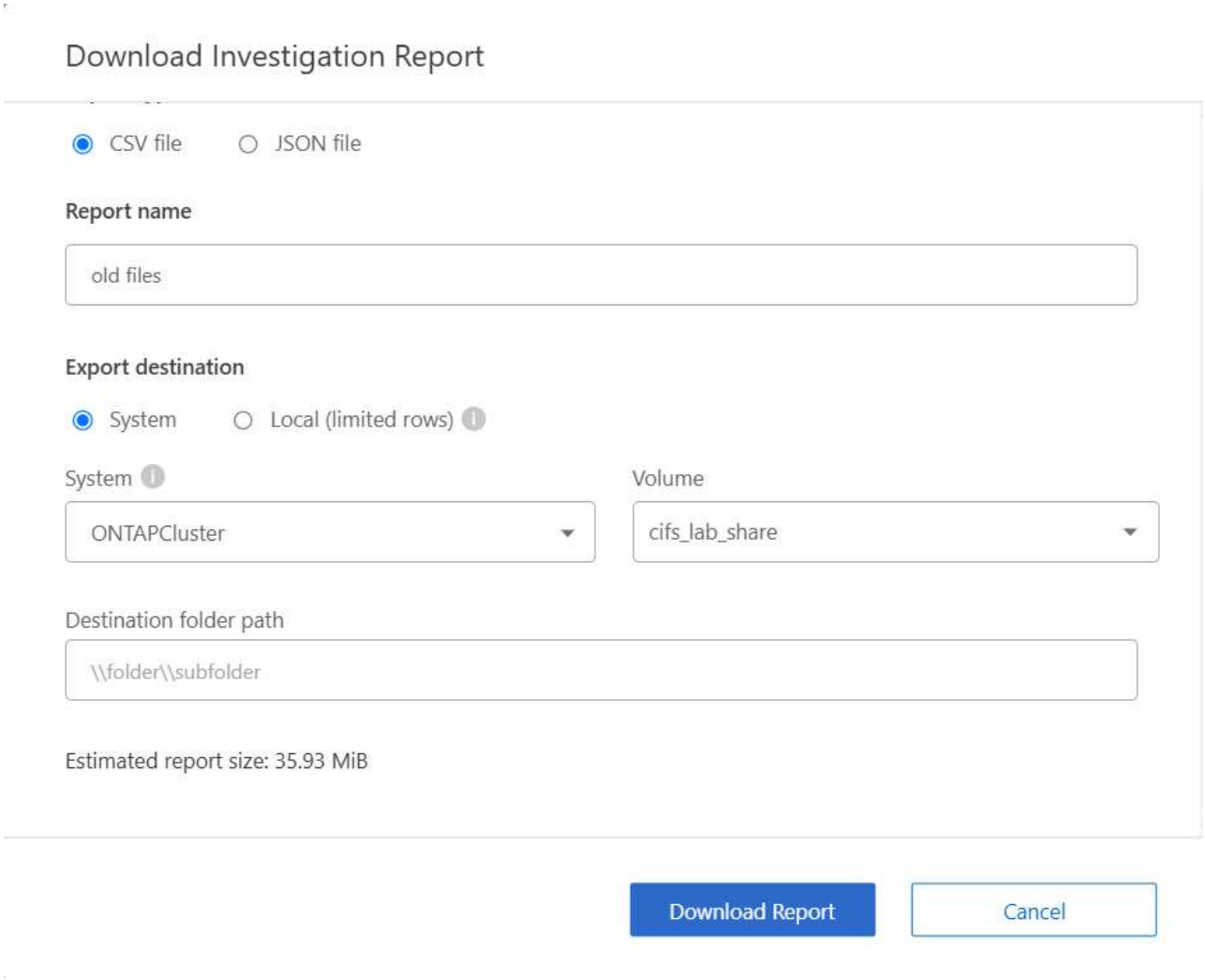
   a. Wenn Sie das Download-Symbol auswählen, konfigurieren Sie Ihre Download-Einstellungen:

      - Wählen Sie das Filmformat: CSV oder JSON
      - Geben Sie einen **Berichtsnamen** ein
      - Wählen Sie das Exportziel: **System** oder Ihren **lokalen** Computer.

