Dokumentation zur NetApp Data Classification

NetApp Data Classification

NetApp
October 14, 2025

Inhalt

Dokumentation zur NetApp Data Classification

Versionshinweise

Was ist neu bei der NetApp Data Classification?

Erfahren Sie, was es Neues bei der NetApp Data Classification gibt.

06. Oktober 2025

Version 1.47

BlueXP classification heißt jetzt NetApp Data Classification

Die BlueXP classification wurde in NetApp Data Classification umbenannt. Neben der Umbenennung wurde auch die Benutzeroberfläche verbessert.

BlueXP heißt jetzt NetApp Console

BlueXP wurde umbenannt und neu gestaltet, um seine Rolle bei der Verwaltung Ihrer Dateninfrastruktur besser widerzuspiegeln.

Die NetApp Console ermöglicht eine zentrale Verwaltung von Speicher- und Datendiensten in lokalen und Cloud-Umgebungen auf Unternehmensebene und liefert Einblicke in Echtzeit, schnellere Workflows und eine vereinfachte Verwaltung.

Einzelheiten zu den Änderungen finden Sie im "Versionshinweise zur NetApp Console" .

Verbesserte Untersuchungserfahrung

Finden und verstehen Sie Ihre Daten schneller mit neuen durchsuchbaren Filtern, Ergebniszählungen pro Wert, Echtzeit-Einblicken, die die wichtigsten Ergebnisse zusammenfassen, und einer aktualisierten Ergebnistabelle mit anpassbaren Spalten und einem ausziehbaren Detailbereich.

Weitere Informationen finden Sie unter "Daten untersuchen" .

Neue Governance- und Compliance-Dashboards

Gewinnen Sie schneller wichtige Erkenntnisse mit intuitiven Widgets, klareren Grafiken und verbesserter Ladeleistung. Weitere Informationen finden Sie unter"Überprüfen Sie die Governance-Informationen zu Ihren Daten" Und"Zeigen Sie Compliance-Informationen zu Ihren Daten an" .

Richtlinien für gespeicherte Abfragen (Vorschau)

Mithilfe der Datenklassifizierung können Sie jetzt die Governance mit bedingten Aktionen automatisieren. Sie können Aufbewahrungsregeln mit automatischer Löschung erstellen und regelmäßige E-Mail-Benachrichtigungen einrichten. Alles wird über eine aktualisierte Seite mit gespeicherten Abfragen verwaltet.

Weitere Informationen finden Sie unter "Erstellen von Richtlinien" .

Aktionen (Vorschau)

Übernehmen Sie die direkte Kontrolle von der Untersuchungsseite aus – löschen, verschieben, kopieren oder markieren Sie Dateien einzeln oder in großen Mengen, für eine effiziente Datenverwaltung und -behebung.

Weitere Informationen finden Sie unter "Daten untersuchen" .

Unterstützung für Google Cloud NetApp Volumes

Die Datenklassifizierung unterstützt jetzt das Scannen auf Google Cloud NetApp Volumes. Fügen Sie Google

Cloud NetApp Volumes einfach über die NetApp Console hinzu, um Daten nahtlos zu scannen und zu klassifizieren.

11. August 2025

Version 1.46

Diese Version der Datenklassifizierung enthält Fehlerbehebungen und die folgenden Updates:

Verbesserte Einblicke in Scan-Ereignisse auf der Audit-Seite

Die Audit-Seite unterstützt jetzt erweiterte Einblicke in Scan-Ereignisse für die BlueXP classification. Auf der Audit-Seite wird jetzt angezeigt, wann der Scan eines Systems beginnt, sowie der Status der Systeme und etwaige Probleme. Status für Freigaben und Systeme sind nur für Mapping-Scans verfügbar.

Weitere Informationen zur Seite „Audit“ finden Sie unter"Überwachen Sie NetApp Console" .

Unterstützung für RHEL 9.6

Diese Version fügt Unterstützung für Red Hat Enterprise Linux v9.6 für die manuelle Vor-Ort-Installation der BlueXP classification hinzu, einschließlich Dark Site-Bereitstellungen.

Die folgenden Betriebssysteme erfordern die Verwendung der Podman-Container-Engine und die BlueXP classification 1.30 oder höher: Red Hat Enterprise Linux Version 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 und 9.5.

14. Juli 2025

Version 1.45

Diese BlueXP classification Klassifizierungsversion enthält Codeänderungen, die die Ressourcennutzung optimieren und:

Verbesserter Workflow zum Hinzufügen von Dateifreigaben zum Scannen

Der Arbeitsablauf zum Hinzufügen von Dateifreigaben zu einer Dateifreigabegruppe wurde vereinfacht. Der Prozess unterscheidet jetzt auch die CIFS-Protokollunterstützung basierend auf dem Authentifizierungstyp (Kerberos oder NTLM).

Weitere Informationen finden Sie unter "Dateifreigaben scannen" .

Erweiterte Informationen zum Dateieigentümer

Sie können jetzt weitere Informationen zu Dateibesitzern für erfasste Dateien auf der Registerkarte „Untersuchung“ anzeigen. Wenn Sie die Metadaten für eine Datei auf der Registerkarte „Untersuchung“ anzeigen, suchen Sie den Dateibesitzer und wählen Sie dann **Details anzeigen** aus, um den Benutzernamen, die E-Mail-Adresse und den SAM-Kontonamen anzuzeigen. Sie können auch andere Elemente anzeigen, die diesem Benutzer gehören. Diese Funktion ist nur für Arbeitsumgebungen mit Active Directory verfügbar.

Weitere Informationen finden Sie unter "Untersuchen Sie die in Ihrer Organisation gespeicherten Daten" .

10. Juni 2025

Version 1.44

Diese BlueXP classification Klassifizierungsversion umfasst:

Verbesserte Aktualisierungszeiten für das Governance-Dashboard

Die Aktualisierungszeiten für einzelne Komponenten des Governance-Dashboards wurden verbessert. Die folgende Tabelle zeigt die Aktualisierungshäufigkeit für jede Komponente.

Komponente	Aktualisierungszeiten
Zeitalter der Daten	24 Stunden
Kategorien	24 Stunden
Datenübersicht	5 Minuten
Doppelte Dateien	2 Stunden
Dateitypen	24 Stunden
Nicht-geschäftliche Daten	2 Stunden
Berechtigungen öffnen	24 Stunden
Gespeicherte Suchen	2 Stunden
Sensible Daten und umfassende Berechtigungen	24 Stunden
Datengröße	24 Stunden
Veraltete Daten	2 Stunden
Top-Datenspeicher nach Vertraulichkeitsstufe	2 Stunden

Sie können den Zeitpunkt der letzten Aktualisierung anzeigen und die Komponenten „Doppelte Dateien“, „Nicht geschäftliche Daten“, „Gespeicherte Suchen“, „Veraltete Daten“ und „Top-Datenspeicher nach Vertraulichkeitsstufe“ manuell aktualisieren. Weitere Informationen zum Governance-Dashboard finden Sie unter"Zeigen Sie Governance-Details zu den in Ihrer Organisation gespeicherten Daten an" .

Leistungs- und Sicherheitsverbesserungen

Es wurden Verbesserungen vorgenommen, um die Leistung, den Speicherverbrauch und die Sicherheit der BlueXP Klassifizierung zu verbessern.

Fehlerbehebungen

Redis wurde aktualisiert, um die Zuverlässigkeit der BlueXP classification zu verbessern. Die BlueXP classification verwendet jetzt Elasticsearch, um die Genauigkeit der Dateianzahlberichterstattung während der Scans zu verbessern.

12. Mai 2025

Version 1.43

Diese Version der Datenklassifizierung umfasst:

Priorisieren Sie Klassifizierungsscans

Die Datenklassifizierung unterstützt die Möglichkeit, neben reinen Mapping-Scans auch Map- und Classify-Scans zu priorisieren, sodass Sie auswählen können, welche Scans zuerst abgeschlossen werden. Die Priorisierung von Map & Classify-Scans wird während und vor Beginn der Scans unterstützt. Wenn Sie einem laufenden Scan Priorität einräumen, werden sowohl die Zuordnungs- als auch die Klassifizierungsscans priorisiert.

Weitere Informationen finden Sie unter "Priorisieren Sie Scans" .

Unterstützung für kanadische Datenkategorien personenbezogener Daten (PII)

Datenklassifizierungsscans identifizieren kanadische PII-Datenkategorien. Zu diesen Kategorien gehören Bankdaten, Passnummern, Sozialversicherungsnummern, Führerscheinnummern und Krankenversicherungskartennummern für alle kanadischen Provinzen und Territorien.

Weitere Informationen finden Sie unter "Kategorien personenbezogener Daten" .

Benutzerdefinierte Klassifizierung (Vorschau)

Die Datenklassifizierung unterstützt benutzerdefinierte Klassifizierungen für Map & Classify-Scans. Mit benutzerdefinierten Klassifizierungen können Sie Datenklassifizierungsscans anpassen, um mithilfe regulärer Ausdrücke unternehmensspezifische Daten zu erfassen. Diese Funktion befindet sich derzeit in der Vorschau.

Weitere Informationen finden Sie unter "Benutzerdefinierte Klassifizierungen hinzufügen" .

Registerkarte „Gespeicherte Suchen“

Die Registerkarte **Richtlinien** wurde umbenannt**"Gespeicherte Suchen"** . Die Funktionalität bleibt unverändert.

Scanereignisse an die Audit-Seite senden

Die Datenklassifizierung unterstützt das Senden von Klassifizierungsereignissen (wenn ein Scan gestartet wird und wenn er endet) an die"NetApp Console Audit-Seite" .

Sicherheitsupdates

- Das Keras-Paket wurde aktualisiert, um Schwachstellen (BDSA-2025-0107 und BDSA-2025-1984) zu beheben.
- Die Konfiguration der Docker-Container wurde aktualisiert. Der Container hat keinen Zugriff mehr auf die Netzwerkschnittstellen des Hosts, um rohe Netzwerkpakete zu erstellen. Durch die Reduzierung unnötiger Zugriffe mindert das Update potenzielle Sicherheitsrisiken.

Leistungsverbesserungen

Es wurden Codeverbesserungen implementiert, um die RAM-Nutzung zu reduzieren und die Gesamtleistung der Datenklassifizierung zu verbessern.

Fehlerbehebungen

Fehler, die dazu führten, dass StorageGRID -Scans fehlschlugen, die Filteroptionen der Untersuchungsseite nicht geladen wurden und die Data Discovery-Bewertung bei Bewertungen mit hohem Volumen nicht heruntergeladen wurde, wurden behoben.

14. April 2025

Version 1.42

Diese BlueXP classification Klassifizierungsversion umfasst:

Massenscannen für Arbeitsumgebungen

Die BlueXP classification unterstützt Massenvorgänge für Arbeitsumgebungen. Sie können Mapping-Scans aktivieren, Map & Classify-Scans aktivieren, Scans deaktivieren oder eine benutzerdefinierte Konfiguration über Volumes in der Arbeitsumgebung hinweg erstellen. Wenn Sie eine Auswahl für ein einzelnes Volume treffen, wird die Massenauswahl überschrieben. Um einen Massenvorgang durchzuführen, navigieren Sie zur Seite **Konfiguration** und treffen Sie Ihre Auswahl.

Untersuchungsbericht lokal herunterladen

Die BlueXP classification unterstützt die Möglichkeit, Datenuntersuchungsberichte lokal herunterzuladen und im Browser anzuzeigen. Wenn Sie die lokale Option wählen, ist die Datenuntersuchung nur im CSV-Format verfügbar und zeigt nur die ersten 10.000 Datenzeilen an.

Weitere Informationen finden Sie unter "Untersuchen Sie die in Ihrer Organisation gespeicherten Daten mit der BlueXP classification" .

10. März 2025

Version 1.41

Diese BlueXP classification Klassifizierungsversion enthält allgemeine Verbesserungen und Fehlerbehebungen. Es beinhaltet außerdem:

Scanstatus

Die BlueXP classification verfolgt den Echtzeitfortschritt der *ersten* Zuordnungs- und Klassifizierungsscans auf einem Datenträger. Separate progressive Balken verfolgen die Zuordnungs- und Klassifizierungsscans und stellen einen Prozentsatz aller gescannten Dateien dar. Sie können auch mit der Maus über einen Fortschrittsbalken fahren, um die Anzahl der gescannten Dateien und die Gesamtzahl der Dateien anzuzeigen. Durch die Verfolgung des Status Ihrer Scans erhalten Sie tiefere Einblicke in den Scan-Fortschritt, sodass Sie Ihre Scans besser planen und die Ressourcenzuweisung verstehen können.

Um den Status Ihrer Scans anzuzeigen, navigieren Sie in der BlueXP classification zu **Konfiguration** und wählen Sie dann die **Konfiguration der Arbeitsumgebung** aus. Der Fortschritt wird für jeden Band in der Zeile angezeigt.

19. Februar 2025

Version 1.40

Diese BlueXP classification Klassifizierungsversion enthält die folgenden Updates.

Unterstützung für RHEL 9.5

Diese Version bietet zusätzlich zu den zuvor unterstützten Versionen Unterstützung für Red Hat Enterprise Linux v9.5. Dies gilt für jede manuelle Vor-Ort-Installation der BlueXP classification, einschließlich Dark-Site-Bereitstellungen.

Die folgenden Betriebssysteme erfordern die Verwendung der Podman-Container-Engine und die BlueXP classification 1.30 oder höher: Red Hat Enterprise Linux Version 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 und 9.5.

Priorisieren Sie reine Mapping-Scans

Wenn Sie reine Mapping-Scans durchführen, können Sie den wichtigsten Scans Priorität einräumen. Diese Funktion ist hilfreich, wenn Sie über viele Arbeitsumgebungen verfügen und sicherstellen möchten, 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.

Die Priorisierung beschränkt sich auf"Nur-Mapping-Scans" ; es ist nicht für Karten- und Klassifizierungsscans verfügbar.

Weitere Informationen finden Sie unter "Priorisieren Sie Scans" .

Alle Scans wiederholen

Die BlueXP classification unterstützt die Möglichkeit, alle fehlgeschlagenen Scans stapelweise erneut durchzuführen.

Mit der Funktion **Alle wiederholen** können Sie Scans in einem Stapelvorgang erneut versuchen. Wenn Klassifizierungsscans aufgrund eines vorübergehenden Problems wie beispielsweise eines Netzwerkausfalls fehlschlagen, können Sie alle Scans gleichzeitig mit einer Schaltfläche wiederholen, anstatt sie einzeln zu wiederholen. Scans können beliebig oft wiederholt werden.

So wiederholen Sie alle Scans:

1. Wählen Sie im BlueXP classification **Konfiguration** aus.
2. Um alle fehlgeschlagenen Scans erneut durchzuführen, wählen Sie **Alle Scans wiederholen**.

Verbesserte Genauigkeit des Kategorisierungsmodells

Die Genauigkeit des maschinellen Lernmodells für"vordefinierte Kategorien" hat sich um 11 % verbessert.

22. Januar 2025

Version 1.39

Diese BlueXP classification Klassifizierungsversion aktualisiert den Exportprozess für den Datenuntersuchungsbericht. Dieses Export-Update ist nützlich, um zusätzliche Analysen Ihrer Daten durchzuführen, zusätzliche Visualisierungen der Daten zu erstellen oder die Ergebnisse Ihrer Datenuntersuchung mit anderen zu teilen.

Bisher war der Export des Data Investigation-Berichts auf 10.000 Zeilen beschränkt. Mit dieser Version wurde die Beschränkung aufgehoben, sodass Sie alle Ihre Daten exportieren können. Diese Änderung ermöglicht Ihnen den Export von mehr Daten aus Ihren Datenuntersuchungsberichten und bietet Ihnen so mehr Flexibilität bei Ihrer Datenanalyse.

Sie können die Arbeitsumgebung, Volumes, Zielordner und entweder das JSON- oder CSV-Format auswählen. Der exportierte Dateiname enthält einen Zeitstempel, der Ihnen hilft, den Zeitpunkt des Datenexports zu identifizieren.

Zu den unterstützten Arbeitsumgebungen gehören:

- Cloud Volumes ONTAP
- FSx für ONTAP
- ONTAP
- Gruppe „Freigeben“

Für den Export von Daten aus dem Data Investigation-Bericht gelten die folgenden Einschränkungen:

- Die maximale Anzahl der herunterzuladenden Datensätze beträgt 500 Millionen pro Typ (Dateien, Verzeichnisse und Tabellen).
- Der Export von einer Million Datensätzen dauert voraussichtlich etwa 35 Minuten.

Einzelheiten zur Datenuntersuchung und zum Bericht finden Sie unter "Untersuchen Sie die in Ihrer Organisation gespeicherten Daten" .

16. Dezember 2024

Version 1.38

Diese BlueXP classification Klassifizierungsversion enthält allgemeine Verbesserungen und Fehlerbehebungen.

4. November 2024

Version 1.37

Diese BlueXP classification Klassifizierungsversion enthält die folgenden Updates.

Unterstützung für RHEL 8.10

Diese Version bietet zusätzlich zu den zuvor unterstützten Versionen Unterstützung für Red Hat Enterprise Linux v8.10. Dies gilt für jede manuelle Vor-Ort-Installation der BlueXP classification, einschließlich Dark-Site-Bereitstellungen.

Die folgenden Betriebssysteme erfordern die Verwendung der Podman-Container-Engine und die BlueXP classification 1.30 oder höher: Red Hat Enterprise Linux Version 8.8, 8.10, 9.0, 9.1, 9.2, 9.3 und 9.4.

Erfahren Sie mehr über "BlueXP classification" .

Unterstützung für NFS v4.1

Diese Version bietet zusätzlich zu den zuvor unterstützten Versionen Unterstützung für NFS v4.1.

Erfahren Sie mehr über "BlueXP classification" .

10. Oktober 2024

Version 1.36

Unterstützung für RHEL 9.4

Diese Version bietet zusätzlich zu den zuvor unterstützten Versionen Unterstützung für Red Hat Enterprise Linux v9.4. Dies gilt für jede manuelle Vor-Ort-Installation der BlueXP classification, einschließlich Dark-Site-Bereitstellungen.

Die folgenden Betriebssysteme erfordern die Verwendung der Podman-Container-Engine und die BlueXP classification 1.30 oder höher: Red Hat Enterprise Linux Version 8.8, 9.0, 9.1, 9.2, 9.3 und 9.4.

Erfahren Sie mehr über "Übersicht über die BlueXP classification" .

Verbesserte Scan-Leistung

Diese Version bietet eine verbesserte Scanleistung.

2. September 2024

Version 1.35

Scannen Sie StorageGRID Daten

Die BlueXP classification unterstützt das Scannen von Daten in StorageGRID.

Weitere Einzelheiten finden Sie unter"Scannen Sie StorageGRID Daten" .

05. August 2024

Version 1.34

Diese BlueXP classification Klassifizierungsversion enthält das folgende Update.

Wechsel von CentOS zu Ubuntu

Die BlueXP classification hat ihr Linux-Betriebssystem für Microsoft Azure und Google Cloud Platform (GCP) von CentOS 7.9 auf Ubuntu 22.04 aktualisiert.

Einzelheiten zur Bereitstellung finden Sie unter "Installieren Sie auf einem Linux-Host mit Internetzugang und bereiten Sie das Linux-Hostsystem vor" .

01. Juli 2024

Version 1.33

Ubuntu unterstützt

Diese Version unterstützt die Linux-Plattform Ubuntu 24.04.

Mapping-Scans erfassen Metadaten

Die folgenden Metadaten werden während Mapping-Scans aus Dateien extrahiert und in den Dashboards „Governance“, „Compliance“ und „Untersuchung“ angezeigt:

- Arbeitsumfeld
- Art der Arbeitsumgebung
- Speicherrepository
- Dateityp
- Genutzte Kapazität
- Anzahl der Dateien
- Dateigröße
- Dateierstellung
- Letzter Dateizugriff
- Datei zuletzt geändert
- Uhrzeit der Dateierkennung
- Berechtigungsextraktion

Zusätzliche Daten in Dashboards

Diese Version aktualisiert, welche Daten während Mapping-Scans in den Dashboards „Governance“, „Compliance“ und „Untersuchung“ angezeigt werden.

Weitere Informationen finden Sie unter "Was ist der Unterschied zwischen Mapping- und Klassifizierungsscans?" .

05. Juni 2024

Version 1.32

Neue Spalte „Mapping-Status“ auf der Konfigurationsseite

Diese Version zeigt jetzt auf der Konfigurationsseite eine neue Spalte mit dem Zuordnungsstatus an. Mithilfe der neuen Spalte können Sie erkennen, ob die Zuordnung ausgeführt wird, sich in der Warteschlange befindet, angehalten wurde oder mehr.

Erläuterungen zu den Status finden Sie unter "Scaneinstellungen ändern" .

15. Mai 2024

Version 1.31

Die Klassifizierung ist als Kerndienst innerhalb von BlueXP verfügbar

Die BlueXP classification ist jetzt als Kernfunktion innerhalb von BlueXP ohne zusätzliche Kosten für bis zu 500 TiB gescannter Daten pro Connector verfügbar. Es ist keine Klassifizierungslizenz oder kostenpflichtiges Abonnement erforderlich. Da wir die BlueXP classification mit dieser neuen Version auf das Scannen von NetApp -Speichersystemen konzentrieren, stehen einige ältere Funktionen nur Kunden zur Verfügung, die zuvor eine Lizenz erworben haben. Die Nutzung dieser Legacy-Funktionen erlischt mit Ablauf des kostenpflichtigen Vertrags.

Die Datenklassifizierung setzt keine Begrenzung für die Menge der Daten, die gescannt werden kann. Jeder Konsolenagent unterstützt das Scannen und Anzeigen von 500 TiB Daten. Um mehr als 500 TiB Daten zu scannen,"einen anderen Konsolenagenten installieren" Dann"eine weitere Data Classification-Instanz bereitstellen" . + Die Konsolen-Benutzeroberfläche zeigt Daten von einem einzelnen Connector an. Tipps zum Anzeigen von Daten von mehreren Konsolenagenten finden Sie unter"Arbeiten mit mehreren Konsolenagenten" .

01. April 2024

Version 1.30

Unterstützung für RHEL v8.8 und v9.3 BlueXP classification hinzugefügt

Diese Version bietet Unterstützung für Red Hat Enterprise Linux v8.8 und v9.3 zusätzlich zur zuvor unterstützten Version 9.x, die Podman anstelle der Docker-Engine erfordert. Dies gilt für jede manuelle Vor-Ort-Installation der BlueXP classification.

Die folgenden Betriebssysteme erfordern die Verwendung der Podman-Container-Engine und die BlueXP classification 1.30 oder höher: Red Hat Enterprise Linux Version 8.8, 9.0, 9.1, 9.2 und 9.3.

Erfahren Sie mehr über "Übersicht über die BlueXP classification" .

Die BlueXP classification wird unterstützt, wenn Sie den Connector auf einem RHEL 8- oder 9-Host installieren, der sich vor Ort befindet. Es wird nicht unterstützt, wenn sich der RHEL 8- oder 9-Host in AWS, Azure oder Google Cloud befindet.

Option zum Aktivieren der Überwachungsprotokollerfassung entfernt

Die Option zum Aktivieren der Überwachungsprotokollerfassung wurde deaktiviert.

Scangeschwindigkeit verbessert

Die Scanleistung auf sekundären Scannerknoten wurde verbessert. Sie können weitere Scannerknoten hinzufügen, wenn Sie für Ihre Scans zusätzliche Verarbeitungsleistung benötigen. Weitere Einzelheiten finden Sie unter "Installieren Sie die BlueXP classification auf einem Host mit Internetzugang" .

Automatische Upgrades

Wenn Sie die BlueXP classification auf einem System mit Internetzugang bereitgestellt haben, wird das System automatisch aktualisiert. Bisher erfolgte das Upgrade nach einer bestimmten Zeitspanne seit der letzten Benutzeraktivität. Mit dieser Version wird die BlueXP classification automatisch aktualisiert, wenn die Ortszeit zwischen 1:00 und 5:00 Uhr liegt. Wenn die Ortszeit außerhalb dieser Zeiten liegt, erfolgt das Upgrade nach Ablauf einer bestimmten Zeit seit der letzten Benutzeraktivität. Weitere Einzelheiten finden Sie unter "Installation auf einem Linux-Host mit Internetzugang" .

Wenn Sie die BlueXP classification ohne Internetzugang bereitgestellt haben, müssen Sie ein manuelles Upgrade durchführen. Weitere Einzelheiten finden Sie unter "Installieren Sie die BlueXP classification auf einem Linux-Host ohne Internetzugang" .

04. März 2024

Version 1.29

Jetzt können Sie das Scannen von Daten ausschließen, die sich in bestimmten Datenquellenverzeichnissen befinden

Wenn Sie möchten, dass die BlueXP classification das Scannen von Daten ausschließt, die sich in bestimmten Datenquellenverzeichnissen befinden, können Sie diese Verzeichnisnamen zu einer Konfigurationsdatei hinzufügen, die von der BlueXP classification verarbeitet wird. Mit dieser Funktion können Sie das Scannen von Verzeichnissen vermeiden, die unnötig sind oder zu falsch positiven Ergebnissen bezüglich personenbezogener Daten führen würden.

"Mehr erfahren" .

Die Unterstützung für extragroße Instanzen ist jetzt qualifiziert

Wenn Sie die BlueXP classification zum Scannen von mehr als 250 Millionen Dateien benötigen, können Sie eine extragroße Instanz in Ihrer Cloud-Bereitstellung oder lokalen Installation verwenden. Ein solches System kann bis zu 500 Millionen Dateien scannen.

"Mehr erfahren" .

10. Januar 2024

Version 1.27

Auf der Untersuchungsseite werden neben der Gesamtzahl der Elemente auch die Gesamtgröße angezeigt.

Die gefilterten Ergebnisse auf der Untersuchungsseite zeigen neben der Gesamtzahl der Dateien auch die Gesamtgröße der Elemente an. Dies kann beim Verschieben, Löschen von Dateien und mehr hilfreich sein.

Konfigurieren Sie zusätzliche Gruppen-IDs als „Offen für die Organisation“.

Jetzt können Sie Gruppen-IDs in NFS so konfigurieren, dass sie direkt aus der BlueXP classification als „Offen für die Organisation“ betrachtet werden, wenn die Gruppe ursprünglich nicht mit dieser Berechtigung eingerichtet wurde. Alle Dateien und Ordner, an die diese Gruppen-IDs angehängt sind, werden auf der Seite „Untersuchungsdetails“ als „Für Organisation geöffnet“ angezeigt. Erfahren Sie, wie Sie"zusätzliche Gruppen-

IDs als „offen für die Organisation“ hinzufügen" .

14. Dezember 2023

Version 1.26.6

Diese Version enthielt einige kleinere Verbesserungen.

Mit der Version wurden außerdem die folgenden Optionen entfernt:

- Die Option zum Aktivieren der Überwachungsprotokollerfassung wurde deaktiviert.
- Während der Verzeichnisuntersuchung ist die Option zum Berechnen der Anzahl personenbezogener Daten (PII) nach Verzeichnissen nicht verfügbar. Weitere Informationen finden Sie unter "Untersuchen Sie die in Ihrer Organisation gespeicherten Daten" .
- Die Option zum Integrieren von Daten mithilfe von Azure Information Protection (AIP)-Beschriftungen wurde deaktiviert.

06. November 2023

Version 1.26.3

Die folgenden Probleme wurden in dieser Version behoben

- Eine Inkonsistenz bei der Anzeige der Anzahl der vom System gescannten Dateien in Dashboards wurde behoben.
- Verbessertes Scanverhalten durch Verarbeitung und Meldung von Dateien und Verzeichnissen mit Sonderzeichen im Namen und in den Metadaten.

04. Oktober 2023

Version 1.26

Unterstützung für lokale Installationen der BlueXP classification auf RHEL Version 9

Die Versionen 8 und 9 von Red Hat Enterprise Linux unterstützen die Docker-Engine nicht, die für die Installation der BlueXP classification erforderlich war. Wir unterstützen jetzt die Installation der BlueXP classification auf RHEL 9.0, 9.1 und 9.2 unter Verwendung von Podman Version 4 oder höher als Container-Infrastruktur. Wenn Ihre Umgebung die Verwendung der neuesten Versionen von RHEL erfordert, können Sie jetzt bei der Verwendung von Podman die BlueXP classification (Version 1.26 oder höher) installieren.

Derzeit unterstützen wir bei der Verwendung von RHEL 9.x keine Dark-Site-Installationen oder verteilten Scan-Umgebungen (mit einem Master und Remote-Scannerknoten).

05. September 2023

Version 1.25

Kleine und mittlere Bereitstellungen vorübergehend nicht verfügbar

Wenn Sie eine Instanz der BlueXP classification in AWS bereitstellen, ist die Option zum Auswählen von **Bereitstellen > Konfiguration** und zum Auswählen einer kleinen oder mittelgroßen Instanz derzeit nicht verfügbar. Sie können die Instanz weiterhin mit der großen Instanzgröße bereitstellen, indem Sie **Bereitstellen > Bereitstellen** auswählen.

Wenden Sie Tags auf bis zu 100.000 Elemente von der Seite „Untersuchungsergebnisse“ an

In der Vergangenheit konnten Sie auf der Seite „Untersuchungsergebnisse“ Tags immer nur auf eine Seite gleichzeitig anwenden (20 Elemente). Jetzt können Sie **alle** Elemente auf den Seiten mit den Untersuchungsergebnissen auswählen und allen Elementen Tags zuweisen – bis zu 100.000 Elementen gleichzeitig.

Identifizieren Sie doppelte Dateien mit einer Mindestdateigröße von 1 MB

Die BlueXP classification diente früher nur zur Identifizierung doppelter Dateien, wenn die Dateien 50 MB oder größer waren. Jetzt können doppelte Dateien ab 1 MB identifiziert werden. Sie können die Filter „Dateigröße“ und „Duplikate“ auf der Untersuchungsseite verwenden, um zu sehen, welche Dateien einer bestimmten Größe in Ihrer Umgebung dupliziert sind.

17. Juli 2023

Version 1.24

Zwei neue Arten deutscher personenbezogener Daten werden durch die BlueXP classification identifiziert

Die BlueXP classification kann Dateien identifizieren und kategorisieren, die die folgenden Datentypen enthalten:

- Deutscher Personalausweisnummer
- Deutsche Sozialversicherungsnummer

"Sehen Sie sich alle Arten personenbezogener Daten an, die die BlueXP classification in Ihren Daten identifizieren kann" .

Die BlueXP classification wird im eingeschränkten und privaten Modus vollständig unterstützt.

Die BlueXP classification wird jetzt auf Websites ohne Internetzugang (privater Modus) und mit begrenztem ausgehenden Internetzugang (eingeschränkter Modus) vollständig unterstützt. "Erfahren Sie mehr über die BlueXP -Bereitstellungsmodi für den Connector" .

Möglichkeit, Versionen beim Upgrade einer Installation im privaten Modus der BlueXP classification zu überspringen

Jetzt können Sie auf eine neuere Version der BlueXP classification aktualisieren, auch wenn diese nicht sequentiell ist. Dies bedeutet, dass die derzeitige Einschränkung, die BlueXP classification jeweils um eine Version zu aktualisieren, nicht mehr erforderlich ist. Diese Funktion ist ab Version 1.24 relevant.

Die BlueXP classification -API ist jetzt verfügbar

Mit der BlueXP classification -API können Sie Aktionen ausführen, Abfragen erstellen und Informationen zu den von Ihnen gescannten Daten exportieren. Die interaktive Dokumentation ist mit Swagger verfügbar. Die Dokumentation ist in mehrere Kategorien unterteilt, darunter Untersuchung, Compliance, Governance und Konfiguration. Jede Kategorie ist ein Verweis auf die Registerkarten in der BlueXP classification -Benutzeroberfläche.

"Erfahren Sie mehr über die BlueXP classification -APIs" .

06. Juni 2023

Version 1.23

Bei der Suche nach Namen betroffener Personen wird jetzt Japanisch unterstützt

Bei der Suche nach dem Namen einer Person als Antwort auf eine Anfrage zum Zugriff auf personenbezogene

Daten (Data Subject Access Request, DSAR) können jetzt japanische Namen eingegeben werden. Sie können eine"Bericht über die Auskunftsersuchen betroffener Personen" mit den daraus resultierenden Informationen. Sie können auch japanische Namen in das Feld eingeben."Filter „Betroffene Person“ auf der Seite „Datenuntersuchung“" um Dateien zu identifizieren, die den Namen des Betreffs enthalten.

Ubuntu ist jetzt eine unterstützte Linux-Distribution, auf der Sie die BlueXP classification installieren können

Ubuntu 22.04 wurde als unterstütztes Betriebssystem für die BlueXP classification qualifiziert. Sie können die BlueXP classification auf einem Ubuntu Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud installieren, wenn Sie Version 1.23 des Installationsprogramms verwenden. "Erfahren Sie, wie Sie die BlueXP classification auf einem Host mit installiertem Ubuntu installieren." .

Red Hat Enterprise Linux 8.6 und 8.7 werden bei Installationen der neuen BlueXP classification nicht mehr unterstützt

Diese Versionen werden bei neuen Bereitstellungen nicht unterstützt, da Red Hat Docker nicht mehr unterstützt, was jedoch eine Voraussetzung ist. Wenn Sie über eine vorhandene BlueXP classification Klassifizierungsmaschine verfügen, die unter RHEL 8.6 oder 8.7 läuft, wird NetApp Ihre Konfiguration weiterhin unterstützen.

Die BlueXP classification kann als FPolicy Collector konfiguriert werden, um FPolicy-Ereignisse von ONTAP -Systemen zu empfangen

Sie können die Erfassung von Dateizugriffs-Auditprotokollen in Ihrem BlueXP classification Klassifizierungssystem für Dateizugriffsereignisse aktivieren, die auf Volumes in Ihren Arbeitsumgebungen erkannt wurden. Die BlueXP classification kann die folgenden Arten von FPolicy-Ereignissen und die Benutzer erfassen, die die Aktionen an Ihren Dateien ausgeführt haben: Erstellen, Lesen, Schreiben, Löschen, Umbenennen, Besitzer/Berechtigungen ändern und SACL/DACL ändern.

Data Sense BYOL-Lizenzen werden jetzt in Dark Sites unterstützt

Jetzt können Sie Ihre Data Sense BYOL-Lizenz in die BlueXP digital wallet auf einer Dark Site hochladen, sodass Sie benachrichtigt werden, wenn Ihre Lizenz fast aufgebraucht ist.

03. April 2023

Version 1.22

Neuer Data Discovery-Bewertungsbericht

Der Data Discovery Assessment Report bietet eine umfassende Analyse Ihrer gescannten Umgebung, um die Ergebnisse des Systems hervorzuheben und Problembereiche sowie mögliche Abhilfemaßnahmen aufzuzeigen. Das Ziel dieses Berichts besteht darin, das Bewusstsein für Bedenken hinsichtlich der Datenverwaltung, Datensicherheitsrisiken und Datenkonformitätslücken Ihres Datensatzes zu schärfen. "Erfahren Sie, wie Sie den Data Discovery Assessment Report erstellen und verwenden" .

Möglichkeit, die BlueXP classification auf kleineren Instanzen in der Cloud bereitzustellen

Wenn Sie die BlueXP classification von einem BlueXP Connector in einer AWS-Umgebung bereitstellen, können Sie jetzt aus zwei kleineren Instanztypen auswählen, als bei der Standardinstanz verfügbar sind. Wenn Sie eine kleine Umgebung scannen, können Sie auf diese Weise Cloud-Kosten sparen. Bei der Verwendung der kleineren Instanz gibt es jedoch einige Einschränkungen. "Sehen Sie sich die verfügbaren Instanztypen und Einschränkungen an" .

Jetzt ist ein eigenständiges Skript verfügbar, um Ihr Linux-System vor der Installation der BlueXP classification zu qualifizieren

Wenn Sie unabhängig von der Ausführung der BlueXP classification überprüfen möchten, ob Ihr Linux-System alle Voraussetzungen erfüllt, können Sie ein separates Skript herunterladen, das nur die Voraussetzungen testet. "Erfahren Sie, wie Sie überprüfen können, ob Ihr Linux-Host für die Installation der BlueXP classification

bereit ist." .

07. März 2023

Version 1.21

Neue Funktionalität zum Hinzufügen Ihrer eigenen benutzerdefinierten Kategorien aus der BlueXP classification -Benutzeroberfläche

Mit der BlueXP classification können Sie jetzt Ihre eigenen benutzerdefinierten Kategorien hinzufügen, sodass die BlueXP classification die Dateien identifiziert, die in diese Kategorien passen. Die BlueXP classification hat viele "vordefinierte Kategorien" , sodass Sie mit dieser Funktion benutzerdefinierte Kategorien hinzufügen können, um zu ermitteln, wo in Ihren Daten Informationen zu finden sind, die für Ihr Unternehmen einzigartig sind.

Jetzt können Sie benutzerdefinierte Schlüsselwörter aus der BlueXP classification -Benutzeroberfläche hinzufügen

Die BlueXP classification bietet seit einiger Zeit die Möglichkeit, benutzerdefinierte Schlüsselwörter hinzuzufügen, die die BlueXP classification in zukünftigen Scans identifiziert. Sie mussten sich jedoch beim Linux-Host der BlueXP classification anmelden und eine Befehlszeilenschnittstelle verwenden, um die Schlüsselwörter hinzuzufügen. In dieser Version können Sie in der BlueXP classification -Benutzeroberfläche benutzerdefinierte Schlüsselwörter hinzufügen, sodass das Hinzufügen und Bearbeiten dieser Schlüsselwörter sehr einfach ist.

Möglichkeit, die BlueXP classification so einzustellen, dass Dateien nicht gescannt werden, wenn die „letzte Zugriffszeit“ geändert wird

Wenn die BlueXP classification nicht über ausreichende Schreibberechtigungen verfügt, scannt das System standardmäßig keine Dateien in Ihren Volumes, da die BlueXP classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen jedoch egal ist, ob die letzte Zugriffszeit in Ihren Dateien auf die ursprüngliche Zeit zurückgesetzt wird, können Sie dieses Verhalten auf der Konfigurationsseite überschreiben, sodass die BlueXP classification die Volumes unabhängig von den Berechtigungen scannt.

In Verbindung mit dieser Funktion wurde ein neuer Filter mit dem Namen „Scan Analysis Event“ hinzugefügt, sodass Sie die Dateien anzeigen können, die nicht klassifiziert wurden, weil die BlueXP classification den letzten Zugriffszeitpunkt nicht wiederherstellen konnte, oder die Dateien, die klassifiziert wurden, obwohl die BlueXP classification den letzten Zugriffszeitpunkt nicht wiederherstellen konnte.

"Erfahren Sie mehr über den „Zeitstempel des letzten Zugriffs“ und die Berechtigungen, die für die BlueXP classification erforderlich sind" .

Drei neue Arten personenbezogener Daten werden durch die BlueXP classification identifiziert

Die BlueXP classification kann Dateien identifizieren und kategorisieren, die die folgenden Datentypen enthalten:

- Nummer des Personalausweises für Botswana (Omang).
- Botswana-Passnummer
- Nationaler Registrierungsausweis von Singapur (NRIC)

"Sehen Sie sich alle Arten personenbezogener Daten an, die die BlueXP classification in Ihren Daten identifizieren kann" .

Aktualisierte Funktionalität für Verzeichnisse

- Die Option „Light CSV Report“ für Datenuntersuchungsberichte enthält jetzt Informationen aus Verzeichnissen.
- Der Zeitfilter „Letzter Zugriff“ zeigt jetzt sowohl für Dateien als auch für Verzeichnisse die letzte Zugriffszeit an.

Installationsverbesserungen

- Das BlueXP classification Klassifizierungsinstallationsprogramm für Websites ohne Internetzugang (Dark Sites) führt jetzt eine Vorprüfung durch, um sicherzustellen, dass Ihre System- und Netzwerkanforderungen für eine erfolgreiche Installation erfüllt sind.
- Die Installations-Audit-Logdateien werden nun gespeichert. Sie werden in `/ops/netapp/install_logs` .

05. Februar 2023

Version 1.20

Möglichkeit, richtlinienbasierte Benachrichtigungs-E-Mails an jede E-Mail-Adresse zu senden

In früheren Versionen der BlueXP classification konnten Sie den BlueXP Benutzern in Ihrem Konto E-Mail-Benachrichtigungen senden, wenn bestimmte kritische Richtlinien Ergebnisse zurückgaben. Mit dieser Funktion können Sie Benachrichtigungen zum Schutz Ihrer Daten erhalten, wenn Sie nicht online sind. Jetzt können Sie E-Mail-Benachrichtigungen aus Richtlinien auch an alle anderen Benutzer (bis zu 20 E-Mail-Adressen) senden, die nicht in Ihrem BlueXP Konto sind.

"Erfahren Sie mehr über das Senden von E-Mail-Benachrichtigungen basierend auf Richtlinienergebnissen" .

Jetzt können Sie persönliche Muster aus der BlueXP classification -UI hinzufügen

Die BlueXP classification bietet seit einiger Zeit die Möglichkeit, benutzerdefinierte „persönliche Daten“ hinzuzufügen, die die BlueXP classification bei zukünftigen Scans identifiziert. Sie mussten sich jedoch beim Linux-Host der BlueXP classification anmelden und eine Befehlszeile verwenden, um die benutzerdefinierten Muster hinzuzufügen. In dieser Version besteht die Möglichkeit, persönliche Muster mithilfe eines regulären Ausdrucks hinzuzufügen, in der BlueXP classification -Benutzeroberfläche, wodurch das Hinzufügen und Bearbeiten dieser benutzerdefinierten Muster sehr einfach wird.

Möglichkeit zum Verschieben von 15 Millionen Dateien mithilfe der BlueXP classification

In der Vergangenheit konnten Sie mit der BlueXP classification maximal 100.000 Quelldateien auf eine beliebige NFS-Freigabe verschieben. Jetzt können Sie bis zu 15 Millionen Dateien gleichzeitig verschieben.

Möglichkeit, die Anzahl der Benutzer anzuzeigen, die Zugriff auf SharePoint Online-Dateien haben

Der Filter „Anzahl der Benutzer mit Zugriff“ unterstützt jetzt Dateien, die in SharePoint Online-Repositorys gespeichert sind. In der Vergangenheit wurden nur Dateien auf CIFS-Freigaben unterstützt. Beachten Sie, dass SharePoint-Gruppen, die nicht auf Active Directory basieren, derzeit nicht in diesem Filter gezählt werden.

Der neue Status „Teilweiser Erfolg“ wurde zum Aktionsstatus-Bereich hinzugefügt

Der neue Status „Teilweise erfolgreich“ zeigt an, dass eine BlueXP classification Klassifizierungsaktion abgeschlossen ist und einige Elemente fehlgeschlagen und andere erfolgreich waren, beispielsweise wenn Sie 100 Dateien verschieben oder löschen. Darüber hinaus wurde der Status „Fertig“ in „Erfolgreich“ umbenannt. In der Vergangenheit listete der Status „Abgeschlossen“ möglicherweise erfolgreiche und fehlgeschlagene Aktionen auf. Jetzt bedeutet der Status „Erfolgreich“, dass alle Aktionen für alle Elemente erfolgreich waren. "So zeigen Sie das Aktionsstatusfeld an" .

09. Januar 2023

Version 1.19

Möglichkeit, ein Diagramm von Dateien anzuzeigen, die vertrauliche Daten enthalten und zu freizügig sind

Dem Governance-Dashboard wurde ein neuer Bereich „Sensible Daten und umfassende Berechtigungen“ hinzugefügt, der eine Heatmap von Dateien bereitstellt, die sensible Daten enthalten (einschließlich sensibler und sensibler personenbezogener Daten) und zu freizügig sind. Auf diese Weise können Sie erkennen, wo bei sensiblen Daten möglicherweise Risiken bestehen. "Mehr erfahren" .

Auf der Seite „Datenuntersuchung“ sind drei neue Filter verfügbar

Es stehen neue Filter zur Verfügung, um die auf der Seite „Datenuntersuchung“ angezeigten Ergebnisse zu verfeinern:

- Der Filter „Anzahl der Benutzer mit Zugriff“ zeigt an, welche Dateien und Ordner für eine bestimmte Anzahl von Benutzern geöffnet sind. Sie können einen Zahlenbereich auswählen, um die Ergebnisse zu verfeinern – beispielsweise um zu sehen, auf welche Dateien 51–100 Benutzer zugreifen können.
- Mit den Filtern „Erstellungszeit“, „Entdeckungszeit“, „Zuletzt geändert“ und „Zuletzt aufgerufen“ können Sie jetzt einen benutzerdefinierten Datumsbereich erstellen, anstatt nur einen vordefinierten Tagesbereich auszuwählen. Sie können beispielsweise nach Dateien suchen, deren „Erstellungszeit“ älter als 6 Monate ist, oder deren „Zuletzt geändert“-Datum innerhalb der „letzten 10 Tage“ liegt.
- Mit dem Filter „Dateipfad“ können Sie jetzt Pfade angeben, die Sie aus den gefilterten Abfrageergebnissen ausschließen möchten. Wenn Sie Pfade eingeben, um bestimmte Daten sowohl ein- als auch auszuschließen, sucht die BlueXP classification zuerst nach allen Dateien in den eingeschlossenen Pfaden, entfernt dann Dateien aus ausgeschlossenen Pfaden und zeigt anschließend die Ergebnisse an.

"Sehen Sie sich die Liste aller Filter an, die Sie zur Untersuchung Ihrer Daten verwenden können" .

Die BlueXP classification kann die japanische Individualnummer identifizieren

Die BlueXP classification kann Dateien identifizieren und kategorisieren, die die japanische Individualnummer (auch als „Meine Nummer“ bekannt) enthalten. Dies umfasst sowohl die persönliche als auch die geschäftliche My Number. "Sehen Sie sich alle Arten personenbezogener Daten an, die die BlueXP classification in Ihren Daten identifizieren kann" .

Bekannte Einschränkungen bei der NetApp Data Classification

Bekannte Einschränkungen kennzeichnen Funktionen, die in dieser Version nicht unterstützt werden oder nicht richtig zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

Deaktivierte Optionen für die NetApp Data Classification

Mit der Version vom Dezember 2023 (Version 1.26.6) wurden die folgenden Optionen entfernt:

- Die Option zum Aktivieren der Überwachungsprotokollerfassung wurde deaktiviert.
- Während der Verzeichnisuntersuchung ist die Option zum Berechnen der Anzahl personenbezogener Daten (PII) nach Verzeichnissen nicht verfügbar.
- Die Option zum Integrieren von Daten mithilfe von Azure Information Protection (AIP)-Beschriftungen wurde deaktiviert.

Datenklassifizierungsscan

Bei Datenklassifizierungsscans treten die folgenden Einschränkungen auf.

Die Datenklassifizierung scannt nur eine Freigabe unter einem Volume

Wenn Sie mehrere Dateifreigaben unter einem einzigen Volume haben, scannt die Datenklassifizierung die Freigabe mit der höchsten Hierarchie. Wenn Sie beispielsweise Aktien wie die folgenden haben:

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

In dieser Konfiguration werden nur die Daten in /A gescannt. Die Daten in /C und /D werden nicht gescannt.

Problemumgehung

Es gibt eine Problemumgehung, um sicherzustellen, dass Sie Daten von allen Freigaben in Ihrem Volume scannen. Gehen Sie folgendermaßen vor:

1. Fügen Sie im System das zu scannende Volume hinzu.
2. Nachdem die Datenklassifizierung das Scannen des Volumes abgeschlossen hat, gehen Sie zur Seite *Datenuntersuchung* und erstellen Sie einen Filter, um zu sehen, welche Freigabe gescannt wird:

   Filtern Sie die Daten nach „Systemname“ und „Verzeichnistyp = Freigabe“, um zu sehen, welche Freigabe gescannt wird.

3. Rufen Sie die vollständige Liste der im Volume vorhandenen Freigaben ab, damit Sie sehen können, welche Freigaben nicht gescannt werden.
4. "Die restlichen Anteile einer Anteilsgruppe hinzufügen" .

   Fügen Sie alle Anteile einzeln hinzu, zum Beispiel:

   ```
   /C
   /D
   ```

5. Führen Sie diese Schritte für jedes Volume im System aus, das über mehrere Freigaben verfügt.

Zeitstempel des letzten Zugriffs

Wenn Data Classification einen Scan eines Verzeichnisses durchführt, wirkt sich der Scan auf das Feld **Zuletzt aufgerufen** des Verzeichnisses aus. Wenn Sie das Feld **Letzter Zugriff** anzeigen, geben diese Metadaten entweder das Datum und die Uhrzeit des Scans oder den letzten Zeitpunkt wieder, zu dem ein Benutzer auf das Verzeichnis zugegriffen hat.

Erste Schritte

Erfahren Sie mehr über die NetApp Data Classification

NetApp Data Classification ist ein Data-Governance-Service für die NetApp Console , der Ihre unternehmenseigenen Datenquellen vor Ort und in der Cloud scannt, um Daten zuzuordnen und zu klassifizieren und private Informationen zu identifizieren. Dies kann dazu beitragen, Ihr Sicherheits- und Compliance-Risiko zu verringern, die Speicherkosten zu senken und Ihre Datenmigrationsprojekte zu unterstützen.

Ab Version 1.31 ist die Datenklassifizierung als Kernfunktion in der NetApp Console verfügbar. Es fallen keine zusätzlichen Kosten an. Es ist keine Klassifizierungslizenz oder kein Abonnement erforderlich. + Wenn Sie die Vorgängerversion 1.30 oder früher verwendet haben, ist diese Version verfügbar, bis Ihr Abonnement abläuft.

NetApp Console

Auf die Datenklassifizierung kann über die NetApp Console zugegriffen werden.

Die NetApp Console ermöglicht eine zentrale Verwaltung von NetApp -Speicher- und Datendiensten in lokalen und Cloud-Umgebungen auf Unternehmensebene. Die Konsole ist für den Zugriff auf und die Nutzung der NetApp -Datendienste erforderlich. Als Verwaltungsschnittstelle ermöglicht es Ihnen, viele Speicherressourcen über eine Schnittstelle zu verwalten. Konsolenadministratoren können den Zugriff auf Speicher und Dienste für alle Systeme innerhalb des Unternehmens steuern.

Sie benötigen weder eine Lizenz noch ein Abonnement, um die NetApp Console zu verwenden. Es fallen nur dann Kosten an, wenn Sie Konsolenagenten in Ihrer Cloud bereitstellen müssen, um die Konnektivität zu Ihren Speichersystemen oder NetApp -Datendiensten sicherzustellen. Einige NetApp -Datendienste, auf die über die Konsole zugegriffen werden kann, sind jedoch lizenz- oder abonnementbasiert.

Erfahren Sie mehr über die"NetApp Console" .

Features

Bei der Datenklassifizierung werden künstliche Intelligenz (KI), natürliche Sprachverarbeitung (NLP) und maschinelles Lernen (ML) verwendet, um die gescannten Inhalte zu verstehen, Entitäten zu extrahieren und die Inhalte entsprechend zu kategorisieren. Dadurch kann die Datenklassifizierung die folgenden Funktionsbereiche bereitstellen.

"Erfahren Sie mehr über Anwendungsfälle für die Datenklassifizierung" .

Einhaltung der Vorschriften

Die Datenklassifizierung bietet mehrere Tools, die Sie bei Ihren Compliance-Bemühungen unterstützen können. Sie können die Datenklassifizierung für Folgendes verwenden:

- Identifizieren Sie personenbezogene Daten (PII).
- Identifizieren Sie ein breites Spektrum sensibler personenbezogener Daten gemäß den Datenschutzbestimmungen DSGVO, CCPA, PCI und HIPAA.
- Beantworten Sie Anfragen zum Zugriff auf personenbezogene Daten (DSAR) basierend auf Name oder E-Mail-Adresse.

Stärkung der Sicherheit

Durch die Datenklassifizierung können Daten identifiziert werden, bei denen das Risiko besteht, dass für kriminelle Zwecke auf sie zugegriffen wird. Sie können die Datenklassifizierung für Folgendes verwenden:

- Identifizieren Sie alle Dateien und Verzeichnisse (Freigaben und Ordner) mit offenen Berechtigungen, die Ihrer gesamten Organisation oder der Öffentlichkeit zugänglich sind.
- Identifizieren Sie vertrauliche Daten, die sich außerhalb des ursprünglichen, dedizierten Speicherorts befinden.
- Halten Sie die Richtlinien zur Datenaufbewahrung ein.
- Verwenden Sie *Richtlinien*, um neue Sicherheitsprobleme automatisch zu erkennen, damit das Sicherheitspersonal sofort Maßnahmen ergreifen kann.

Optimieren Sie die Speichernutzung

Die Datenklassifizierung bietet Tools, die Ihnen bei der Reduzierung der Gesamtbetriebskosten (TCO) Ihres Speichers helfen können. Sie können die Datenklassifizierung für Folgendes verwenden:

- Steigern Sie die Speichereffizienz, indem Sie doppelte oder nicht geschäftsbezogene Daten identifizieren.
- Sparen Sie Speicherkosten, indem Sie inaktive Daten identifizieren, die Sie in einen kostengünstigeren Objektspeicher verschieben können. "Erfahren Sie mehr über das Tiering von Cloud Volumes ONTAP -Systemen" . "Erfahren Sie mehr über das Tiering von On-Premises ONTAP -Systemen" .

Unterstützte Systeme und Datenquellen

Die Datenklassifizierung kann strukturierte und unstrukturierte Daten aus den folgenden Systemtypen und Datenquellen scannen und analysieren:

Systeme

- Amazon FSx for NetApp ONTAP -Verwaltung
- Azure NetApp Files
- Cloud Volumes ONTAP (bereitgestellt in AWS, Azure oder GCP)
- On-Premises- ONTAP -Cluster
- StorageGRID
- Google Cloud NetApp Volumes

Datenquellen

- NetApp -Dateifreigaben
- Datenbanken:
  - Amazon Relational Database Service (Amazon RDS)
  - MongoDB
  - MySQL
  - Orakel
  - PostgreSQL
  - SAP HANA
  - SQL Server (MSSQL)

Die Datenklassifizierung unterstützt die NFS-Versionen 3.x, 4.0 und 4.1 sowie die CIFS-Versionen 1.x, 2.0, 2.1 und 3.0.

Kosten

Die Nutzung der Datenklassifizierung ist kostenlos. Es ist keine Klassifizierungslizenz oder kostenpflichtiges Abonnement erforderlich.

Infrastrukturkosten

- Für die Installation der Datenklassifizierung in der Cloud ist die Bereitstellung einer Cloud-Instanz erforderlich, wofür vom Cloud-Anbieter, bei dem die Instanz bereitgestellt wird, Gebühren anfallen. Sehen der Instanztyp, der für jeden Cloud-Anbieter bereitgestellt wird . Wenn Sie Data Classification auf einem lokalen System installieren, fallen keine Kosten an.
- Für die Datenklassifizierung müssen Sie einen Konsolenagenten bereitgestellt haben. In vielen Fällen verfügen Sie aufgrund anderer Speicher und Dienste, die Sie in der Konsole verwenden, bereits über einen Konsolenagenten. Für die Konsolen-Agentinstanz fallen Gebühren seitens des Cloud-Anbieters an, bei dem sie bereitgestellt wird. Siehe die "Typ der Instanz, die für jeden Cloud-Anbieter bereitgestellt wird" . Wenn Sie den Konsolenagenten auf einem lokalen System installieren, fallen keine Kosten an.

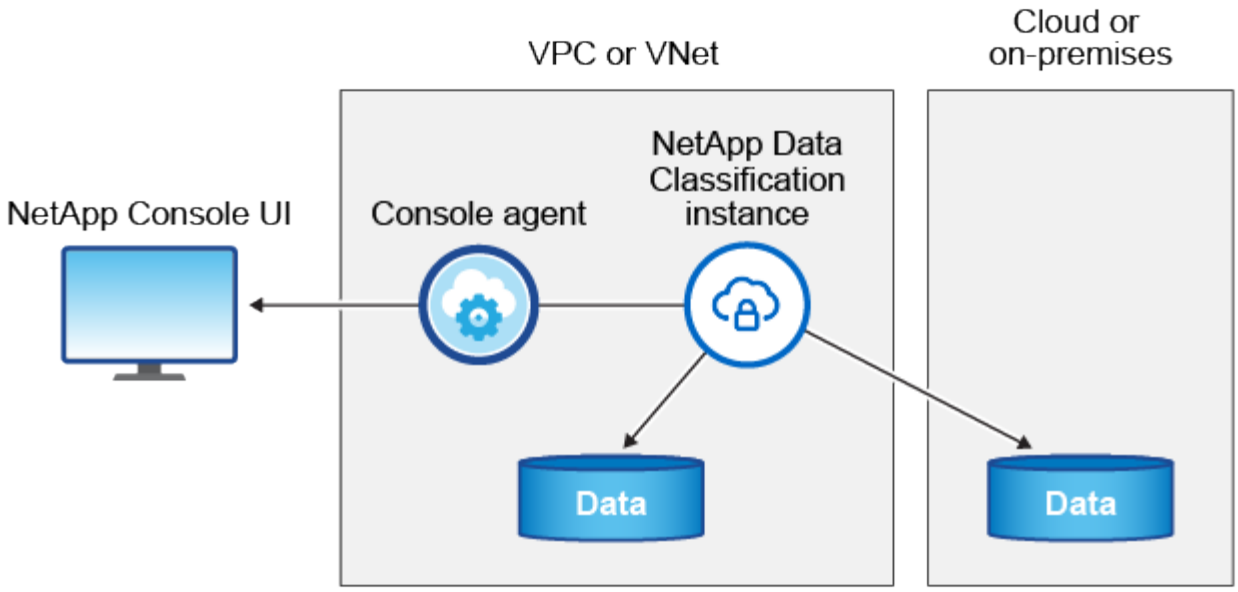
Kosten für die Datenübertragung

Die Kosten für die Datenübertragung hängen von Ihrer Konfiguration ab. Wenn sich die Datenklassifizierungsinstanz und die Datenquelle in derselben Verfügbarkeitszone und Region befinden, fallen keine Datenübertragungskosten an. Wenn sich die Datenquelle, beispielsweise ein Cloud Volumes ONTAP -System, jedoch in einer anderen Availability Zone oder Region befindet, werden Ihnen von Ihrem Cloud-Anbieter die Kosten für die Datenübertragung in Rechnung gestellt. Weitere Einzelheiten finden Sie unter diesen Links:

- "AWS: Preise für Amazon Elastic Compute Cloud (Amazon EC2)"
- "Microsoft Azure: Details zu den Bandbreitenpreisen"
- "Google Cloud: Preise für Storage Transfer Service"

Die Datenklassifizierungsinstanz

Wenn Sie die Datenklassifizierung in der Cloud bereitstellen, stellt die Konsole die Instanz im selben Subnetz wie der Konsolenagent bereit. "Erfahren Sie mehr über den Konsolenagenten."



Beachten Sie Folgendes zur Standardinstanz:

- In AWS läuft die Datenklassifizierung auf einem "m6i.4xlarge-Instanz" mit einer 500 GiB GP2-Festplatte. Das Betriebssystem-Image ist Amazon Linux 2. Bei der Bereitstellung in AWS können Sie eine kleinere Instanzgröße wählen, wenn Sie eine kleine Datenmenge scannen.
- In Azure läuft die Datenklassifizierung auf einem"Standard_D16s_v3 VM" mit einer 500-GiB-Festplatte. Das Betriebssystem-Image ist Ubuntu 22.04.
- In GCP läuft die Datenklassifizierung auf einem"n2-standard-16 VM" mit einer persistenten 500-GiB-Standardfestplatte. Das Betriebssystem-Image ist Ubuntu 22.04.
- In Regionen, in denen die Standardinstanz nicht verfügbar ist, wird die Datenklassifizierung auf einer alternativen Instanz ausgeführt. "Alternative Instance-Typen anzeigen" .
- Die Instanz trägt den Namen *CloudCompliance* und ist mit einem generierten Hash (UUID) verknüpft. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Pro Konsolenagent wird nur eine Datenklassifizierungsinstanz bereitgestellt.

Sie können die Datenklassifizierung auch auf einem Linux-Host in Ihren Räumlichkeiten oder auf einem Host bei Ihrem bevorzugten Cloud-Anbieter bereitstellen. Die Software funktioniert unabhängig von der gewählten Installationsmethode auf genau dieselbe Weise. Upgrades der Datenklassifizierungssoftware werden automatisiert, solange die Instanz über einen Internetzugang verfügt.

Die Instanz sollte ständig ausgeführt werden, da die Datenklassifizierung die Daten kontinuierlich scannt.

Auf verschiedenen Instanztypen bereitstellen

Überprüfen Sie die folgenden Spezifikationen für Instanztypen:

Systemgröße	Technische Daten	Einschränkungen
Extragroß	32 CPUs, 128 GB RAM, 1 TiB SSD	Kann bis zu 500 Millionen Dateien scannen.
Groß (Standard)	16 CPUs, 64 GB RAM, 500 GiB SSD	Kann bis zu 250 Millionen Dateien scannen.

Wenn Sie bei der Bereitstellung der Datenklassifizierung in Azure oder GCP Unterstützung benötigen und einen kleineren Instanztyp verwenden möchten, senden Sie eine E-Mail an ng-contact-data-sense@netapp.com.

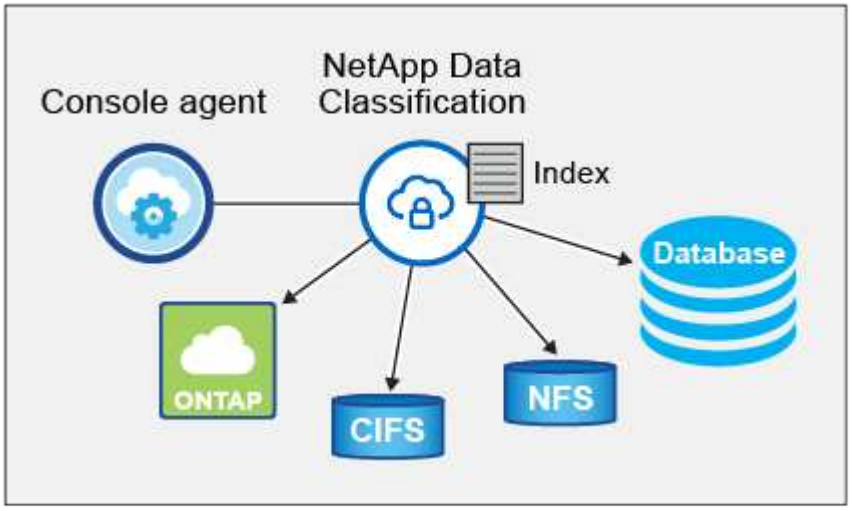
Funktionsweise des Datenklassifizierungsscans

Im Großen und Ganzen funktioniert das Scannen der Datenklassifizierung folgendermaßen:

1. Sie stellen eine Instanz der Datenklassifizierung in der Konsole bereit.
2. Sie aktivieren die Zuordnung auf hoher Ebene (sogenannte *Mapping only*-Scans) oder die Tiefenscans (sogenannte *Map & Classify*-Scans) für eine oder mehrere Datenquellen.
3. Bei der Datenklassifizierung werden Daten mithilfe eines KI-Lernprozesses gescannt.
4. Sie verwenden die bereitgestellten Dashboards und Berichtstools, um Ihre Compliance- und Governance-Bemühungen zu unterstützen.

Nachdem Sie die Datenklassifizierung aktiviert und die zu scannenden Repositories ausgewählt haben (das sind die Volumes, Datenbankschemata oder andere Benutzerdaten), beginnt das Programm sofort mit dem Scannen der Daten, um persönliche und vertrauliche Daten zu identifizieren. In den meisten Fällen sollten Sie sich auf das Scannen von Live-Produktionsdaten konzentrieren, anstatt auf Backups, Spiegel oder DR-Sites. Anschließend ordnet die Datenklassifizierung Ihre Organisationsdaten zu, kategorisiert jede Datei und identifiziert und extrahiert Entitäten und vordefinierte Muster in den Daten. Das Ergebnis des Scans ist ein Index mit persönlichen Informationen, sensiblen persönlichen Informationen, Datenkategorien und Dateitypen.

Data Classification stellt wie jeder andere Client eine Verbindung zu den Daten her, indem es NFS- und CIFS-Volumes einbindet. Auf NFS-Volumes wird automatisch schreibgeschützt zugegriffen, während Sie zum Scannen von CIFS-Volumes Active Directory-Anmeldeinformationen angeben müssen.



Nach dem ersten Scan scannt die Datenklassifizierung Ihre Daten kontinuierlich im Round-Robin-Verfahren, um inkrementelle Änderungen zu erkennen. Aus diesem Grund ist es wichtig, die Instanz am Laufen zu halten.

Sie können Scans auf Volume- oder Datenbankschemaebene aktivieren und deaktivieren.

Die Datenklassifizierung setzt keine Begrenzung für die Menge der Daten, die gescannt werden kann. Jeder Konsolenagent unterstützt das Scannen und Anzeigen von 500 TiB Daten. Um mehr als 500 TiB Daten zu scannen,"einen anderen Konsolenagenten installieren" Dann"eine weitere Data Classification-Instanz bereitstellen" . + Die Konsolen-Benutzeroberfläche zeigt Daten von einem einzelnen Connector an. Tipps zum Anzeigen von Daten von mehreren Konsolenagenten finden Sie unter"Arbeiten mit mehreren Konsolenagenten" .

Was ist der Unterschied zwischen Mapping- und Klassifizierungsscans?

Sie können in der Datenklassifizierung zwei Arten von Scans durchführen:

- **Nur-Mapping-Scans** bieten nur einen allgemeinen Überblick über Ihre Daten und werden für ausgewählte Datenquellen durchgeführt. Reine Mapping-Scans benötigen weniger Zeit als Mapping- und Klassifizierungs-Scans, da sie nicht auf Dateien zugreifen, um die darin enthaltenen Daten anzuzeigen. Möglicherweise möchten Sie dies zunächst tun, um Forschungsbereiche zu identifizieren und dann einen Map & Classify-Scan für diese Bereiche durchführen.
- **Map & Classify-Scans** ermöglichen ein gründliches Scannen Ihrer Daten.

Einzelheiten zu den Unterschieden zwischen Mapping- und Klassifizierungsscans finden Sie unter"Was ist der Unterschied zwischen Mapping- und Klassifizierungsscans?" .

Informationen, die durch die Datenklassifizierung kategorisiert werden

Die Datenklassifizierung sammelt, indiziert und ordnet die folgenden Daten Kategorien zu:

- **Standardmetadaten** zu Dateien: Dateityp, Größe, Erstellungs- und Änderungsdatum usw.
- **Personenbezogene Daten**: Persönlich identifizierbare Informationen (PII) wie E-Mail-Adressen, Identifikationsnummern oder Kreditkartennummern, die durch die Datenklassifizierung anhand bestimmter Wörter, Zeichenfolgen und Muster in den Dateien identifiziert werden. "Erfahren Sie mehr über personenbezogene Daten" .
- **Sensible personenbezogene Daten**: Besondere Arten sensibler personenbezogener Daten (SPII), wie Gesundheitsdaten, ethnische Herkunft oder politische Meinungen, wie in der Datenschutz-Grundverordnung (DSGVO) und anderen Datenschutzbestimmungen definiert. "Erfahren Sie mehr über sensible personenbezogene Daten" .
- **Kategorien**: Die Datenklassifizierung nimmt die gescannten Daten und unterteilt sie in verschiedene Kategorien. Kategorien sind Themen, die auf einer KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Mehr über Kategorien erfahren" .
- **Typen**: Die Datenklassifizierung nimmt die gescannten Daten und unterteilt sie nach Dateityp. "Erfahren Sie mehr über Typen" .
- **Namensentitätserkennung**: Die Datenklassifizierung verwendet KI, um die natürlichen Namen von Personen aus Dokumenten zu extrahieren. "Erfahren Sie mehr über die Beantwortung von Auskunftsersuchen betroffener Personen" .

Netzwerkübersicht

Data Classification stellt einen einzelnen Server oder Cluster bereit, wo immer Sie möchten: in der Cloud oder vor Ort. Die Server stellen über Standardprotokolle eine Verbindung zu den Datenquellen her und indizieren die Ergebnisse in einem Elasticsearch-Cluster, der ebenfalls auf denselben Servern bereitgestellt wird. Dies ermöglicht die Unterstützung von Multi-Cloud-, Cross-Cloud-, Private-Cloud- und On-Premises-Umgebungen.

Die Konsole stellt die Datenklassifizierungsinstanz mit einer Sicherheitsgruppe bereit, die eingehende HTTP-

Verbindungen vom Konsolenagenten ermöglicht.

Wenn Sie die Konsole im SaaS-Modus verwenden, wird die Verbindung zur Konsole über HTTPS bereitgestellt und die privaten Daten, die zwischen Ihrem Browser und der Datenklassifizierungsinstanz gesendet werden, werden mit einer End-to-End-Verschlüsselung unter Verwendung von TLS 1.2 gesichert, was bedeutet, dass NetApp und Dritte sie nicht lesen können.

Die Outbound-Regeln sind völlig offen. Für die Installation und Aktualisierung der Datenklassifizierungssoftware sowie zum Senden von Nutzungsmetriken ist ein Internetzugang erforderlich.

Wenn Sie strenge Netzwerkanforderungen haben,"Erfahren Sie mehr über die Endpunkte, die die Datenklassifizierung kontaktiert" .

Zugriff auf die NetApp Data Classification

Sie können über die NetApp Console auf die NetApp Data Classification zugreifen.

Um sich bei der Konsole anzumelden, können Sie Ihre Anmeldeinformationen für die NetApp Support-Site verwenden oder sich mit Ihrer E-Mail-Adresse und einem Kennwort für die NetApp Console anmelden. "Erfahren Sie mehr über die Anmeldung bei der Konsole" .

Für bestimmte Aufgaben sind bestimmte Konsolenbenutzerrollen erforderlich. "Erfahren Sie mehr über die Konsolenzugriffsrollen für alle Dienste" .

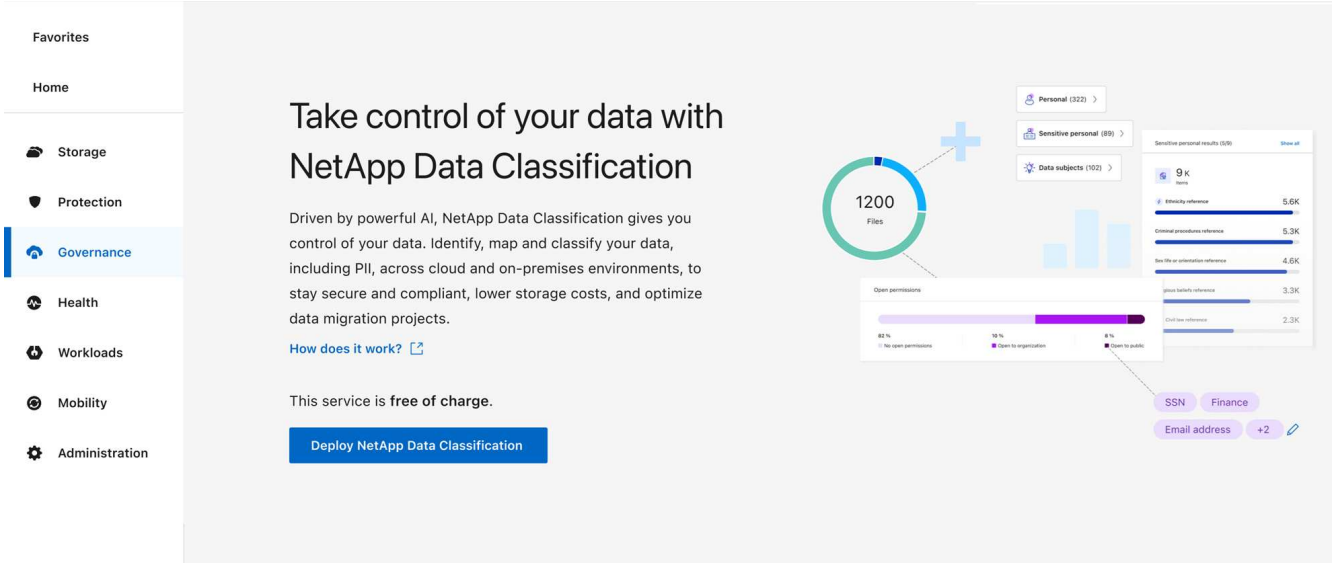
Bevor Sie beginnen

- "Sie sollten einen Konsolenagenten hinzufügen."
- "Finden Sie heraus, welcher Bereitstellungsstil für die Datenklassifizierung zu Ihrer Arbeitslast passt."

Schritte

1. Navigieren Sie in einem Webbrowser zu"Konsole" .
2. Melden Sie sich bei der Konsole an.
3. Wählen Sie auf der Hauptseite der NetApp Console*Governance* > **Datenklassifizierung**.
4. Wenn Sie zum ersten Mal auf die Datenklassifizierung zugreifen, wird die Zielseite angezeigt.

   Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**, um mit der Bereitstellung Ihrer Klassifizierungsinstanz zu beginnen. Weitere Informationen finden Sie unter"Welche Datenklassifizierungsbereitstellung sollten Sie verwenden?"



Andernfalls wird das Dashboard zur Datenklassifizierung angezeigt.

Datenklassifizierung bereitstellen

Welche NetApp Data Classification Bereitstellung sollten Sie verwenden?

Sie können NetApp Data Classification auf verschiedene Arten bereitstellen. Erfahren Sie, welche Methode Ihren Anforderungen entspricht.

Die Datenklassifizierung kann auf folgende Arten bereitgestellt werden:

- "Bereitstellung in der Cloud mithilfe der Konsole" . Die Konsole stellt die Datenklassifizierungsinstanz im selben Cloud-Anbieternetzwerk bereit wie der Konsolenagent.
- "Installation auf einem Linux-Host mit Internetzugang" . Installieren Sie Data Classification auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud, der über Internetzugang verfügt. Diese Art der Installation kann eine gute Option sein, wenn Sie lokale ONTAP -Systeme lieber mit einer Datenklassifizierungsinstanz scannen möchten, die sich ebenfalls vor Ort befindet. Dies ist jedoch keine Voraussetzung.
- "Installation auf einem Linux-Host an einem lokalen Standort ohne Internetzugang", auch als *privater Modus* bekannt. Dieser Installationstyp, der ein Installationsskript verwendet, hat keine Verbindung zur SaaS-Ebene der Konsole.

> Der private BlueXP Modus (alte BlueXP -Schnittstelle) wird normalerweise in lokalen Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, darunter AWS Secret Cloud, AWS Top Secret Cloud und Azure IL6. NetApp unterstützt diese Umgebungen weiterhin mit der alten BlueXP Schnittstelle. Die Dokumentation zum privaten Modus in der alten BlueXP Schnittstelle finden Sie unter"PDF-Dokumentation für den privaten Modus von BlueXP" .

Sowohl die Installation auf einem Linux-Host mit Internetzugang als auch die lokale Installation auf einem Linux-Host ohne Internetzugang verwenden ein Installationsskript. Das Skript prüft zunächst, ob das System und die Umgebung die Voraussetzungen erfüllen. Wenn die Voraussetzungen erfüllt sind, beginnt die Installation. Wenn Sie die Voraussetzungen unabhängig von der Ausführung der Data Classification-Installation überprüfen möchten, können Sie ein separates Softwarepaket herunterladen, das nur die

Voraussetzungen testet.

Weitere Informationen finden Sie unter "Überprüfen Sie, ob Ihr Linux-Host für die Installation der Datenklassifizierung bereit ist." .

Stellen Sie NetApp Data Classification mithilfe der NetApp Console in der Cloud bereit

Sie können NetApp Data Classification mit der NetApp Console in der Cloud bereitstellen. Die Konsole stellt die Datenklassifizierungsinstanz im selben Cloud-Anbieternetzwerk bereit wie der Konsolenagent.

Beachten Sie, dass Sie auch"Installieren Sie Data Classification auf einem Linux-Host mit Internetzugang" . Diese Art der Installation kann eine gute Option sein, wenn Sie es vorziehen, lokale ONTAP -Systeme mit einer Datenklassifizierungsinstanz zu scannen, die sich ebenfalls vor Ort befindet – dies ist jedoch keine Voraussetzung. Die Software funktioniert unabhängig von der gewählten Installationsmethode auf genau dieselbe Weise.

Schnellstart

Beginnen Sie schnell, indem Sie diese Schritte befolgen, oder scrollen Sie nach unten zu den restlichen Abschnitten, um alle Einzelheiten zu erfahren.

Erstellen eines Konsolenagenten

Wenn Sie noch keinen Konsolenagenten haben, erstellen Sie einen. Sehen "Erstellen eines Konsolenagenten in AWS" , "Erstellen eines Konsolenagenten in Azure" , oder "Erstellen eines Konsolenagenten in GCP" .

Sie können auch "Installieren Sie den Konsolen-Agenten vor Ort" auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud.

Voraussetzungen

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllt. Dazu gehören der ausgehende Internetzugriff für die Instanz, die Konnektivität zwischen dem Konsolenagenten und der Datenklassifizierung über Port 443 und mehr. siehe vollständige Liste.

Datenklassifizierung bereitstellen

Starten Sie den Installationsassistenten, um die Data Classification-Instanz in der Cloud bereitzustellen.

Erstellen eines Konsolenagenten

Wenn Sie noch keinen Konsolenagenten haben, erstellen Sie einen Konsolenagenten bei Ihrem Cloud-Anbieter. Sehen "Erstellen eines Konsolenagenten in AWS" oder "Erstellen eines Konsolenagenten in Azure" , oder "Erstellen eines Konsolenagenten in GCP" . In den meisten Fällen haben Sie wahrscheinlich einen Konsolenagenten eingerichtet, bevor Sie versuchen, die Datenklassifizierung zu aktivieren, da die meisten "Für Konsolenfunktionen ist ein Konsolenagent erforderlich" , aber es gibt Fälle, in denen Sie jetzt eines einrichten müssen.

Es gibt einige Szenarien, in denen Sie einen Konsolenagenten verwenden müssen, der bei einem bestimmten

Cloud-Anbieter bereitgestellt wird:

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS oder Amazon FSx für ONTAP -Buckets verwenden Sie einen Konsolenagenten in AWS.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konsolenagenten in Azure.
  - Für Azure NetApp Files muss es in derselben Region bereitgestellt werden wie die Volumes, die Sie scannen möchten.
- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP verwenden Sie einen Konsolenagenten in GCP.

Lokale ONTAP -Systeme, NetApp Dateifreigaben und Datenbanken können mit einem dieser Cloud-Konsolen-Agenten gescannt werden.

Beachten Sie, dass Sie auch "Installieren Sie den Konsolen-Agenten vor Ort" auf einem Linux-Host in Ihrem Netzwerk oder in der Cloud. Einige Benutzer, die die Datenklassifizierung vor Ort installieren möchten, entscheiden sich möglicherweise auch für die Installation des Konsolenagenten vor Ort.

Wie Sie sehen, kann es Situationen geben, in denen Sie verwenden müssen "mehrere Konsolenagenten" .

Die Datenklassifizierung setzt keine Begrenzung für die Menge der Daten, die gescannt werden kann. Jeder Konsolenagent unterstützt das Scannen und Anzeigen von 500 TiB Daten. Um mehr als 500 TiB Daten zu scannen,"einen anderen Konsolenagenten installieren" Dann"eine weitere Data Classification-Instanz bereitstellen" . + Die Konsolen-Benutzeroberfläche zeigt Daten von einem einzelnen Connector an. Tipps zum Anzeigen von Daten von mehreren Konsolenagenten finden Sie unter"Arbeiten mit mehreren Konsolenagenten" .

Unterstützung der Regierung in der Region

Die Datenklassifizierung wird unterstützt, wenn der Konsolenagent in einer Regierungsregion (AWS GovCloud, Azure Gov oder Azure DoD) bereitgestellt wird. Bei einer Bereitstellung auf diese Weise unterliegt die Datenklassifizierung den folgenden Einschränkungen:

"Weitere Informationen zum Bereitstellen des Konsolenagenten in einer Regierungsregion" .

Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie die Datenklassifizierung in der Cloud bereitstellen. Wenn Sie die Datenklassifizierung in der Cloud bereitstellen, befindet sie sich im selben Subnetz wie der Konsolenagent.

Ausgehenden Internetzugriff von der Datenklassifizierung aus aktivieren

Für die Datenklassifizierung ist ein ausgehender Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxyserver für den Internetzugang verwendet, stellen Sie sicher, dass die Datenklassifizierungsinstanz über ausgehenden Internetzugang verfügt, um die folgenden Endpunkte zu kontaktieren. Der Proxy muss intransparent sein. Transparente Proxys werden derzeit nicht unterstützt.

Sehen Sie sich die entsprechende Tabelle unten an, je nachdem, ob Sie die Datenklassifizierung in AWS, Azure oder GCP bereitstellen.

Erforderliche Endpunkte für AWS

Endpunkte	Zweck
https://api.console.netapp.com	Kommunikation mit dem Konsolendienst, der NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-Website zur zentralen Benutzerauthentifizierung.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Prüfdatensätzen.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	Ermöglicht der Datenklassifizierung den Zugriff auf und das Herunterladen von Manifesten und Vorlagen sowie das Senden von Protokollen und Metriken.

Erforderliche Endpunkte für Azure

Endpunkte	Zweck
https://api.console.netapp.com	Kommunikation mit dem Konsolendienst, der NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-Website zur zentralen Benutzerauthentifizierung.
https://support.compliance.api.console.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und ermöglicht das Senden von Protokollen und Metriken.
https://support.compliance.api.console.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Prüfdatensätzen.

Erforderliche Endpunkte für GCP

Endpunkte	Zweck
https://api.console.netapp.com	Kommunikation mit dem Konsolendienst, der NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-Website zur zentralen Benutzerauthentifizierung.

Endpunkte	Zweck
https://support.compliance.api.console.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und ermöglicht das Senden von Protokollen und Metriken.
https://support.compliance.api.console.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Prüfdatensätzen.

Stellen Sie sicher, dass die Datenklassifizierung über die erforderlichen Berechtigungen verfügt

Stellen Sie sicher, dass Data Classification über die Berechtigung zum Bereitstellen von Ressourcen und Erstellen von Sicherheitsgruppen für die Data Classification-Instanz verfügt.

- "Google Cloud-Berechtigungen"
- "AWS-Berechtigungen"
- "Azure-Berechtigungen"

Stellen Sie sicher, dass der Konsolenagent auf die Datenklassifizierung zugreifen kann.

Stellen Sie die Konnektivität zwischen dem Konsolenagenten und der Datenklassifizierungsinstanz sicher. Die Sicherheitsgruppe für den Konsolenagenten muss eingehenden und ausgehenden Datenverkehr über Port 443 zur und von der Datenklassifizierungsinstanz zulassen. Diese Verbindung ermöglicht die Bereitstellung der Datenklassifizierungsinstanz und ermöglicht Ihnen die Anzeige von Informationen auf den Registerkarten „Compliance“ und „Governance“. Die Datenklassifizierung wird in Regierungsregionen in AWS und Azure unterstützt.

Für AWS- und AWS GovCloud-Bereitstellungen sind zusätzliche Sicherheitsgruppenregeln für eingehenden und ausgehenden Datenverkehr erforderlich. Sehen "Regeln für den Konsolenagenten in AWS" für Details.

Für Azure- und Azure Government-Bereitstellungen sind zusätzliche Sicherheitsgruppenregeln für eingehenden und ausgehenden Datenverkehr erforderlich. Sehen "Regeln für den Konsolen-Agent in Azure" für Details.

Stellen Sie sicher, dass die Datenklassifizierung weiterhin ausgeführt werden kann

Die Instanz zur Datenklassifizierung muss eingeschaltet bleiben, um Ihre Daten kontinuierlich zu scannen.

Sicherstellen der Webbrowser-Konnektivität zur Datenklassifizierung

Stellen Sie nach der Aktivierung der Datenklassifizierung sicher, dass Benutzer von einem Host aus auf die Konsolenschnittstelle zugreifen, der über eine Verbindung zur Datenklassifizierungsinstanz verfügt.

Die Datenklassifizierungsinstanz verwendet eine private IP-Adresse, um sicherzustellen, dass die indizierten Daten nicht über das Internet zugänglich sind. Daher muss der Webbrowser, den Sie für den Zugriff auf die Konsole verwenden, über eine Verbindung zu dieser privaten IP-Adresse verfügen. Diese Verbindung kann von einer direkten Verbindung zu Ihrem Cloud-Anbieter (z. B. einem VPN) oder von einem Host stammen, der sich im selben Netzwerk wie die Datenklassifizierungsinstanz befindet.

Überprüfen Sie Ihre vCPU-Grenzen

Stellen Sie sicher, dass das vCPU-Limit Ihres Cloud-Anbieters die Bereitstellung einer Instanz mit der erforderlichen Anzahl von Kernen zulässt. Sie müssen das vCPU-Limit für die entsprechende Instanzfamilie in der Region überprüfen, in der die Konsole ausgeführt wird. "Sehen Sie sich die erforderlichen

Instanztypen an" .

Weitere Einzelheiten zu vCPU-Grenzwerten finden Sie unter den folgenden Links:

- "AWS-Dokumentation: Amazon EC2-Servicekontingente"
- "Azure-Dokumentation: vCPU-Kontingente virtueller Computer"
- "Google Cloud-Dokumentation: Ressourcenkontingente"

Datenklassifizierung in der Cloud bereitstellen

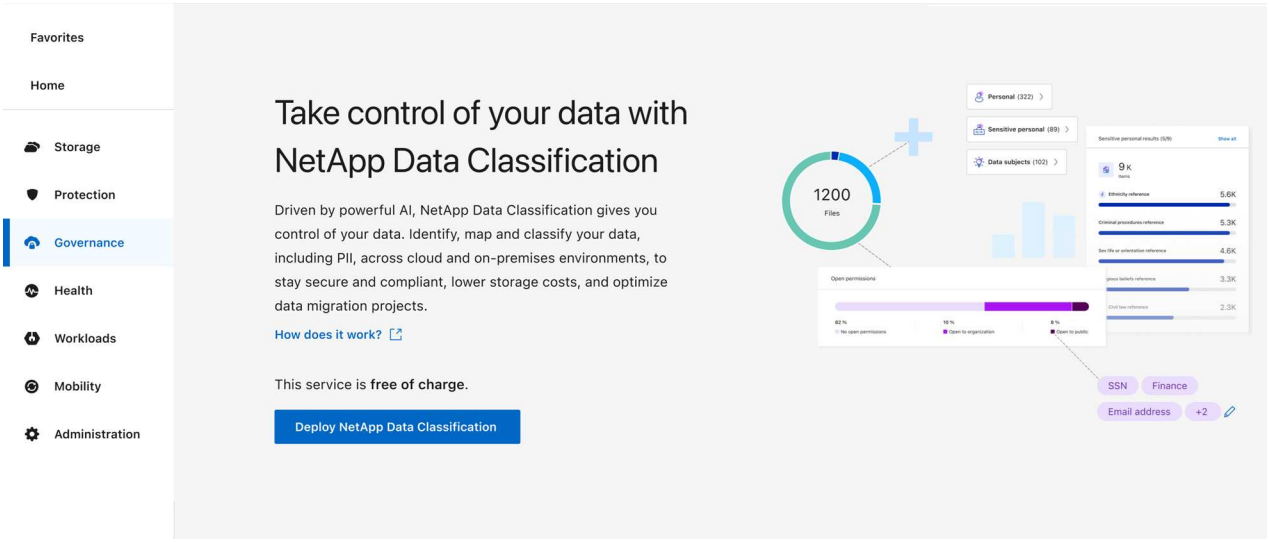
Befolgen Sie diese Schritte, um eine Instanz von Data Classification in der Cloud bereitzustellen. Der Konsolenagent stellt die Instanz in der Cloud bereit und installiert dann die Datenklassifizierungssoftware auf dieser Instanz.

In Regionen, in denen der Standardinstanztyp nicht verfügbar ist, läuft die Datenklassifizierung auf einem"alternativer Instanztyp" .

Bereitstellung in AWS

Schritte

1. Wählen Sie auf der Hauptseite der Datenklassifizierung die Option **Klassifizierung vor Ort oder in der Cloud bereitstellen**.

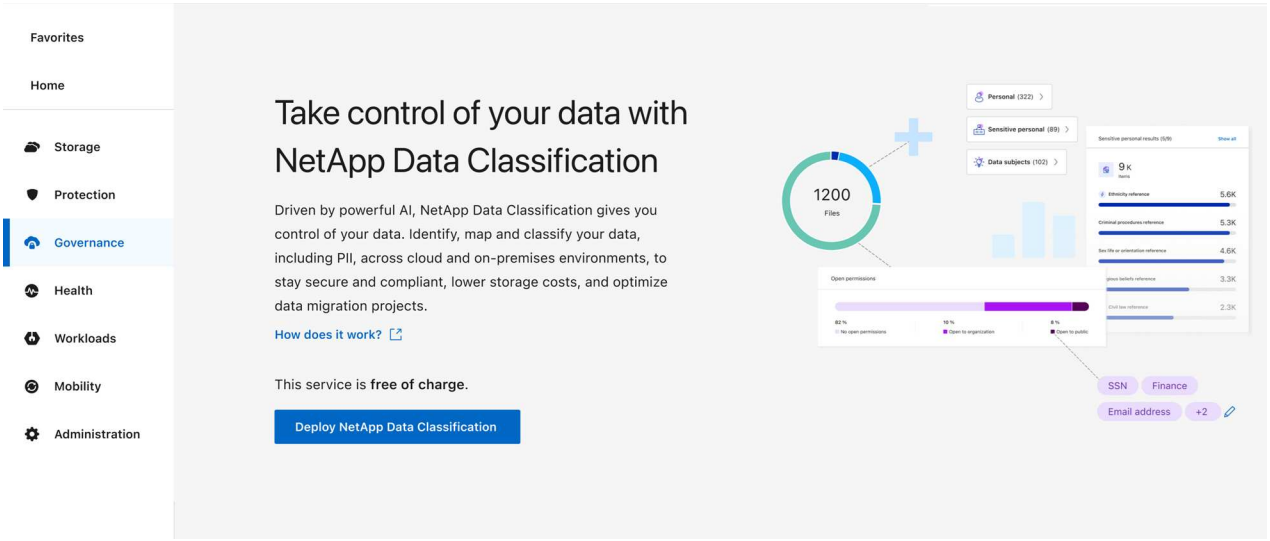


2. Wählen Sie auf der Seite „Installation“ die Option „Bereitstellen > Bereitstellen“ aus, um die Instanzgröße „Groß“ zu verwenden und den Cloud-Bereitstellungsassistenten zu starten.
3. Der Assistent zeigt den Fortschritt an, während er die Bereitstellungsschritte durchläuft. Wenn Eingaben erforderlich sind oder Probleme auftreten, werden Sie dazu aufgefordert.
4. Wenn die Instanz bereitgestellt und die Datenklassifizierung installiert ist, wählen Sie **Weiter zur Konfiguration**, um zur Seite *Konfiguration* zu gelangen.

Bereitstellen in Azure

Schritte

1. Wählen Sie auf der Hauptseite der Datenklassifizierung die Option **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



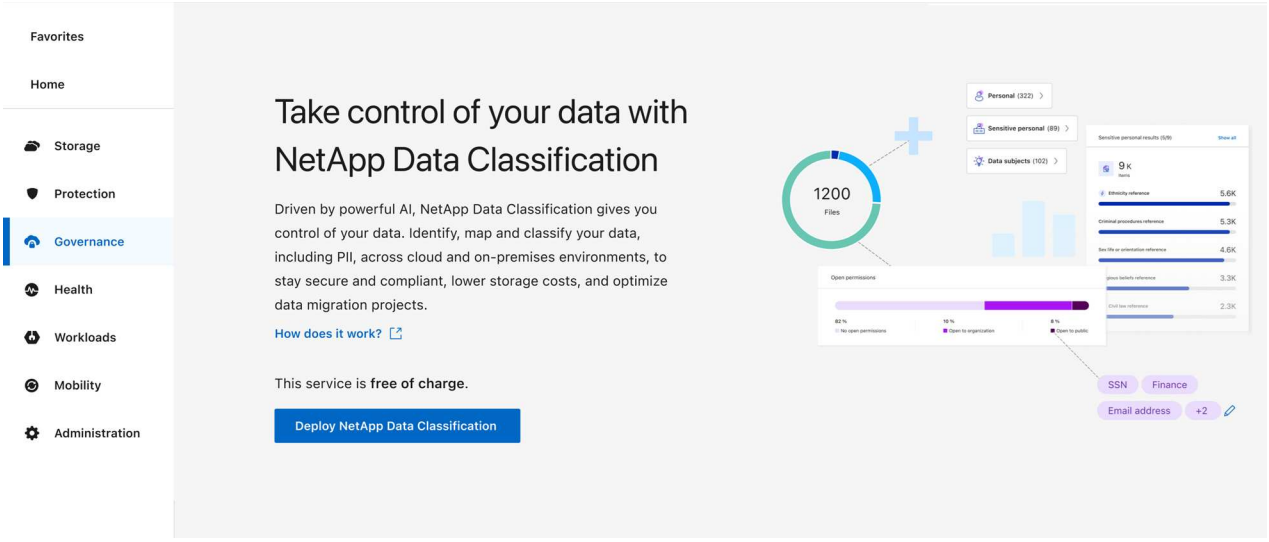
2. Wählen Sie **Bereitstellen**, um den Cloud-Bereitstellungsassistenten zu starten.

3. Der Assistent zeigt den Fortschritt an, während er die Bereitstellungsschritte durchläuft. Wenn Probleme auftreten, wird es angehalten und zur Eingabe aufgefordert.
4. Wenn die Instanz bereitgestellt und die Datenklassifizierung installiert ist, wählen Sie **Weiter zur Konfiguration**, um zur Seite *Konfiguration* zu gelangen.