        Wenn Sie „System“ wählen, werden alle Daten heruntergeladen. Sie müssen auch **System**, **Volume** und **Zielordnerpfad** auswählen.

Wenn Sie **Lokal** wählen, wird der Bericht auf die ersten 10.000 Zeilen unstrukturierter Daten, 5.000 Zeilen unstrukturierter Daten und 1.000 Zeilen strukturierter Daten beschränkt.

a. Wählen Sie **Bericht herunterladen**, um den Download zu starten.



Bericht zum Health Insurance Portability and Accountability Act (HIPAA)

Der Bericht zum Health Insurance Portability and Accountability Act (HIPAA) kann Ihnen dabei helfen, Dateien mit Gesundheitsinformationen zu identifizieren. Es soll Ihr Unternehmen dabei unterstützen, die HIPAA-Datenschutzgesetze einzuhalten. Die Datenklassifizierung sucht unter anderem nach folgenden Informationen:

- Gesundheitsreferenzmuster
- ICD-10-CM Medizinischer Code
- ICD-9-CM Medizinischer Code
- HR – Kategorie Gesundheit
- Kategorie „Gesundheitsanwendungsdaten“

Der Bericht enthält die folgenden Informationen:

- Übersicht: In wie vielen Dateien sind Gesundheitsinformationen enthalten und in welchen Systemen.
- Verschlüsselung: Der Prozentsatz der Dateien mit Gesundheitsinformationen, die sich auf verschlüsselten

oder unverschlüsselten Systemen befinden. Diese Informationen gelten speziell für Cloud Volumes ONTAP.

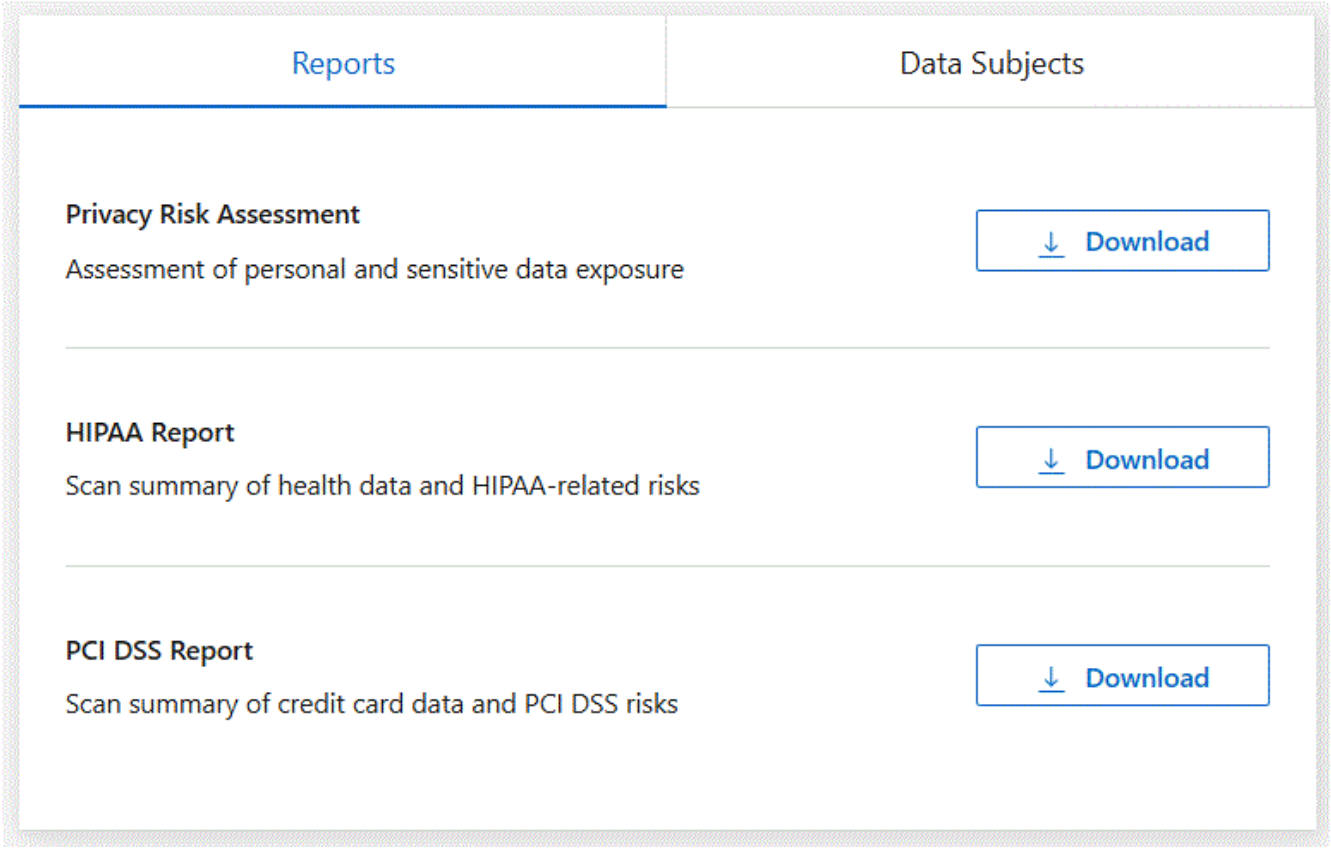
- Ransomware-Schutz: Der Prozentsatz der Dateien mit Gesundheitsinformationen, die sich auf Systemen befinden, auf denen der Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen gelten speziell für Cloud Volumes ONTAP.
- Aufbewahrung: Der Zeitraum, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, da Sie Gesundheitsinformationen nicht länger aufbewahren sollten, als Sie für deren Verarbeitung benötigen.
- Verteilung von Gesundheitsinformationen: Die Systeme, auf denen die Gesundheitsinformationen gefunden wurden, und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