Bereitstellung in Google Cloud

Schritte

1. Wählen Sie auf der Hauptseite der Datenklassifizierung **Governance > Klassifizierung** aus.
2. Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



3. Wählen Sie **Bereitstellen**, um den Cloud-Bereitstellungsassistenten zu starten.
4. Der Assistent zeigt den Fortschritt an, während er die Bereitstellungsschritte durchläuft. Wenn Probleme auftreten, wird es angehalten und zur Eingabe aufgefordert.
5. Wenn die Instanz bereitgestellt und die Datenklassifizierung installiert ist, wählen Sie **Weiter zur Konfiguration**, um zur Seite *Konfiguration* zu gelangen.

Ergebnis

Die Konsole stellt die Datenklassifizierungsinstanz bei Ihrem Cloud-Anbieter bereit.

Upgrades des Konsolenagenten und der Datenklassifizierungssoftware erfolgen automatisiert, solange die Instanzen über eine Internetverbindung verfügen.

Was kommt als Nächstes

Auf der Konfigurationsseite können Sie die Datenquellen auswählen, die Sie scannen möchten.

Installieren Sie NetApp Data Classification auf einem Host mit Internetzugang

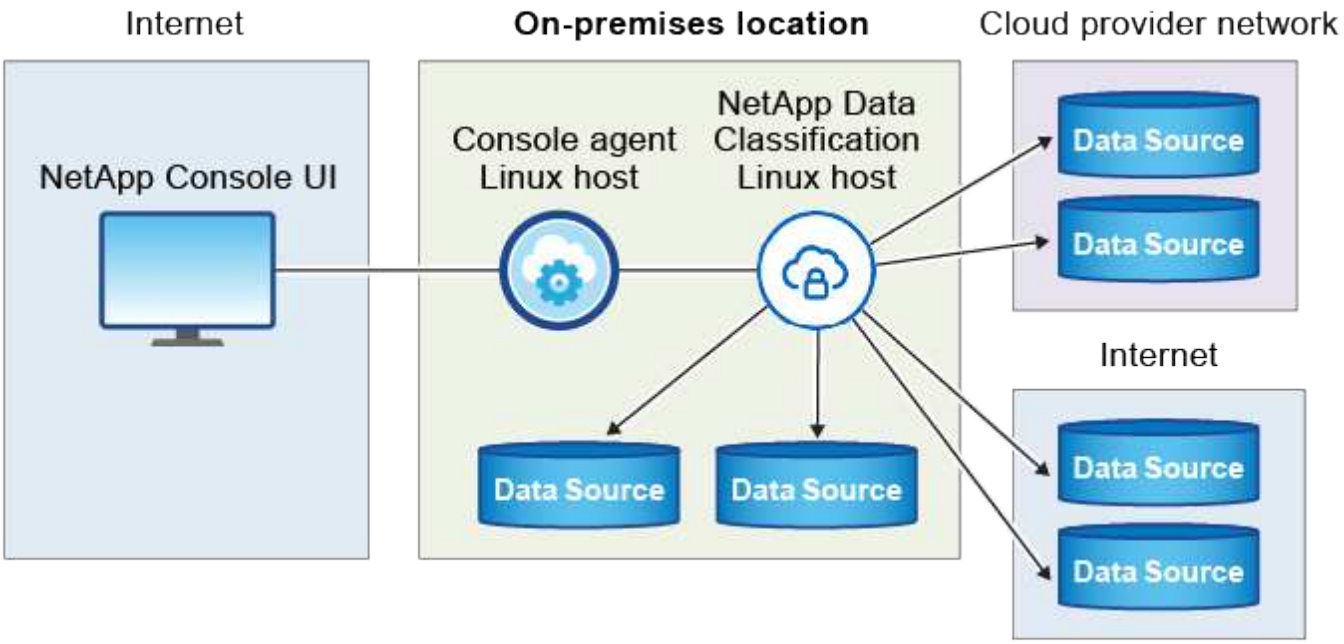
Um NetApp Data Classification auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud mit Internetzugang bereitzustellen, müssen Sie den Linux-Host manuell in Ihrem Netzwerk oder in der Cloud bereitstellen.

Die lokale Installation ist eine gute Option, wenn Sie lokale ONTAP -Systeme lieber mit einer Datenklassifizierungsinstanz scannen möchten, die sich ebenfalls vor Ort befindet. Dies ist keine

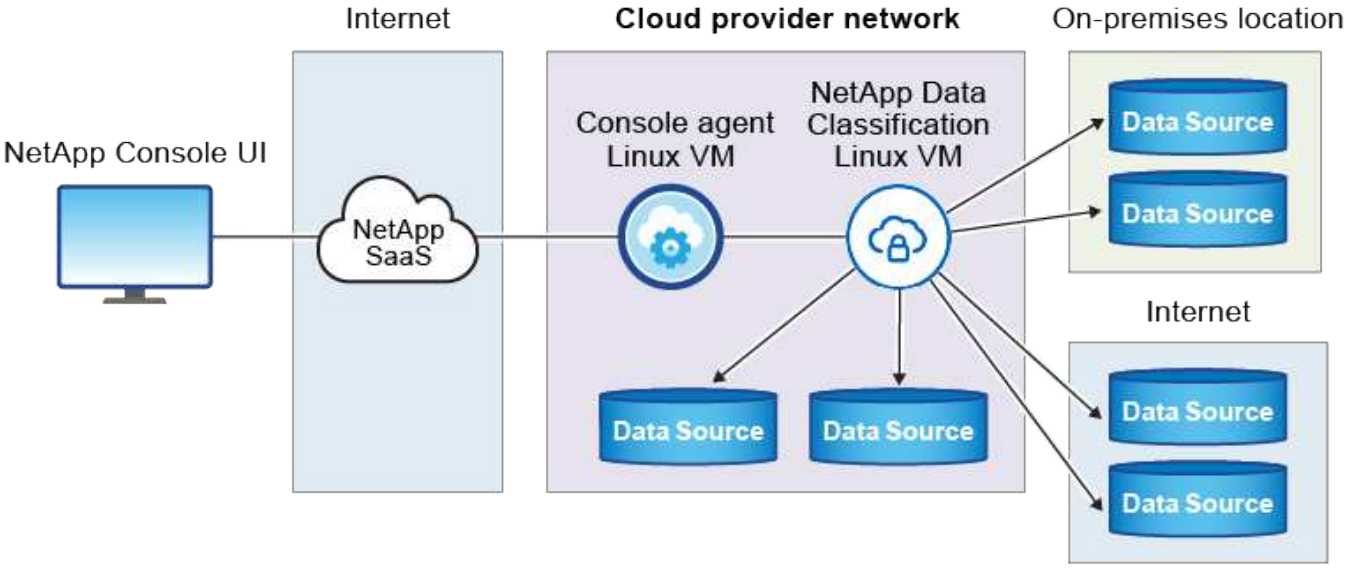
Voraussetzung. Die Software funktioniert unabhängig von der gewählten Installationsmethode gleich.

Das Installationsskript für die Datenklassifizierung prüft zunächst, ob das System und die Umgebung die erforderlichen Voraussetzungen erfüllen. Wenn alle Voraussetzungen erfüllt sind, beginnt die Installation. Wenn Sie die Voraussetzungen unabhängig von der Ausführung der Data Classification-Installation überprüfen möchten, können Sie ein separates Softwarepaket herunterladen, das nur die Voraussetzungen testet. "Erfahren Sie, wie Sie überprüfen können, ob Ihr Linux-Host für die Installation der Datenklassifizierung bereit ist." .

Die typische Installation auf einem Linux-Host *in Ihren Räumlichkeiten* verfügt über die folgenden Komponenten und Verbindungen.



Die typische Installation auf einem Linux-Host *in der Cloud* verfügt über die folgenden Komponenten und Verbindungen.



Schnellstart

Beginnen Sie schnell, indem Sie diese Schritte befolgen, oder scrollen Sie nach unten zu den restlichen Abschnitten, um alle Einzelheiten zu erfahren.

1 Erstellen eines Konsolenagenten

Wenn Sie noch keinen Konsolenagenten haben, "Stellen Sie den Konsolenagenten vor Ort bereit" auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud.

Sie können auch einen Konsolenagenten bei Ihrem Cloud-Anbieter erstellen. Sehen "Erstellen eines Konsolenagenten in AWS" , "Erstellen eines Konsolenagenten in Azure" , oder "Erstellen eines Konsolenagenten in GCP" .

2 Überprüfen der Voraussetzungen

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllt. Dazu gehören der ausgehende Internetzugriff für die Instanz, die Konnektivität zwischen dem Konsolenagenten und der Datenklassifizierung über Port 443 und mehr. Vollständige Liste anzeigen .

Sie benötigen außerdem ein Linux-System, das diefolgende Anforderungen .

3 Herunterladen und Bereitstellen der Datenklassifizierung

Laden Sie die Cloud Data Classification-Software von der NetApp -Support-Site herunter und kopieren Sie die Installationsdatei auf den Linux-Host, den Sie verwenden möchten. Starten Sie dann den Installationsassistenten und folgen Sie den Anweisungen zum Bereitstellen der Data Classification-Instanz.

Erstellen eines Konsolenagenten

Bevor Sie Data Classification installieren und verwenden können, ist ein Konsolenagent erforderlich. In den meisten Fällen haben Sie wahrscheinlich einen Konsolenagenten eingerichtet, bevor Sie versuchen, die Datenklassifizierung zu aktivieren, da die meisten "Für Konsolenfunktionen ist ein Konsolenagent erforderlich" , aber es gibt Fälle, in denen Sie jetzt eines einrichten müssen.

Informationen zum Erstellen eines solchen in der Umgebung Ihres Cloud-Anbieters finden Sie unter "Erstellen eines Konsolenagenten in AWS" , "Erstellen eines Konsolenagenten in Azure" , oder "Erstellen eines Konsolenagenten in GCP" .

Es gibt einige Szenarien, in denen Sie einen Konsolenagenten verwenden müssen, der bei einem bestimmten Cloud-Anbieter bereitgestellt wird:

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS oder Amazon FSx für ONTAP verwenden Sie einen Konsolenagenten in AWS.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konsolenagenten in Azure.

  Für Azure NetApp Files muss es in derselben Region bereitgestellt werden wie die Volumes, die Sie scannen möchten.

- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP verwenden Sie einen Konsolenagenten in GCP.

Lokale ONTAP -Systeme, NetApp Dateifreigaben und Datenbankkonten können mit jedem dieser Cloud-Konsolen-Agenten gescannt werden.

Beachten Sie, dass Sie auch "Stellen Sie den Konsolenagenten vor Ort bereit" auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud. Einige Benutzer, die Data Classification vor Ort installieren möchten, entscheiden sich möglicherweise auch für die Installation des Konsolenagenten vor Ort.

Sie benötigen die IP-Adresse oder den Hostnamen des Konsolenagentensystems, wenn Sie die Datenklassifizierung installieren. Sie verfügen über diese Informationen, wenn Sie den Konsolenagenten in Ihren Räumlichkeiten installiert haben. Wenn der Konsolenagent in der Cloud bereitgestellt wird, finden Sie diese Informationen in der Konsole: Wählen Sie das Hilfesymbol, dann **Support** und dann **Konsolenagent**.

Vorbereiten des Linux-Hostsystems

Datenklassifizierungssoftware muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Softwareanforderungen usw. erfüllt. Der Linux-Host kann sich in Ihrem Netzwerk oder in der Cloud befinden.

Stellen Sie sicher, dass die Datenklassifizierung weiterhin ausgeführt werden kann. Die Datenklassifizierungsmaschine muss eingeschaltet bleiben, um Ihre Daten kontinuierlich zu scannen.

- Die Datenklassifizierung wird auf einem Host, der gemeinsam mit anderen Anwendungen genutzt wird, nicht unterstützt – der Host muss ein dedizierter Host sein.
- Beim Aufbau des Hostsystems in Ihren Räumlichkeiten können Sie je nach Größe des Datensatzes, für den Sie einen Datenklassifizierungsscan durchführen möchten, zwischen diesen Systemgrößen wählen.

Systemgröße	CPU	RAM (Auslagerungsspeicher muss deaktiviert sein)	Scheibe
Extra groß	32 CPUs	128 GB RAM	• 1 TiB SSD auf / oder 100 GiB verfügbar auf /opt • 895 GiB verfügbar auf /var/lib/docker • 5 GiB auf /tmp • **Für Podman, 30 GB auf /var/tmp**
Groß	16 CPUs	64 GB RAM	• 500 GiB SSD auf / oder 100 GiB verfügbar auf /opt • 400 GiB verfügbar auf /var/lib/docker oder für Podman /var/lib/containers • 5 GiB auf /tmp • **Für Podman, 30 GB auf /var/tmp**

- Wenn Sie für Ihre Data Classification-Installation eine Compute-Instanz in der Cloud bereitstellen, wird empfohlen, ein System zu verwenden, das die oben genannten Systemanforderungen für „Groß“ erfüllt:

- **Amazon Elastic Compute Cloud (Amazon EC2)-Instanztyp**: „m6i.4xlarge“. "Weitere AWS-Instanztypen anzeigen" .
- **Azure-VM-Größe**: „Standard_D16s_v3“. "Weitere Azure-Instanztypen anzeigen" .
- **GCP-Maschinentyp**: „n2-standard-16“. "Weitere GCP-Instanztypen anzeigen" .

- **UNIX-Ordnerberechtigungen**: Die folgenden UNIX-Mindestberechtigungen sind erforderlich:

Ordner	Mindestberechtigungen
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Betriebssystem**:
  - Die folgenden Betriebssysteme erfordern die Verwendung der Docker-Container-Engine:
    - Red Hat Enterprise Linux Version 7.8 und 7.9
    - Ubuntu 22.04 (erfordert Data Classification Version 1.23 oder höher)
    - Ubuntu 24.04 (erfordert Data Classification Version 1.23 oder höher)
  - Die folgenden Betriebssysteme erfordern die Verwendung der Podman-Container-Engine und erfordern Data Classification Version 1.30 oder höher:
    - Red Hat Enterprise Linux Version 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 und 9.6.
  - Advanced Vector Extensions (AVX2) müssen auf dem Hostsystem aktiviert sein.
- **Red Hat Subscription Management**: Der Host muss bei Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositories zugreifen, um erforderliche Software von Drittanbietern zu aktualisieren.
- **Zusätzliche Software**: Sie müssen die folgende Software auf dem Host installieren, bevor Sie Data Classification installieren:
  - Abhängig vom verwendeten Betriebssystem müssen Sie eine der Container-Engines installieren:
    - Docker Engine Version 19.3.1 oder höher. "Installationsanweisungen anzeigen" .
    - Podman Version 4 oder höher. Um Podman zu installieren, geben Sie ein(`sudo yum install podman netavark -y`).
- Python Version 3.6 oder höher. "Installationsanweisungen anzeigen" .
  - **NTP-Überlegungen**: NetApp empfiehlt, das Datenklassifizierungssystem für die Verwendung eines Network Time Protocol (NTP)-Dienstes zu konfigurieren. Die Zeit muss zwischen dem Datenklassifizierungssystem und dem Konsolenagentsystem synchronisiert werden.
- **Firewalld-Überlegungen**: Wenn Sie planen, `firewalld` , wir empfehlen, dass Sie es vor der Installation der Datenklassifizierung aktivieren. Führen Sie die folgenden Befehle aus, um zu konfigurieren `firewalld` damit es mit der Datenklassifizierung kompatibel ist:

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

Wenn Sie zusätzliche Datenklassifizierungshosts als Scannerknoten verwenden möchten, fügen Sie Ihrem primären System jetzt diese Regeln hinzu:

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

Beachten Sie, dass Sie Docker oder Podman neu starten müssen, wenn Sie aktivieren oder aktualisieren `firewalld` Einstellungen.

Die IP-Adresse des Data Classification-Hostsystems kann nach der Installation nicht mehr geändert werden.

Ausgehenden Internetzugriff von der Datenklassifizierung aus aktivieren

Für die Datenklassifizierung ist ein ausgehender Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxyserver für den Internetzugang verwendet, stellen Sie sicher, dass die Datenklassifizierungsinstanz über ausgehenden Internetzugang verfügt, um die folgenden Endpunkte zu kontaktieren.

Endpunkte	Zweck
https://api.console.netapp.com	Kommunikation mit der Konsole, die NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-Website zur zentralen Benutzerauthentifizierung.
https://support.compliance.api.console.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und ermöglicht das Senden von Protokollen und Metriken.
https://support.compliance.api.console.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Prüfdatensätzen.
https://github.com/docker https://download.docker.com	Stellt erforderliche Pakete für die Docker-Installation bereit.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Stellt erforderliche Pakete für die Ubuntu-Installation bereit.

Stellen Sie sicher, dass alle erforderlichen Ports aktiviert sind

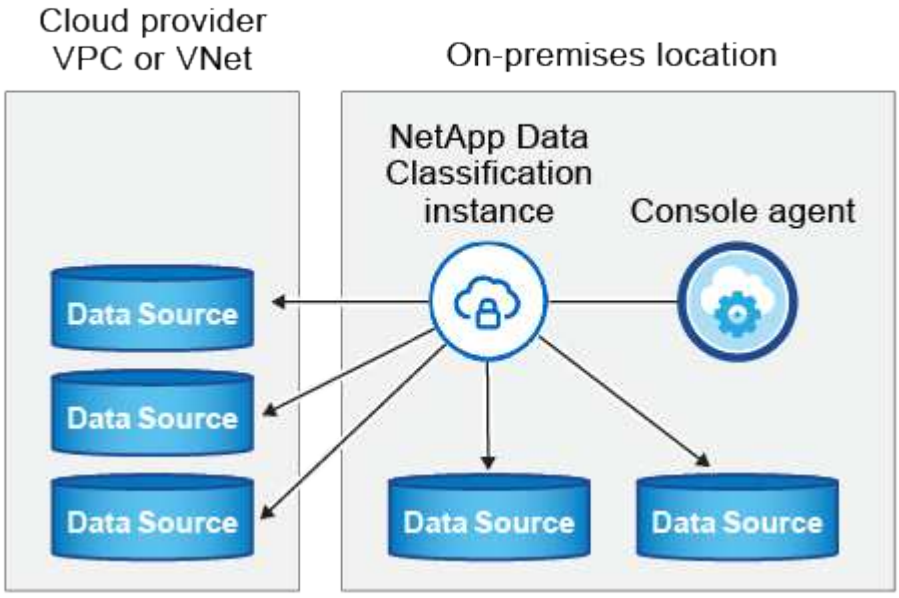
Sie müssen sicherstellen, dass alle erforderlichen Ports für die Kommunikation zwischen dem Konsolenagenten, der Datenklassifizierung, Active Directory und Ihren Datenquellen geöffnet sind.

Verbindungstyp	Häfen	Beschreibung
Konsolenagent <> Datenklassifizierung	8080 (TCP), 443 (TCP) und 80. 9000	Die Firewall- oder Routing-Regeln für den Konsolen-Agenten müssen eingehenden und ausgehenden Datenverkehr über Port 443 zur und von der Datenklassifizierungsinstanz zulassen. Stellen Sie sicher, dass Port 8080 geöffnet ist, damit Sie den Installationsfortschritt in der Konsole sehen können. Wenn auf dem Linux-Host eine Firewall verwendet wird, wird Port 9000 für interne Prozesse innerhalb eines Ubuntu-Servers benötigt.
Konsolenagent <> ONTAP -Cluster (NAS)	443 (TCP)	Die Konsole erkennt ONTAP Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen: • Der Konsolen-Agent-Host muss ausgehenden HTTPS-Zugriff über Port 443 zulassen. Wenn sich der Konsolenagent in der Cloud befindet, wird die gesamte ausgehende Kommunikation durch die vordefinierten Firewall- oder Routing-Regeln zugelassen. • Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen. Die standardmäßige Firewall-Richtlinie „mgmt“ erlaubt eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert oder Ihre eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff vom Konsolen-Agent-Host aus aktivieren.
Datenklassifizierung <> ONTAP -Cluster	• Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS – 139 (TCP\UDP) und 445 (TCP\UDP)	Für die Datenklassifizierung ist eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder On-Premise ONTAP System erforderlich. Firewalls oder Routing-Regeln für Cloud Volumes ONTAP müssen eingehende Verbindungen von der Data Classification-Instanz zulassen. Stellen Sie sicher, dass diese Ports für die Data Classification-Instanz geöffnet sind: • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 NFS-Volume-Exportrichtlinien müssen den Zugriff von der Datenklassifizierungsinstanz aus zulassen.

Verbindungstyp	Häfen	Beschreibung
Datenklassifizierung <> Active Directory	389 (TCP und UDP), 636 (TCP), 3268 (TCP) und 3269 (TCP)	Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben. Darüber hinaus benötigt die Datenklassifizierung Active Directory-Anmeldeinformationen, um CIFS-Volumes zu scannen. Sie benötigen die Informationen für das Active Directory: • DNS-Server-IP-Adresse oder mehrere IP-Adressen • Benutzername und Passwort für den Server • Domänenname (Active Directory-Name) • Ob Sie sicheres LDAP (LDAPS) verwenden oder nicht • LDAP-Server-Port (normalerweise 389 für LDAP und 636 für sicheres LDAP)

Installieren Sie Data Classification auf dem Linux-Host

Bei typischen Konfigurationen installieren Sie die Software auf einem einzelnen Hostsystem. Sehen Sie sich diese Schritte hier an .



SehenVorbereiten des Linux-Hostsystems UndVoraussetzungen überprüfen für die vollständige Liste der Anforderungen, bevor Sie die Datenklassifizierung bereitstellen.

Upgrades der Datenklassifizierungssoftware erfolgen automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Data Classification kann derzeit keine S3-Buckets, Azure NetApp Files oder FSx für ONTAP scannen, wenn die Software vor Ort installiert ist. In diesen Fällen müssen Sie einen separaten Konsolenagenten und eine Instanz der Datenklassifizierung in der Cloud bereitstellen und "zwischen Anschlüssen wechseln" für Ihre verschiedenen Datenquellen.

Single-Host-Installation für typische Konfigurationen

Überprüfen Sie die Anforderungen und befolgen Sie diese Schritte, wenn Sie die Datenklassifizierungssoftware auf einem einzelnen lokalen Host installieren.

"Sehen Sie sich dieses Video an"um zu sehen, wie die Datenklassifizierung installiert wird.

Beachten Sie, dass bei der Installation von Data Classification alle Installationsaktivitäten protokolliert werden. Wenn während der Installation Probleme auftreten, können Sie den Inhalt des Installationsüberwachungsprotokolls anzeigen. Es ist geschrieben an `/opt/netapp/install_logs/` .

Bevor Sie beginnen

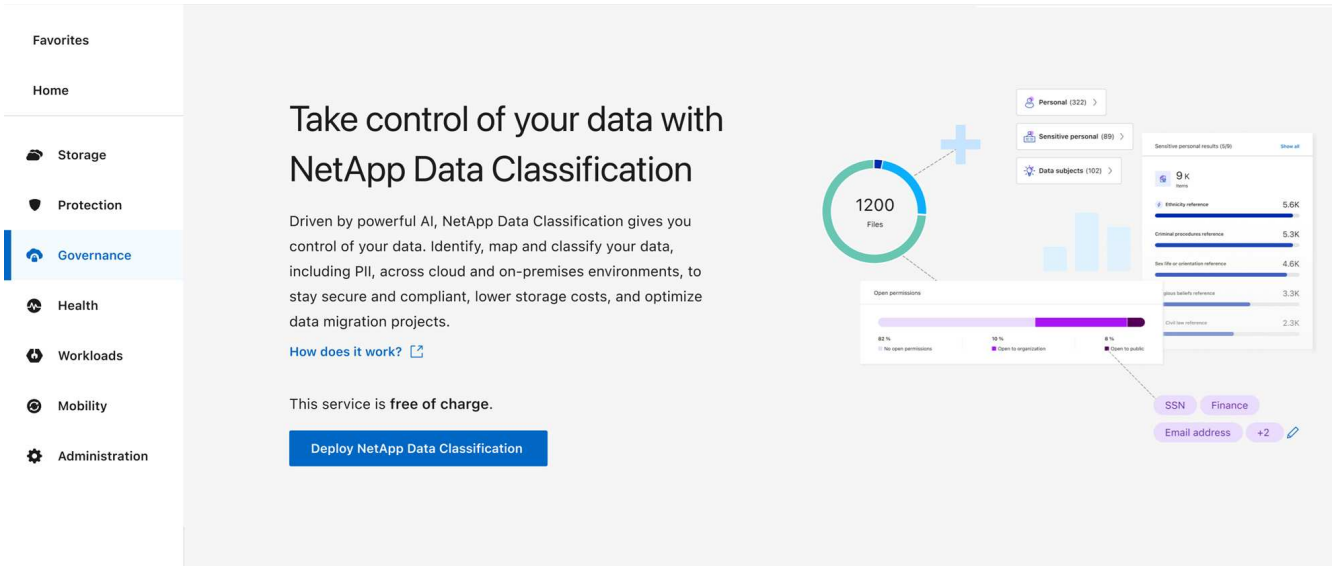
- Überprüfen Sie, ob Ihr Linux-System dieHostanforderungen .
- Stellen Sie sicher, dass auf dem System die beiden erforderlichen Softwarepakete installiert sind (Docker Engine oder Podman und Python 3).
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.
- Wenn Sie einen Proxy für den Internetzugang verwenden:
  - Sie benötigen die Proxyserver-Informationen (IP-Adresse oder Hostname, Verbindungsport, Verbindungsschema: https oder http, Benutzername und Passwort).
  - Wenn der Proxy eine TLS-Abfangfunktion ausführt, müssen Sie den Pfad auf dem Data Classification Linux-System kennen, in dem die TLS-CA-Zertifikate gespeichert sind.
  - Der Proxy muss intransparent sein. Die Datenklassifizierung unterstützt derzeit keine transparenten Proxys.
  - Der Benutzer muss ein lokaler Benutzer sein. Domänenbenutzer werden nicht unterstützt.
- Überprüfen Sie, ob Ihre Offline-Umgebung die erforderlichenBerechtigungen und Konnektivität .

Schritte

1. Laden Sie die Datenklassifizierungssoftware von der "NetApp Support Site" . Die Datei, die Sie auswählen sollten, heißt **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Kopieren Sie die Installationsdatei auf den Linux-Host, den Sie verwenden möchten (mit `scp` oder eine andere Methode).
3. Entpacken Sie die Installationsdatei auf dem Hostcomputer, zum Beispiel:

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

4. Wählen Sie in der Konsole **Governance > Klassifizierung** aus.
5. Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



6. Je nachdem, ob Sie Data Classification auf einer Instanz installieren, die Sie in der Cloud vorbereitet haben, oder auf einer Instanz, die Sie bei Ihnen vor Ort vorbereitet haben, wählen Sie die entsprechende Schaltfläche **Bereitstellen** aus, um die Installation von Data Classification zu starten.

   [Ein Screenshot der Auswahl der Schaltfläche zum Bereitstellen der Datenklassifizierung auf einem Computer in der Cloud oder bei Ihnen vor Ort.]

7. Das Dialogfeld „Datenklassifizierung vor Ort bereitstellen“ wird angezeigt. Kopieren Sie den bereitgestellten Befehl (zum Beispiel: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`) und fügen Sie es in eine Textdatei ein, damit Sie es später verwenden können. Wählen Sie dann **Schließen**, um das Dialogfeld zu schließen.
8. Geben Sie auf dem Hostcomputer den kopierten Befehl ein und folgen Sie dann einer Reihe von Eingabeaufforderungen. Alternativ können Sie den vollständigen Befehl einschließlich aller erforderlichen Parameter als Befehlszeilenargumente angeben.

   Beachten Sie, dass das Installationsprogramm eine Vorprüfung durchführt, um sicherzustellen, dass Ihre System- und Netzwerkanforderungen für eine erfolgreiche Installation erfüllt sind. "Sehen Sie sich dieses Video an" um die Vorabprüfungsnachrichten und Auswirkungen zu verstehen.

Geben Sie die Parameter wie aufgefordert ein:	Geben Sie den vollständigen Befehl ein:
a. Fügen Sie den Befehl ein, den Sie in Schritt 7 kopiert haben: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` Wenn Sie die Installation auf einer Cloud-Instanz (nicht bei Ihnen vor Ort) durchführen, fügen Sie hinzu `--manual-cloud-install <cloud_provider>`. b. Geben Sie die IP-Adresse oder den Hostnamen des Data Classification-Hostcomputers ein, damit das Konsolenagentsystem darauf zugreifen kann. c. Geben Sie die IP-Adresse oder den Hostnamen des Hostcomputers des Konsolenagenten ein, damit das Datenklassifizierungssystem darauf zugreifen kann. d. Geben Sie die Proxy-Details wie aufgefordert ein. Wenn Ihr Konsolenagent bereits einen Proxy verwendet, müssen Sie diese Informationen hier nicht erneut eingeben, da die Datenklassifizierung automatisch den vom Konsolenagenten verwendeten Proxy verwendet.	Alternativ können Sie den gesamten Befehl im Voraus erstellen und dabei die erforderlichen Host- und Proxy-Parameter angeben: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>`

Variablenwerte:

- *account_id* = NetApp Konto-ID
- *client_id* = Client-ID des Konsolenagenten (fügen Sie der Client-ID das Suffix „clients“ hinzu, falls es nicht bereits vorhanden ist)
- *user_token* = JWT-Benutzerzugriffstoken
- *ds_host* = IP-Adresse oder Hostname des Data Classification Linux-Systems.
- *cm_host* = IP-Adresse oder Hostname des Konsolenagentensystems.
- *cloud_provider* = Geben Sie bei der Installation auf einer Cloud-Instanz je nach Cloud-Anbieter „AWS“, „Azure“ oder „Gcp“ ein.
- *proxy_host* = IP oder Hostname des Proxyservers, wenn sich der Host hinter einem Proxyserver befindet.
- *proxy_port* = Port für die Verbindung mit dem Proxyserver (Standard 80).
- *proxy_scheme* = Verbindungsschema: https oder http (Standard: http).
- *proxy_user* = Authentifizierter Benutzer zur Verbindung mit dem Proxyserver, wenn eine Basisauthentifizierung erforderlich ist. Der Benutzer muss ein lokaler Benutzer sein – Domänenbenutzer werden nicht unterstützt.
- *proxy_password* = Passwort für den von Ihnen angegebenen Benutzernamen.
- *ca_cert_dir* = Pfad auf dem Data Classification-Linux-System, der zusätzliche TLS-CA-

Zertifikatspakete enthält. Nur erforderlich, wenn der Proxy eine TLS-Abfangfunktion durchführt.

Ergebnis

Das Data Classification-Installationsprogramm installiert Pakete, registriert die Installation und installiert Data Classification. Die Installation kann 10 bis 20 Minuten dauern.

Wenn zwischen dem Hostcomputer und der Konsolen-Agentinstanz eine Verbindung über Port 8080 besteht, wird der Installationsfortschritt auf der Registerkarte „Datenklassifizierung“ in der Konsole angezeigt.

Was kommt als Nächstes

Auf der Konfigurationsseite können Sie die Datenquellen auswählen, die Sie scannen möchten.

Installieren Sie NetApp Data Classification auf einem Linux-Host ohne Internetzugang

Die Installation von NetApp Data Classification auf einem Linux-Host an einem lokalen Standort ohne Internetzugang wird als *privater Modus* bezeichnet. Bei dieser Art der Installation, bei der ein Installationsskript verwendet wird, besteht keine Verbindung zur SaaS-Schicht der NetApp Console .

> Der private BlueXP Modus (alte BlueXP -Schnittstelle) wird normalerweise in lokalen Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, darunter AWS Secret Cloud, AWS Top Secret Cloud und Azure IL6. NetApp unterstützt diese Umgebungen weiterhin mit der alten BlueXP Schnittstelle. Die Dokumentation zum privaten Modus in der alten BlueXP Schnittstelle finden Sie unter"PDF-Dokumentation für den privaten Modus von BlueXP" .

Überprüfen Sie, ob Ihr Linux-Host für die Installation von NetApp Data Classification bereit ist.

Bevor Sie NetApp Data Classification manuell auf einem Linux-Host installieren, führen Sie optional ein Skript auf dem Host aus, um zu überprüfen, ob alle Voraussetzungen für die Installation von Data Classification erfüllt sind. Sie können dieses Skript auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud ausführen. Der Host kann mit dem Internet verbunden sein oder sich an einem Standort ohne Internetzugang befinden (ein „Dark Site“).

Es gibt auch ein erforderliches Testskript, das Teil des Installationsskripts für die Datenklassifizierung ist. Das hier beschriebene Skript ist speziell für Benutzer konzipiert, die den Linux-Host unabhängig von der Ausführung des Installationsskripts zur Datenklassifizierung überprüfen möchten.

Erste Schritte

Sie führen die folgenden Aufgaben aus.

1. Installieren Sie optional einen Konsolenagenten, falls Sie noch keinen installiert haben. Sie können das Testskript ausführen, ohne dass ein Konsolenagent installiert ist. Das Skript prüft jedoch die Konnektivität zwischen dem Konsolenagenten und dem Hostcomputer der Datenklassifizierung. Daher wird empfohlen, dass Sie über einen Konsolenagenten verfügen.
2. Bereiten Sie den Hostcomputer vor und überprüfen Sie, ob er alle Anforderungen erfüllt.

3. Aktivieren Sie den ausgehenden Internetzugriff vom Data Classification-Hostcomputer.
4. Stellen Sie sicher, dass alle erforderlichen Ports auf allen Systemen aktiviert sind.
5. Laden Sie das Prerequisite-Testskript herunter und führen Sie es aus.

Erstellen eines Konsolenagenten

Bevor Sie Data Classification installieren und verwenden können, ist ein Konsolenagent erforderlich. Sie können das Skript „Voraussetzungen“ jedoch ohne einen Konsolenagenten ausführen.

Du kannst "Installieren Sie den Konsolen-Agenten vor Ort" auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud. Einige Benutzer, die Data Classification vor Ort installieren möchten, entscheiden sich möglicherweise auch für die Installation des Konsolenagenten vor Ort.

Informationen zum Erstellen eines Konsolenagenten in der Umgebung Ihres Cloud-Anbieters finden Sie unter "Erstellen eines Konsolenagenten in AWS" , "Erstellen eines Konsolenagenten in Azure" , oder "Erstellen eines Konsolenagenten in GCP" .

Sie benötigen die IP-Adresse oder den Hostnamen des Konsolenagentensystems, wenn Sie das Voraussetzungen-Skript ausführen. Sie verfügen über diese Informationen, wenn Sie den Konsolenagenten in Ihren Räumlichkeiten installiert haben. Wenn der Konsolenagent in der Cloud bereitgestellt wird, finden Sie diese Informationen in der Konsole: Wählen Sie das Hilfesymbol, dann **Support** und dann **Konsolenagent**.

Überprüfen der Hostanforderungen

Datenklassifizierungssoftware muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Softwareanforderungen usw. erfüllt.

- Die Datenklassifizierung wird auf einem Host, der gemeinsam mit anderen Anwendungen genutzt wird, nicht unterstützt – der Host muss ein dedizierter Host sein.
- Beim Aufbau des Hostsystems in Ihren Räumlichkeiten können Sie je nach Größe des Datensatzes, für den Sie einen Datenklassifizierungsscan durchführen möchten, zwischen diesen Systemgrößen wählen.

Systemgröße	CPU	RAM (Auslagerungsspeicher muss deaktiviert sein)	Scheibe
Extra groß	32 CPUs	128 GB RAM	• 1 TiB SSD auf / oder 100 GiB verfügbar auf /opt • 895 GiB verfügbar auf /var/lib/docker • 5 GiB auf /tmp • **Für Podman, 30 GB auf /var/tmp**

Systemgröße	CPU	RAM (Auslagerungsspeicher muss deaktiviert sein)	Scheibe
Groß	16 CPUs	64 GB RAM	• 500 GiB SSD auf / oder 100 GiB verfügbar auf /opt • 400 GiB verfügbar auf /var/lib/docker oder für Podman /var/lib/containers • 5 GiB auf /tmp • **Für Podman, 30 GB auf /var/tmp**

- Wenn Sie für Ihre Data Classification-Installation eine Compute-Instanz in der Cloud bereitstellen, wird empfohlen, ein System zu verwenden, das die oben genannten Systemanforderungen für „Groß“ erfüllt:
  - **Amazon Elastic Compute Cloud (Amazon EC2)-Instanztyp**: „m6i.4xlarge“. "Weitere AWS-Instanztypen anzeigen" .
  - **Azure-VM-Größe**: „Standard_D16s_v3“. "Weitere Azure-Instanztypen anzeigen" .
  - **GCP-Maschinentyp**: „n2-standard-16“. "Weitere GCP-Instanztypen anzeigen" .
- **UNIX-Ordnerberechtigungen**: Die folgenden UNIX-Mindestberechtigungen sind erforderlich:

Ordner	Mindestberechtigungen
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Betriebssystem**:
  - Die folgenden Betriebssysteme erfordern die Verwendung der Docker-Container-Engine:
    - Red Hat Enterprise Linux Version 7.8 und 7.9
    - Ubuntu 22.04 (erfordert Data Classification Version 1.23 oder höher)
    - Ubuntu 24.04 (erfordert Data Classification Version 1.23 oder höher)
  - Die folgenden Betriebssysteme erfordern die Verwendung der Podman-Container-Engine und erfordern Data Classification Version 1.30 oder höher:
    - Red Hat Enterprise Linux Version 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 und 9.6.
  - Advanced Vector Extensions (AVX2) müssen auf dem Hostsystem aktiviert sein.
- **Red Hat Subscription Management**: Der Host muss bei Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositories zugreifen, um erforderliche Software von Drittanbietern zu aktualisieren.
- **Zusätzliche Software**: Sie müssen die folgende Software auf dem Host installieren, bevor Sie Data Classification installieren:
  - Abhängig vom verwendeten Betriebssystem müssen Sie eine der Container-Engines installieren:

- Docker Engine Version 19.3.1 oder höher. "Installationsanweisungen anzeigen" .
- Podman Version 4 oder höher. Um Podman zu installieren, geben Sie ein(`sudo yum install podman netavark -y`).

- Python Version 3.6 oder höher. "Installationsanweisungen anzeigen" .
  - **NTP-Überlegungen**: NetApp empfiehlt, das Datenklassifizierungssystem für die Verwendung eines Network Time Protocol (NTP)-Dienstes zu konfigurieren. Die Zeit muss zwischen dem Datenklassifizierungssystem und dem Konsolenagentsystem synchronisiert werden.
- **Firewalld-Überlegungen**: Wenn Sie planen, `firewalld` , wir empfehlen, dass Sie es vor der Installation der Datenklassifizierung aktivieren. Führen Sie die folgenden Befehle aus, um zu konfigurieren `firewalld` damit es mit der Datenklassifizierung kompatibel ist:

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

Wenn Sie planen, zusätzliche Datenklassifizierungshosts als Scannerknoten (in einem verteilten Modell) zu verwenden, fügen Sie Ihrem primären System jetzt diese Regeln hinzu:

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

Beachten Sie, dass Sie Docker oder Podman neu starten müssen, wenn Sie aktivieren oder aktualisieren `firewalld` Einstellungen.

Ausgehenden Internetzugriff von der Datenklassifizierung aus aktivieren

Für die Datenklassifizierung ist ein ausgehender Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxyserver für den Internetzugang verwendet, stellen Sie sicher, dass die Datenklassifizierungsinstanz über ausgehenden Internetzugang verfügt, um die folgenden Endpunkte zu kontaktieren.

Dieser Abschnitt ist für Hostsysteme, die an Standorten ohne Internetverbindung installiert sind, nicht erforderlich.

Endpunkte	Zweck
https://api.console.netapp.com	Kommunikation mit dem Konsolendienst, der NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-Website zur zentralen Benutzerauthentifizierung.

Endpunkte	Zweck
https://support.compliance.api.console.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und ermöglicht das Senden von Protokollen und Metriken.
https://support.compliance.api.console.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Prüfdatensätzen.
https://github.com/docker https://download.docker.com	Stellt erforderliche Pakete für die Docker-Installation bereit.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Stellt erforderliche Pakete für die Ubuntu-Installation bereit.

Stellen Sie sicher, dass alle erforderlichen Ports aktiviert sind

Sie müssen sicherstellen, dass alle erforderlichen Ports für die Kommunikation zwischen dem Konsolenagenten, der Datenklassifizierung, Active Directory und Ihren Datenquellen geöffnet sind.

Verbindungstyp	Häfen	Beschreibung
Konsolenagent <> Datenklassifizierung	8080 (TCP), 443 (TCP) und 80. 9000	Die Firewall- oder Routing-Regeln für den Konsolen-Agenten müssen eingehenden und ausgehenden Datenverkehr über Port 443 zur und von der Datenklassifizierungsinstanz zulassen. Stellen Sie sicher, dass Port 8080 geöffnet ist, damit Sie den Installationsfortschritt in der Konsole sehen können. Wenn auf dem Linux-Host eine Firewall verwendet wird, wird Port 9000 für interne Prozesse innerhalb eines Ubuntu-Servers benötigt.
Konsolenagent <> ONTAP -Cluster (NAS)	443 (TCP)	Die Konsole erkennt ONTAP Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, muss der Konsolen-Agent-Host ausgehenden HTTPS-Zugriff über Port 443 zulassen. Wenn sich der Konsolenagent in der Cloud befindet, wird die gesamte ausgehende Kommunikation durch die vordefinierten Firewall- oder Routing-Regeln zugelassen.

Ausführen des Voraussetzungenskripts für die Datenklassifizierung

Führen Sie die folgenden Schritte aus, um das Voraussetzungenskript für die Datenklassifizierung auszuführen.

"Sehen Sie sich dieses Video an"um zu sehen, wie Sie das Voraussetzungen-Skript ausführen und die Ergebnisse interpretieren.

Bevor Sie beginnen

- Überprüfen Sie, ob Ihr Linux-System dieHostanforderungen .

- Stellen Sie sicher, dass auf dem System die beiden erforderlichen Softwarepakete installiert sind (Docker Engine oder Podman und Python 3).
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.

Schritte

1. Laden Sie das Skript „Data Classification Prerequisites“ von der "NetApp Support Site" . Die Datei, die Sie auswählen sollten, hat den Namen **standalone-pre-requisite-tester-<version>**.
2. Kopieren Sie die Datei auf den Linux-Host, den Sie verwenden möchten (mit `scp` oder eine andere Methode).
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

4. Führen Sie das Skript mit dem folgenden Befehl aus.

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

   Fügen Sie die Option „--darksite“ nur hinzu, wenn Sie das Skript auf einem Host ausführen, der keinen Internetzugang hat. Bestimmte Voraussetzungstests werden übersprungen, wenn der Host nicht mit dem Internet verbunden ist.

5. Das Skript fordert Sie zur Eingabe der IP-Adresse des Data Classification-Hostcomputers auf.
   - Geben Sie die IP-Adresse oder den Hostnamen ein.
6. Das Skript fragt, ob Sie einen installierten Konsolenagenten haben.
   - Geben Sie **N** ein, wenn Sie keinen installierten Konsolenagenten haben.
   - Geben Sie **Y** ein, wenn Sie einen installierten Konsolenagenten haben. Geben Sie dann die IP-Adresse oder den Hostnamen des Konsolenagenten ein, damit das Testskript diese Konnektivität testen kann.
7. Das Skript führt verschiedene Tests auf dem System aus und zeigt im Verlauf die Ergebnisse an. Wenn es fertig ist, schreibt es ein Protokoll der Sitzung in eine Datei namens `prerequisites-test-<timestamp>.log` im Verzeichnis `/opt/netapp/install_logs` .

Ergebnis

Wenn alle erforderlichen Tests erfolgreich ausgeführt wurden, können Sie Data Classification auf dem Host installieren, wenn Sie bereit sind.

Wenn Probleme entdeckt wurden, werden sie zur Behebung als „Empfohlen“ oder „Erforderlich“ kategorisiert. Bei den empfohlenen Problemen handelt es sich in der Regel um Elemente, die die Ausführung der Scan- und Kategorisierungsaufgaben zur Datenklassifizierung verlangsamen würden. Diese Punkte müssen nicht korrigiert werden, Sie möchten sie aber möglicherweise dennoch ansprechen.

Wenn Sie „Erforderliche“ Probleme haben, sollten Sie diese beheben und das Voraussetzungen-Testskript erneut ausführen.

Aktivieren Sie das Scannen Ihrer Datenquellen

Scannen Sie Datenquellen mit NetApp Data Classification

NetApp Data Classification scannt die Daten in den von Ihnen ausgewählten Repositories (Volumes, Datenbankschemata oder andere Benutzerdaten), um persönliche und vertrauliche Daten zu identifizieren. Die Datenklassifizierung ordnet dann Ihre Organisationsdaten zu, kategorisiert jede Datei und identifiziert vordefinierte Muster in den Daten. Das Ergebnis des Scans ist ein Index mit persönlichen Informationen, sensiblen persönlichen Informationen, Datenkategorien und Dateitypen.

Nach dem ersten Scan scannt die Datenklassifizierung Ihre Daten kontinuierlich im Round-Robin-Verfahren, um inkrementelle Änderungen zu erkennen. Aus diesem Grund ist es wichtig, die Instanz am Laufen zu halten.

Sie können Scans auf Volume-Ebene oder auf Datenbankschemaebene aktivieren und deaktivieren.

Was ist der Unterschied zwischen Mapping- und Klassifizierungsscans?

Sie können in der Datenklassifizierung zwei Arten von Scans durchführen:

- **Nur-Mapping-Scans** bieten nur einen allgemeinen Überblick über Ihre Daten und werden für ausgewählte Datenquellen durchgeführt. Scans, die nur eine Zuordnung vornehmen, benötigen weniger Zeit als Scans, die eine Zuordnung und Klassifizierung vornehmen, da sie nicht auf Dateien zugreifen, um die darin enthaltenen Daten anzuzeigen. Möglicherweise möchten Sie dies zunächst tun, um Forschungsbereiche zu identifizieren und dann einen Map & Classify-Scan für diese Bereiche durchzuführen.
- **Map & Classify-Scans** ermöglichen ein gründliches Scannen Ihrer Daten.

Die folgende Tabelle zeigt einige der Unterschiede:

Funktion	Scans zuordnen und klassifizieren	Nur-Mapping-Scans
Scangeschwindigkeit	Langsam	Schnell
Preise	Frei	Frei
Kapazität	Begrenzt auf 500 TiB*	Begrenzt auf 500 TiB*
Liste der Dateitypen und der verwendeten Kapazität	Ja	Ja
Anzahl der Dateien und genutzte Kapazität	Ja	Ja
Alter und Größe der Dateien	Ja	Ja
Fähigkeit zur Ausführung eines"Datenzuordnungsbericht"	Ja	Ja
Seite „Datenuntersuchung“ zum Anzeigen von Dateidetails	Ja	Nein
Suchen nach Namen in Dateien	Ja	Nein
Erstellen"gespeicherte Abfragen" die benutzerdefinierte Suchergebnisse bereitstellen	Ja	Nein
Möglichkeit, andere Berichte auszuführen	Ja	Nein
Möglichkeit, Metadaten aus Dateien anzuzeigen**	Nein	Ja

* Die Datenklassifizierung setzt keine Begrenzung für die Datenmenge, die gescannt werden kann. Jeder Konsolenagent unterstützt das Scannen und Anzeigen von 500 TiB Daten. Um mehr als 500 TiB Daten zu scannen,"einen anderen Konsolenagenten installieren" Dann"eine weitere Data Classification-Instanz bereitstellen" . + Die Konsolen-Benutzeroberfläche zeigt Daten von einem einzelnen Connector an. Tipps zum Anzeigen von Daten von mehreren Konsolenagenten finden Sie unter"Arbeiten mit mehreren Konsolenagenten" .

** Die folgenden Metadaten werden während Mapping-Scans aus Dateien extrahiert:

- System
- Systemtyp
- Speicherrepository
- Dateityp
- Genutzte Kapazität
- Anzahl der Dateien
- Dateigröße
- Dateierstellung
- Letzter Dateizugriff
- Datei zuletzt geändert
- Uhrzeit der Dateierkennung
- Berechtigungsextraktion

Unterschiede im Governance-Dashboard:

Funktion	Kartieren und klassifizieren	Karte
Veraltete Daten	Ja	Ja
Nicht-geschäftliche Daten	Ja	Ja
Duplizierte Dateien	Ja	Ja
Vordefinierte gespeicherte Abfragen	Ja	Nein
Standardmäßig gespeicherte Abfragen	Ja	Ja
DDA-Bericht	Ja	Ja
Mapping-Bericht	Ja	Ja
Erkennung der Empfindlichkeitsstufe	Ja	Nein
Sensible Daten mit umfassenden Berechtigungen	Ja	Nein
Berechtigungen öffnen	Ja	Ja
Alter der Daten	Ja	Ja
Datenmenge	Ja	Ja
Kategorien	Ja	Nein
Dateitypen	Ja	Ja

Unterschiede im Compliance-Dashboard:

Funktion	Kartieren und klassifizieren	Karte
Persönliche Informationen	Ja	Nein
Sensible persönliche Informationen	Ja	Nein
Bericht zur Bewertung des Datenschutzrisikos	Ja	Nein
HIPAA-Bericht	Ja	Nein
PCI DSS-Bericht	Ja	Nein

Unterschiede bei den Untersuchungsfiltern:

Funktion	Kartieren und klassifizieren	Karte
Gespeicherte Abfragen	Ja	Ja
Systemtyp	Ja	Ja
System	Ja	Ja
Speicherrepository	Ja	Ja
Dateityp	Ja	Ja
Dateigröße	Ja	Ja
Erstellungszeit	Ja	Ja
Entdeckte Zeit	Ja	Ja
Zuletzt geändert	Ja	Ja
Letzter Zugriff	Ja	Ja
Berechtigungen öffnen	Ja	Ja
Dateiverzeichnispfad	Ja	Ja
Kategorie	Ja	Nein
Empfindlichkeitsstufe	Ja	Nein
Anzahl der Kennungen	Ja	Nein
personenbezogene Daten	Ja	Nein
Sensible personenbezogene Daten	Ja	Nein
Betroffene Person	Ja	Nein
Duplikate	Ja	Ja
Klassifizierungsstatus	Ja	Der Status ist immer „Eingeschränkte Einblicke“
Scan-Analyseereignis	Ja	Ja
Datei-Hash	Ja	Ja
Anzahl der Benutzer mit Zugriff	Ja	Ja
Benutzer-/Gruppenberechtigungen	Ja	Ja
Dateieigentümer	Ja	Ja
Verzeichnistyp	Ja	Ja

Wie schnell scannt die Datenklassifizierung Daten

Die Scangeschwindigkeit wird durch Netzwerklatenz, Festplattenlatenz, Netzwerkbandbreite, Umgebungsgröße und Dateiverteilungsgrößen beeinflusst.

- Bei der Durchführung von reinen Mapping-Scans kann die Datenklassifizierung zwischen 100 und 150 TiB Daten pro Tag scannen.
- Beim Durchführen von Map- und Klassifizierungsscans kann die Datenklassifizierung zwischen 15 und 40 TiB Daten pro Tag scannen.

Scannen von Azure NetApp Files Volumes mit NetApp Data Classification

Führen Sie einige Schritte aus, um mit der NetApp Data Classification für Azure NetApp Files zu beginnen.

Ermitteln Sie das Azure NetApp Files -System, das Sie scannen möchten.

Wenn das Azure NetApp Files -System, das Sie scannen möchten, nicht bereits in der NetApp Console als System vorhanden ist,"fügen Sie es auf der Seite „Systeme“ hinzu" .

Bereitstellen der Datenklassifizierungsinstanz

"Datenklassifizierung bereitstellen"wenn noch keine Instanz bereitgestellt ist.

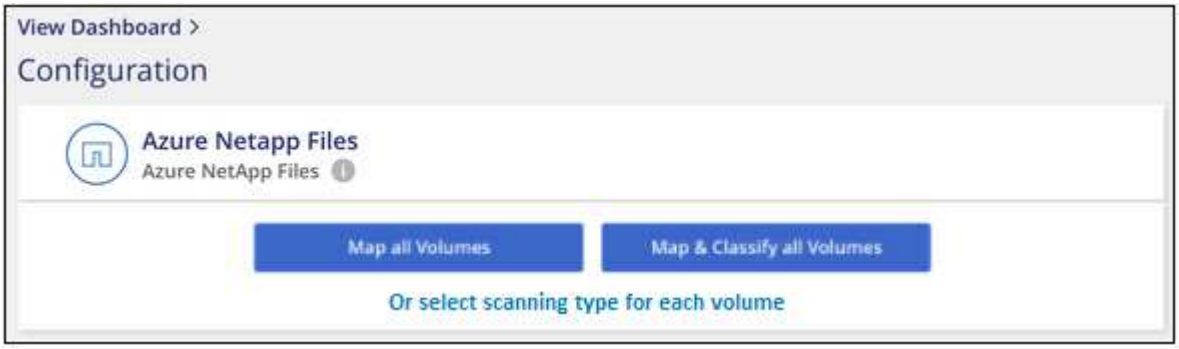
Die Datenklassifizierung muss beim Scannen von Azure NetApp Files Volumes in der Cloud bereitgestellt werden und zwar in derselben Region wie die Volumes, die Sie scannen möchten.

Hinweis: Die Bereitstellung der Datenklassifizierung an einem lokalen Standort wird beim Scannen von Azure NetApp Files -Volumes derzeit nicht unterstützt.

Aktivieren Sie die Datenklassifizierung in Ihren Systemen

Sie können die Datenklassifizierung auf Ihren Azure NetApp Files Volumes aktivieren.

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



2. Wählen Sie aus, wie Sie die Volumes in jedem System scannen möchten. "Erfahren Sie mehr über Mapping- und Klassifizierungsscans":
   - Um alle Volumes zuzuordnen, wählen Sie **Alle Volumes zuordnen**.
   - Um alle Volumes zuzuordnen und zu klassifizieren, wählen Sie **Alle Volumes zuordnen und klassifizieren**.
   - Um das Scannen für jedes Volume anzupassen, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus** und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

     SehenAktivieren und Deaktivieren von Compliance-Scans auf Volumes für Details.

3. Wählen Sie im Bestätigungsdialogfeld **Genehmigen** aus.

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse sind im Compliance-Dashboard verfügbar, sobald die Datenklassifizierung die ersten Scans abgeschlossen hat. Die dafür benötigte Zeit hängt von der Datenmenge ab und kann einige Minuten oder Stunden betragen. Sie können den Fortschritt des ersten Scans verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die **Systemkonfiguration** auswählen. Der Fortschritt jedes Scans wird als Fortschrittsbalken angezeigt. Sie können auch mit der Maus über den Fortschrittsbalken fahren, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen.

- Wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, scannt das System die Dateien in Ihren Volumes standardmäßig nicht, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus**. Auf der resultierenden Seite können Sie eine Einstellung aktivieren, sodass die Datenklassifizierung die Volumes unabhängig von den Berechtigungen scannt.
- Die Datenklassifizierung scannt nur eine Dateifreigabe unter einem Volume. Wenn Ihre Volumes mehrere Freigaben enthalten, müssen Sie diese anderen Freigaben separat als Freigabegruppe scannen. "Erfahren Sie mehr über diese Einschränkung der Datenklassifizierung" .

Überprüfen Sie, ob die Datenklassifizierung Zugriff auf die Volumes hat.

Stellen Sie sicher, dass die Datenklassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien überprüfen. Sie müssen Data Classification CIFS-Anmeldeinformationen bereitstellen, damit es auf CIFS-Volumes zugreifen kann.

Bei Azure NetApp Files kann die Datenklassifizierung nur Volumes in derselben Region wie die Konsole scannen.

Checklist

- Stellen Sie sicher, dass zwischen der Data Classification-Instanz und jedem Netzwerk, das Volumes für Azure NetApp Files enthält, eine Netzwerkverbindung besteht.
- Stellen Sie sicher, dass die folgenden Ports für die Data Classification-Instanz geöffnet sind:
  - Für NFS – Ports 111 und 2049.
  - Für CIFS – Ports 139 und 445.
- Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Classification-Instanz enthalten, damit diese auf die Daten auf jedem Volume zugreifen kann.

Schritte

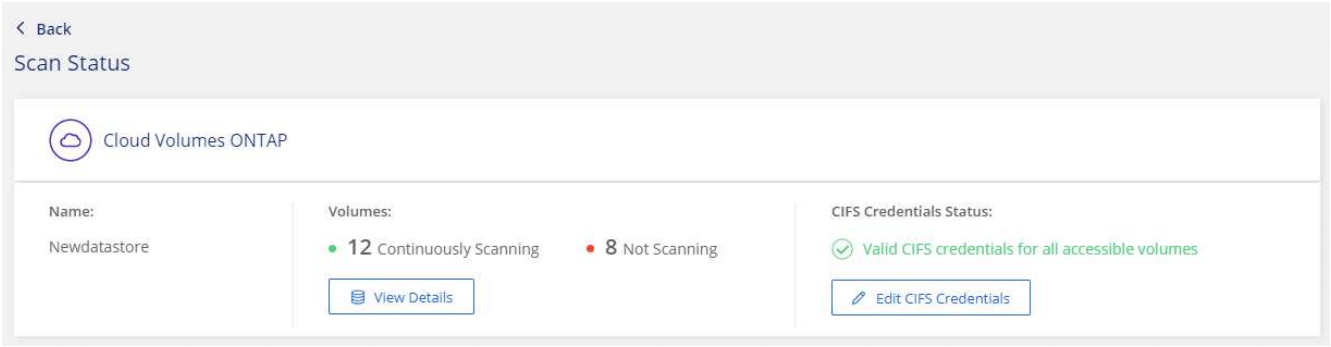
1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.

   a. Wenn Sie CIFS (SMB) verwenden, stellen Sie sicher, dass die Active Directory-Anmeldeinformationen korrekt sind. Wählen Sie für jedes System **CIFS-Anmeldeinformationen bearbeiten** und geben Sie dann den Benutzernamen und das Kennwort ein, die Data Classification für den Zugriff auf CIFS-Volumes auf dem System benötigt.

      Die Anmeldeinformationen können schreibgeschützt sein, durch die Angabe von Administratoranmeldeinformationen wird jedoch sichergestellt, dass die Datenklassifizierung alle Daten lesen kann, für die erweiterte Berechtigungen erforderlich sind. Die Anmeldeinformationen werden auf der Data Classification-Instanz gespeichert.

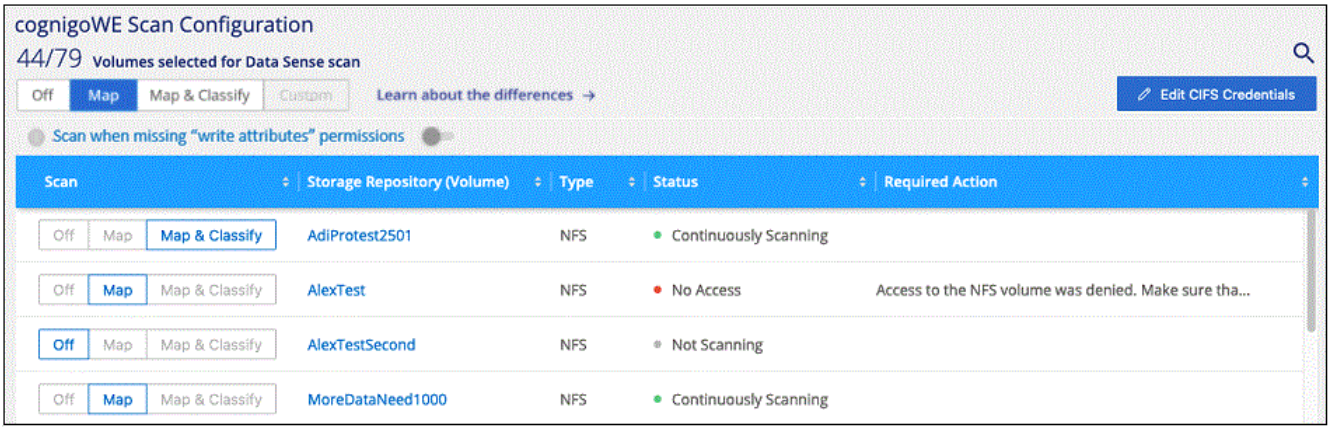
Wenn Sie sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Datenklassifizierungsscans unverändert bleiben, wird empfohlen, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

Nachdem Sie die Anmeldeinformationen eingegeben haben, sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.



2. Wählen Sie auf der Konfigurationsseite **Details anzeigen** aus, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und etwaige Fehler zu beheben.

   Das folgende Bild zeigt beispielsweise vier Volumes, von denen Data Classification eines aufgrund von Netzwerkverbindungsproblemen zwischen der Data Classification-Instanz und dem Volume nicht scannen kann.



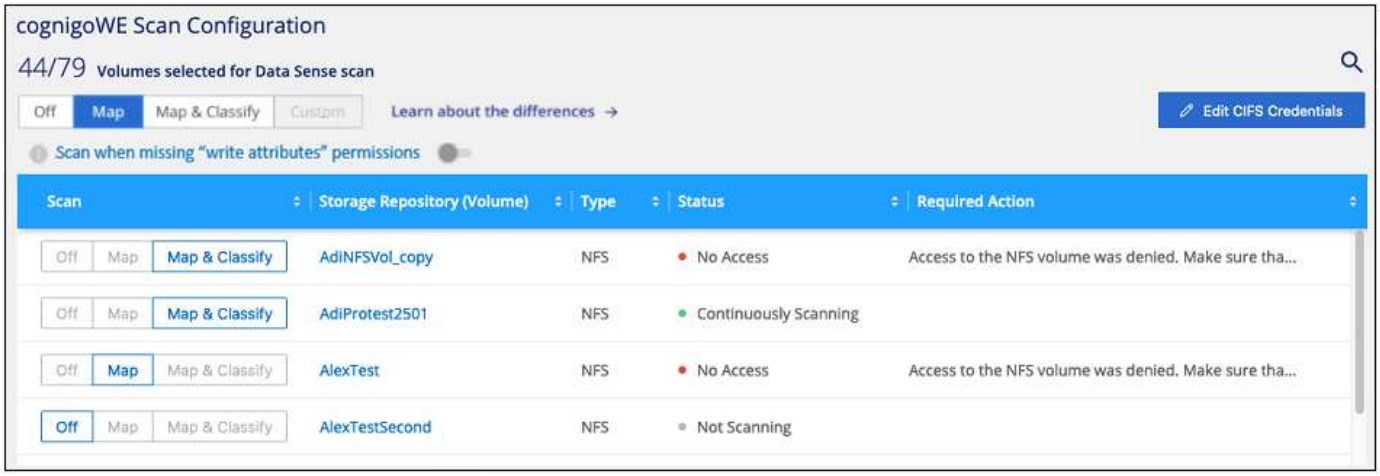
Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

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. Wir empfehlen Ihnen, alle Bände zu scannen.

Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und Klassifizieren** festgelegt haben. Wenn Sie im Überschriftenbereich die Option **Benutzerdefiniert** oder **Aus** einstellen, müssen Sie die Zuordnung und/oder das vollständige Scannen für jedes neue Volume aktivieren, das Sie dem System hinzufügen.

Der Schalter oben auf der Seite für **Scannen, wenn Berechtigungen zum Schreiben von Attributen fehlen**

ist standardmäßig deaktiviert. Dies bedeutet, dass das System die Dateien nicht scannt, wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter auf EIN und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Mehr erfahren" .



Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Führen Sie einen der folgenden Schritte aus:
   - Um Nur-Mapping-Scans auf einem Volume zu aktivieren, wählen Sie im Volume-Bereich **Map** aus. Um die Funktion auf allen Volumes zu aktivieren, wählen Sie im Überschriftenbereich **Karte** aus.
   - Um das vollständige Scannen eines Volumes zu aktivieren, wählen Sie im Volumebereich **Zuordnen und klassifizieren** aus. Um die Funktion auf allen Volumes zu aktivieren, wählen Sie im Überschriftenbereich **Zuordnen und klassifizieren** aus.
   - Um das Scannen auf einem Volume zu deaktivieren, wählen Sie im Volumebereich **Aus**. Um das Scannen auf allen Volumes zu deaktivieren, wählen Sie im Überschriftenbereich **Aus**.

Amazon FSx nach ONTAP -Volumes mit NetApp Data Classification scannen

Führen Sie einige Schritte aus, um mit dem Scannen des Amazon FSx für ONTAP -Volumes mit NetApp Data Classification zu beginnen.

Bevor Sie beginnen

- Sie benötigen einen aktiven Konsolenagenten in AWS, um die Datenklassifizierung bereitzustellen und zu verwalten.
- Die Sicherheitsgruppe, die Sie beim Erstellen des Systems ausgewählt haben, muss Datenverkehr von der Data Classification-Instanz zulassen. Sie können die zugehörige Sicherheitsgruppe mithilfe der mit dem FSx for ONTAP Dateisystem verbundenen ENI finden und mithilfe der AWS Management Console bearbeiten.

  "AWS-Sicherheitsgruppen für Linux-Instanzen"

  "AWS-Sicherheitsgruppen für Windows-Instances"

  "Elastische AWS-Netzwerkschnittstellen (ENI)"

- Stellen Sie sicher, dass die folgenden Ports für die Data Classification-Instanz geöffnet sind:
  - Für NFS – Ports 111 und 2049.
  - Für CIFS – Ports 139 und 445.

Bereitstellen der Datenklassifizierungsinstanz

"Datenklassifizierung bereitstellen"wenn noch keine Instanz bereitgestellt ist.

Sie sollten die Datenklassifizierung im selben AWS-Netzwerk bereitstellen wie den Konsolenagenten für AWS und die FSx-Volumes, die Sie scannen möchten.

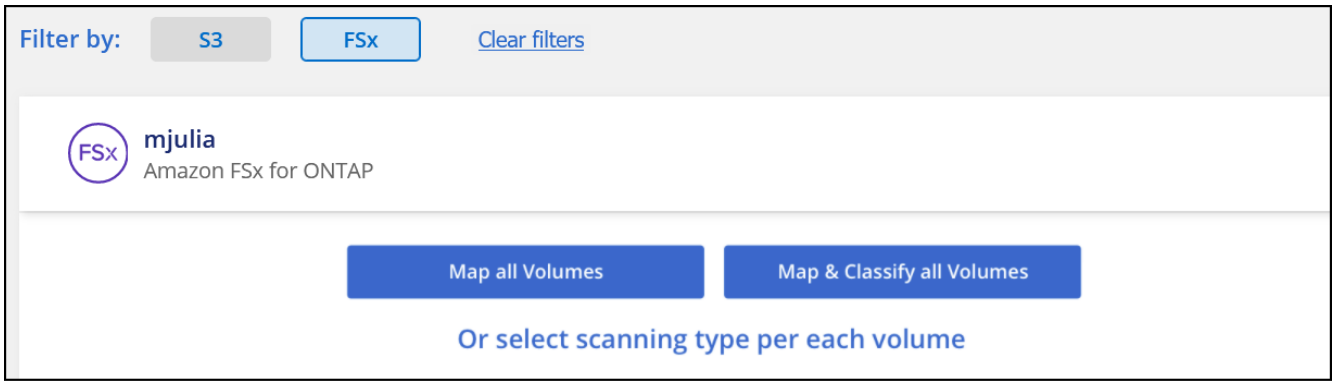
Hinweis: Die Bereitstellung der Datenklassifizierung an einem lokalen Standort wird beim Scannen von FSx-Volumes derzeit nicht unterstützt.

Upgrades der Datenklassifizierungssoftware erfolgen automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Aktivieren Sie die Datenklassifizierung in Ihren Systemen

Sie können die Datenklassifizierung für FSx für ONTAP -Volumes aktivieren.

1. In der NetApp Console: **Governance > Klassifizierung**.
2. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.



3. Wählen Sie aus, wie Sie die Volumes in jedem System scannen möchten. "Erfahren Sie mehr über Mapping- und Klassifizierungsscans":
   - Um alle Volumes zuzuordnen, wählen Sie **Alle Volumes zuordnen**.
   - Um alle Volumes zuzuordnen und zu klassifizieren, wählen Sie **Alle Volumes zuordnen und klassifizieren**.
   - Um das Scannen für jedes Volume anzupassen, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus** und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.
4. Wählen Sie im Bestätigungsdialogfeld **Genehmigen** aus, damit die Datenklassifizierung mit dem Scannen Ihrer Datenträger beginnt.

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse stehen im Compliance-Dashboard zur Verfügung, sobald die Datenklassifizierung die ersten Scans abgeschlossen hat. Die dafür benötigte Zeit hängt von der Datenmenge ab und kann einige Minuten oder Stunden betragen. Sie können den Fortschritt des ersten Scans verfolgen, indem Sie zum Menü

Konfiguration navigieren und dann die **Systemkonfiguration** auswählen. Der Fortschritt jedes Scans wird als Fortschrittsbalken angezeigt. Sie können auch mit der Maus über den Fortschrittsbalken fahren, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen.

- Wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, scannt das System die Dateien in Ihren Volumes standardmäßig nicht, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus**. Auf der resultierenden Seite können Sie eine Einstellung aktivieren, sodass die Datenklassifizierung die Volumes unabhängig von den Berechtigungen scannt.
- Die Datenklassifizierung scannt nur eine Dateifreigabe unter einem Volume. Wenn Ihre Volumes mehrere Freigaben enthalten, müssen Sie diese anderen Freigaben separat als Freigabegruppe scannen. "Weitere Einzelheiten zu dieser Datenklassifizierungsbeschränkung" .

Überprüfen Sie, ob die Datenklassifizierung Zugriff auf die Volumes hat.

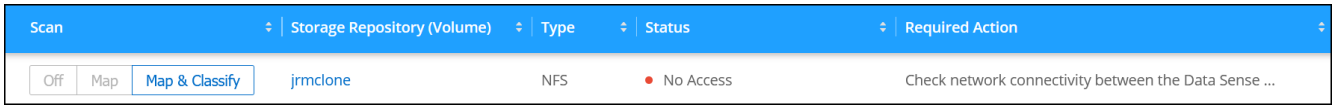
Stellen Sie sicher, dass die Datenklassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien überprüfen.

Sie müssen Data Classification CIFS-Anmeldeinformationen bereitstellen, damit es auf CIFS-Volumes zugreifen kann.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite **Details anzeigen** aus, um den Status zu überprüfen und etwaige Fehler zu beheben.

   Das folgende Bild zeigt beispielsweise ein Volume, das Data Classification aufgrund von Netzwerkverbindungsproblemen zwischen der Data Classification-Instanz und dem Volume nicht scannen kann.



3. Stellen Sie sicher, dass zwischen der Data Classification-Instanz und jedem Netzwerk, das Volumes für FSx for ONTAP enthält, eine Netzwerkverbindung besteht.

   Bei FSx for ONTAP kann die Datenklassifizierung Volumes nur in derselben Region wie die Konsole scannen.

4. Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Classification-Instanz enthalten, damit diese auf die Daten auf jedem Volume zugreifen kann.
5. Wenn Sie CIFS verwenden, stellen Sie der Datenklassifizierung Active Directory-Anmeldeinformationen zur Verfügung, damit CIFS-Volumes gescannt werden können.

   a. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
   b. Wählen Sie für jedes System **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Data Classification für den Zugriff auf CIFS-Volumes auf dem System benötigt.

Die Anmeldeinformationen können schreibgeschützt sein, durch die Angabe von Administratoranmeldeinformationen wird jedoch sichergestellt, dass die Datenklassifizierung alle Daten lesen kann, für die erweiterte Berechtigungen erforderlich sind. Die Anmeldeinformationen werden auf der Data Classification-Instanz gespeichert.

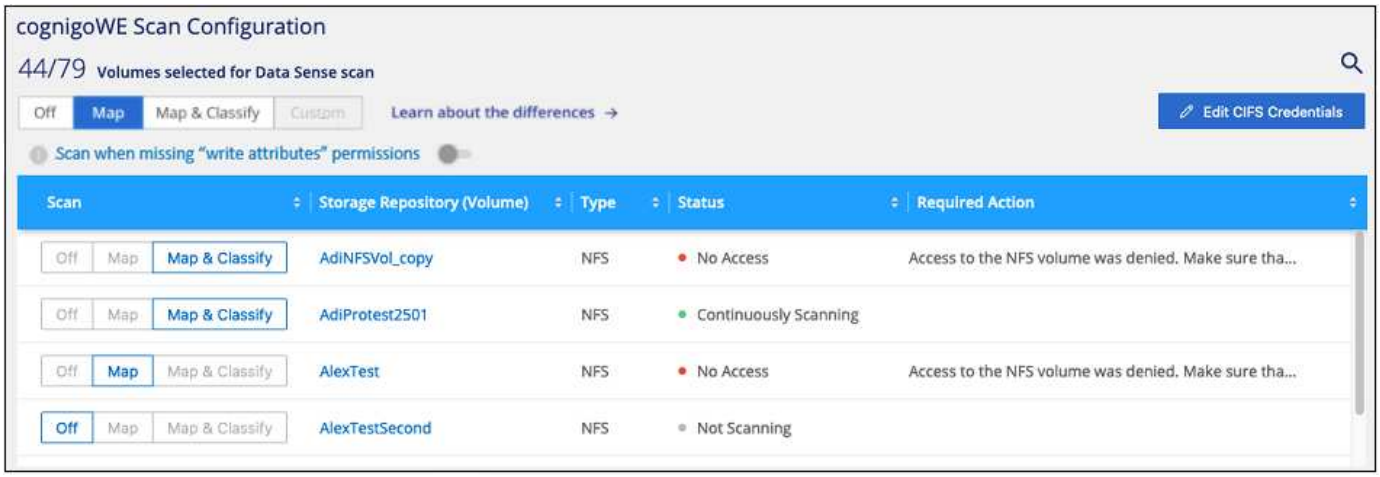
Wenn Sie sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Datenklassifizierungsscans unverändert bleiben, wird empfohlen, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

Nachdem Sie die Anmeldeinformationen eingegeben haben, sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.

Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

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. Wir empfehlen Ihnen, alle Bände zu scannen.

Der Schalter oben auf der Seite für **Scannen, wenn Berechtigungen zum Schreiben von Attributen fehlen** ist standardmäßig deaktiviert. Dies bedeutet, dass das System die Dateien nicht scannt, wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter auf EIN und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Mehr erfahren" .



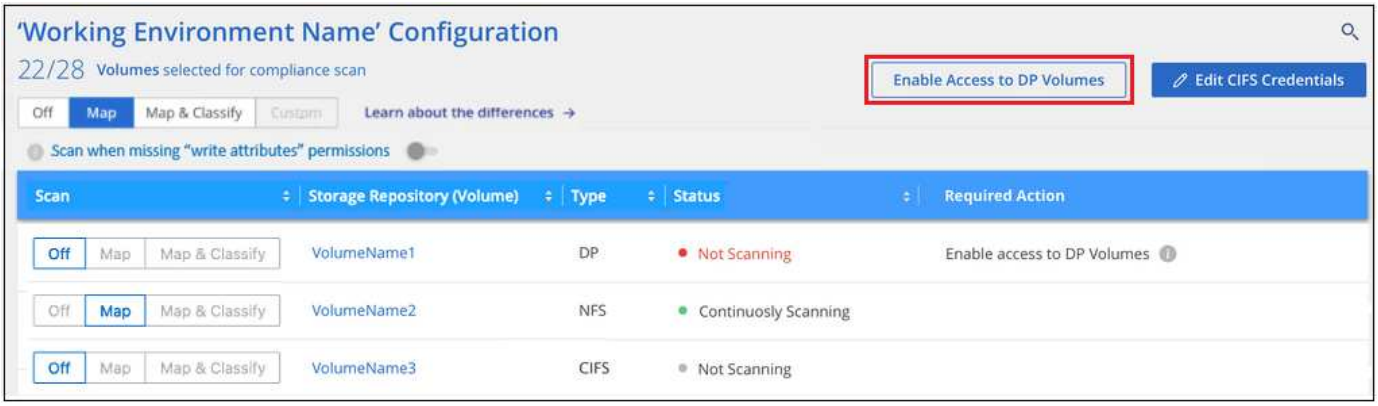
1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Suchen Sie auf der Konfigurationsseite das System mit den Volumes, die Sie scannen möchten.
3. Führen Sie einen der folgenden Schritte aus:
   - Um Nur-Mapping-Scans auf einem Volume zu aktivieren, wählen Sie im Volume-Bereich **Map** aus. Oder wählen Sie zum Aktivieren auf allen Volumes im Überschriftenbereich **Karte** aus. Um das vollständige Scannen eines Volumes zu aktivieren, wählen Sie im Volumebereich **Zuordnen und klassifizieren** aus. Oder wählen Sie zur Aktivierung auf allen Volumes im Überschriftenbereich **Zuordnen und klassifizieren** aus.
   - Um das Scannen auf einem Volume zu deaktivieren, wählen Sie im Volumebereich **Aus**. Um das Scannen auf allen Volumes zu deaktivieren, wählen Sie im Überschriftenbereich **Aus**.

Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und Klassifizieren** festgelegt haben. Wenn Sie im Überschriftenbereich die Option **Benutzerdefiniert** oder **Aus** einstellen, müssen Sie die Zuordnung und/oder das vollständige Scannen für jedes neue Volume aktivieren, das Sie dem System hinzufügen.

Scannen von Datenschutzvolumes

Standardmäßig werden Datenschutzvolumes (DP) nicht gescannt, da sie nicht extern verfügbar sind und die Datenklassifizierung nicht auf sie zugreifen kann. Dies sind die Zielvolumes für SnapMirror -Vorgänge von einem FSx für ONTAP Dateisystem.

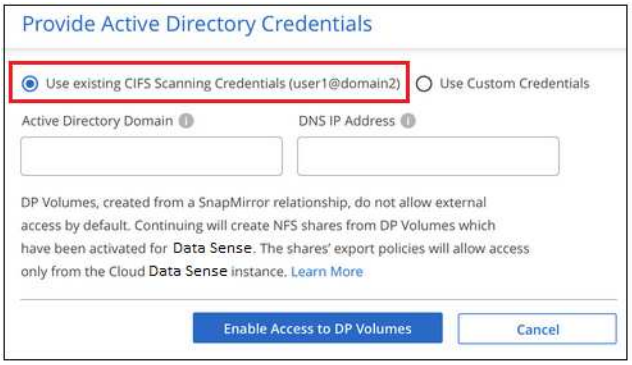
Zunächst werden diese Volumes in der Volumeliste als *Typ* **DP** mit dem *Status* **Nicht scannen** und der *Erforderlichen Aktion* **Zugriff auf DP-Volumes aktivieren** identifiziert.

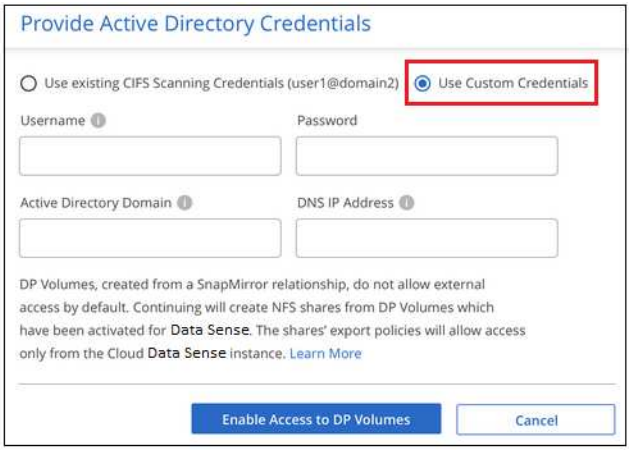


Schritte

Wenn Sie diese Datenschutzvolumes scannen möchten:

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie oben auf der Seite **Zugriff auf DP-Volumes aktivieren** aus.
3. Überprüfen Sie die Bestätigungsnachricht und wählen Sie erneut **Zugriff auf DP-Volumes aktivieren**.
    - Volumes, die ursprünglich als NFS-Volumes im Quell-FSx für ONTAP -Dateisystem erstellt wurden, sind aktiviert.
    - Für Volumes, die ursprünglich als CIFS-Volumes im Quelldateisystem FSx for ONTAP erstellt wurden, müssen Sie CIFS-Anmeldeinformationen eingeben, um diese DP-Volumes zu scannen. Wenn Sie bereits Active Directory-Anmeldeinformationen eingegeben haben, damit Data Classification CIFS-Volumes scannen kann, können Sie diese Anmeldeinformationen verwenden oder einen anderen Satz von Administratoranmeldeinformationen angeben.





4. Aktivieren Sie jedes DP-Volume, das Sie scannen möchten.

Ergebnis

Nach der Aktivierung erstellt die Datenklassifizierung eine NFS-Freigabe aus jedem DP-Volume, das zum Scannen aktiviert wurde. Die Freigabeexportrichtlinien erlauben nur den Zugriff von der Datenklassifizierungsinstanz.

Wenn Sie beim ersten Aktivieren des Zugriffs auf DP-Volumes keine CIFS-Datensicherungsvolumes hatten und später welche hinzufügen, wird oben auf der Konfigurationsseite die Schaltfläche **Zugriff auf CIFS DP aktivieren** angezeigt. Wählen Sie diese Schaltfläche und fügen Sie CIFS-Anmeldeinformationen hinzu, um den Zugriff auf diese CIFS-DP-Volumes zu ermöglichen.

Active Directory-Anmeldeinformationen werden nur in der Speicher-VM des ersten CIFS-DP-Volumes registriert, daher werden alle DP-Volumes auf dieser SVM gescannt. Bei Volumes, die sich auf anderen SVMs befinden, sind die Active Directory-Anmeldeinformationen nicht registriert, sodass diese DP-Volumes nicht gescannt werden.

Scannen Sie Cloud Volumes ONTAP und lokale ONTAP Volumes mit NetApp Data Classification

Führen Sie einige Schritte aus, um mit dem Scannen Ihrer Cloud Volumes ONTAP und lokalen ONTAP Volumes mithilfe der NetApp Data Classification zu beginnen.

Voraussetzungen

Stellen Sie vor dem Aktivieren der Datenklassifizierung sicher, dass Sie über eine unterstützte Konfiguration verfügen.

- Wenn Sie Cloud Volumes ONTAP und lokale ONTAP -Systeme scannen, die über das Internet zugänglich sind, können Sie"Datenklassifizierung in der Cloud bereitstellen" oder"an einem lokalen Standort mit Internetzugang" .
- Wenn Sie lokale ONTAP -Systeme scannen, die an einem Dark Site ohne Internetzugang installiert wurden, müssen Sie"Stellen Sie die Datenklassifizierung am selben lokalen Standort bereit, der keinen Internetzugang hat" . Dazu muss der Konsolenagent am selben lokalen Standort bereitgestellt werden.

Aktivieren Sie die Datenklassifizierungsüberprüfung in Ihren Systemen

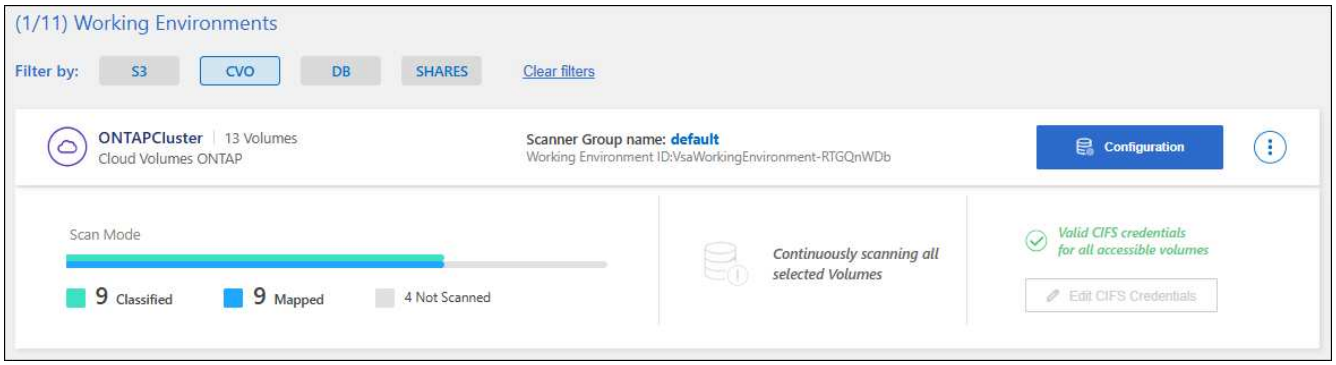
Sie können das Scannen der Datenklassifizierung auf Cloud Volumes ONTAP -Systemen bei jedem

unterstützten Cloud-Anbieter und auf lokalen ONTAP Clustern aktivieren.

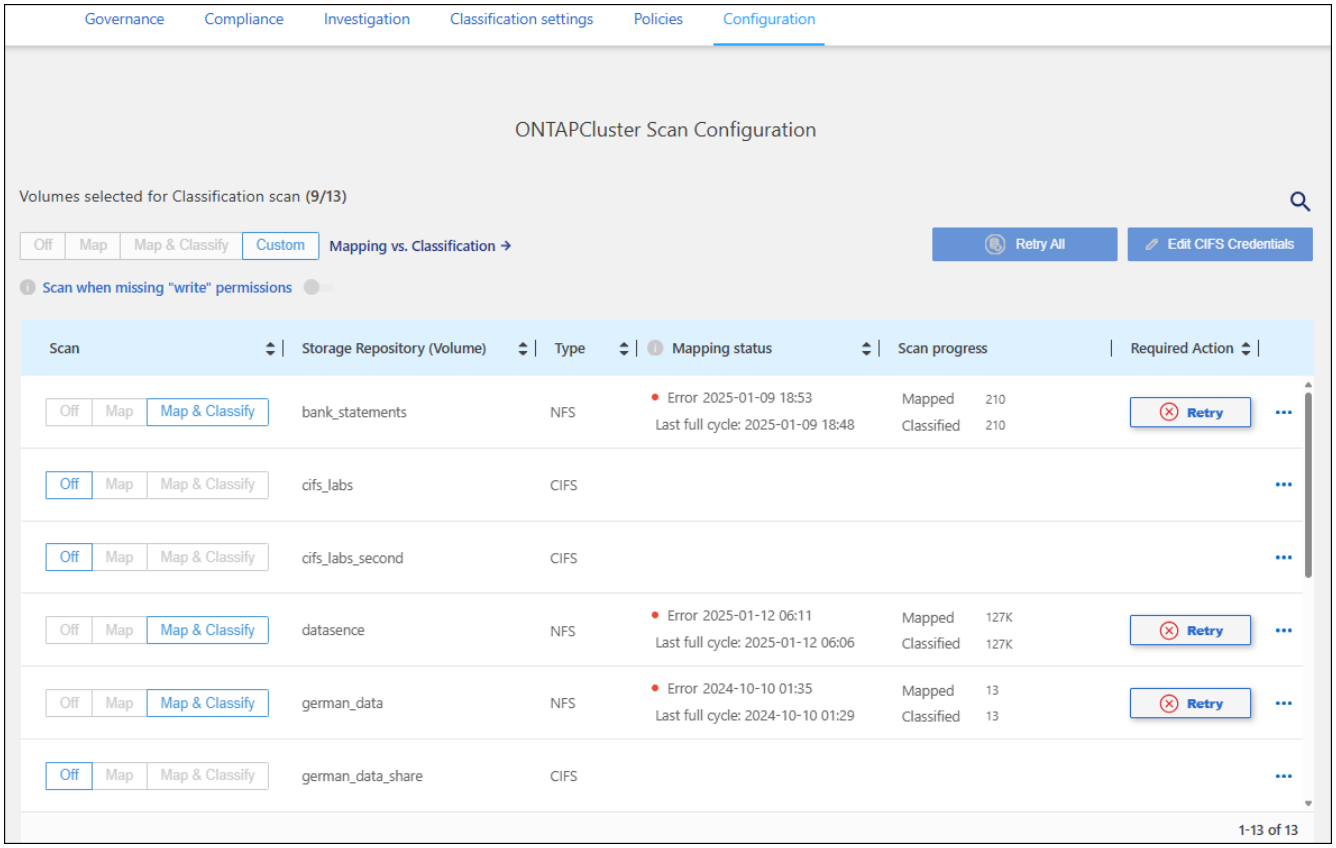
Schritte

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

   Auf der Konfigurationsseite werden mehrere Systeme angezeigt.



2. Wählen Sie ein System und dann **Konfiguration**.



3. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter **Scannen bei fehlenden Berechtigungen zum Schreiben von Attributen** ein und alle Dateien werden unabhängig von den Berechtigungen gescannt.

   Der Schalter oben auf der Seite für **Scannen, wenn Berechtigungen zum Schreiben von Attributen fehlen** ist standardmäßig deaktiviert. Dies bedeutet, dass das System die Dateien nicht klassifiziert, wenn die Datenklassifizierung keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, da die Datenklassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. "Mehr erfahren" .

4. Wählen Sie aus, wie Sie die Volumes in jedem System scannen möchten. "Erfahren Sie mehr über Mapping- und Klassifizierungsscans":
   - Um alle Volumes zuzuordnen, wählen Sie **Zuordnen**.
   - Um alle Volumes zuzuordnen und zu klassifizieren, wählen Sie **Zuordnen und klassifizieren**.
   - Um das Scannen für jedes Volume anzupassen, wählen Sie **Benutzerdefiniert** und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.
5. Wählen Sie im Bestätigungsdialogfeld **Genehmigen** aus, damit die Datenklassifizierung mit dem Scannen Ihrer Datenträger beginnt.

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse werden im Compliance-Dashboard angezeigt, sobald die Datenklassifizierung mit dem Scan beginnt. Die dafür benötigte Zeit hängt von der Datenmenge ab und kann einige Minuten oder Stunden betragen.

> Die Datenklassifizierung scannt nur eine Dateifreigabe unter einem Volume. Wenn Ihre Volumes mehrere Freigaben enthalten, müssen Sie diese anderen Freigaben separat als Freigabegruppe scannen. "Weitere Einzelheiten zu dieser Datenklassifizierungsbeschränkung" .

Überprüfen Sie, ob die Datenklassifizierung Zugriff auf die Volumes hat.

Stellen Sie sicher, dass die Datenklassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien überprüfen. Sie müssen Data Classification CIFS-Anmeldeinformationen bereitstellen, damit es auf CIFS-Volumes zugreifen kann.

Checklist

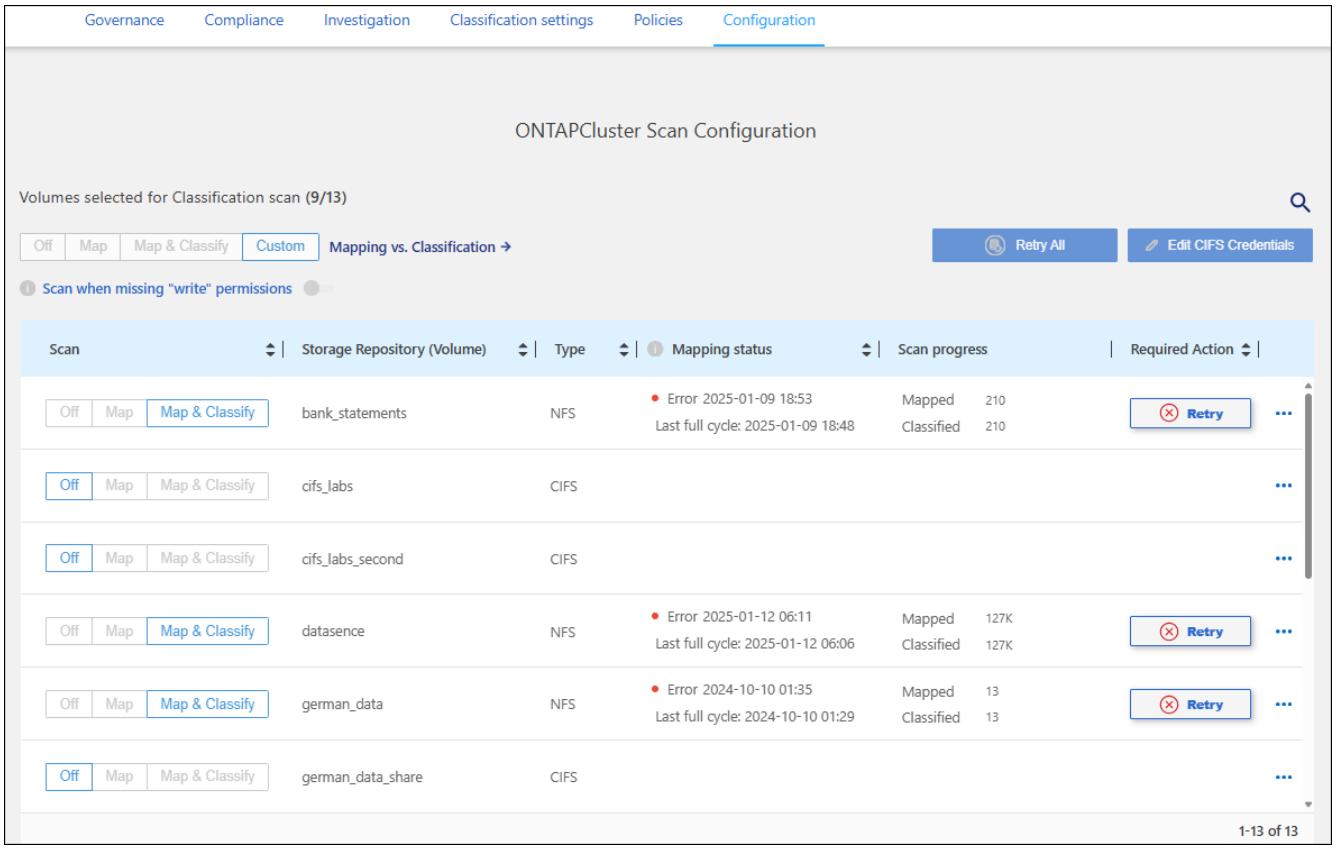
- Stellen Sie sicher, dass zwischen der Data Classification-Instanz und jedem Netzwerk, das Volumes für Cloud Volumes ONTAP oder lokale ONTAP Cluster enthält, eine Netzwerkverbindung besteht.
- Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr von der Data Classification-Instanz zulässt.