HIPAA-Bericht erstellen

Gehen Sie zur Registerkarte „Compliance“, um den Bericht zu erstellen.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Compliance“ aus.
2. Suchen Sie den **Berichtsbereich**. Wählen Sie das Download-Symbol neben **HIPAA-Bericht**.



Ergebnis

Die Datenklassifizierung generiert einen PDF-Bericht.

Bericht zum Payment Card Industry Data Security Standard (PCI DSS)

Mithilfe des Berichts zum Payment Card Industry Data Security Standard (PCI DSS) können Sie die Verteilung von Kreditkarteninformationen in Ihren Dateien ermitteln.

Der Bericht enthält die folgenden Informationen:

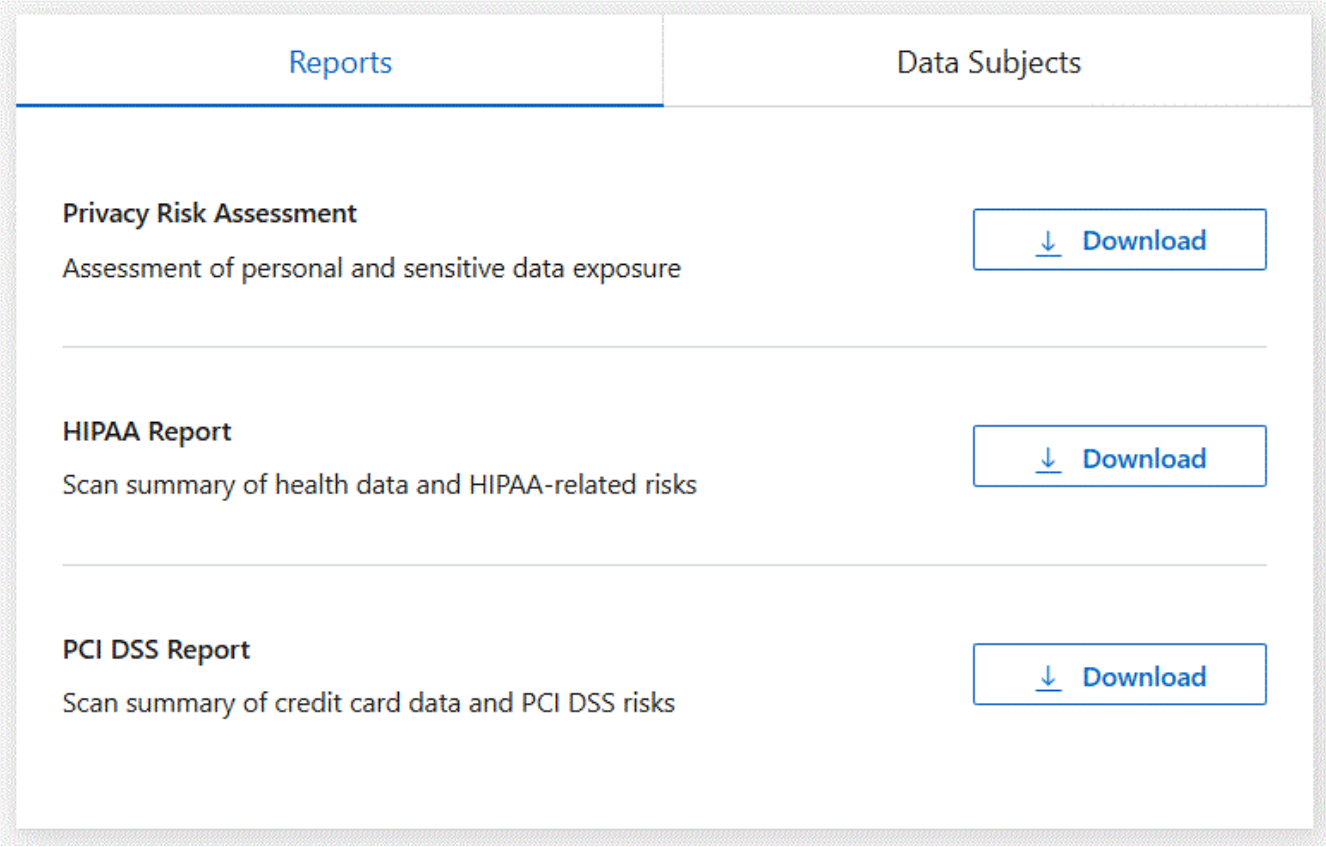
- Übersicht: In wie vielen Dateien sind Kreditkarteninformationen enthalten und in welchen Systemen.
- Verschlüsselung: Der Prozentsatz der Dateien mit Kreditkarteninformationen, die sich auf verschlüsselten oder unverschlüsselten Systemen befinden. Diese Informationen gelten speziell für Cloud Volumes ONTAP.
- Ransomware-Schutz: Der Prozentsatz der Dateien mit Kreditkarteninformationen, die sich auf Systemen befinden, auf denen der Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen gelten speziell für Cloud Volumes ONTAP.
- Aufbewahrung: Der Zeitraum, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, da Sie Kreditkarteninformationen nicht länger aufbewahren sollten, als Sie für die Verarbeitung benötigen.
- Verbreitung von Kreditkarteninformationen: Die Systeme, auf denen die Kreditkarteninformationen gefunden wurden, und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

PCI DSS-Bericht erstellen

Gehen Sie zur Registerkarte „Compliance“, um den Bericht zu erstellen.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Compliance“ aus.
2. Suchen Sie den **Berichtsbereich**. Wählen Sie das Download-Symbol neben **PCI DSS-Bericht**.



Ergebnis

Die Datenklassifizierung generiert einen PDF-Bericht, den Sie überprüfen und bei Bedarf an andere Gruppen senden können.

Bericht zur Bewertung des Datenschutzrisikos

Der Bericht zur Bewertung des Datenschutzrisikos bietet einen Überblick über den Datenschutzrisikostatus Ihres Unternehmens, wie es Datenschutzbestimmungen wie die DSGVO und das CCPA vorschreiben.