  Sie können die Sicherheitsgruppe entweder für den Datenverkehr von der IP-Adresse der Data Classification-Instanz öffnen oder Sie können die Sicherheitsgruppe für den gesamten Datenverkehr innerhalb des virtuellen Netzwerks öffnen.

- Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Classification-Instanz enthalten, damit diese auf die Daten auf jedem Volume zugreifen kann.

Schritte

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



.. Wenn Sie CIFS verwenden, stellen Sie der Datenklassifizierung Active Directory-Anmeldeinformationen zur Verfügung, damit CIFS-Volumes gescannt werden können. Wählen Sie für jedes System **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Data Classification für den Zugriff auf CIFS-Volumes auf dem System benötigt.

+ Die Anmeldeinformationen können schreibgeschützt sein, aber durch die Bereitstellung von Administratoranmeldeinformationen wird sichergestellt, dass die Datenklassifizierung alle Daten lesen kann, die erweiterte Berechtigungen erfordern. Die Anmeldeinformationen werden auf der Data Classification-Instanz gespeichert.

+ Wenn Sie sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Datenklassifizierungsscans unverändert bleiben, wird empfohlen, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

+ Nachdem Sie die Anmeldeinformationen eingegeben haben, sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.

2. Wählen Sie auf der Konfigurationsseite **Konfiguration** aus, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und etwaige Fehler zu beheben.

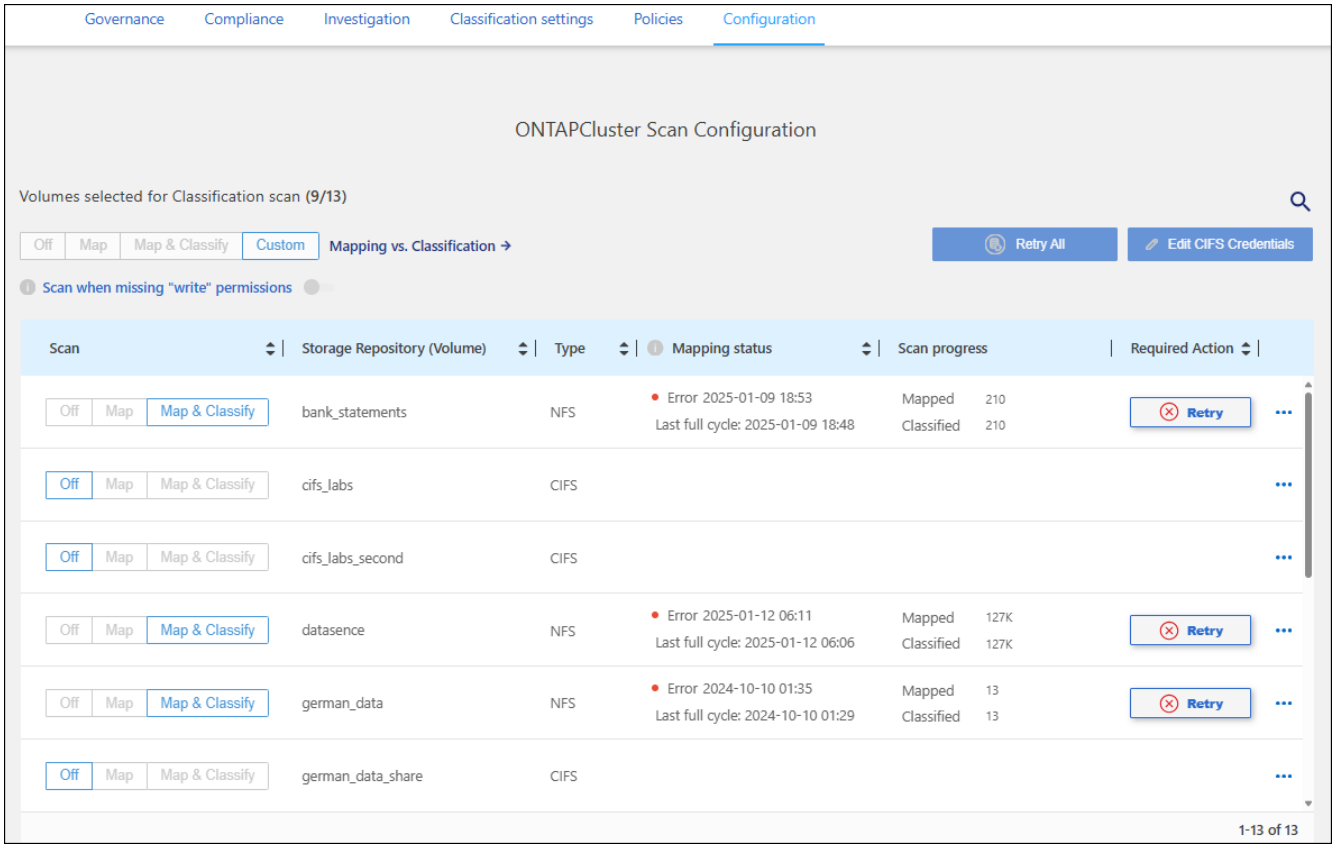
Deaktivieren von Compliance-Scans auf Volumes

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. Wir empfehlen Ihnen, alle Bände zu scannen.

Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und Klassifizieren** festgelegt haben. Wenn die Option im Überschriftenbereich auf **Benutzerdefiniert** oder **Aus** eingestellt ist, müssen Sie die Zuordnung und/oder das vollständige Scannen für jedes neue Volume aktivieren, das Sie dem System hinzufügen.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie die Schaltfläche **Konfiguration** für das System, das Sie ändern möchten.



3. Führen Sie einen der folgenden Schritte aus:
   - Um das Scannen auf einem Volume zu deaktivieren, wählen Sie im Volumebereich **Aus**.
   - Um das Scannen auf allen Volumes zu deaktivieren, wählen Sie im Überschriftenbereich **Aus**.

Scannen Sie Datenbankschemata mit NetApp Data Classification

Führen Sie einige Schritte aus, um mit dem Scannen Ihrer Datenbankschemata mit NetApp Data Classification zu beginnen.

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie die Datenklassifizierung aktivieren.

Unterstützte Datenbanken

Die Datenklassifizierung kann Schemata aus den folgenden Datenbanken scannen:

- Amazon Relational Database Service (Amazon RDS)
- MongoDB
- MySQL
- Orakel
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

Die Funktion zum Sammeln von Statistiken **muss** in der Datenbank aktiviert sein.

Datenbankanforderungen

Jede Datenbank mit Verbindung zur Datenklassifizierungsinstanz kann gescannt werden, unabhängig davon, wo sie gehostet wird. Um eine Verbindung zur Datenbank herzustellen, benötigen Sie lediglich die folgenden Informationen:

- IP-Adresse oder Hostname
- Hafen
- Dienstname (nur für den Zugriff auf Oracle-Datenbanken)
- Anmeldeinformationen, die Lesezugriff auf die Schemata ermöglichen

  Bei der Auswahl eines Benutzernamens und Kennworts ist es wichtig, dass Sie einen Benutzernamen und ein Kennwort auswählen, der über vollständige Leseberechtigungen für alle Schemata und Tabellen verfügt, die Sie scannen möchten. Wir empfehlen Ihnen, einen dedizierten Benutzer für das Datenklassifizierungssystem mit allen erforderlichen Berechtigungen zu erstellen.

Für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

Bereitstellen der Datenklassifizierungsinstanz

Stellen Sie die Datenklassifizierung bereit, wenn noch keine Instanz bereitgestellt ist.

Wenn Sie Datenbankschemata scannen, die über das Internet zugänglich sind, können Sie"Datenklassifizierung in der Cloud bereitstellen" oder"Stellen Sie die Datenklassifizierung an einem lokalen Standort mit Internetzugang bereit" .

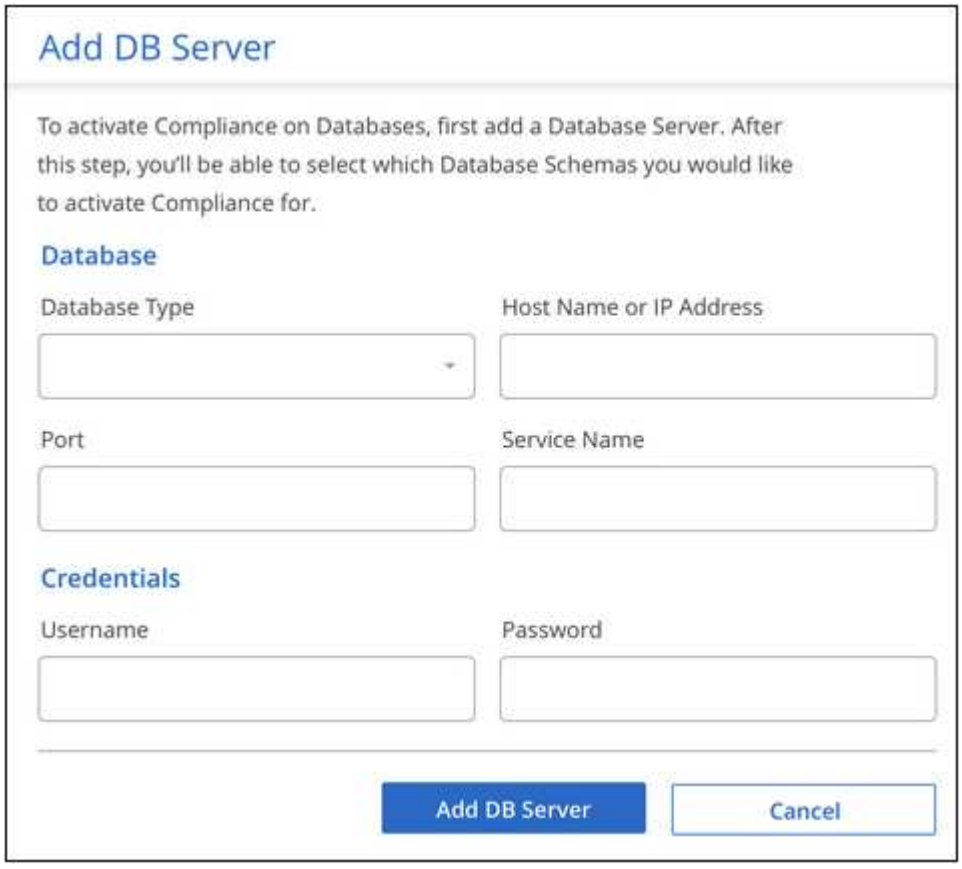
Wenn Sie Datenbankschemata scannen, die in einer Dark Site ohne Internetzugang installiert wurden, müssen Sie"Stellen Sie die Datenklassifizierung am selben lokalen Standort bereit, der keinen Internetzugang hat" . Dies erfordert auch, dass der Konsolenagent am selben lokalen Standort bereitgestellt wird.

Hinzufügen des Datenbankservers

Fügen Sie den Datenbankserver hinzu, auf dem sich die Schemas befinden.

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

2. Wählen Sie auf der Konfigurationsseite **System hinzufügen** > **Datenbankserver hinzufügen**.
3. Geben Sie die erforderlichen Informationen zur Identifizierung des Datenbankservers ein.
   a. Wählen Sie den Datenbanktyp aus.
   b. Geben Sie den Port und den Hostnamen oder die IP-Adresse ein, um eine Verbindung zur Datenbank herzustellen.
   c. Geben Sie für Oracle-Datenbanken den Dienstnamen ein.
   d. Geben Sie die Anmeldeinformationen ein, damit Data Classification auf den Server zugreifen kann.
   e. Wählen Sie **DB-Server hinzufügen**.



Die Datenbank wird der Liste der Systeme hinzugefügt.

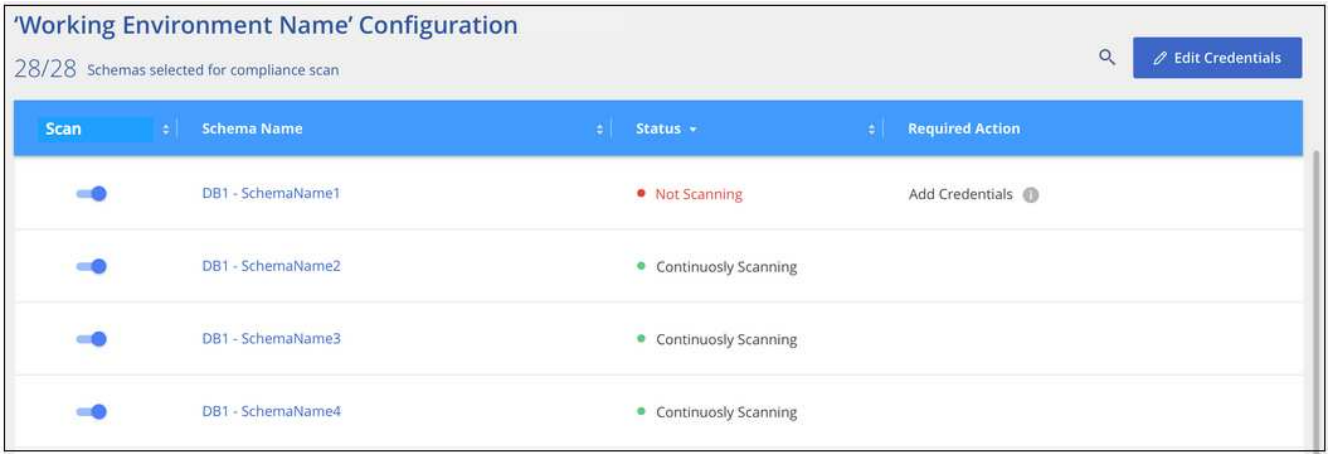
Aktivieren und Deaktivieren von Compliance-Scans für Datenbankschemata

Sie können den vollständigen Scan Ihrer Schemata jederzeit stoppen oder starten.

Es gibt keine Option zum Auswählen von Nur-Mapping-Scans für Datenbankschemata.

1. Wählen Sie auf der Konfigurationsseite die Schaltfläche **Konfiguration** für die Datenbank aus, die Sie konfigurieren möchten.

2. Wählen Sie die Schemata aus, die Sie scannen möchten, indem Sie den Schieberegler nach rechts bewegen.



Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen aktivierten Datenbankschemata. Sie können den Fortschritt des ersten Scans verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die **Systemkonfiguration** auswählen. Der Fortschritt jedes Scans wird als Fortschrittsbalken angezeigt. Sie können auch mit der Maus über den Fortschrittsbalken fahren, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen. Wenn Fehler vorliegen, werden diese zusammen mit der erforderlichen Aktion zur Behebung des Fehlers in der Spalte „Status“ angezeigt.

Die Datenklassifizierung scannt Ihre Datenbanken einmal pro Tag; Datenbanken werden nicht kontinuierlich gescannt wie andere Datenquellen.

Scannen Sie Dateifreigaben mit NetApp Data Classification

Um Dateifreigaben zu scannen, müssen Sie zunächst eine Dateifreigabegruppe in NetApp Data Classification erstellen. Dateifreigabegruppen sind für NFS- oder CIFS-Freigaben (SMB), die vor Ort oder in der Cloud gehostet werden.

Das Scannen von Daten aus Nicht- NetApp Dateifreigaben wird in der Kernversion der Datenklassifizierung nicht unterstützt.

Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie die Datenklassifizierung aktivieren.

- Die Freigaben können überall gehostet werden, auch in der Cloud oder vor Ort. CIFS-Freigaben von älteren NetApp 7-Mode-Speichersystemen können als Dateifreigaben gescannt werden.
  - Die Datenklassifizierung kann aus 7-Mode-Systemen weder Berechtigungen noch die „letzte Zugriffszeit“ extrahieren.
  - Aufgrund eines bekannten Problems zwischen einigen Linux-Versionen und CIFS-Freigaben auf 7-Mode-Systemen müssen Sie die Freigabe so konfigurieren, dass nur SMBv1 mit aktivierter NTLM-Authentifizierung verwendet wird.
- Zwischen der Data Classification-Instanz und den Freigaben muss eine Netzwerkverbindung bestehen.
- Sie können eine DFS-Freigabe (Distributed File System) als normale CIFS-Freigabe hinzufügen. Da die Datenklassifizierung nicht erkennt, dass die Freigabe auf mehreren Servern/Volumes basiert, die zu einer einzigen CIFS-Freigabe zusammengefasst sind, erhalten Sie möglicherweise Berechtigungs- oder Verbindungsfehler bezüglich der Freigabe, obwohl die Meldung tatsächlich nur für einen der Ordner/Freigaben gilt, der sich auf einem anderen Server/Volume befindet.
- Stellen Sie bei CIFS-Freigaben (SMB) sicher, dass Sie über Active Directory-Anmeldeinformationen verfügen, die Lesezugriff auf die Freigaben ermöglichen. Administratoranmeldeinformationen werden bevorzugt, wenn die Datenklassifizierung Daten scannen muss, für die erweiterte Berechtigungen erforderlich sind.

  Wenn Sie sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Datenklassifizierungsscans unverändert bleiben, wird empfohlen, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

- Alle CIFS-Dateifreigaben in einer Gruppe müssen dieselben Active Directory-Anmeldeinformationen verwenden.
- Sie können NFS- und CIFS-Freigaben (entweder mit Kerberos oder NTLM) mischen. Sie müssen die Freigaben separat zur Gruppe hinzufügen. Das heißt, Sie müssen den Vorgang zweimal durchführen – einmal pro Protokoll.
  - Sie können keine Dateifreigabegruppe erstellen, die CIFS-Authentifizierungstypen (Kerberos und NTLM) mischt.
- Wenn Sie CIFS mit Kerberos-Authentifizierung verwenden, stellen Sie sicher, dass die angegebene IP-Adresse für die Datenklassifizierung zugänglich ist. Die Dateifreigaben können nicht hinzugefügt werden, wenn die IP-Adresse nicht erreichbar ist.

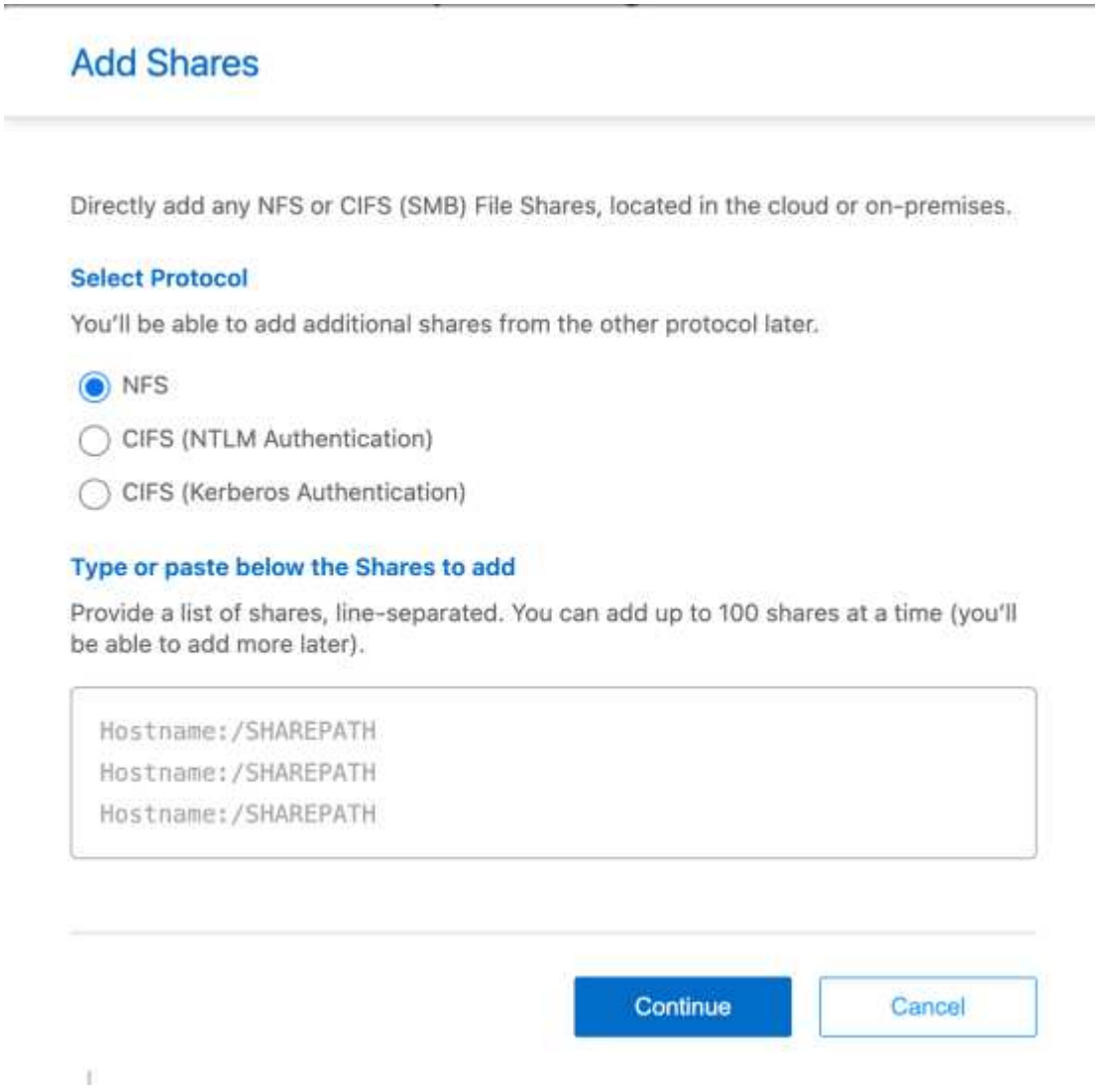
Erstellen einer Dateifreigabegruppe

Wenn Sie Dateifreigaben zur Gruppe hinzufügen, müssen Sie das Format verwenden `<host_name>:/<share_path>`.

Sie können Dateifreigaben einzeln hinzufügen oder eine zeilengetrennte Liste der Dateifreigaben eingeben, die Sie scannen möchten. Sie können bis zu 100 Aktien gleichzeitig hinzufügen.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite **System hinzufügen** > **Dateifreigabegruppe hinzufügen**.
3. Geben Sie im Dialogfeld „Dateifreigabegruppe hinzufügen“ den Namen für die Freigabegruppe ein und wählen Sie dann **Weiter**.
4. Wählen Sie das Protokoll für die Dateifreigaben aus, die Sie hinzufügen.



a. Wenn Sie CIFS-Freigaben mit NTLM-Authentifizierung hinzufügen, geben Sie die Active Directory-Anmeldeinformationen ein, um auf die CIFS-Volumes zuzugreifen. Obwohl schreibgeschützte Anmeldeinformationen unterstützt werden, wird empfohlen, den Vollzugriff mit Administratoranmeldeinformationen zu gewähren. Wählen Sie **Speichern**.

5. Fügen Sie die Dateifreigaben hinzu, die Sie scannen möchten (eine Dateifreigabe pro Zeile). Wählen Sie dann **Weiter**.
6. Ein Bestätigungsdialogfeld zeigt die Anzahl der hinzugefügten Freigaben an.

   Wenn im Dialogfeld Freigaben aufgelistet sind, die nicht hinzugefügt werden konnten, erfassen Sie diese Informationen, damit Sie das Problem beheben können. Wenn das Problem eine Namenskonvention betrifft, können Sie die Freigabe mit einem korrigierten Namen erneut hinzufügen.

7. Konfigurieren Sie das Scannen auf dem Volume:
   - Um Nur-Mapping-Scans auf Dateifreigaben zu aktivieren, wählen Sie **Map**.
   - Um vollständige Scans von Dateifreigaben zu aktivieren, wählen Sie **Zuordnen und klassifizieren**.
   - Um das Scannen von Dateifreigaben zu deaktivieren, wählen Sie **Aus**.

Der Schalter oben auf der Seite für **Scannen, wenn Berechtigungen zum Schreiben von Attributen fehlen** ist standardmäßig deaktiviert. Dies bedeutet, dass das System die Dateien nicht scannt, wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. + Wenn Sie **Scannen bei fehlenden Berechtigungen zum Schreiben von Attributen** auf **Ein** stellen, setzt der Scan die letzte Zugriffszeit zurück und scannt alle Dateien unabhängig von den Berechtigungen. + Weitere Informationen zum Zeitstempel des letzten Zugriffs finden Sie unter"Aus Datenquellen in der Datenklassifizierung gesammelte Metadaten" .

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der Dateien in den von Ihnen hinzugefügten Dateifreigaben. Du kannstVerfolgen Sie den Scan-Fortschritt und sehen Sie sich die Ergebnisse des Scans im **Dashboard** an.

Wenn der Scan für eine CIFS-Konfiguration mit Kerberos-Authentifizierung nicht erfolgreich abgeschlossen wird, überprüfen Sie die Registerkarte **Konfiguration** auf Fehler.

Bearbeiten einer Dateifreigabegruppe

Nachdem Sie eine Dateifreigabegruppe erstellt haben, können Sie das CIFS-Protokoll bearbeiten oder Dateifreigaben hinzufügen und entfernen.

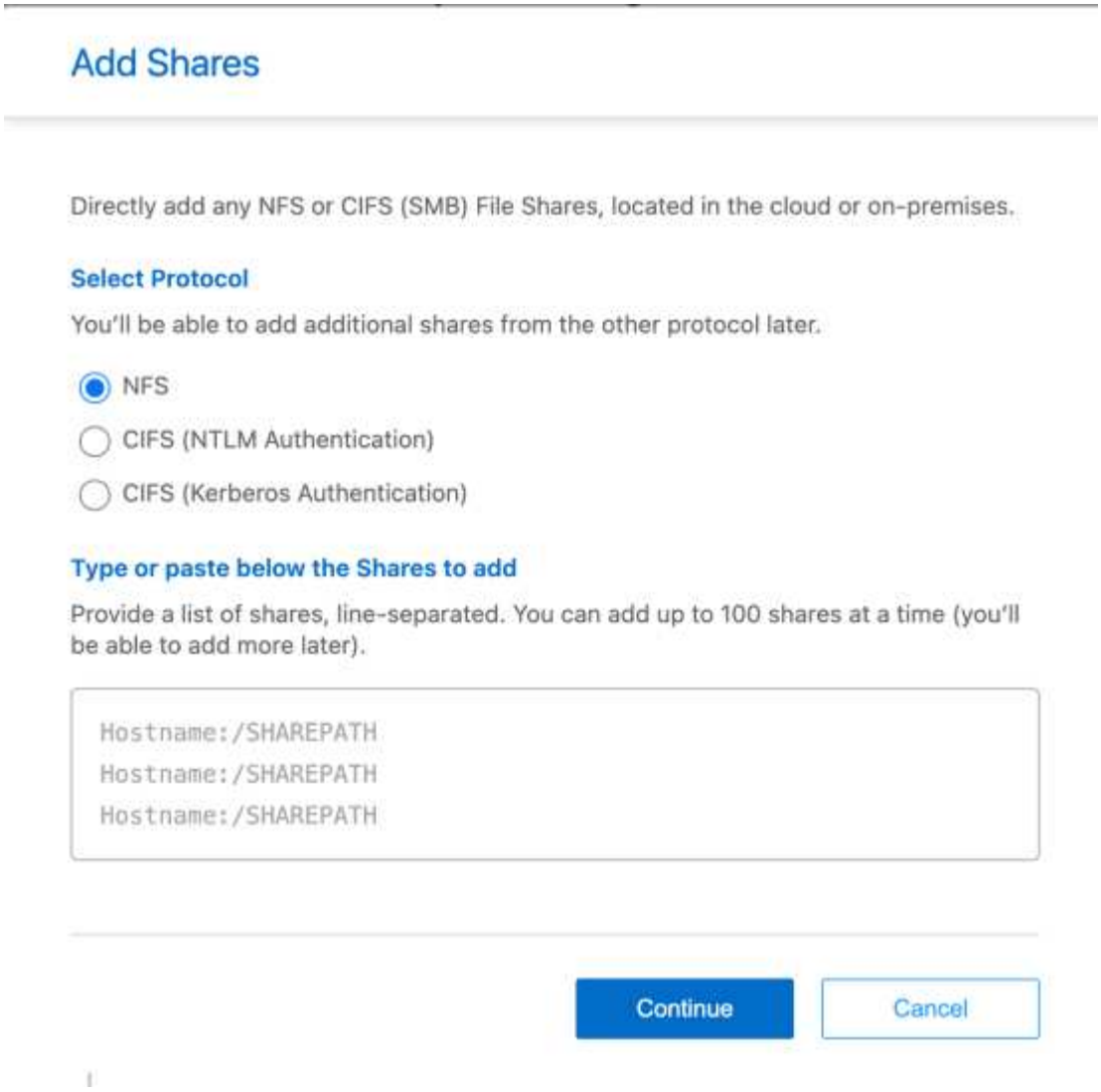
Bearbeiten Sie die CIFS-Protokollkonfiguration

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite die Dateifreigabegruppe aus, die Sie ändern möchten.
3. Wählen Sie **CIFS-Anmeldeinformationen bearbeiten**.

4. Wählen Sie die Authentifizierungsmethode: **NTLM** oder **Kerberos**.
5. Geben Sie den **Benutzernamen** und das **Passwort** von Active Directory ein.
6. Wählen Sie **Speichern**, um den Vorgang abzuschließen.

Dateifreigaben zu Compliance-Scans hinzufügen

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite die Dateifreigabegruppe aus, die Sie ändern möchten.
3. Wählen Sie **+ Freigaben hinzufügen**.
4. Wählen Sie das Protokoll für die Dateifreigaben aus, die Sie hinzufügen.



Wenn Sie Dateifreigaben zu einem bereits konfigurierten Protokoll hinzufügen, sind keine Änderungen erforderlich.

Wenn Sie Dateifreigaben mit einem zweiten Protokoll hinzufügen, stellen Sie sicher, dass Sie die Authentifizierung ordnungsgemäß konfiguriert haben, wie im"Voraussetzungen" .

5. Fügen Sie die Dateifreigaben hinzu, die Sie scannen möchten (eine Dateifreigabe pro Zeile), und verwenden Sie dabei das Format `<host_name>:/<share_path>` .
6. Wählen Sie **Weiter**, um das Hinzufügen der Dateifreigaben abzuschließen.

Entfernen einer Dateifreigabe aus Compliance-Scans

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie das System aus, von dem Sie Dateifreigaben entfernen möchten.
3. Wählen Sie **Konfiguration**.
4. Wählen Sie auf der Konfigurationsseite die Aktionen ••• für die Dateifreigabe, die Sie entfernen möchten.
5. Wählen Sie im Menü „Aktionen“ die Option „Freigabe entfernen“ aus.

Verfolgen Sie den Scan-Fortschritt

Sie können den Fortschritt des ersten Scans verfolgen.

1. Wählen Sie das Menü **Konfiguration**.
2. Wählen Sie die **Systemkonfiguration**.
3. Überprüfen Sie für das Speicherrepository die Spalte „Scan-Fortschritt“, um den Status anzuzeigen.

Scannen Sie StorageGRID -Daten mit NetApp Data Classification

Führen Sie einige Schritte aus, um mit dem Scannen von Daten in StorageGRID direkt mit NetApp Data Classification zu beginnen.

Überprüfen Sie die StorageGRID Anforderungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie die Datenklassifizierung aktivieren.

- Sie benötigen die Endpunkt-URL, um eine Verbindung mit dem Objektspeicherdienst herzustellen.
- Sie benötigen den Zugriffsschlüssel und den geheimen Schlüssel von StorageGRID , damit die Datenklassifizierung auf die Buckets zugreifen kann.

Bereitstellen der Datenklassifizierungsinstanz

Stellen Sie die Datenklassifizierung bereit, wenn noch keine Instanz bereitgestellt ist.

Wenn Sie Daten von StorageGRID scannen, die über das Internet zugänglich sind, können Sie"Datenklassifizierung in der Cloud bereitstellen" oder"Stellen Sie die Datenklassifizierung an einem lokalen Standort mit Internetzugang bereit" .

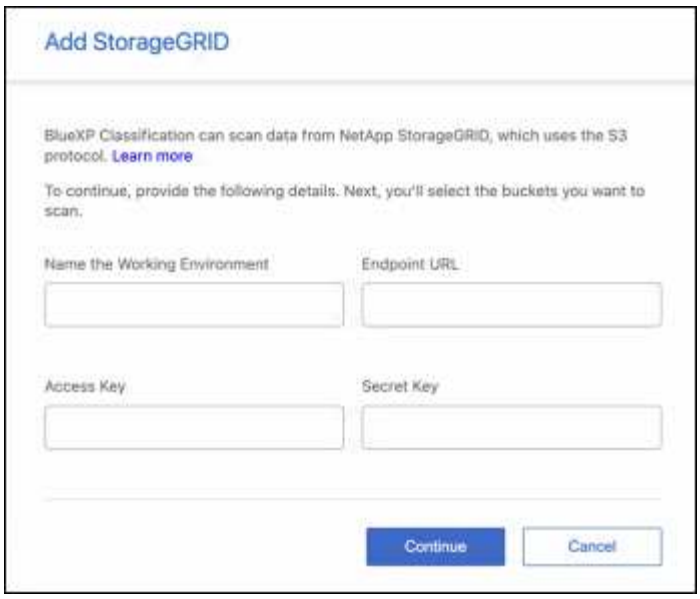
Wenn Sie Daten von StorageGRID scannen, das in einer Dark Site ohne Internetzugang installiert wurde, müssen Sie"Stellen Sie die Datenklassifizierung am selben lokalen Standort bereit, der keinen Internetzugang hat" . Dies erfordert auch, dass der Konsolenagent am selben lokalen Standort bereitgestellt wird.

Fügen Sie den StorageGRID -Dienst zur Datenklassifizierung hinzu

Fügen Sie den StorageGRID -Dienst hinzu.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite **System hinzufügen** > * StorageGRID hinzufügen*.
3. Geben Sie im Dialogfeld „StorageGRID -Dienst hinzufügen“ die Details für den StorageGRID -Dienst ein und wählen Sie **Weiter**.
   a. Geben Sie den Namen ein, den Sie für das System verwenden möchten. Dieser Name sollte den Namen des StorageGRID -Dienstes widerspiegeln, mit dem Sie eine Verbindung herstellen.
   b. Geben Sie die Endpunkt-URL ein, um auf den Objektspeicherdienst zuzugreifen.
   c. Geben Sie den Zugriffsschlüssel und den geheimen Schlüssel ein, damit die Datenklassifizierung auf die Buckets in StorageGRID zugreifen kann.



Ergebnis

StorageGRID wird zur Liste der Systeme hinzugefügt.

Aktivieren und Deaktivieren von Compliance-Scans für StorageGRID -Buckets

Nachdem Sie die Datenklassifizierung auf StorageGRID aktiviert haben, besteht der nächste Schritt darin, die Buckets zu konfigurieren, die Sie scannen möchten. Die Datenklassifizierung erkennt diese Buckets und zeigt sie in dem von Ihnen erstellten System an.

Schritte

1. Suchen Sie auf der Konfigurationsseite das StorageGRID -System.
2. Wählen Sie auf der StorageGRID -Systemkachel **Konfiguration** aus.
3. Führen Sie einen der folgenden Schritte aus, um das Scannen zu aktivieren oder zu deaktivieren:
   - Um Nur-Mapping-Scans für einen Bucket zu aktivieren, wählen Sie **Map**.
   - Um vollständige Scans für einen Bucket zu aktivieren, wählen Sie **Zuordnen und klassifizieren**.
   - Um das Scannen eines Buckets zu deaktivieren, wählen Sie **Aus**.

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen aktivierten Buckets. Sie können den Fortschritt des ersten Scans verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die **Systemkonfiguration** auswählen. Der Fortschritt jedes Scans wird als Fortschrittsbalken angezeigt. Sie können auch mit der Maus über den Fortschrittsbalken fahren, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen. Wenn Fehler vorliegen, werden diese zusammen mit der erforderlichen Aktion zur Behebung des Fehlers in der Spalte „Status“ angezeigt.

Integrieren Sie Ihr Active Directory mit NetApp Data Classification

Sie können ein globales Active Directory mit NetApp Data Classification integrieren, um die von Data Classification gemeldeten Ergebnisse zu Dateibesitzern und zu den Benutzern und Gruppen, die Zugriff auf Ihre Dateien haben, zu verbessern.

Wenn Sie bestimmte Datenquellen (unten aufgeführt) einrichten, müssen Sie Active Directory-Anmeldeinformationen eingeben, damit Data Classification CIFS-Volumes scannen kann. Diese Integration bietet der Datenklassifizierung Details zu Dateieigentümern und Berechtigungen für die in diesen Datenquellen gespeicherten Daten. Das für diese Datenquellen eingegebene Active Directory kann sich von den globalen Active Directory-Anmeldeinformationen unterscheiden, die Sie hier eingeben. Die Datenklassifizierung sucht in allen integrierten Active Directorys nach Benutzer- und Berechtigungsdetails.

Diese Integration bietet zusätzliche Informationen an den folgenden Stellen in der Datenklassifizierung:

- Sie können den "Dateibesitzer" verwenden"Filter" und sehen Sie sich die Ergebnisse in den Metadaten der Datei im Untersuchungsbereich an. Anstelle des Dateibesitzers, der die SID (Security IDentifier) enthält, wird der tatsächliche Benutzername eingetragen.

  Sie können auch weitere Details zum Dateibesitzer anzeigen: Kontoname, E-Mail-Adresse und SAM-Kontoname oder Elemente anzeigen, die diesem Benutzer gehören.

- Sie können sehen"vollständige Dateiberechtigungen" für jede Datei und jedes Verzeichnis, wenn Sie auf die Schaltfläche „Alle Berechtigungen anzeigen“ klicken.
- Im"Governance-Dashboard" , zeigt das Bedienfeld „Berechtigungen öffnen“ einen größeren Detaillierungsgrad zu Ihren Daten an.

Lokale Benutzer-SIDs und SIDs aus unbekannten Domänen werden nicht in den tatsächlichen Benutzernamen übersetzt.

Unterstützte Datenquellen

Eine Active Directory-Integration mit Datenklassifizierung kann Daten aus den folgenden Datenquellen identifizieren:

- On-Premises- ONTAP -Systeme
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSx für ONTAP

Stellen Sie eine Verbindung zu Ihrem Active Directory-Server her

Nachdem Sie die Datenklassifizierung bereitgestellt und das Scannen Ihrer Datenquellen aktiviert haben, können Sie die Datenklassifizierung in Ihr Active Directory integrieren. Auf Active Directory kann über eine DNS-Server-IP-Adresse oder eine LDAP-Server-IP-Adresse zugegriffen werden.

Die Active Directory-Anmeldeinformationen können schreibgeschützt sein, durch die Bereitstellung von Administratoranmeldeinformationen wird jedoch sichergestellt, dass die Datenklassifizierung alle Daten lesen kann, für die erweiterte Berechtigungen erforderlich sind. Die Anmeldeinformationen werden auf der Data Classification-Instanz gespeichert.

Wenn Sie bei CIFS-Volumes/Dateifreigaben sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Klassifizierungsscans der Datenklassifizierung unverändert bleiben, muss der Benutzer über die Berechtigung „Attribute schreiben“ verfügen. Wenn möglich, empfehlen wir, den in Active Directory konfigurierten Benutzer zu einem Teil einer übergeordneten Gruppe in der Organisation zu machen, die über Berechtigungen für alle Dateien verfügt.

Anforderungen

- Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben.
- Sie benötigen die Informationen für das Active Directory:
  - DNS-Server-IP-Adresse oder mehrere IP-Adressen

    oder

  LDAP-Server-IP-Adresse oder mehrere IP-Adressen
  - Benutzername und Passwort für den Zugriff auf den Server
  - Domänenname (Active Directory-Name)
  - Ob Sie sicheres LDAP (LDAPS) verwenden oder nicht
  - LDAP-Server-Port (normalerweise 389 für LDAP und 636 für sicheres LDAP)
- Die folgenden Ports müssen für die ausgehende Kommunikation durch die Data Classification-Instanz geöffnet sein:

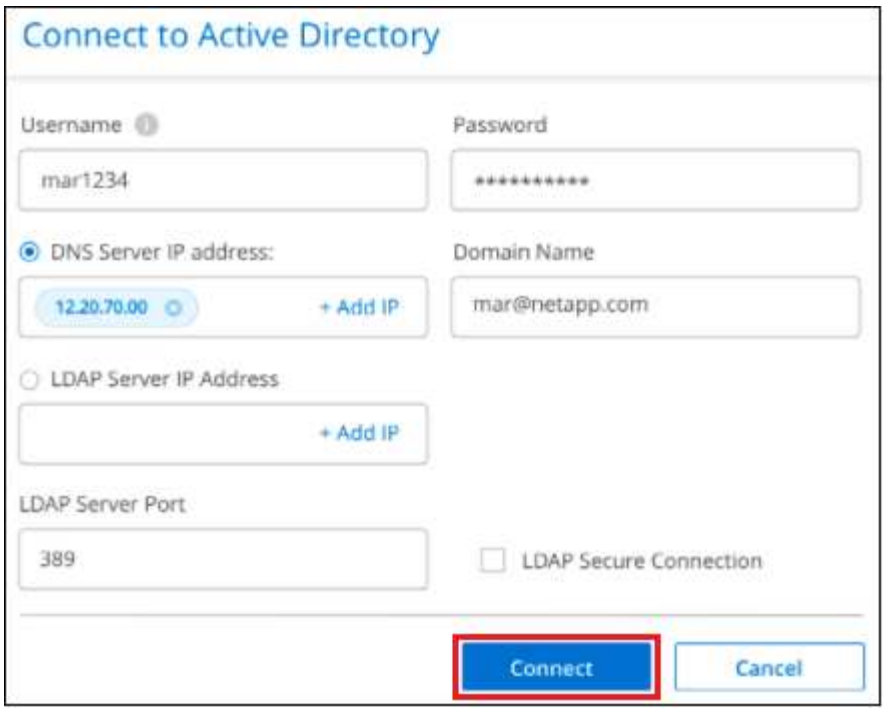
Protokoll	Hafen	Ziel	Zweck
TCP und UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP über SSL
TCP	3268	Active Directory	Globaler Katalog
TCP	3269	Active Directory	Globaler Katalog über SSL

Schritte

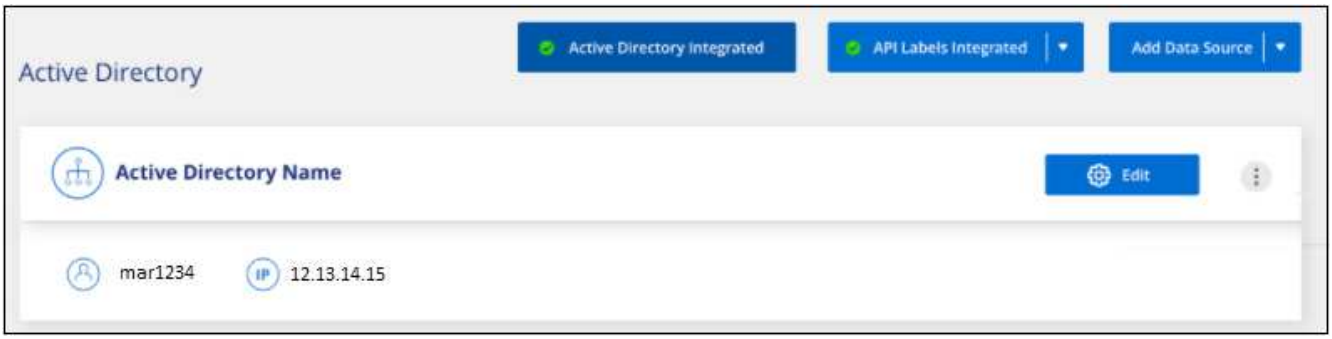
1. Klicken Sie auf der Seite „Datenklassifizierungskonfiguration“ auf **Active Directory hinzufügen**.

2. Geben Sie im Dialogfeld „Mit Active Directory verbinden“ die Active Directory-Details ein und klicken Sie auf **Verbinden**.

   Sie können bei Bedarf mehrere IP-Adressen hinzufügen, indem Sie **IP hinzufügen** auswählen.



Die Datenklassifizierung wird in das Active Directory integriert und der Konfigurationsseite wird ein neuer Abschnitt hinzugefügt.



Verwalten Sie Ihre Active Directory-Integration

Wenn Sie Werte in Ihrer Active Directory-Integration ändern müssen, klicken Sie auf die Schaltfläche **Bearbeiten** und nehmen Sie die Änderungen vor.

Sie können die Integration auch löschen, indem Sie das Klicken Sie auf die Schaltfläche „Active Directory entfernen“ und dann auf „Active Directory entfernen“.

Datenklassifizierung verwenden

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

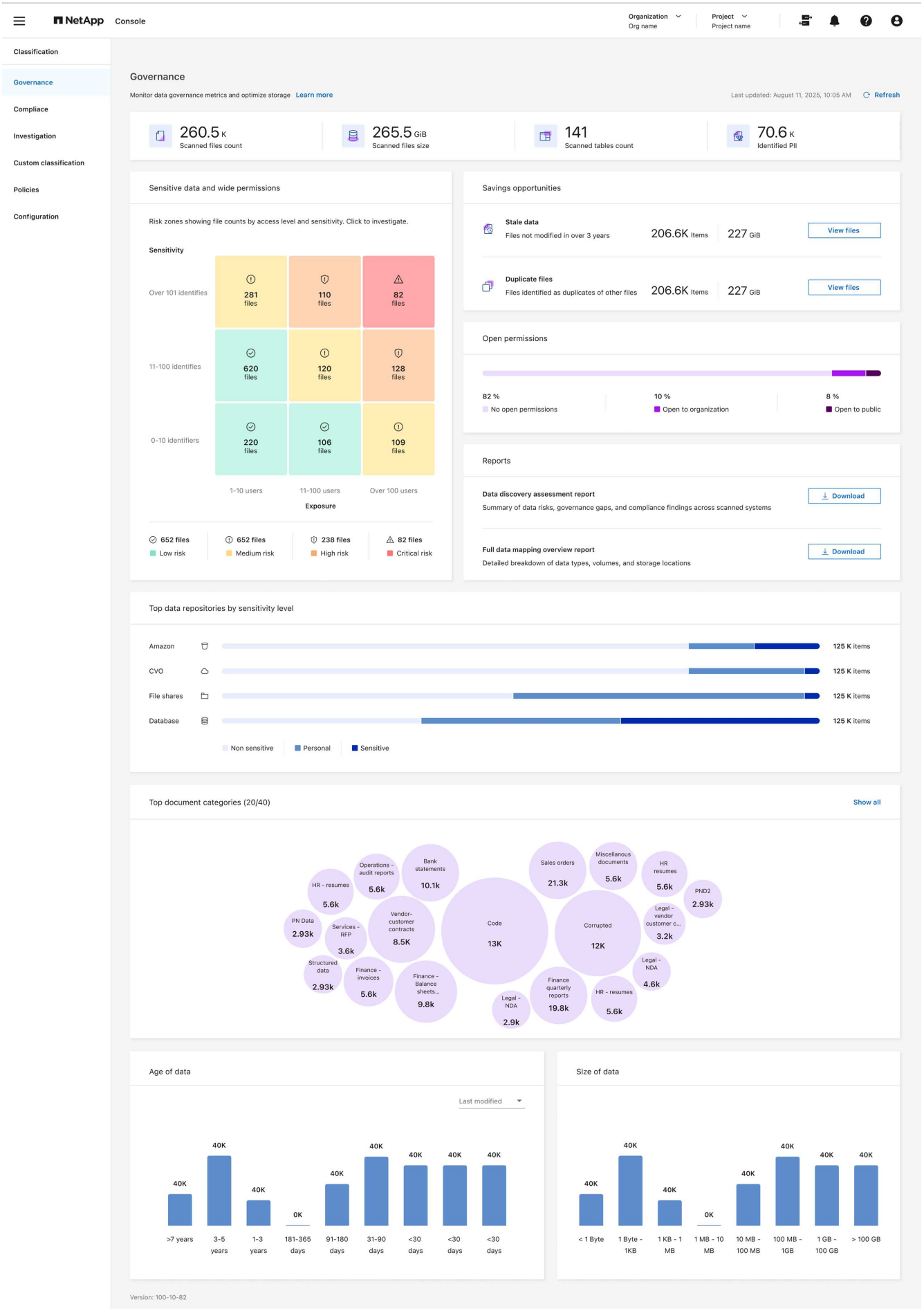
Behalten Sie die Kontrolle über die Kosten im Zusammenhang mit den Daten auf den Speicherressourcen Ihres Unternehmens. NetApp Data Classification ermittelt die Menge veralteter Daten, doppelter Dateien und sehr großer Dateien in Ihren Systemen, sodass Sie entscheiden können, ob Sie einige Dateien entfernen 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** – Daten, die zuletzt vor über 3 Jahren geändert wurden.
   - **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).

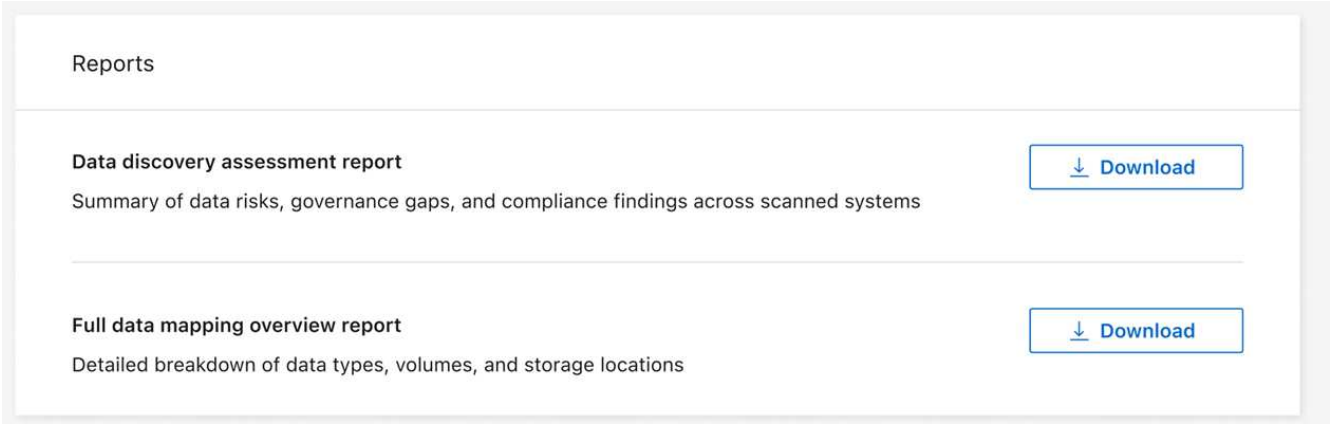
Mit dem Bericht können Sie folgende Aktionen ausführen:

- 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

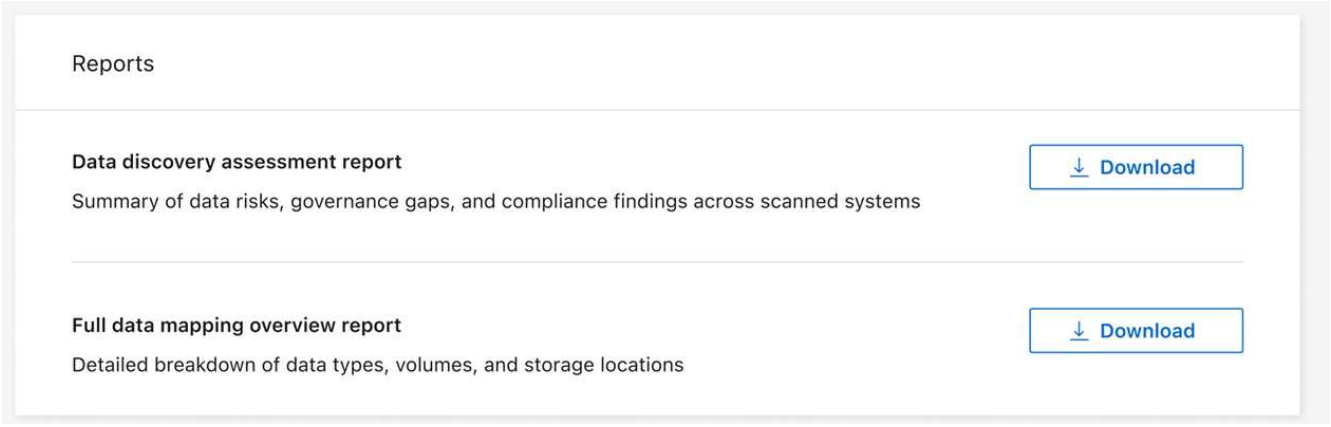
Der Übersichtsbericht zur Datenzuordnung bietet einen Überblick über die in Ihren Unternehmensdatenquellen gespeicherten Daten und unterstützt Sie bei Entscheidungen zu Migrations-, Sicherungs-, Sicherheits- und Compliance-Prozessen. Der Bericht fasst alle Systeme und Datenquellen zusammen. Es bietet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

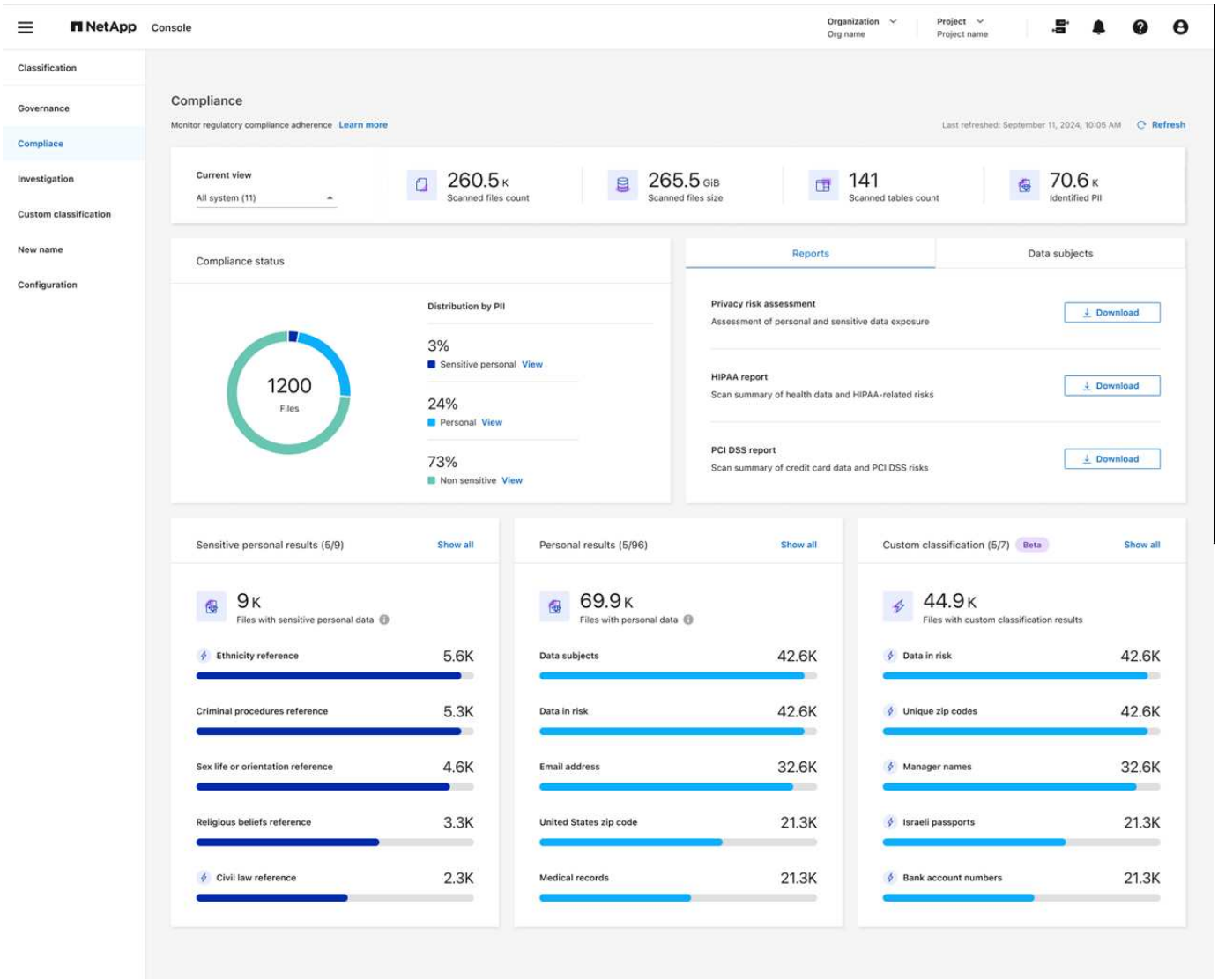
Mit NetApp Data Classification können Sie Compliance-Details zu den in Ihrem Unternehmen gespeicherten privaten Daten einsehen.

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.

Details zur Konformität 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. xref:./"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.

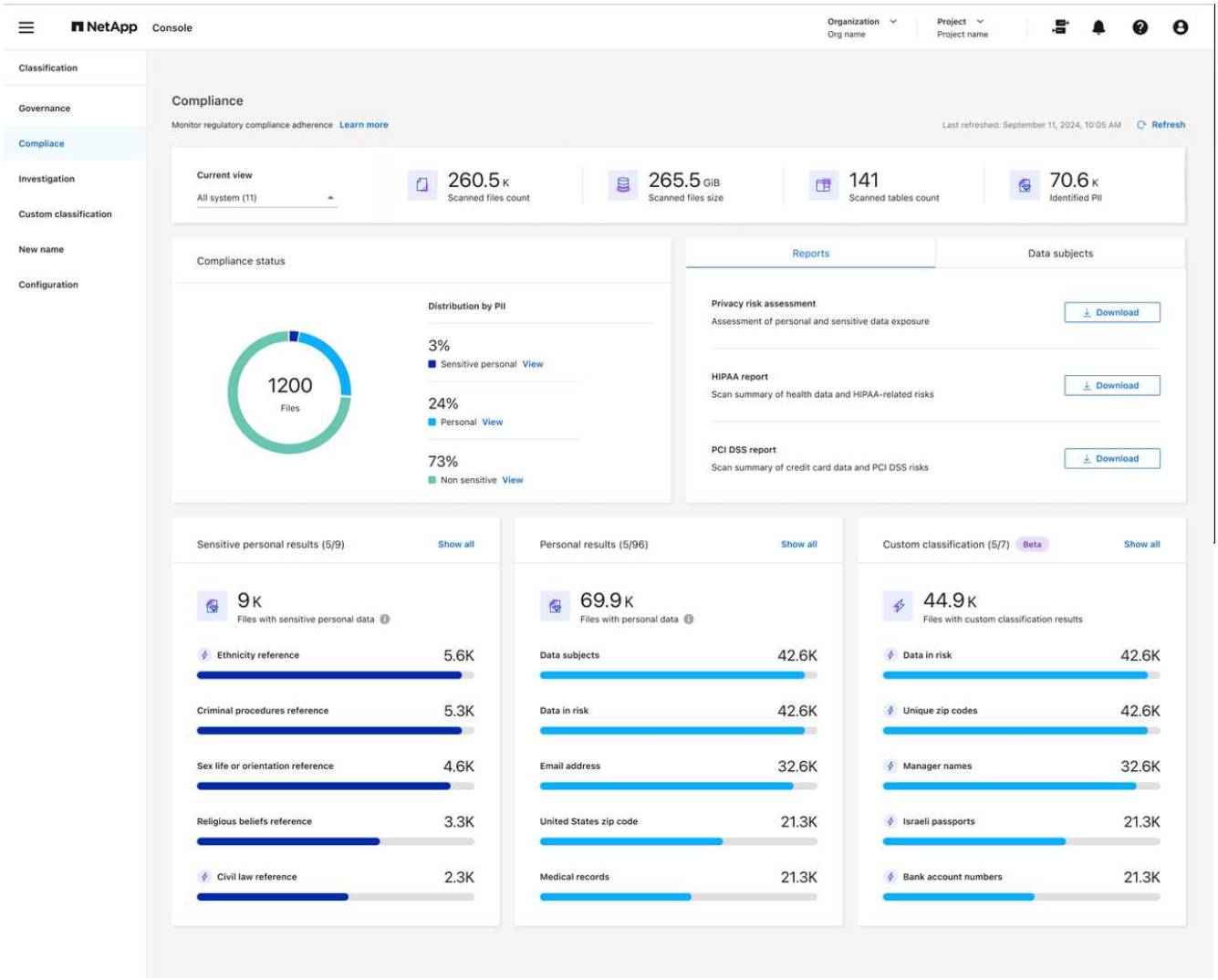
Sie können auch benutzerdefinierte Suchbegriffe erstellen, um personenbezogene Daten zu identifizieren, die

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

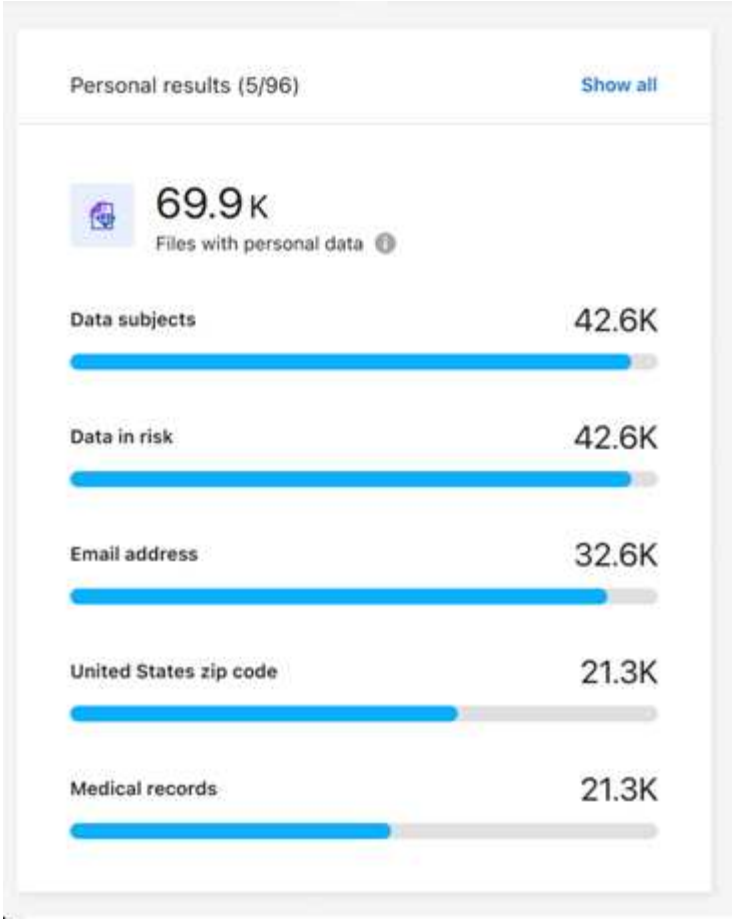
Für einige Arten personenbezogener Daten verwendet die Datenklassifizierung eine Näherungsvalidierung, um ihre Ergebnisse zu validieren. Die Validierung erfolgt durch die Suche nach einem oder mehreren vordefinierten Schlüsselwörtern in der Nähe der gefundenen personenbezogenen Daten. Beispielsweise 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.

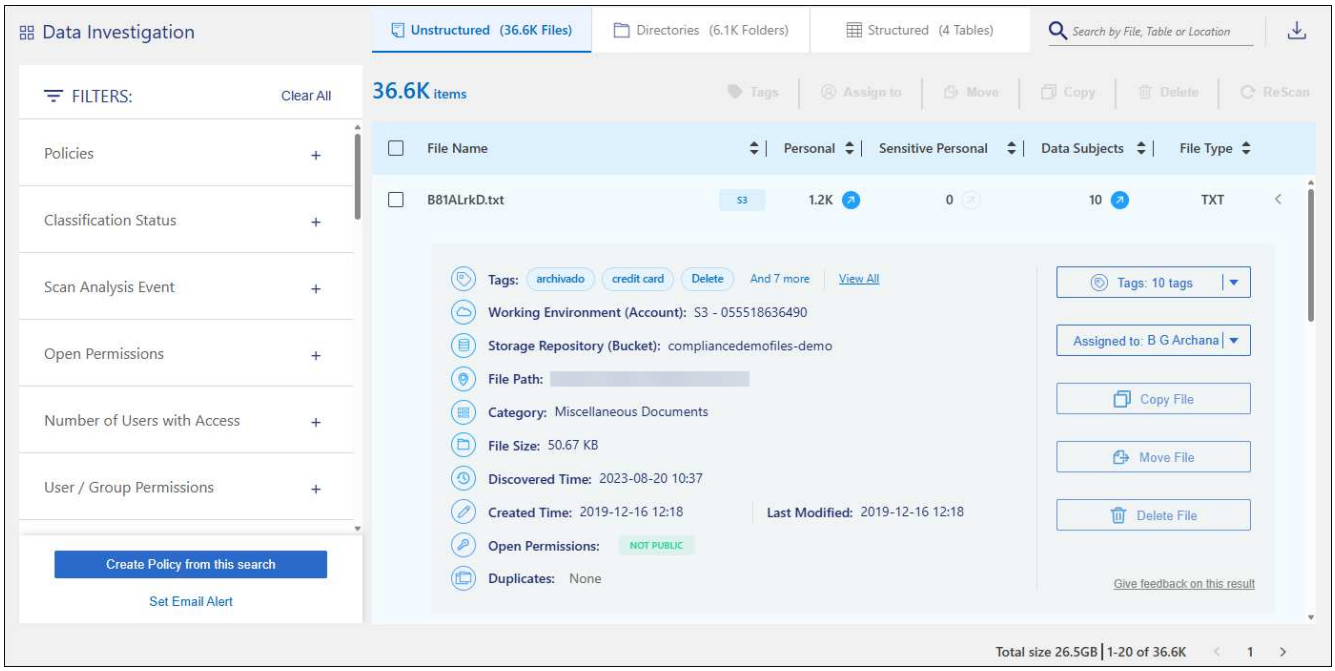


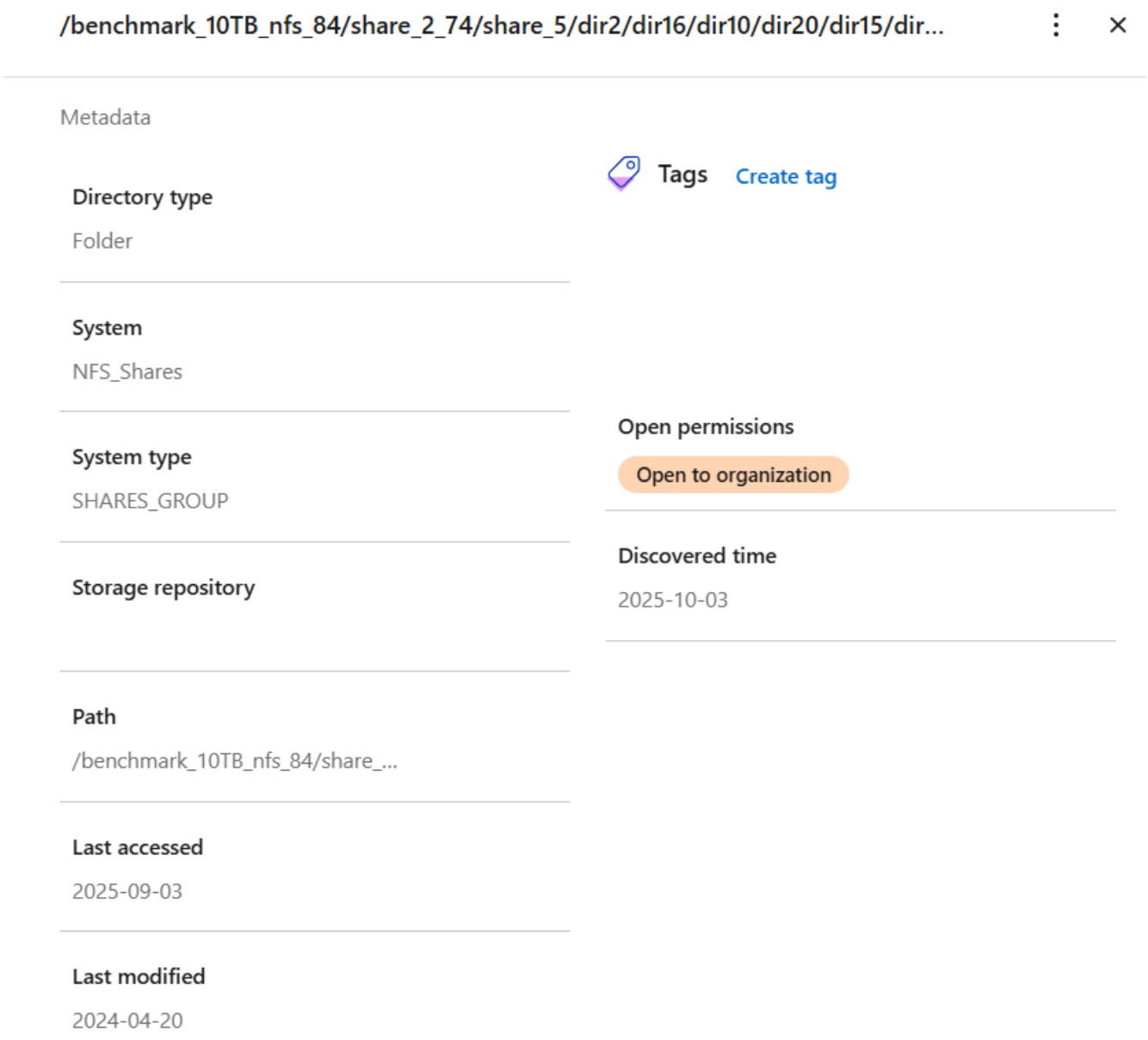
3. Um die Details für einen bestimmten Typ personenbezogener Daten zu untersuchen, wählen Sie **Alle anzeigen** und dann das Pfeilsymbol **Ergebnisse untersuchen** für einen bestimmten Typ personenbezogener Daten, beispielsweise E-Mail-Adressen.



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.

   Das folgende Bild zeigt 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.

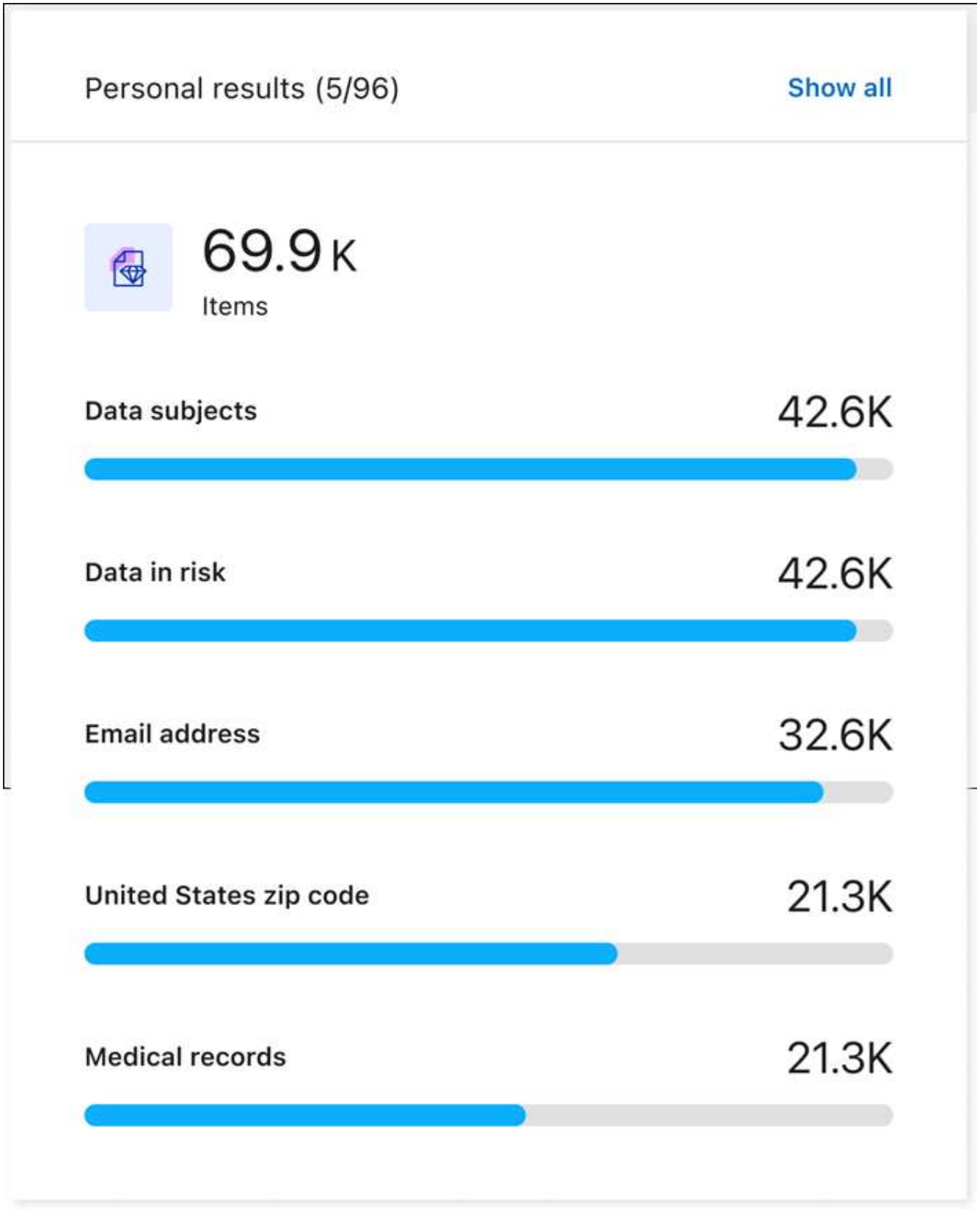
Eine sensible Datenkategorie der DSGVO ist beispielsweise die ethnische Herkunft. Aufgrund seiner NLP-Fähigkeiten kann die Datenklassifizierung den Unterschied zwischen einem Satz erkennen, der lautet: „George ist Mexikaner“ (was auf sensible Daten gemäß Artikel 9 der DSGVO hinweist) und „George isst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

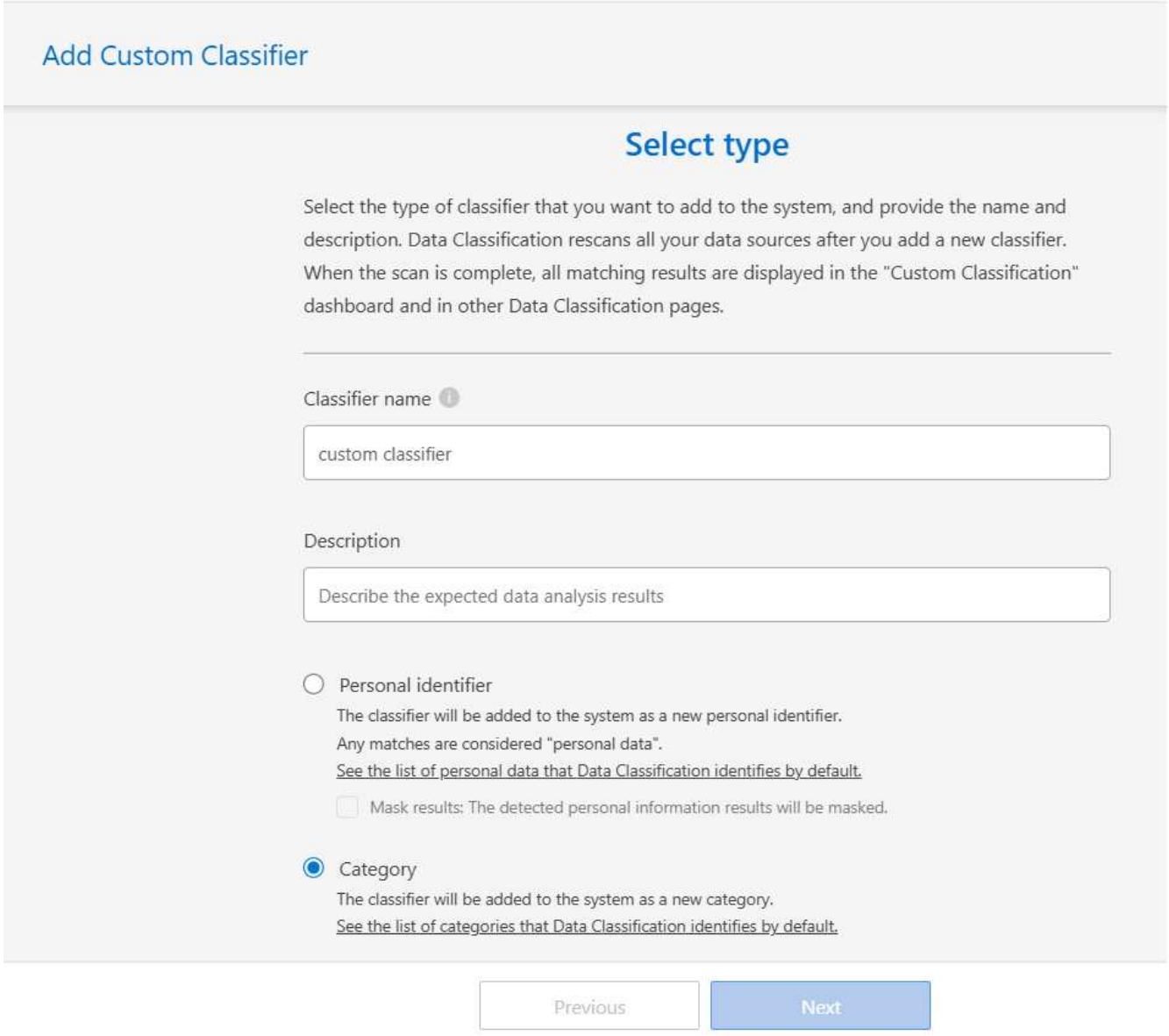
Mit NetApp Data Classification können Sie eine benutzerdefinierte Suche nach vertraulichen Informationen erstellen. Die Suche kann auf einen regulären Ausdruck (Regex) beschränkt werden.

Erstellen einer benutzerdefinierten Klassifizierung

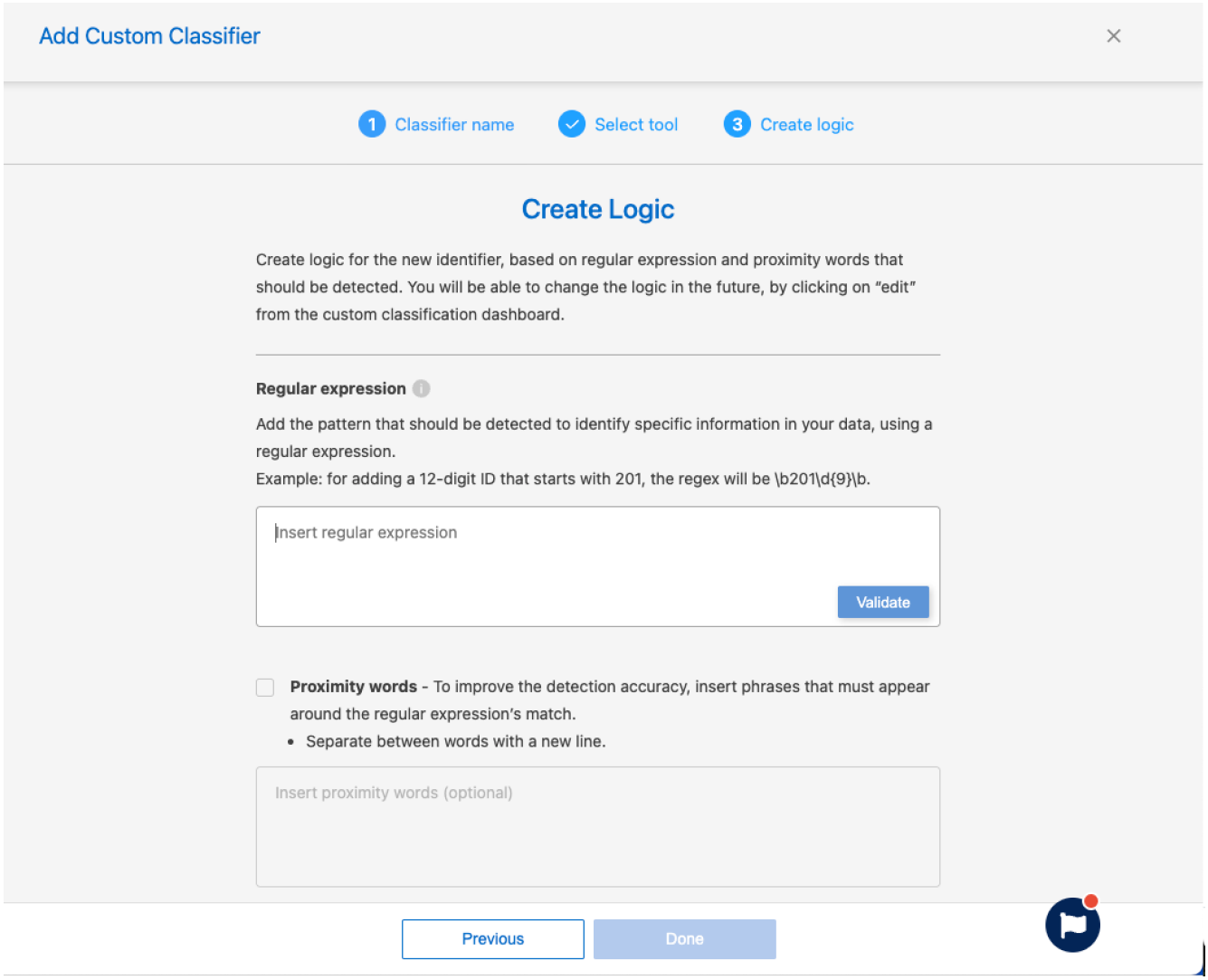
Die benutzerdefinierte Klassifizierung ist nur für Map- und Classify-Scans verfügbar, nicht für reine Mapping-Scans. Diese Funktion befindet sich derzeit in der Vorschau.

Schritte

1. Wählen Sie die Registerkarte **Benutzerdefinierte Klassifizierung**.
2. Wählen Sie die Schaltfläche **Neuen Klassifikator hinzufügen**.
3. Fügen Sie einen Klassifikatornamen und eine Beschreibung für den neuen Klassifikator hinzu.
4. Wählen Sie, ob Sie den Klassifikator als **Persönliche Kennung** oder **Kategorie** hinzufügen möchten.



5. Wählen Sie **Weiter**.
6. Um die Anpassung als regulären Ausdruck hinzuzufügen, wählen Sie **Benutzerdefinierter regulärer Ausdruck** und dann **Weiter**.
7. Fügen Sie ein Muster hinzu, um die spezifischen Informationen Ihrer Daten zu erkennen. Wählen Sie **Validieren**, um die Syntax Ihrer Eingabe zu bestätigen.



8. Wählen Sie **Fertig**, um die benutzerdefinierte Klassifizierung zu erstellen.

Die neue Anpassung wird beim nächsten geplanten Scan erfasst. Um die Ergebnisse anzuzeigen, sieheErstellen 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

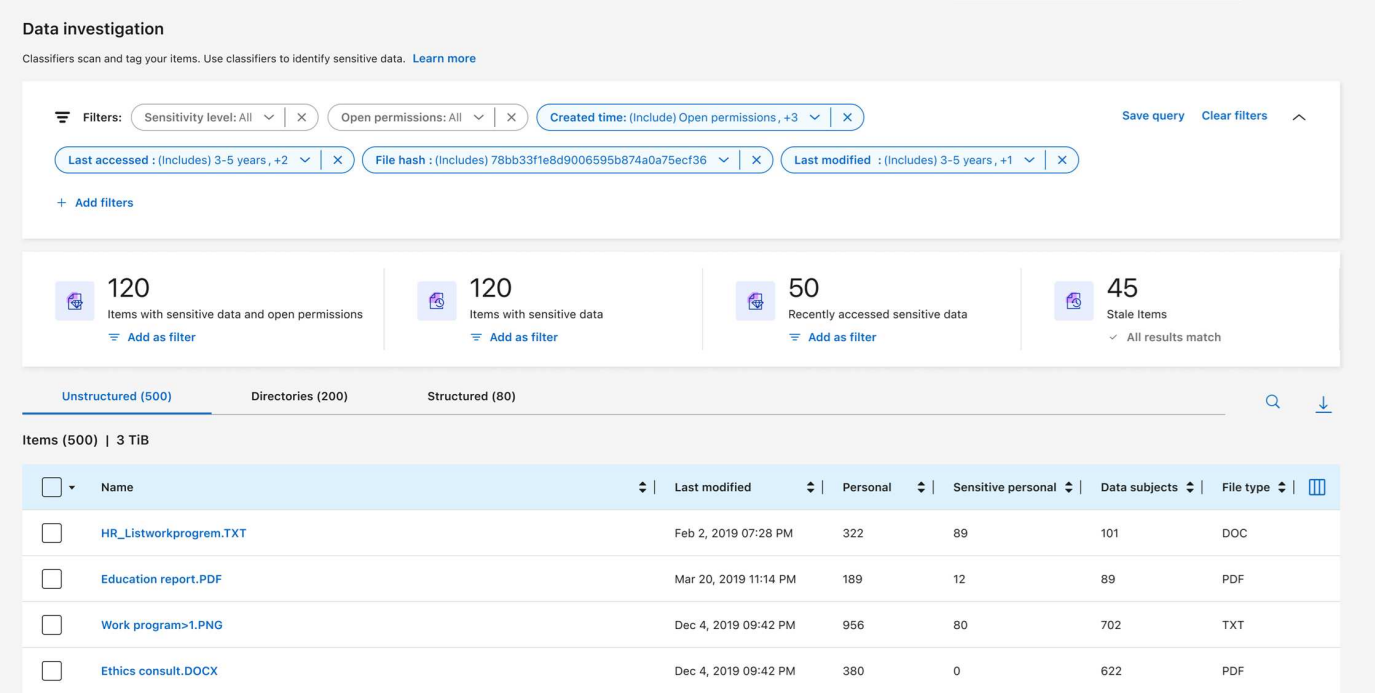
Auf der Seite „Datenuntersuchung“ werden die Daten in drei Registerkarten sortiert:

- **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.

Filter	Details
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.

Filter	Details
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.
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.

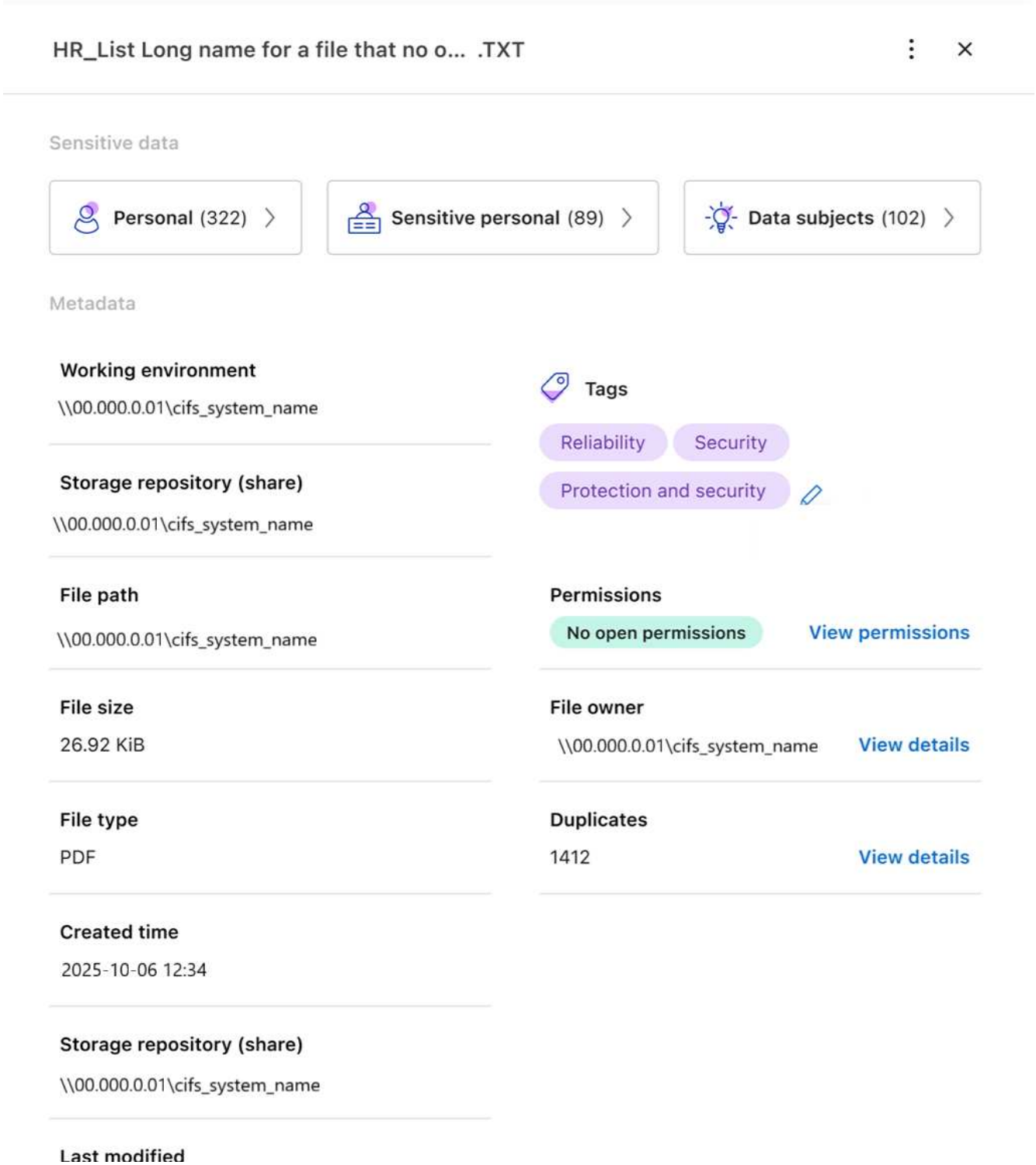
Dateimetadaten anzeigen

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.

Alle Ihre Dateien (Datenbanken ausgenommen), die 1 MB oder größer sind oder persönliche oder vertrauliche persönliche Informationen enthalten, werden auf Duplikate verglichen.

Bei der Datenklassifizierung wird Hashing-Technologie verwendet, um doppelte Dateien zu ermitteln. Wenn eine Datei denselben Hashcode wie eine andere Datei hat, können Sie 100 % sicher sein, dass es sich bei den Dateien um exakte Duplikate handelt – auch 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:

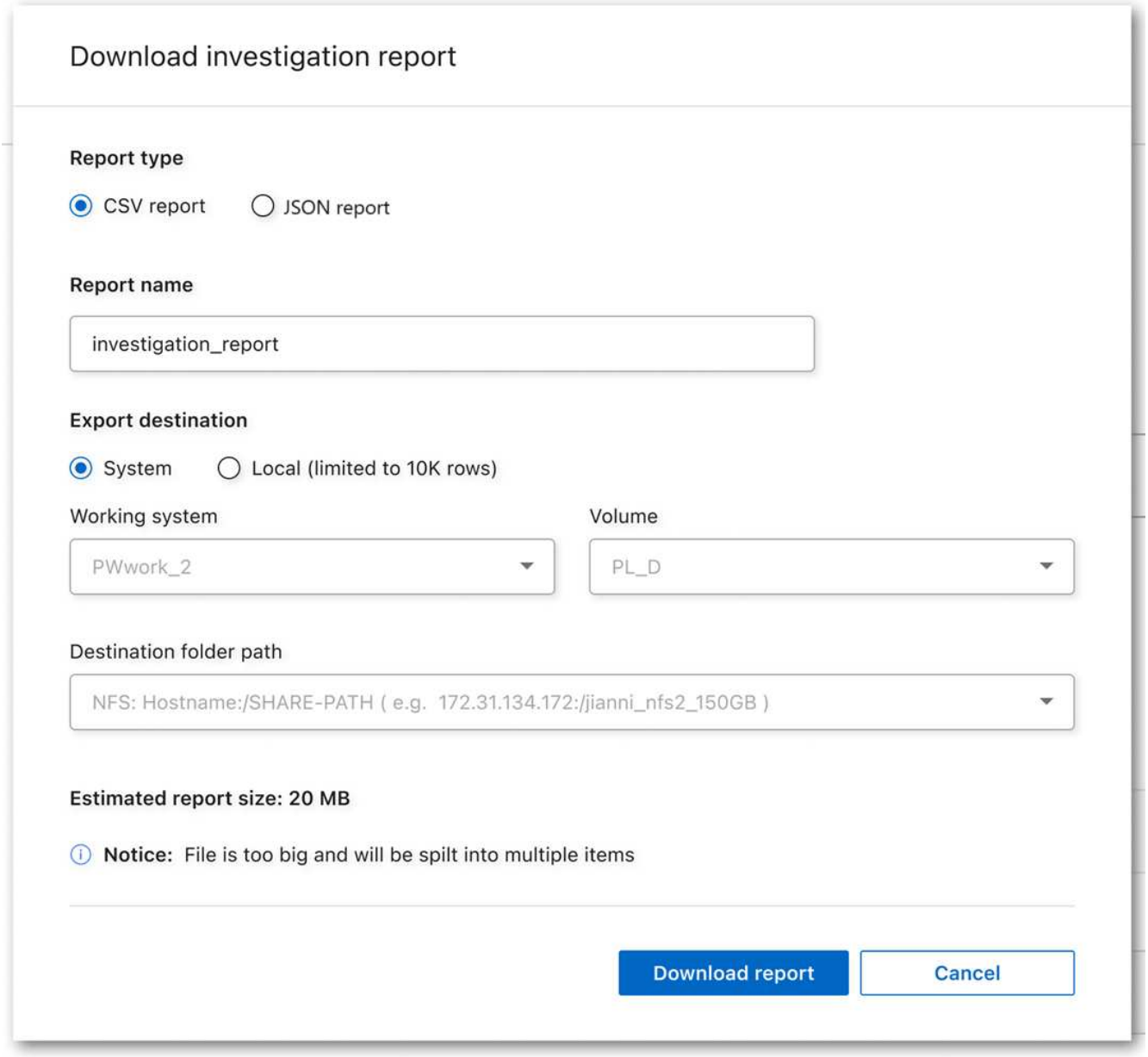
- DB-Tabellenname
- Standorttyp
- Systemname
- Speicherrepository (z. B. ein Schema)
- Spaltenanzahl
- Zeilenanzahl
- Persönliche Informationen
- Sensible persönliche Informationen

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**.