Der Bericht enthält die folgenden Informationen:

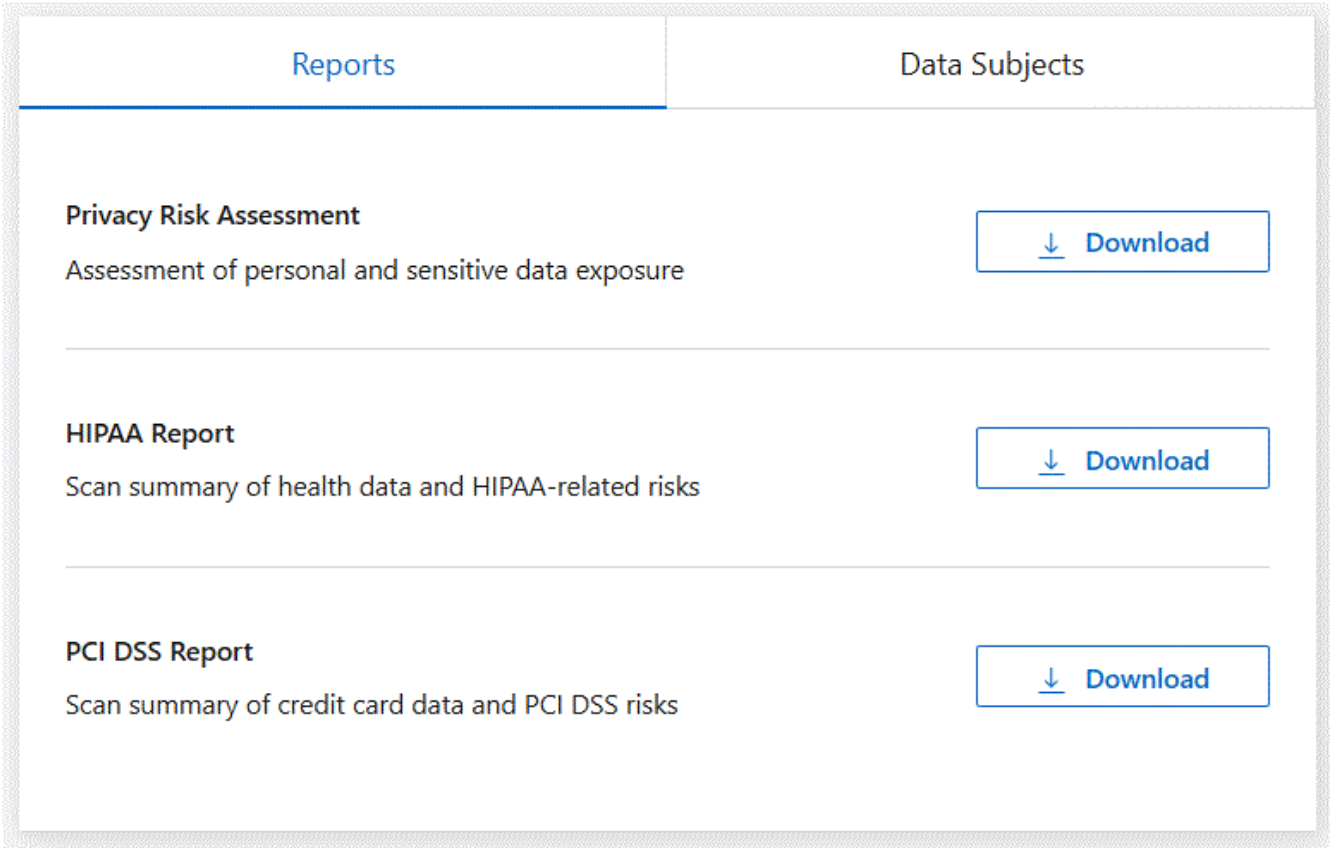
- Compliance-Status: Ein Schweregrad und die Verteilung der Daten, unabhängig davon, ob es sich um nicht vertrauliche, persönliche oder vertrauliche persönliche Daten handelt.
- Bewertungsübersicht: Eine Aufschlüsselung der gefundenen Arten personenbezogener Daten sowie der Datenkategorien.
- Betroffene Personen dieser Bewertung: Die Anzahl der Personen nach Standort, für die nationale Kennungen gefunden wurden.

Bericht zur Datenschutzrisikobewertung erstellen

Gehen Sie zur Registerkarte „Compliance“, um den Bericht zu erstellen.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Compliance“ aus.
2. Suchen Sie den **Berichtsbereich**. Wählen Sie das Download-Symbol neben **Bericht zur Bewertung des Datenschutzrisikos**.