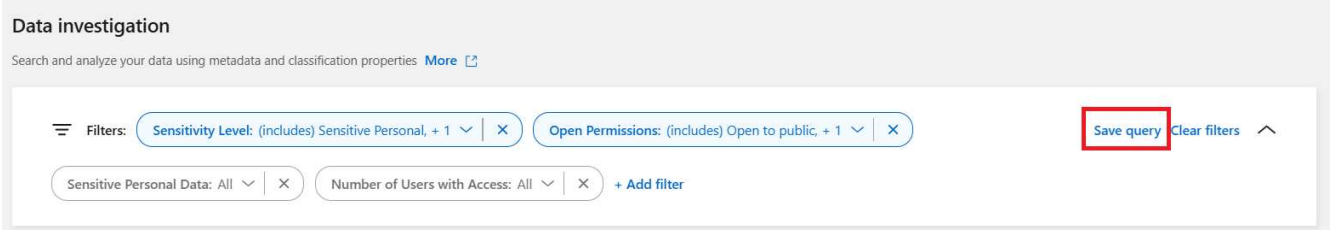
Ergebnis

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

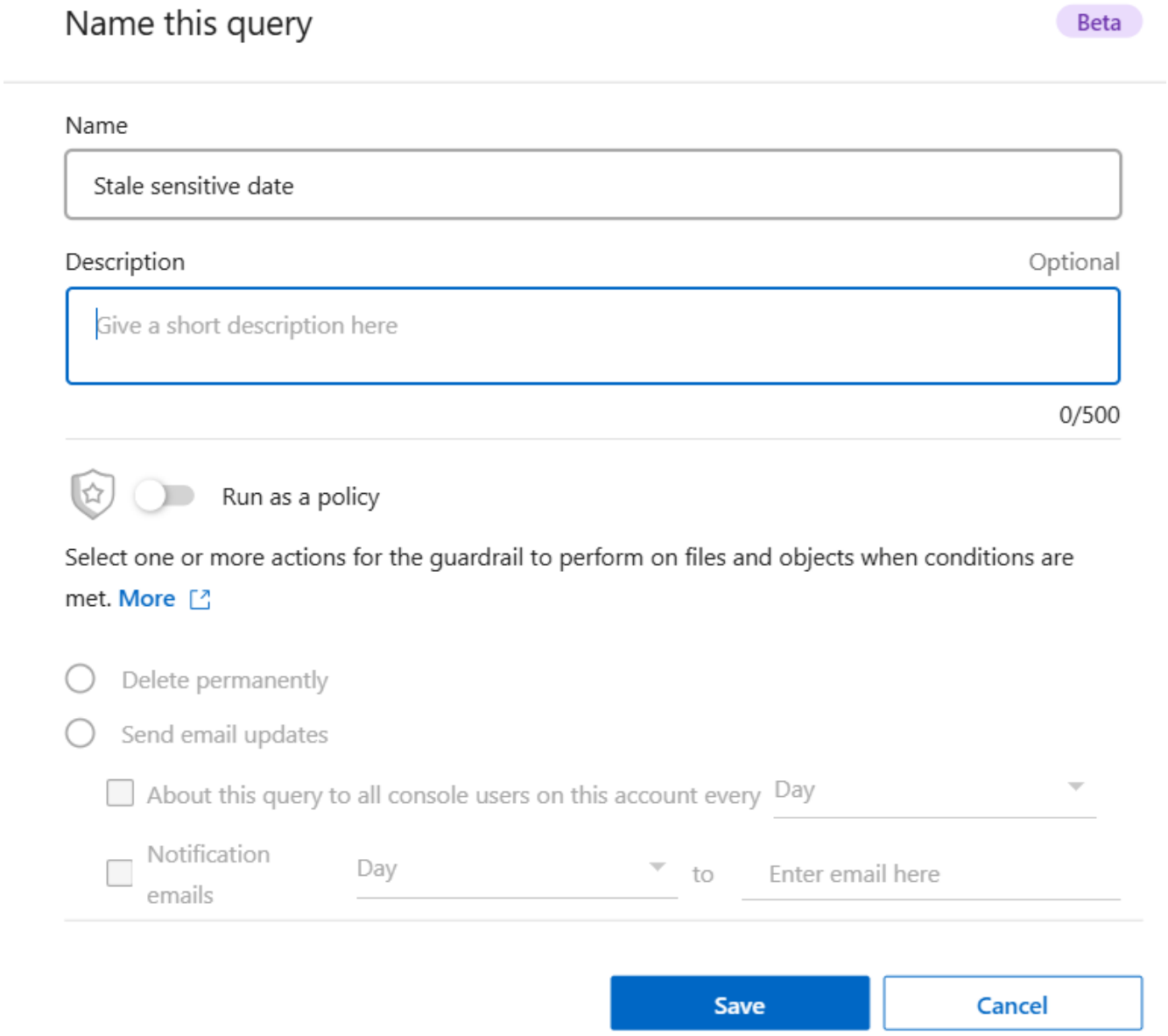
Erstellen Sie eine gespeicherte Abfrage basierend auf ausgewählten Filtern

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.

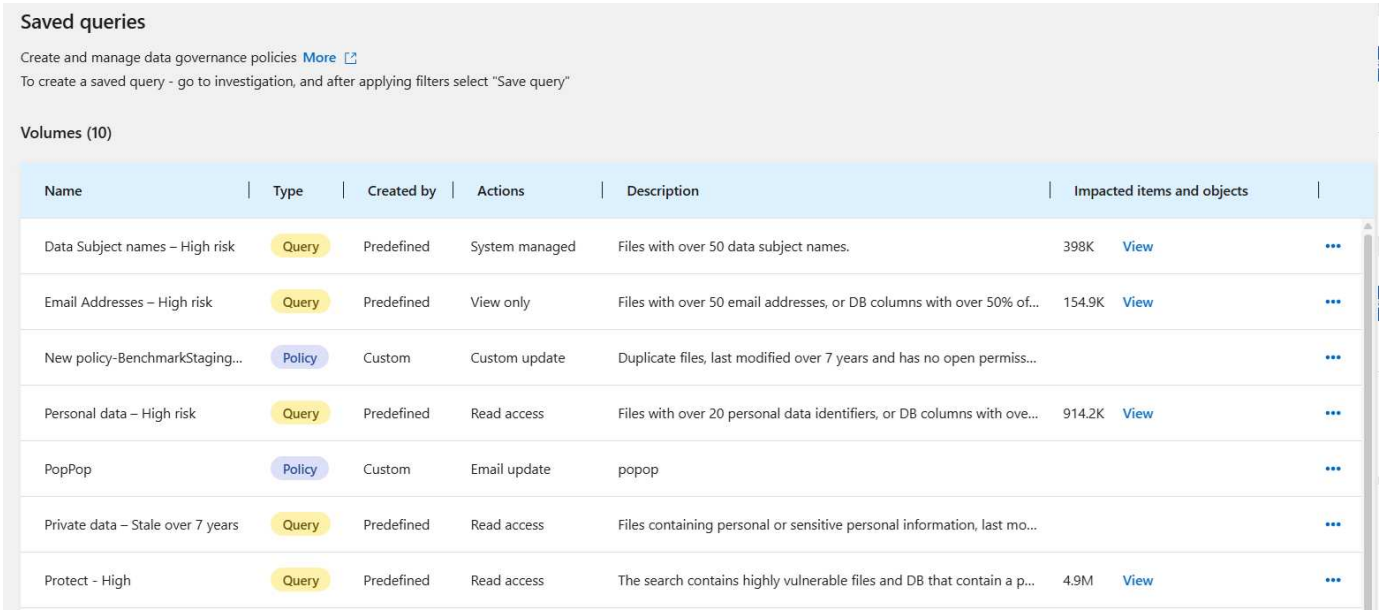
Verwalten gespeicherter Abfragen mit NetApp Data Classification

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“

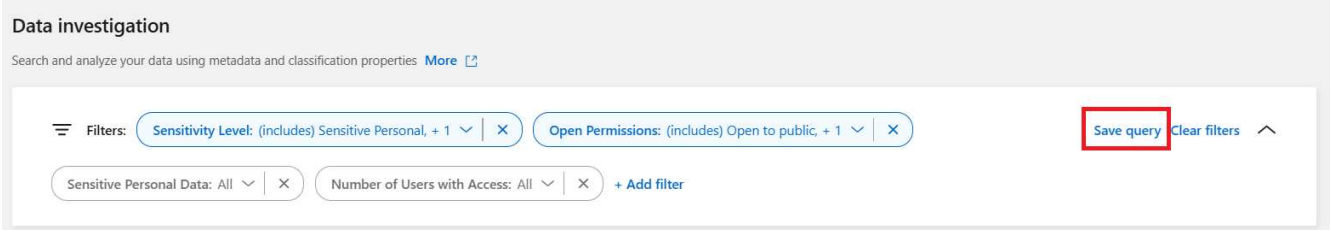
Um die Ergebnisse einer gespeicherten Abfrage auf der Seite „Untersuchung“ anzuzeigen, wählen Sie das Klicken Sie auf die Schaltfläche für eine bestimmte Suche und wählen Sie dann **Ergebnisse untersuchen** aus.

Erstellen gespeicherter Abfragen und Richtlinien

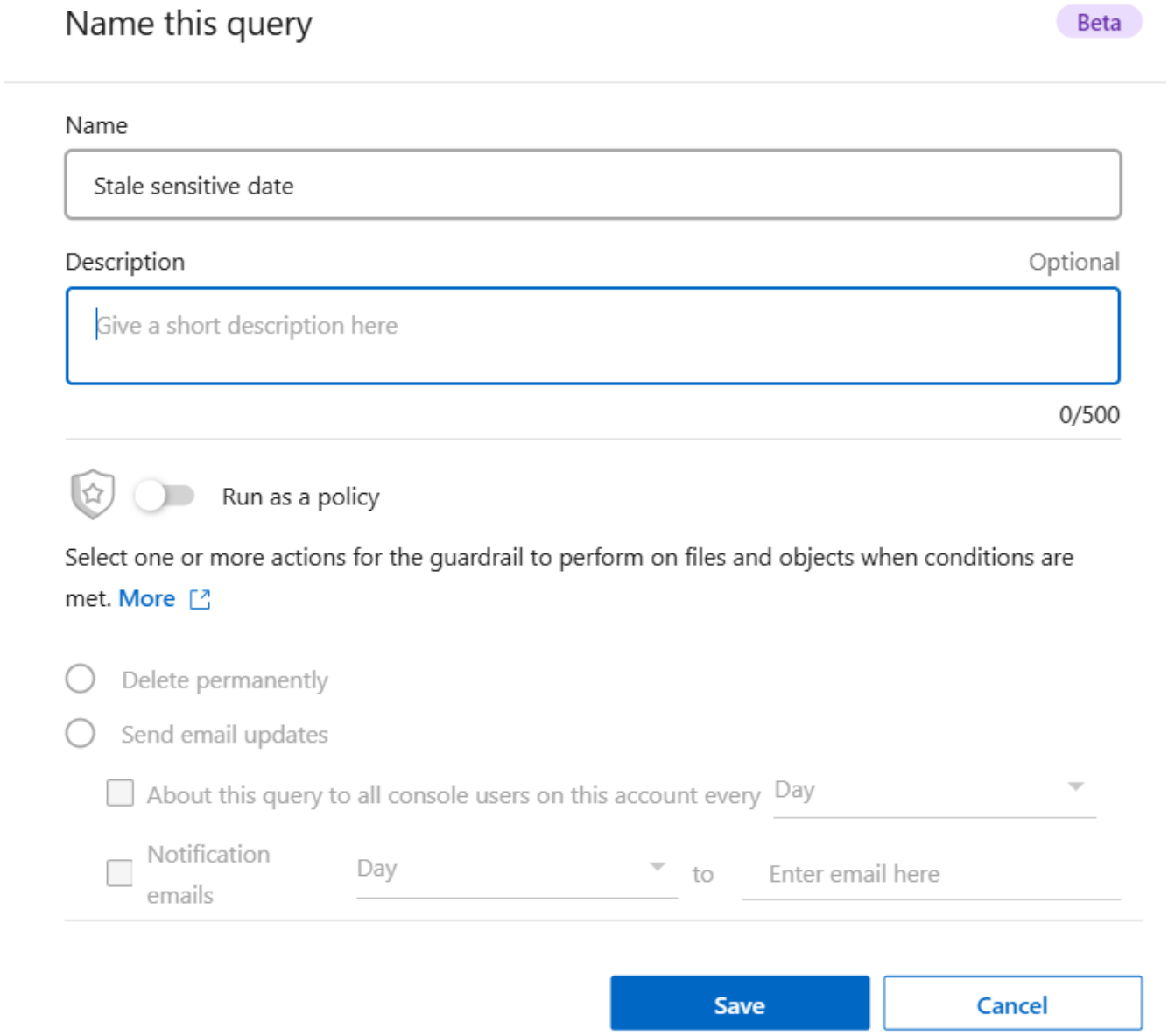
Sie können Ihre eigenen benutzerdefinierten gespeicherten Abfragen erstellen, die Ergebnisse für Abfragen liefern, die für Ihre Organisation spezifisch sind. Es werden Ergebnisse für alle Dateien und Verzeichnisse (Freigaben und Ordner) zurückgegeben, die den Suchkriterien entsprechen.

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.

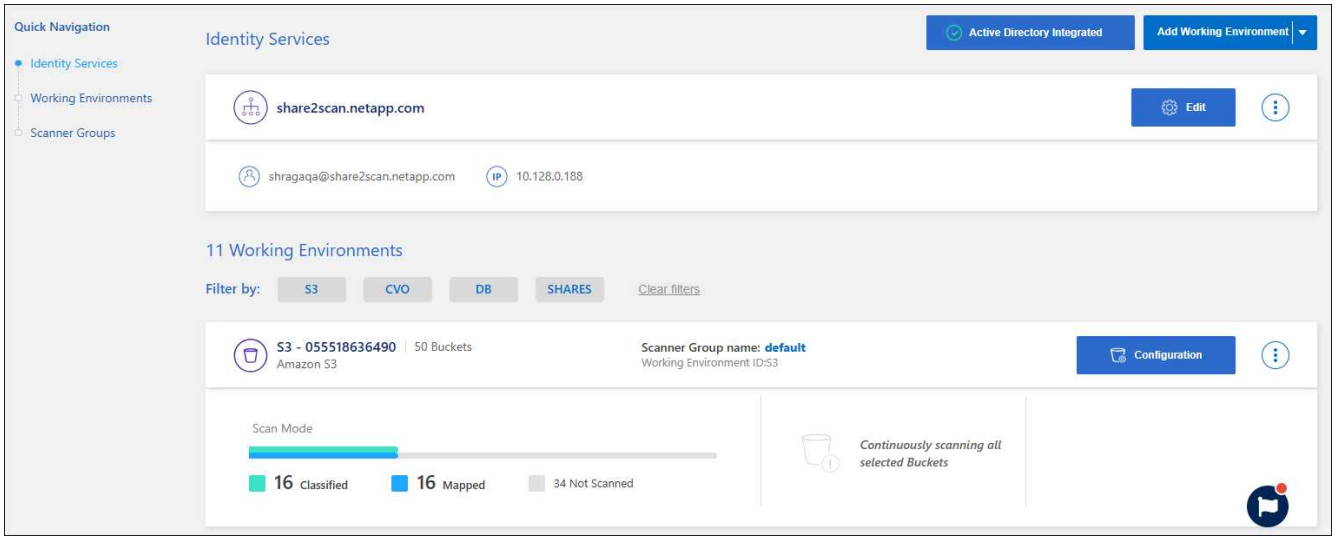
Sie können den Scan-Status jeder Arbeitsumgebung auf der Konfigurationsseite anzeigen:

- **Initialisierung** (hellblauer Punkt): Die Karten- oder Klassifizierungskonfiguration wird aktiviert. Dies wird einige Sekunden lang angezeigt, bevor der Status „Ausstehende Warteschlange“ beginnt.
- **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 die Option „Pause“ ausgewählt, um den Scanvorgang anzuhalten. Während die Volumenänderungen nicht im System angezeigt werden, werden die gescannten Erkenntnisse weiterhin angezeigt.

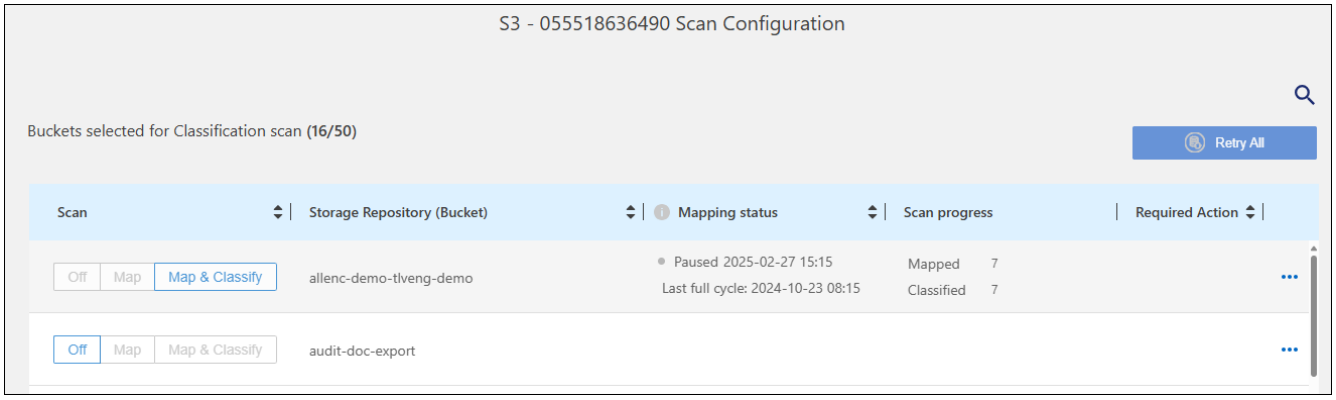
- **Fehler** (roter Punkt): Der Scan kann nicht abgeschlossen werden, da Probleme aufgetreten sind. Wenn Sie eine Aktion abschließen müssen, wird der Fehler im Tooltip unter der Spalte „Erforderliche Aktion“ angezeigt. Andernfalls zeigt das System den Status „Fehler“ an und versucht, die Wiederherstellung 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 den Cursor über das Diagramm in der Spalte „Mapping-Status“, um die Anzahl der Dateien anzuzeigen, die in jedem Repository (in diesem Beispiel Bucket) noch zugeordnet oder klassifiziert werden müssen.

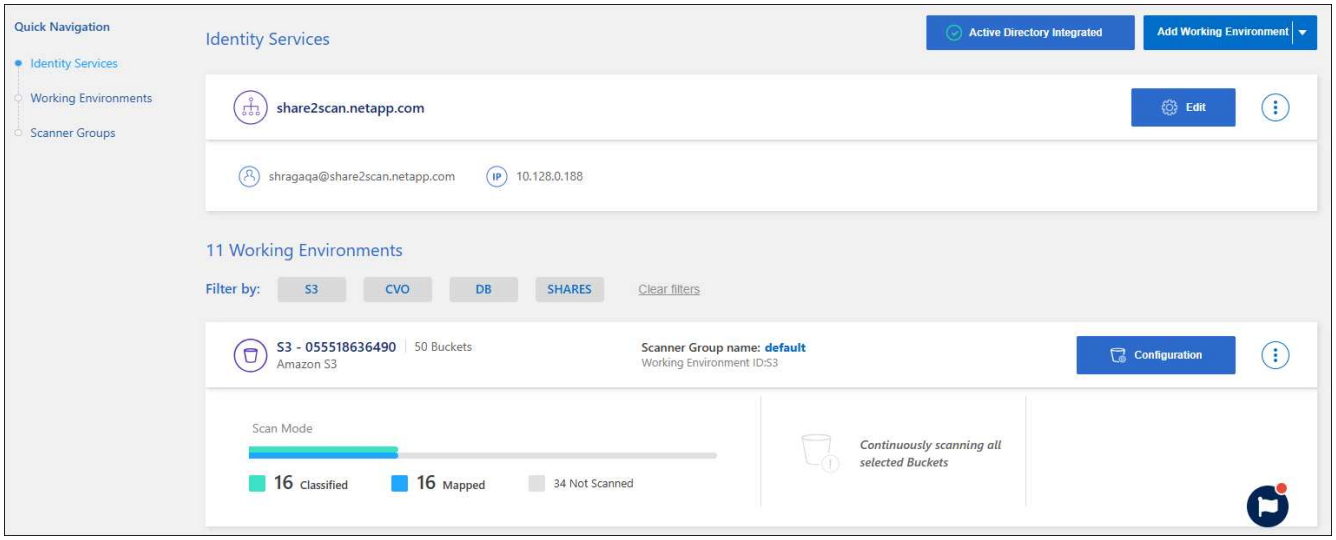
Ändern des Scan-Typs für ein Repository

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.

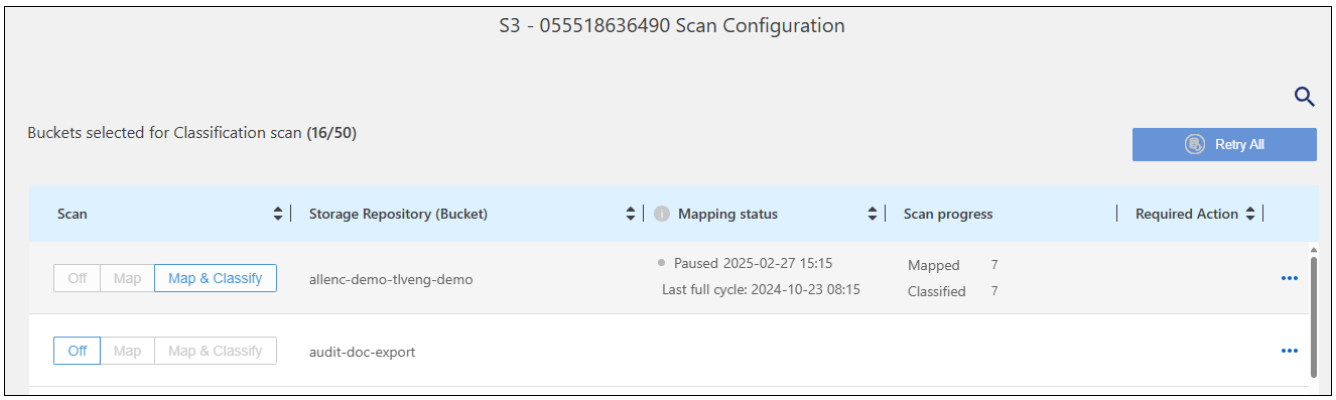
Datenbanken können nicht auf reine Mapping-Scans eingestellt werden. Das Scannen der Datenbank kann aktiviert oder deaktiviert werden, wobei „A“ dem Zuordnen und Klassifizieren entspricht.

Schritte

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

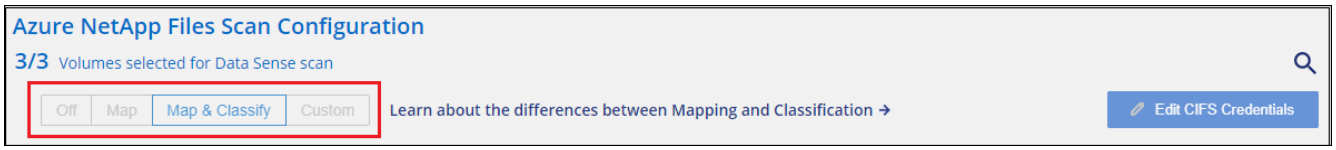


3. Ändern Sie auf der Seite „Scan-Konfiguration“ beliebige Repositories (in diesem Beispiel Buckets), um **Map**- oder **Map & Classify**-Scans durchzuführen.



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

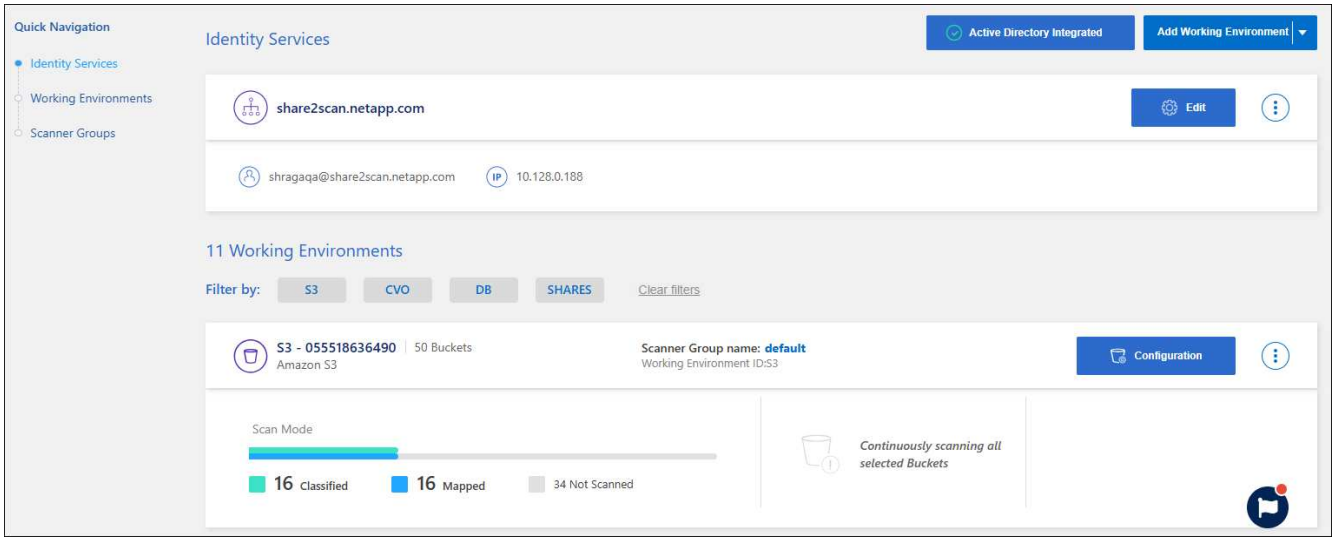
1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie die Ressourcen aus, die Sie priorisieren möchten.
3. Von den Aktionen … Wählen Sie als Option **Scan priorisieren**.

Scannen nach einem Repository beenden

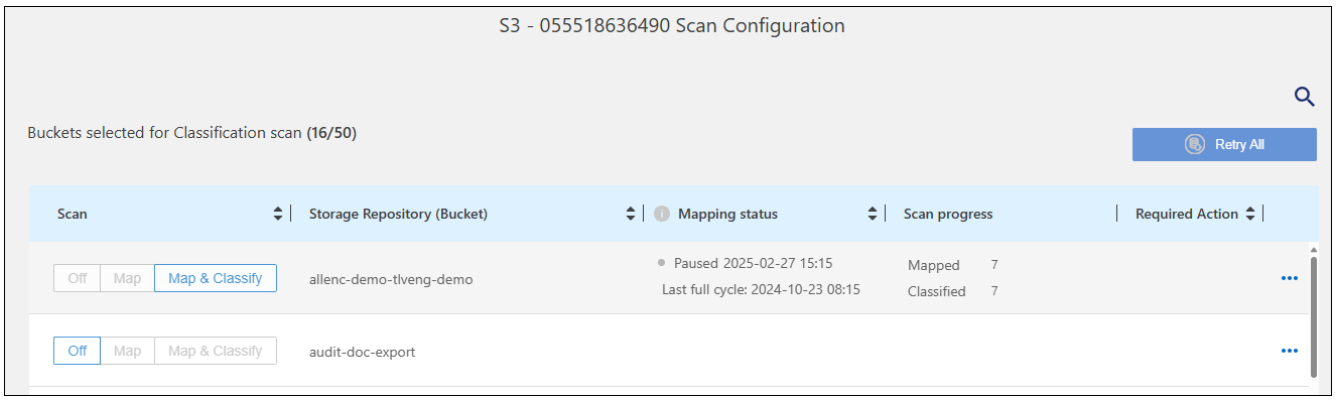
Sie können das Scannen eines Repositorys (z. B. eines Volumes) beenden, wenn Sie es nicht mehr auf Konformität überwachen müssen. Dies erreichen Sie, indem Sie das Scannen „ausschalten“. Wenn das Scannen deaktiviert wird, werden alle Indizes und Informationen zu diesem Datenträger aus dem System entfernt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



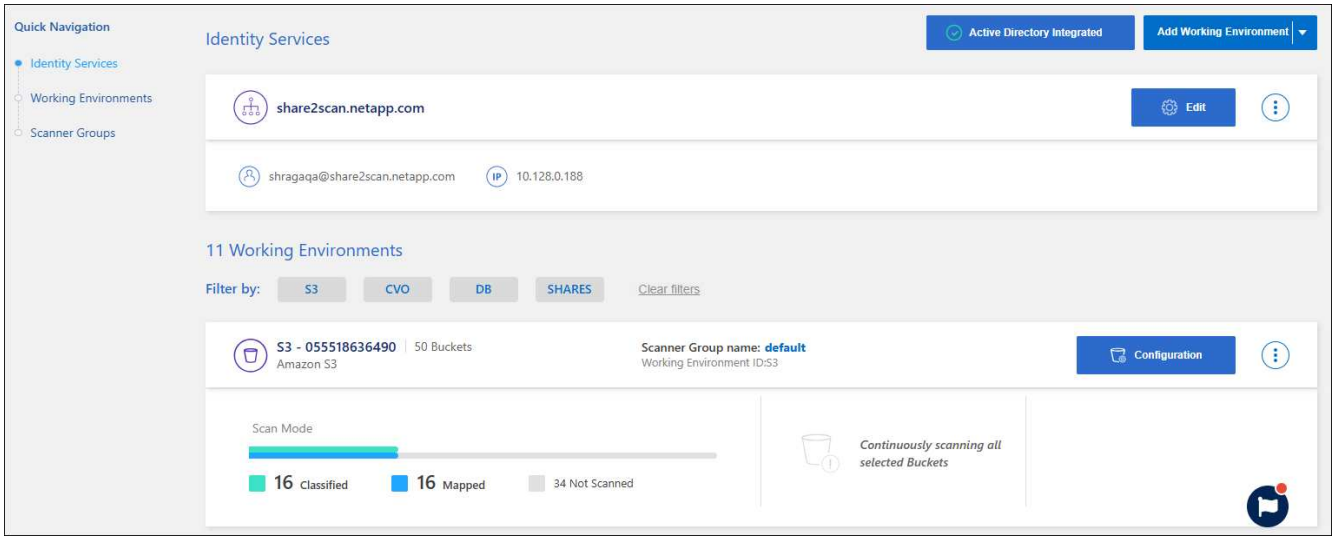
Scannen nach einem Repository anhalten und fortsetzen

Sie können das Scannen eines Repositorys „anhalten“, wenn Sie das Scannen bestimmter Inhalte vorübergehend beenden möchten. Das Anhalten des Scans bedeutet, dass Data Classification keine zukünftigen Scans nach Änderungen oder Ergänzungen am Repository durchführt, aber alle aktuellen Ergebnisse weiterhin im System angezeigt werden. Durch das Anhalten des Scanvorgangs werden die Kosten für die gescannten Daten nicht aufgehoben, da die Daten weiterhin 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.
- **Datenzuordnungsbericht**: Bietet Informationen zur Größe und Anzahl der Dateien in Ihren Systemen. Hierzu zählen Nutzungskapazität, Alter der Daten, Datengröße und Dateitypen.
- **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.
- **HIPAA-Bericht**: Hilft Ihnen, die Verteilung von Gesundheitsinformationen in Ihren Dateien zu identifizieren.
- **PCI DSS-Bericht**: Hilft Ihnen, die Verteilung von Kreditkarteninformationen in Ihren Dateien zu identifizieren.
- **Bericht zur Bewertung des Datenschutzrisikos**: Bietet Einblicke in den Datenschutz Ihrer Daten und eine Bewertung des Datenschutzrisikos.
- **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.

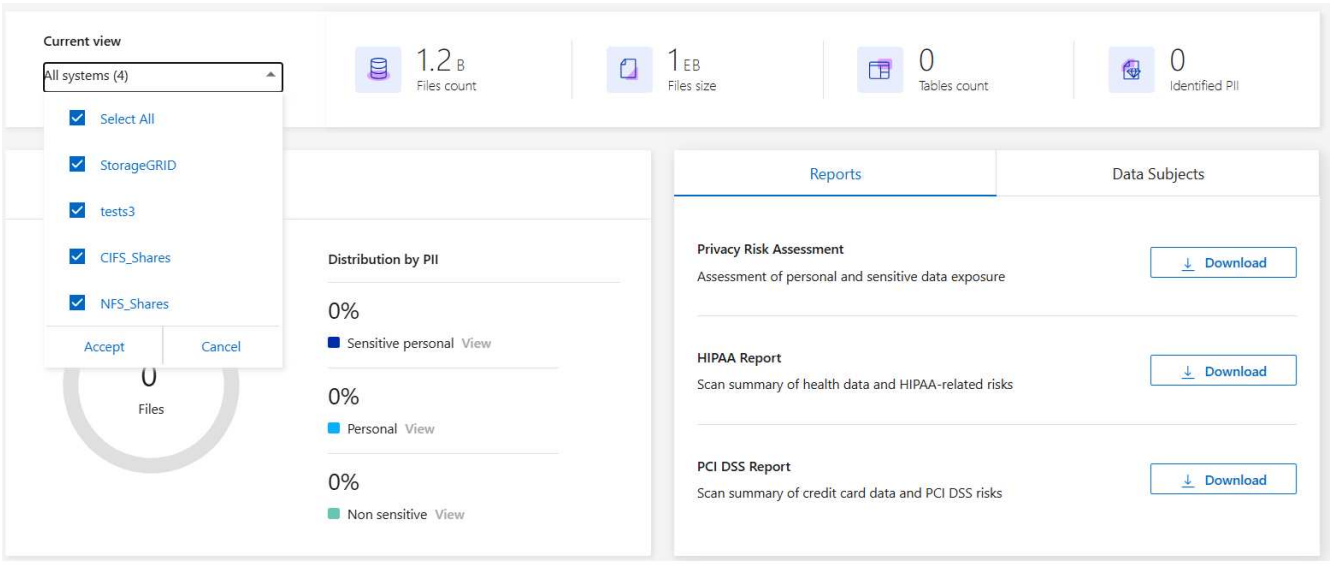
Wählen Sie die Systeme für Berichte aus

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

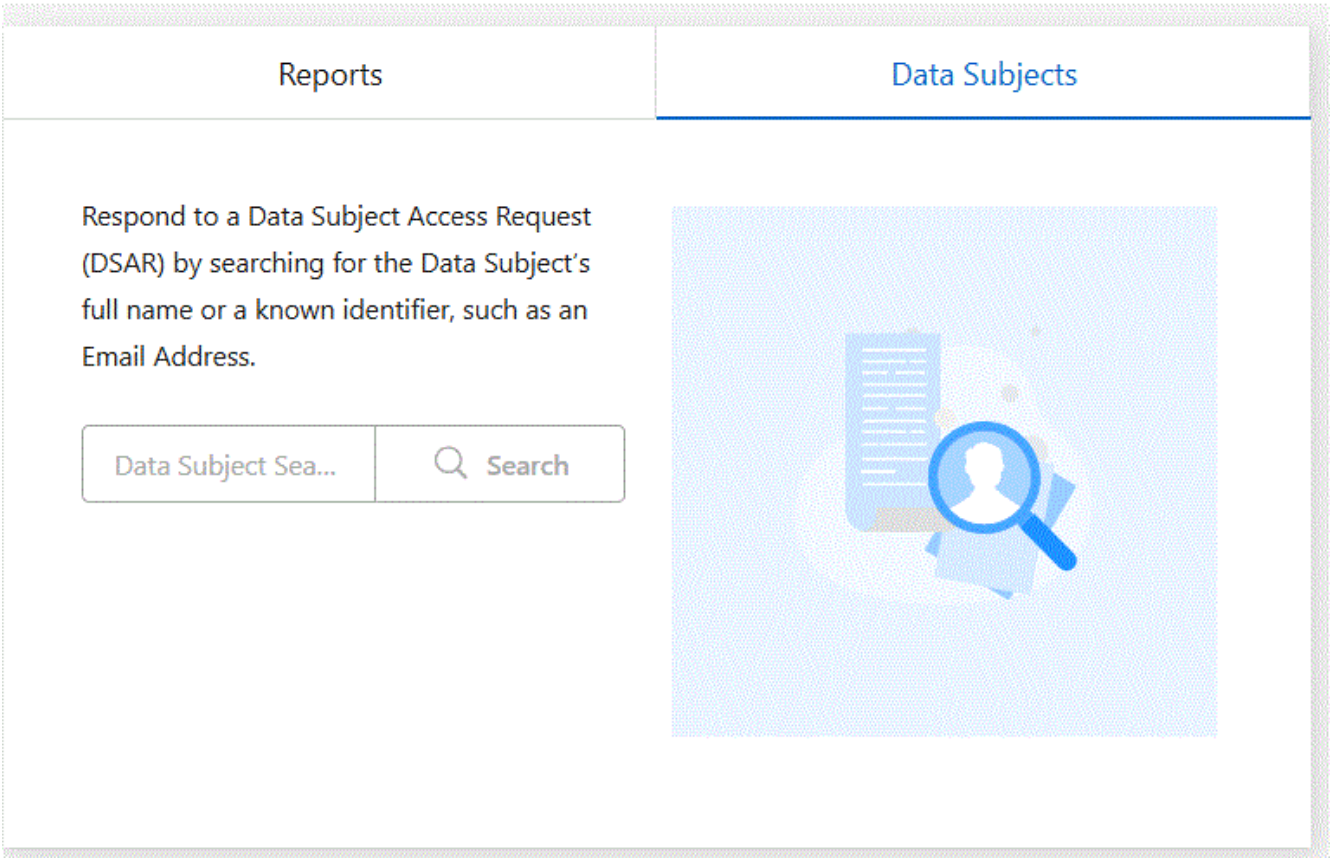
Suchen Sie nach dem vollständigen Namen oder einer bekannten Kennung der betroffenen Person und laden Sie dann einen Dateilistenbericht oder DSAR-Bericht herunter. Sie können suchen nach"alle Arten persönlicher Informationen" .

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. Wählen Sie auf der Compliance-Seite **Datensubjekte** aus.
3. Suchen Sie nach dem vollständigen Namen oder einer bekannten Kennung der betroffenen Person.

   Hier ist ein Beispiel, das eine Suche nach dem Namen *john doe* zeigt:



4. Wählen Sie eine der verfügbaren Optionen:
   - **DSAR-Bericht herunterladen**: Eine formelle Antwort auf die Zugriffsanfrage, die Sie an die betroffene Person senden können. Dieser Bericht enthält automatisch generierte Informationen auf Grundlage der von Data Classification zur betroffenen Person ermittelten Daten und dient als Vorlage. Sie sollten das Formular ausfüllen und intern prüfen, bevor Sie es an die betroffene Person senden.
   - **Ergebnisse untersuchen**: Eine Seite, auf der Sie die Daten untersuchen können, indem Sie nach einer bestimmten Datei suchen, sie sortieren, Details erweitern und die Dateiliste herunterladen.

     Bei mehr als 10.000 Ergebnissen werden nur die ersten 10.000 in der Dateiliste angezeigt.

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:

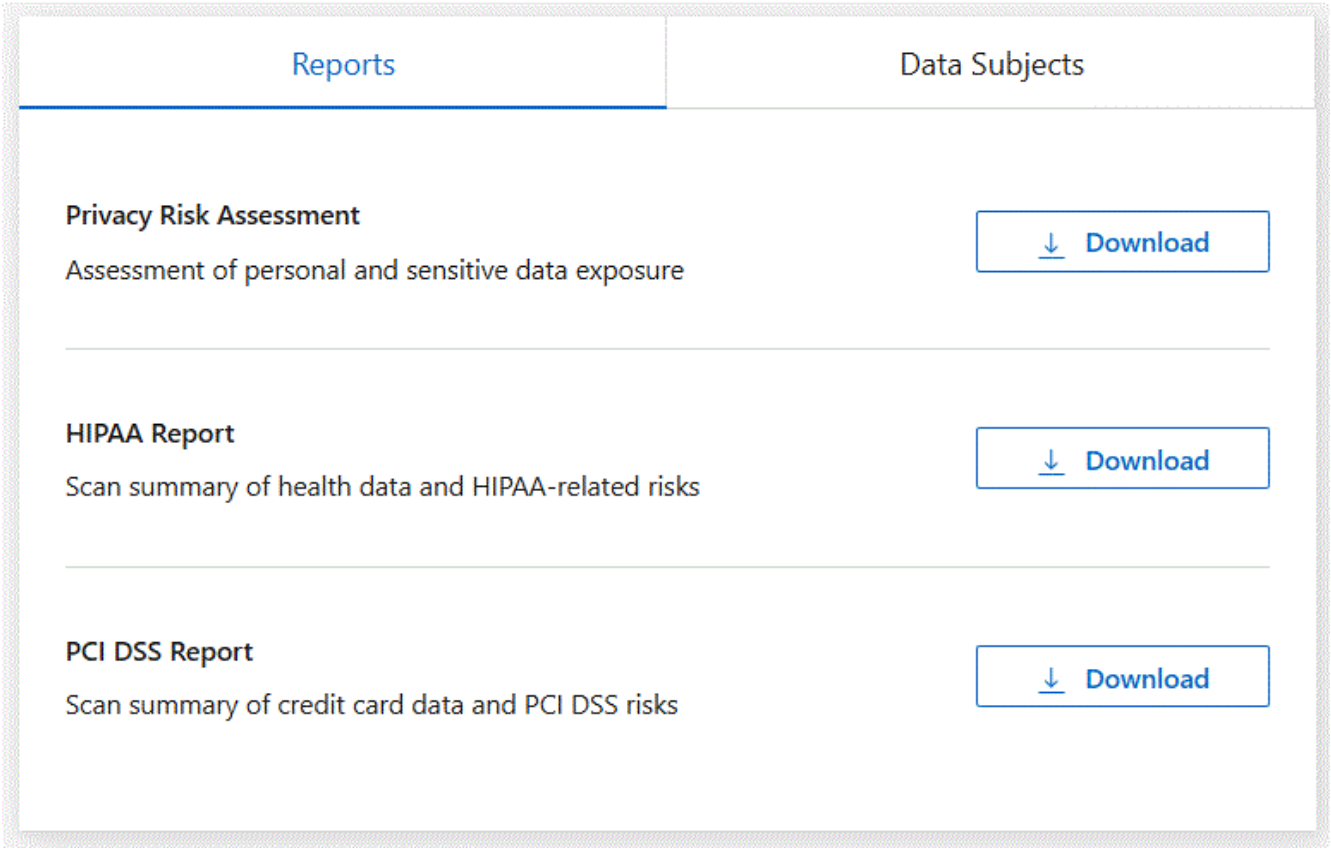
- Übersicht: In wie vielen Dateien sind Gesundheitsinformationen enthalten und in welchen Systemen.
- Verschlüsselung: Der Prozentsatz der Dateien mit Gesundheitsinformationen, die sich auf verschlüsselten oder unverschlüsselten Systemen befinden. Diese Informationen gelten speziell für Cloud Volumes 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, den Sie überprüfen und bei Bedarf an andere Gruppen senden können.