Ergebnis

Die Datenklassifizierung generiert einen PDF-Bericht, den Sie überprüfen und bei Bedarf an andere Gruppen senden können.

Schweregrad

Die Datenklassifizierung berechnet den Schweregrad für den Bericht zur Bewertung des Datenschutzrisikos auf der Grundlage von drei Variablen:

- Der Prozentsatz personenbezogener Daten an allen Daten.
- Der Prozentsatz sensibler personenbezogener Daten an allen Daten.
- Der Prozentsatz der Dateien, die betroffene Personen enthalten, wird durch nationale Kennungen wie Personalausweise, Sozialversicherungsnummern und Steuernummern bestimmt.

Die zur Ermittlung der Punktzahl verwendete Logik lautet wie folgt:

Schweregrad	Logik
0	Alle drei Variablen sind genau 0 %
1	Eine der Variablen ist größer als 0 %
2	Eine der Variablen ist größer als 3 %
3	Zwei der Variablen sind größer als 3 %
4	Drei der Variablen sind größer als 3 %
5	Eine der Variablen ist größer als 6 %
6	Zwei der Variablen sind größer als 6 %
7	Drei der Variablen sind größer als 6 %
8	Eine der Variablen ist größer als 15 %
9	Zwei der Variablen sind größer als 15 %
10	Drei der Variablen sind größer als 15 %

Überwachung des Zustands der NetApp Data Classification

Das NetApp Data Classification Health Monitor Dashboard bietet Echtzeitüberwachung und Einblicke in die Leistung. Der Health Monitor erfasst Informationen über Ihre Datenklassifizierungsinfrastruktur, den Systemzustand, Nutzungsmetriken und Nutzungsdaten, sodass Sie Probleme erkennen und beheben können.

Erkenntnisse aus dem Gesundheitsmonitor

Das Dashboard des Gesundheitsmonitors präsentiert Informationen in vier Kategorien.

- **Infrastrukturstatus**

  Informationen wie Versionsstatus, Systemstabilität, Bereitstellungstyp und Maschinengröße anzeigen.

- **Problematische Container**

  Überprüfen Sie das Feld „Problematische Container“, um Einblicke in Container zu erhalten, die häufig gestoppt oder neu gestartet werden. Nutzen Sie diese Informationen, um die einzelnen Behälter zu untersuchen.

- **Systeminformationen**

  Das Systeminformationsfeld erfasst wichtige Informationen über die NetApp Console und die Datenklassifizierung, wie z. B. die öffentlichen und privaten IP-Adressen, den Hostnamen, das Betriebssystem, die Konsolenversion und die Konsolen-ID.

- **Nutzung und Verwendung**

  Überprüfen Sie die CPU-Auslastung, die Festplattenauslastung und die Speicherauslastung. Diese Werte werden in Speichereinheiten (GB) oder als Prozentsatz der Gesamtnutzung angezeigt. Wenn in einem Feld eine Warnung angezeigt wird, wählen Sie die Warnung aus, um Informationen und Empfehlungen zur Behebung zu erhalten.

Greifen Sie auf das Dashboard des Gesundheitsmonitors zu.

1. Wählen Sie unter Datenklassifizierung **Konfiguration** aus.
2. Wählen Sie unter der Überschrift **Konfiguration** die Option **Datenklassifizierungs-Integritätsüberwachung**.
3. Im Dashboard des Gesundheitsmonitors können Sie:
   - Überprüfen Sie die Nutzung und den Einsatz. Wenn bei Nutzungs- oder Auslastungsmetriken Warnungen angezeigt werden, wählen Sie die Warnung aus, um Empfehlungen zur Behebung des Problems zu erhalten.
   - Schalten Sie das Diagramm um, um CPU-Auslastung, Festplattenauslastung und Speicherauslastung anzuzeigen. Sie können die x-Achse so ändern, dass Inhalte über Stunden (6, 12 oder 24) oder Tage (2, 7 oder 14) angezeigt werden.
   - Aktualisieren Sie das Dashboard, um die aktuellsten Datenmetriken anzuzeigen.