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:

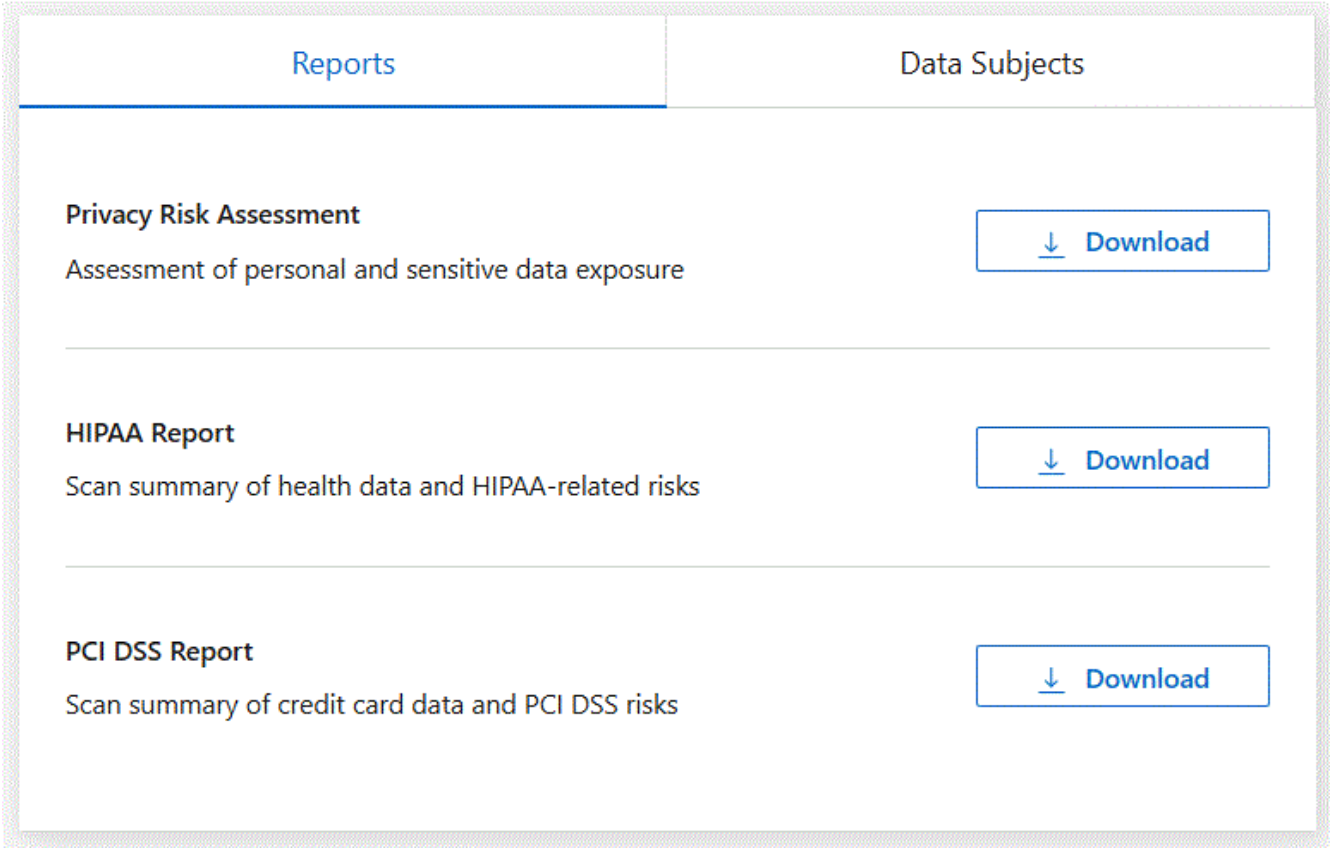
- Übersicht: In wie vielen Dateien sind Kreditkarteninformationen enthalten und in welchen Systemen.
- Verschlüsselung: Der Prozentsatz der Dateien mit Kreditkarteninformationen, die sich auf verschlüsselten oder unverschlüsselten Systemen befinden. Diese Informationen gelten speziell für Cloud Volumes 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:

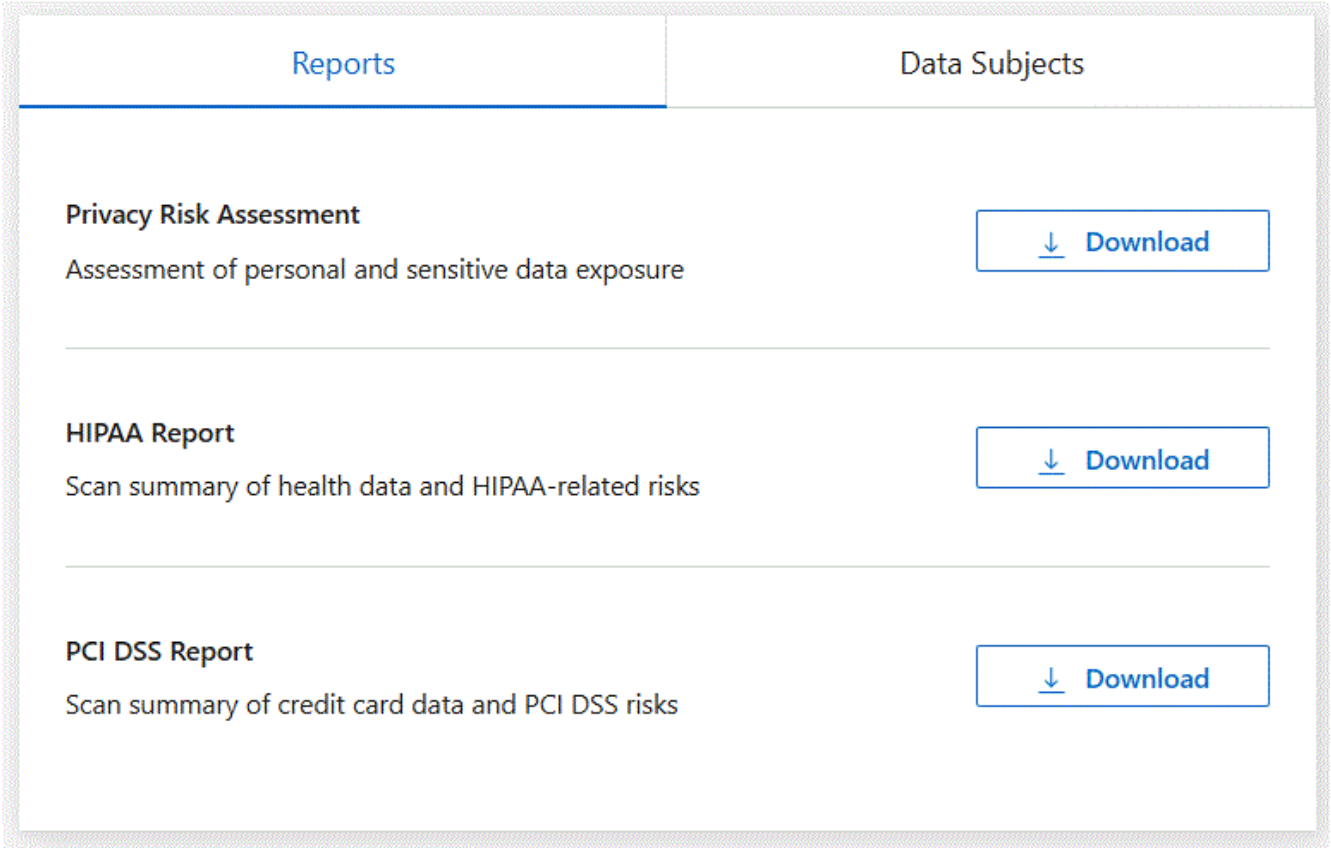
- Compliance-Status: Ein Schweregrad und die Verteilung der Daten, unabhängig davon, ob es sich um nicht vertrauliche, persönliche oder vertrauliche persönliche Daten handelt.
- Bewertungsübersicht: Eine Aufschlüsselung der gefundenen Arten personenbezogener Daten sowie der Datenkategorien.
- Betroffene 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 %

Schweregrad	Logik
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 %

Verwalten der Datenklassifizierung

Schließen Sie bestimmte Verzeichnisse von NetApp Data Classification -Scans aus

Wenn Sie möchten, dass NetApp Data Classification bestimmte Verzeichnisse von Scans ausschließt, können Sie diese Verzeichnisnamen zu einer Konfigurationsdatei hinzufügen. Nachdem Sie diese Änderung angewendet haben, schließt die Datenklassifizierungs-Engine diese Verzeichnisse von Scans aus.

Standardmäßig werden bei Datenklassifizierungsscans Volume-Snapshot-Daten ausgeschlossen, die mit ihrer Quelle im Volume identisch sind.

Unterstützte Datenquellen

Das Ausschließen bestimmter Verzeichnisse von Datenklassifizierungsscans wird für NFS- und CIFS-Freigaben in den folgenden Datenquellen unterstützt:

- On-Premises- ONTAP
- Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Allgemeine Dateifreigaben

Definieren Sie die Verzeichnisse, die vom Scan ausgeschlossen werden sollen

Bevor Sie Verzeichnisse vom Klassifizierungsscan ausschließen können, müssen Sie sich beim Datenklassifizierungssystem anmelden, damit Sie eine Konfigurationsdatei bearbeiten und ein Skript ausführen können. Erfahren Sie, wie Sie"Melden Sie sich beim Datenklassifizierungssystem an" abhängig davon, ob Sie die Software manuell auf einem Linux-Rechner installiert oder die Instanz in der Cloud bereitgestellt haben.

Überlegungen

- Sie können maximal 50 Verzeichnispfade pro Datenklassifizierungssystem ausschließen.
- Das Ausschließen von Verzeichnispfaden kann die Scanzeiten beeinträchtigen.

Schritte

1. Gehen Sie im Datenklassifizierungssystem zu "/opt/netapp/config/custom_configuration" und öffnen Sie die Datei `data_provider.yaml` .
2. Geben Sie im Abschnitt „data_providers“ unter der Zeile „exclude:“ die auszuschließenden Verzeichnispfade ein. Beispiel:

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

Ändern Sie nichts anderes in dieser Datei.

3. Speichern Sie die Änderungen an der Datei.
4. Gehen Sie zu „/opt/netapp/Datasense/tools/customer_configuration/data_providers“ und führen Sie das folgende Skript aus:

```
update_data_providers_from_config_file.sh
```

+ Dieser Befehl übergibt die vom Scannen auszuschließenden Verzeichnisse an die Klassifizierungs-Engine.

Ergebnis

Bei allen nachfolgenden Scans Ihrer Daten werden die angegebenen Verzeichnisse nicht gescannt.

Mit denselben Schritten können Sie Elemente zur Ausschlussliste hinzufügen, bearbeiten oder daraus löschen. Die überarbeitete Ausschlussliste wird aktualisiert, nachdem Sie das Skript ausgeführt haben, um Ihre Änderungen zu bestätigen.

Beispiele

Konfiguration 1:

Jeder Ordner, der irgendwo im Namen „folder1“ enthält, wird von allen Datenquellen ausgeschlossen.

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

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO1/Ordner1
- /CVO1/Ordner1name
- /CVO1/Ordner10
- /CVO1/*Ordner1
- /CVO1/+Ordner1name
- /CVO1/notfolder10
- /CVO22/Ordner1
- /CVO22/Ordner1name
- /CVO22/Ordner10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO1/*Ordner
- /CVO1/Ordnername
- /CVO22/*Ordner20

Konfiguration 2:

Jeder Ordner, der nur am Anfang des Namens „*folder1“ enthält, wird ausgeschlossen.

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

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO/*Ordner1
- /CVO/*Ordner1name
- /CVO/*Ordner10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO/Ordner1
- /CVO/Ordner1name
- /CVO/nicht*Ordner10

Konfiguration 3:
Jeder Ordner in der Datenquelle „CVO22“, der irgendwo im Namen „folder1“ enthält, wird ausgeschlossen.

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

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO22/Ordner1
- /CVO22/Ordner1name
- /CVO22/Ordner10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO1/Ordner1
- /CVO1/Ordner1name
- /CVO1/Ordner10

Escapezeichen für Sonderzeichen in Ordnernamen

Wenn Ihr Ordnername eines der folgenden Sonderzeichen enthält und Sie die Daten in diesem Ordner vom Scannen ausschließen möchten, müssen Sie vor dem Ordnernamen die Escape-Sequenz \\ verwenden.

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

Pfad in der Quelle: `/project/*not_to_scan`

Syntax in der Ausschlussdatei: `"\\*not_to_scan"`

Aktuelle Ausschlussliste anzeigen

Es ist möglich, dass der Inhalt der `data_provider.yaml` Konfigurationsdatei anders sein als das, was tatsächlich nach dem Ausführen des `update_data_providers_from_config_file.sh` Skript. Um die aktuelle Liste der Verzeichnisse anzuzeigen, die Sie vom Datenklassifizierungsscan ausgeschlossen haben, führen Sie den folgenden Befehl von „/opt/netapp/Datasense/tools/customer_configuration/data_providers“ aus:

```
get_data_providers_configuration.sh
```

Definieren Sie zusätzliche Gruppen-IDs als offen für die Organisation in NetApp Data Classification

Wenn Gruppen-IDs (GIDs) an Dateien oder Ordner in NFS-Dateifreigaben angehängt werden, definieren sie die Berechtigungen für die Datei oder den Ordner, beispielsweise, ob sie „für die Organisation geöffnet“ sind. Wenn einige GIDs zunächst nicht mit der Berechtigungsstufe „Für die Organisation offen“ eingerichtet sind, können Sie diese Berechtigung zur GID hinzufügen, sodass alle Dateien und Ordner, an die diese GID angehängt ist, als „für die Organisation offen“ gelten.

Nachdem Sie diese Änderung vorgenommen haben und NetApp Data Classification Ihre Dateien und Ordner erneut scannt, wird diese Berechtigung für alle Dateien und Ordner mit diesen Gruppen-IDs auf der Seite „Untersuchungsdetails“ angezeigt. Außerdem werden sie in Berichten angezeigt, in denen Sie Dateiberechtigungen anzeigen.

Um diese Funktion zu aktivieren, müssen Sie sich beim Datenklassifizierungssystem anmelden, damit Sie eine Konfigurationsdatei bearbeiten und ein Skript ausführen können. Erfahren Sie, wie Sie"Melden Sie sich beim Datenklassifizierungssystem an" abhängig davon, ob Sie die Software manuell auf einem Linux-Rechner installiert oder die Instanz in der Cloud bereitgestellt haben.

Fügen Sie Gruppen-IDs die Berechtigung „Für Organisation öffnen“ hinzu

Sie müssen über die Gruppen-ID-Nummern (GIDs) verfügen, bevor Sie mit dieser Aufgabe beginnen.

Schritte

1. Gehen Sie im Datenklassifizierungssystem zu "/opt/netapp/config/custom_configuration" und öffnen Sie die Datei `data_provider.yaml` .
2. Fügen Sie in der Zeile „organization_group_ids: []“ die Gruppen-IDs hinzu. Beispiel:

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

   Ändern Sie sonst nichts in dieser Datei.
3. Speichern Sie die Änderungen an der Datei.
4. Gehen Sie zu „/opt/netapp/Datasense/tools/customer_configuration/data_providers“ und führen Sie das folgende Skript aus:

```
update_data_providers_from_config_file.sh
```

Dieser Befehl übergibt die überarbeiteten Gruppen-ID-Berechtigungen an die Klassifizierungs-Engine.

Ergebnis

Bei allen nachfolgenden Scans Ihrer Daten werden Dateien oder Ordner mit diesen Gruppen-IDs als „für die Organisation offen“ gekennzeichnet.

Mit denselben Schritten können Sie die Liste der Gruppen-IDs bearbeiten und alle Gruppen-IDs löschen, die Sie in der Vergangenheit hinzugefügt haben. Die überarbeitete Liste der Gruppen-IDs wird aktualisiert, nachdem Sie das Skript ausgeführt haben, um Ihre Änderungen zu übernehmen.

Aktuelle Liste der Gruppen-IDs anzeigen

Es ist möglich, dass der Inhalt der `data_provider.yaml` Konfigurationsdatei von dem abweicht, was nach dem Ausführen des `update_data_providers_from_config_file.sh` Skript. Um die aktuelle Liste der Gruppen-IDs anzuzeigen, die Sie zur Datenklassifizierung hinzugefügt haben, führen Sie den folgenden Befehl von „/opt/netapp/Datasense/tools/customer_configuration/data_providers“ aus:

```
get_data_providers_configuration.sh
```

Datenquellen aus der NetApp Data Classification entfernen

Bei Bedarf können Sie NetApp Data Classification daran hindern, ein oder mehrere Systeme, Datenbanken oder Dateifreigabegruppen zu scannen.

Deaktivieren von Compliance-Scans für ein System

Wenn Sie Scans deaktivieren, scannt Data Classification die Daten auf dem System nicht mehr und entfernt die indizierten Compliance-Erkenntnisse aus der Data Classification-Instanz (die Daten aus dem System selbst werden nicht gelöscht).

1. Wählen Sie auf der Seite *Konfiguration* die Option Klicken Sie in der Zeile für das System auf die Schaltfläche „Datenklassifizierung deaktivieren“ und anschließend auf „Datenklassifizierung deaktivieren“.

Sie können Compliance-Scans für ein System auch im Bereich „Dienste“ deaktivieren, wenn Sie das System auswählen.

Entfernen einer Datenbank aus der Datenklassifizierung

Wenn Sie eine bestimmte Datenbank nicht mehr scannen möchten, können Sie sie aus der Datenklassifizierungsschnittstelle löschen und alle Scans stoppen.

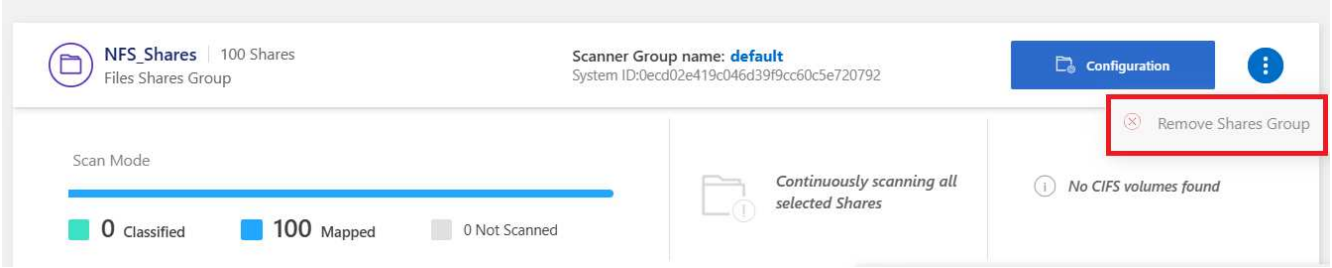
1. Wählen Sie auf der Seite *Konfiguration* die Option Klicken Sie in der Zeile für die Datenbank auf die Schaltfläche „DB-Server entfernen“ und dann auf „DB-Server entfernen“.

Entfernen einer Gruppe von Dateifreigaben aus der Datenklassifizierung

Wenn Sie Benutzerdateien aus einer Dateifreigabegruppe nicht mehr scannen möchten, können Sie die Dateifreigabegruppe aus der Datenklassifizierungsschnittstelle löschen und alle Scans stoppen.

Schritte

1. Wählen Sie auf der Seite *Konfiguration* die Option Klicken Sie in der Zeile für die Dateifreigabegruppe auf die Schaltfläche „Dateifreigabegruppe entfernen“ und dann auf „Dateifreigabegruppe entfernen“.



2. Wählen Sie im Bestätigungsdialogfeld **Freigabegruppe löschen** aus.

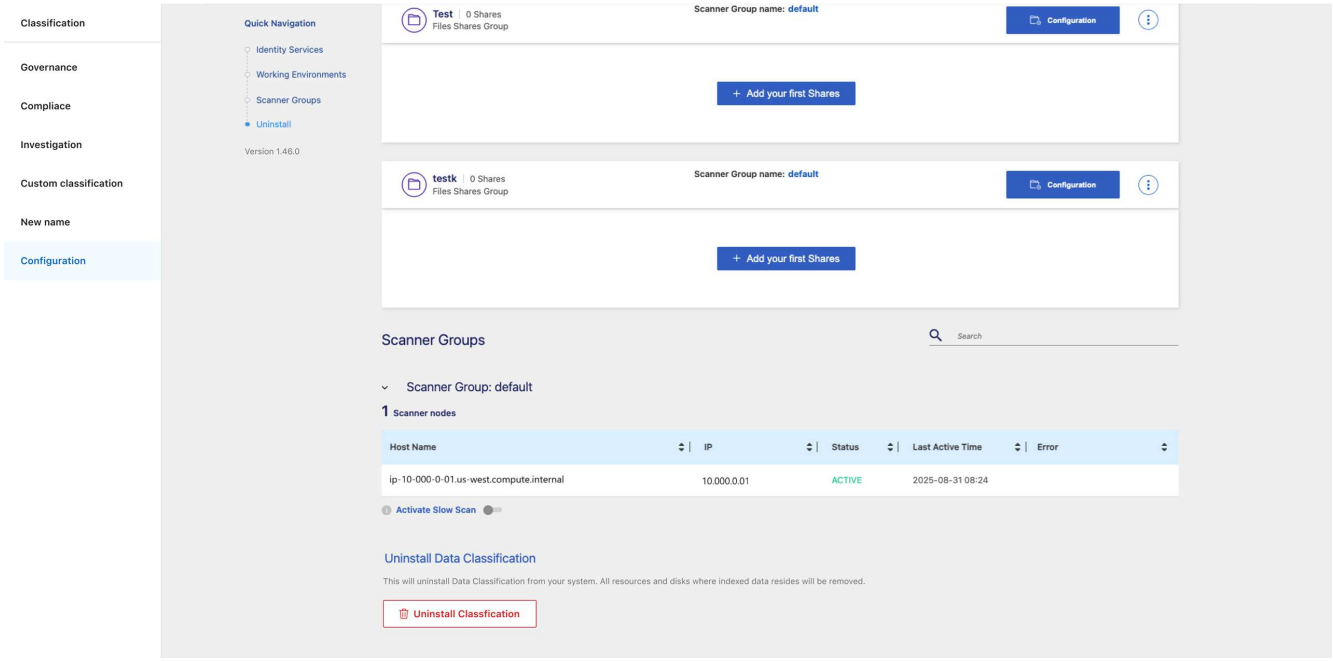
Deinstallieren Sie NetApp Data Classification

Sie können NetApp Data Classification deinstallieren, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen. Durch das Löschen der Instanz werden auch die zugehörigen Datenträger gelöscht, auf denen sich die indizierten Daten befinden. Das bedeutet, dass alle von Data Classification gescannten Informationen dauerhaft gelöscht werden.

Die erforderlichen Schritte hängen davon ab, ob Sie die Datenklassifizierung in der Cloud oder auf einem lokalen Host bereitgestellt haben.

Deinstallieren Sie Data Classification von einem Cloud-Anbieter

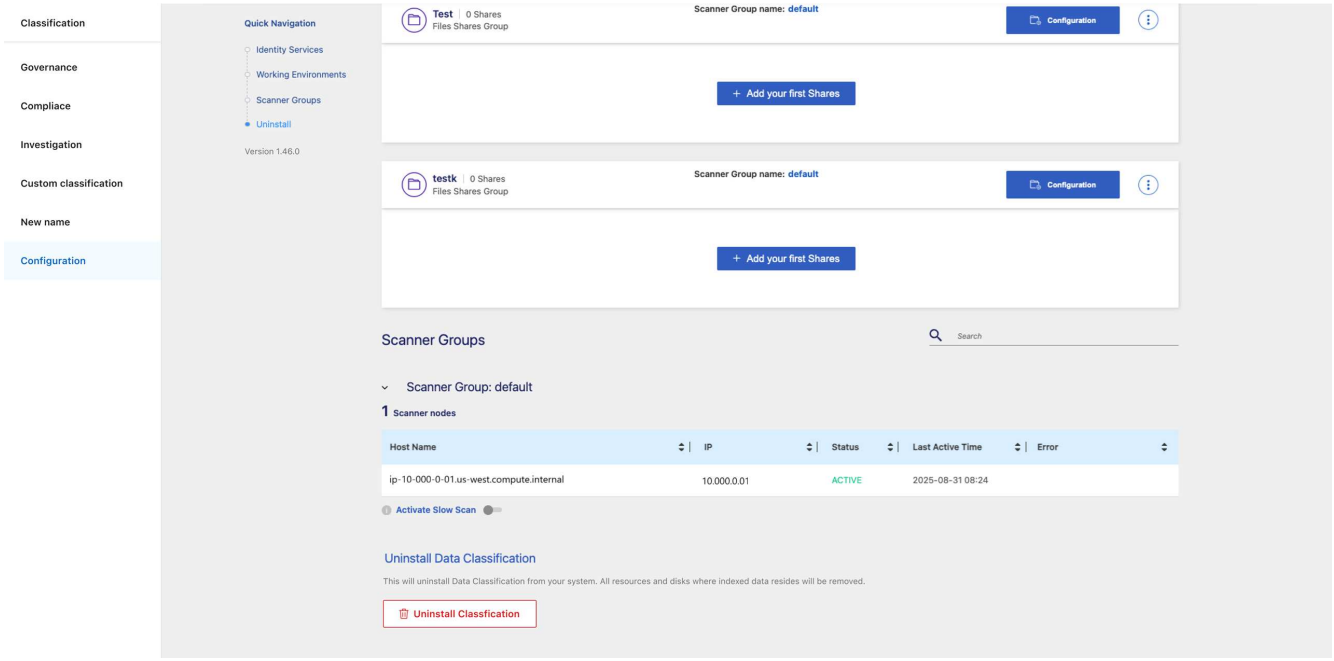
1. Wählen Sie unter „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie unten auf der Konfigurationsseite **Klassifizierung deinstallieren** aus.



3. Geben Sie im Dialogfeld „uninstall“ ein, um mit der Trennung der Data Classification-Instanz vom Konsolenagent fortzufahren. Wählen Sie zur Bestätigung **Deinstallieren**.
4. Geben Sie im Dialogfeld „Klassifizierung deinstallieren“ **deinstallieren** ein, um zu bestätigen, dass Sie die Datenklassifizierungsinstanz vom Konsolenagenten trennen möchten, und wählen Sie dann **Deinstallieren** aus.
5. Um den Deinstallationsvorgang abzuschließen, gehen Sie zur Konsole Ihres Cloud-Anbieters und löschen Sie die Data Classification-Instanz. Die Instanz trägt den Namen *CloudCompliance* und ist mit einem generierten Hash (UUID) verknüpft. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Deinstallieren der Datenklassifizierung aus einer lokalen Bereitstellung

1. Wählen Sie unter „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie unten auf der Konfigurationsseite **Klassifizierung deinstallieren** aus.



3. Geben Sie im Dialogfeld „uninstall“ ein, um mit der Trennung der Data Classification-Instanz vom Konsolenagent fortzufahren. Wählen Sie zur Bestätigung **Deinstallieren**.
4. Um die Software vom Host zu deinstallieren, führen Sie den `cleanup.sh` Skript auf dem Hostcomputer für die Datenklassifizierung, zum Beispiel:

```
cleanup.sh
```

Das Skript befindet sich im `/install/light_probe/onprem_installer/cleanup.sh` Verzeichnis. Erfahren Sie, wie Sie"Melden Sie sich beim Data Classification-Hostcomputer an" .

Referenz

Unterstützte NetApp Data Classification Instanztypen

Die NetApp Data Classification -Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Softwareanforderungen usw. erfüllt. Wenn Sie die Datenklassifizierung in der Cloud bereitstellen, empfehlen wir Ihnen, für die volle Funktionalität ein System mit der Eigenschaft „groß“ zu verwenden.

Sie können die Datenklassifizierung auf einem System mit weniger CPUs und weniger RAM bereitstellen, bei der Verwendung dieser weniger leistungsstarken Systeme gibt es jedoch einige Einschränkungen. "Erfahren Sie mehr über diese Einschränkungen" .

Wenn in den folgenden Tabellen das als „Standard“ gekennzeichnete System in der Region, in der Sie Data Classification installieren, nicht verfügbar ist, wird das nächste System in der Tabelle bereitgestellt.

AWS-Instanztypen

Systemgröße	Technische Daten	Instanztyp
Extragroß	32 CPUs, 128 GB RAM, 1 TiB gp3 SSD	"m6i.8xlarge"(Standard)
Groß	16 CPUs, 64 GB RAM, 500 GiB SSD	"m6i.4xlarge"(Standard) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Medium	8 CPUs, 32 GB RAM, 200 GiB SSD	"m6i.2xlarge"(Standard) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Klein	8 CPUs, 16 GB RAM, 100 GiB SSD	"c6a.2xlarge"(Standard) c5a.2xlarge c5.2xlarge c4.2xlarge

Azure-Instanztypen

Systemgröße	Technische Daten	Instanztyp
Extragroß	32 CPUs, 128 GB RAM, Betriebssystemfestplatte (2.048 GiB, min. 250 MB/s Durchsatz) und Datenfestplatte (1 TiB SSD, min. 750 MB/s Durchsatz)	"Standard_D32_v3"(Standard)
Groß	16 CPUs, 64 GB RAM, 500 GiB SSD	"Standard_D16s_v3"(Standard)

GCP-Instanztypen

Systemgröße	Technische Daten	Instanztyp
Groß	16 CPUs, 64 GB RAM, 500 GiB SSD	"n2-Standard-16"(Standard) n2d-standard-16 n1-standard-16

Aus Datenquellen in der NetApp Data Classification erfasste Metadaten

NetApp Data Classification sammelt bestimmte Metadaten, wenn Klassifizierungsscans für die Daten aus Ihren Datenquellen und Systemen durchgeführt werden. Die Datenklassifizierung kann auf die meisten Metadaten zugreifen, die wir zur Klassifizierung Ihrer Daten benötigen. Es gibt jedoch einige Quellen, bei denen wir nicht auf die benötigten Daten zugreifen können.

	Metadaten	CIFS	NFS
Zeitstempel	*Erstellungszeit*	Verfügbar	Nicht verfügbar (wird unter Linux nicht unterstützt)
	Letzter Zugriffszeitpunkt	Verfügbar	Verfügbar
	Letzte Änderungszeit	Verfügbar	Verfügbar
Berechtigungen	*Öffnen Sie Berechtigungen*	Wenn die Gruppe „JEDER“ Zugriff auf die Datei hat, gilt sie als „Für die Organisation offen“.	Wenn „Andere“ Zugriff auf die Datei haben, gilt sie als „Für die Organisation offen“.
	Benutzer-/Gruppenzugriff	Benutzer- und Gruppeninformationen werden aus LDAP übernommen	Nicht verfügbar (NFS-Benutzer werden normalerweise lokal auf dem Server verwaltet, daher kann dieselbe Person auf jedem Server eine andere UID haben)

- Die Datenklassifizierung extrahiert nicht die „Zeit des letzten Zugriffs“ aus den Datenbankdatenquellen.
- Ältere Versionen des Windows-Betriebssystems (z. B. Windows 7 und Windows 8) deaktivieren die Erfassung des Attributs „Zeit des letzten Zugriffs“ standardmäßig, da dies die Systemleistung beeinträchtigen kann. Wenn dieses Attribut nicht erfasst wird, sind Datenklassifizierungsanalysen, die auf der „Zeit des letzten Zugriffs“ basieren, davon betroffen. Sie können die Erfassung der letzten Zugriffszeit auf diesen älteren Windows-Systemen bei Bedarf aktivieren.

Zeitstempel des letzten Zugriffs

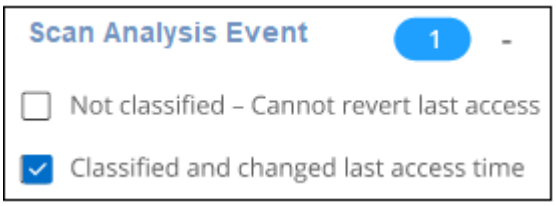
Wenn die Datenklassifizierung Daten aus Dateifreigaben extrahiert, betrachtet das Betriebssystem dies als Zugriff auf die Daten und ändert die „letzte Zugriffszeit“ entsprechend. Nach dem Scannen versucht die Datenklassifizierung, die letzte Zugriffszeit auf den ursprünglichen Zeitstempel zurückzusetzen. Wenn die Datenklassifizierung keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, kann das System die letzte Zugriffszeit nicht auf den ursprünglichen Zeitstempel zurücksetzen. Mit SnapLock konfigurierte ONTAP Volumes verfügen über schreibgeschützte Berechtigungen und können den letzten Zugriffszeitpunkt auch nicht auf den ursprünglichen Zeitstempel zurücksetzen.

Wenn Data Classification nicht über diese Berechtigungen verfügt, scannt das System diese Dateien in Ihren Volumes standardmäßig nicht, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen jedoch egal ist, ob die letzte Zugriffszeit in Ihren Dateien auf

die ursprüngliche Zeit zurückgesetzt wird, können Sie unten auf der Konfigurationsseite den Schalter **Scannen, wenn Berechtigungen zum Schreiben von Attributen fehlen** auswählen, damit die Datenklassifizierung die Volumes unabhängig von den Berechtigungen scannt.

Diese Funktionalität ist auf lokale ONTAP Systeme, Cloud Volumes ONTAP, Azure NetApp Files, Amazon FSx for NetApp ONTAP Management und Dateifreigaben von Drittanbietern anwendbar.

Auf der Untersuchungsseite gibt es einen Filter namens „Scan-Analyse-Ereignis“, mit dem Sie entweder die Dateien anzeigen können, die nicht klassifiziert wurden, weil die Datenklassifizierung den letzten Zugriffszeitpunkt nicht zurücksetzen konnte, oder die Dateien, die klassifiziert wurden, obwohl die Datenklassifizierung den letzten Zugriffszeitpunkt nicht zurücksetzen konnte.



Die Filterauswahl ist:

- „Nicht klassifiziert – Letzter Zugriffszeitpunkt kann nicht zurückgesetzt werden“ – Hier werden die Dateien angezeigt, die aufgrund fehlender Schreibberechtigungen nicht klassifiziert wurden.
- „Klassifiziert und letzte Zugriffszeit aktualisiert“ – Hier werden die Dateien angezeigt, die klassifiziert wurden und bei denen die Datenklassifizierung die letzte Zugriffszeit nicht auf das ursprüngliche Datum zurücksetzen konnte. Dieser Filter ist nur für Umgebungen relevant, in denen Sie **Scannen, wenn Berechtigungen zum Schreiben von Attributen fehlen** aktiviert haben.

Bei Bedarf können Sie diese Ergebnisse in einen Bericht exportieren, sodass Sie sehen können, welche Dateien aufgrund von Berechtigungen gescannt werden und welche nicht. "Erfahren Sie mehr über den Data Investigation Report" .

Melden Sie sich beim NetApp Data Classification System an

Sie müssen sich beim NetApp Data Classification System anmelden, damit Sie auf Protokolldateien zugreifen oder Konfigurationsdateien bearbeiten können.

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 auf die Konfigurationsdatei und das Skript zugreifen.

Wenn die Datenklassifizierung in der Cloud bereitgestellt wird, müssen Sie per SSH auf die Datenklassifizierungsinstanz zugreifen. Sie können per SSH auf das System zugreifen, indem Sie den

Benutzer und das Kennwort eingeben oder den SSH-Schlüssel verwenden, den Sie während der Installation des Konsolenagenten angegeben haben. Der SSH-Befehl lautet:

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

- `<path_to_the_ssh_key>`= Speicherort der SSH-Authentifizierungsschlüssel
- `<machine_user>`:
  - Für AWS: Verwenden Sie den <ec2-user>
  - Für Azure: Verwenden Sie den für die Konsoleninstanz erstellten Benutzer
  - Für GCP: Verwenden Sie den für die Konsoleninstanz erstellten Benutzer
- `<datasense_ip>`= IP-Adresse der virtuellen Maschineninstanz

Sie müssen die eingehenden Regeln der Sicherheitsgruppe ändern, um auf das System in der Cloud zuzugreifen. Weitere Informationen finden Sie unter:

- "Sicherheitsgruppenregeln in AWS"
- "Sicherheitsgruppenregeln in Azure"
- "Firewall-Regeln in Google Cloud"

NetApp Data Classification APIs

Die über die Web-Benutzeroberfläche verfügbaren NetApp Data Classification sind auch über die REST-API verfügbar.

Innerhalb der Datenklassifizierung sind vier Kategorien definiert, die den Registerkarten in der Benutzeroberfläche entsprechen:

- Untersuchung
- Einhaltung
- Führung
- Konfiguration

Mit den APIs in der Swagger-Dokumentation können Sie suchen, Daten aggregieren, Ihre Scans verfolgen und Aktionen wie Kopieren, Verschieben und Löschen ausführen.

Überblick

Mit der API können Sie die folgenden Funktionen ausführen:

- Exportinformationen
  - Alles, was in der Benutzeroberfläche verfügbar ist, kann über die API exportiert werden (mit Ausnahme von Berichten).
  - Daten werden im JSON-Format exportiert (einfach zu analysieren und an Anwendungen von Drittanbietern wie Splunk weiterzuleiten).
- Erstellen Sie Abfragen mit „UND“- und „ODER“-Anweisungen, schließen Sie Informationen ein und aus und mehr.

Sie können beispielsweise Dateien *ohne* spezifische personenbezogene Daten (PII) suchen (Funktion in der Benutzeroberfläche nicht verfügbar). Sie können auch bestimmte Felder vom Exportvorgang ausschließen.

- Aktionen ausführen
  - CIFS-Anmeldeinformationen aktualisieren
  - Aktionen anzeigen und abbrechen
  - Verzeichnisse erneut scannen
  - Daten exportieren

Die API ist sicher und verwendet dieselbe Authentifizierungsmethode wie die Benutzeroberfläche. Informationen zur Authentifizierung finden Sie im"REST API-Dokumentation" .

Zugriff auf die Swagger-API-Referenz

Um auf Swagger zuzugreifen, benötigen Sie die IP-Adresse Ihrer Datenklassifizierungsinstanz. Bei einer Cloud-Bereitstellung verwenden Sie die öffentliche IP-Adresse. Dann müssen Sie zu diesem Endpunkt gelangen:

https://<Klassifizierungs-IP>/documentation

Beispiel für die Verwendung der APIs

Das folgende Beispiel zeigt einen API-Aufruf zum Kopieren von Dateien.

API-Anforderung

Sie müssen zunächst alle relevanten Felder und Optionen für ein System abrufen, um alle Filter auf der Registerkarte „Untersuchung“ anzuzeigen.

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

Antwort

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

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

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

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

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

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

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

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

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

Wir werden diese Antwort in unseren Anforderungsparametern verwenden, um die gewünschten Dateien zu filtern, die wir kopieren möchten.

Sie können eine Aktion auf mehrere Elemente anwenden. Zu den unterstützten Aktionstypen gehören: Verschieben, Löschen und Kopieren.

Wir erstellen die Kopieraktion:

API-Anforderung

Diese nächste API ist die Aktions-API und ermöglicht Ihnen die Erstellung mehrerer Aktionen.

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

Antwort

Die Antwort gibt das Aktionsobjekt zurück, sodass Sie die APIs zum Abrufen und Löschen verwenden können, um den Status der Aktion abzurufen oder sie abzubrechen.

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

Wissen und Unterstützung

Registrieren Sie sich für den NetApp Console Support

Um technischen Support speziell für die NetApp Console und ihre Speicherlösungen und Datendienste zu erhalten, ist eine Support-Registrierung erforderlich. Eine Support-Registrierung ist auch erforderlich, um wichtige Workflows für Cloud Volumes ONTAP Systeme zu aktivieren.

Durch die Registrierung für den Support wird kein NetApp Support für den Dateidienst eines Cloud-Anbieters aktiviert. Technischen Support für den Dateidienst eines Cloud-Anbieters, seine Infrastruktur oder eine Lösung, die den Dienst nutzt, erhalten Sie unter „Hilfe erhalten“ in der Dokumentation des jeweiligen Produkts.

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

Übersicht zur Support-Registrierung

Zur Aktivierung des Supportanspruchs stehen zwei Registrierungsformen zur Verfügung:

- Registrieren Sie die Seriennummer Ihres NetApp Console (Ihre 20-stellige Seriennummer 960xxxxxxxxx, die Sie auf der Seite „Supportressourcen“ in der Konsole finden).

  Dies dient als Ihre einzige Support-Abonnement-ID für alle Dienste innerhalb der Konsole. Jedes Konsolenkonto muss registriert werden.

- Registrieren Sie die mit einem Abonnement verknüpften Cloud Volumes ONTAP Seriennummern im Marktplatz Ihres Cloud-Anbieters (dies sind 20-stellige 909201xxxxxxxx-Seriennummern).

  Diese Seriennummern werden allgemein als *PAYGO-Seriennummern* bezeichnet und von der NetApp Console zum Zeitpunkt der Bereitstellung von Cloud Volumes ONTAP generiert.

Durch die Registrierung beider Seriennummerntypen werden Funktionen wie das Öffnen von Support-Tickets und die automatische Fallgenerierung ermöglicht. Die Registrierung wird abgeschlossen, indem Sie der Konsole NetApp Support Site (NSS)-Konten hinzufügen, wie unten beschrieben.

Registrieren Sie die NetApp Console für den NetApp Support

Um sich für den Support zu registrieren und den Supportanspruch zu aktivieren, muss ein Benutzer in Ihrem NetApp Console seinem Konsolen-Login ein NetApp Support-Site-Konto zuordnen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über ein NetApp Support Site (NSS)-Konto verfügen.

Bestandskunde mit NSS-Konto

Wenn Sie ein NetApp -Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich über die Konsole für den Support registrieren.

Schritte

1. Wählen Sie **Administration** > **Anmeldeinformationen**.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Authentifizierungsaufforderung der NetApp Support Site (NSS).
4. Um zu bestätigen, dass der Registrierungsvorgang erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Konsolenkonto für den Support registriert ist.

   Beachten Sie, dass anderen Konsolenbenutzern dieser Support-Registrierungsstatus nicht angezeigt wird, wenn sie ihrem Login kein NetApp Support Site-Konto zugeordnet haben. Dies bedeutet jedoch nicht, dass Ihr Konto nicht für den Support registriert ist. Sofern ein Benutzer in der Organisation diese Schritte befolgt hat, wurde Ihr Konto registriert.

Bestandskunde, aber kein NSS-Konto

Wenn Sie bereits NetApp -Kunde mit vorhandenen Lizenzen und Seriennummern, aber *keinem* NSS-Konto sind, müssen Sie ein NSS-Konto erstellen und es mit Ihrem Konsolen-Login verknüpfen.

Schritte

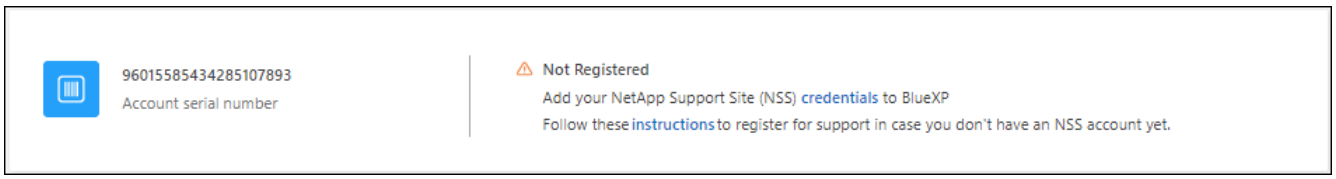
1. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die Seriennummer des Konsolenkontos (960xxxx) zu kopieren, die oben für das Feld „Seriennummer“ verwendet wurde. Dies beschleunigt die Kontobearbeitung.
2. Verknüpfen Sie Ihr neues NSS-Konto mit Ihrem Konsolen-Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

Ganz neu bei NetApp

Wenn Sie NetApp noch nicht kennen und kein NSS-Konto haben, befolgen Sie die nachstehenden Schritte.

Schritte

1. Wählen Sie oben rechts in der Konsole das Hilfesymbol und dann **Support** aus.
2. Suchen Sie auf der Support-Registrierungsseite nach der Seriennummer Ihrer Konto-ID.



3. Navigieren Sie zu "Support-Registrierungssite von NetApp" und wählen Sie **Ich bin kein registrierter NetApp -Kunde**.
4. Füllen Sie die Pflichtfelder (mit roten Sternchen gekennzeichnet) aus.
5. Wählen Sie im Feld **Produktlinie Cloud Manager** und dann Ihren entsprechenden Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer Ihres Kontos aus Schritt 2 oben, schließen Sie die Sicherheitsüberprüfung

ab und bestätigen Sie anschließend, dass Sie die globale Datenschutzrichtlinie von NetApp gelesen haben.

Um diese sichere Transaktion abzuschließen, wird umgehend eine E-Mail an das angegebene Postfach gesendet. Überprüfen Sie unbedingt Ihren Spam-Ordner, wenn die Bestätigungs-E-Mail nicht innerhalb weniger Minuten eintrifft.

7. Bestätigen Sie die Aktion in der E-Mail.

   Durch die Bestätigung wird Ihre Anfrage an NetApp übermittelt und es wird empfohlen, dass Sie ein NetApp Support Site-Konto erstellen.

8. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die oben für das Seriennummernfeld verwendete Kontoseriennummer (960xxxx) zu kopieren. Dadurch wird die Bearbeitung beschleunigt.

Nach Abschluss

NetApp sollte sich während dieses Vorgangs mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Sobald Sie über Ihr NetApp Support Site-Konto verfügen, verknüpfen Sie das Konto mit Ihrem Konsolen-Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

NSS-Anmeldeinformationen für Cloud Volumes ONTAP Support zuordnen

Um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu aktivieren, müssen Sie Ihrem Konsolenkonto Anmeldeinformationen für die NetApp Support Site zuordnen:

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen für den Support

  Die Angabe Ihres NSS-Kontos ist erforderlich, um den Support für Ihr System zu aktivieren und Zugriff auf die technischen Supportressourcen von NetApp zu erhalten.

- Bereitstellen von Cloud Volumes ONTAP mit eigener Lizenz (BYOL)

  Die Angabe Ihres NSS-Kontos ist erforderlich, damit die Konsole Ihren Lizenzschlüssel hochladen und das Abonnement für die von Ihnen erworbene Laufzeit aktivieren kann. Hierzu gehören automatische Updates bei Laufzeitverlängerungen.

- Aktualisieren der Cloud Volumes ONTAP -Software auf die neueste Version

Die Zuordnung von NSS-Anmeldeinformationen zu Ihrem NetApp Console unterscheidet sich von der Zuordnung des NSS-Kontos zu einer Konsolenbenutzeranmeldung.

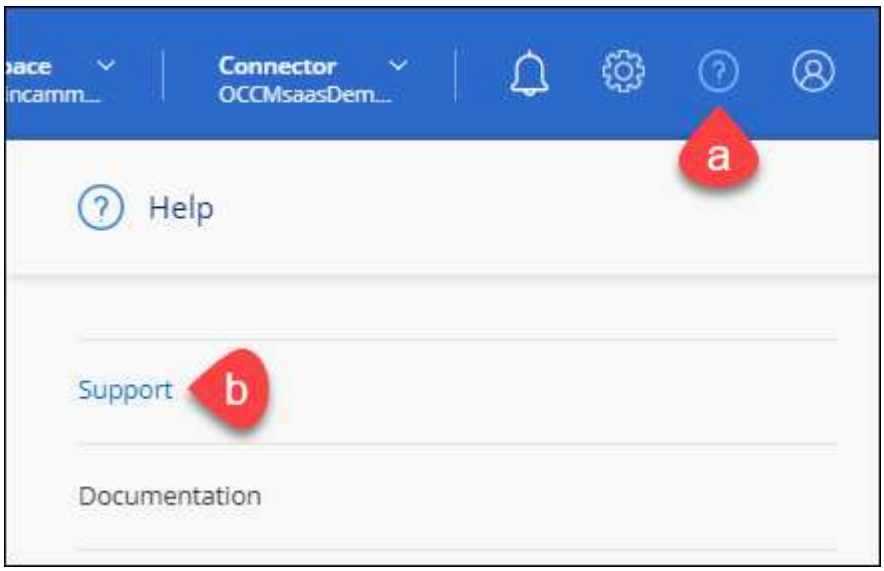
Diese NSS-Anmeldeinformationen sind mit Ihrer spezifischen Konsolenkonto-ID verknüpft. Benutzer, die zur Konsolenorganisation gehören, können über **Support > NSS-Verwaltung** auf diese Anmeldeinformationen zugreifen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.

- Wenn Sie über ein Partner- oder Reseller-Konto verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen, diese können jedoch nicht zusammen mit Konten auf Kundenebene hinzugefügt werden.

Schritte

1. Wählen Sie oben rechts in der Konsole das Hilfesymbol und dann **Support** aus.



2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite weitergeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste speziell für Support und Lizenzierung.

4. Geben Sie auf der Anmeldeseite Ihre bei der NetApp Support Site registrierte E-Mail-Adresse und Ihr Kennwort ein, um den Authentifizierungsprozess durchzuführen.

   Diese Aktionen ermöglichen der Konsole, Ihr NSS-Konto für Dinge wie Lizenzdownloads, Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen zu verwenden.

   Beachten Sie Folgendes:

   - Das NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder temporäres Konto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto geben, wenn es sich bei diesem Konto um ein Konto auf Partnerebene handelt. Wenn Sie versuchen, NSS-Konten auf Kundenebene hinzuzufügen und ein Konto auf Partnerebene vorhanden ist, erhalten Sie die folgende Fehlermeldung:

     „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da bereits NSS-Benutzer eines anderen Typs vorhanden sind.“

   Dasselbe gilt, wenn Sie bereits über NSS-Konten auf Kundenebene verfügen und versuchen, ein Konto auf Partnerebene hinzuzufügen.

   - Nach erfolgreicher Anmeldung speichert NetApp den NSS-Benutzernamen.

     Dies ist eine vom System generierte ID, die Ihrer E-Mail-Adresse zugeordnet ist. Auf der Seite **NSS-Verwaltung** können Sie Ihre E-Mail-Adresse aus dem ••• Speisekarte.

- Wenn Sie Ihre Anmeldeinformationen aktualisieren müssen, gibt es auch die Option **Anmeldeinformationen aktualisieren** im ••• Speisekarte.

  Bei Verwendung dieser Option werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Sie werden durch eine entsprechende Benachrichtigung darauf aufmerksam gemacht.

Holen Sie sich Hilfe zur NetApp Data Classification

NetApp bietet auf vielfältige Weise Support für die NetApp Console und ihre Cloud-Dienste. Umfangreiche kostenlose Selbsthilfeoptionen stehen rund um die Uhr zur Verfügung, beispielsweise Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung beinhaltet technischen Remote-Support per Web-Ticketing.

Erhalten Sie Unterstützung für den Dateidienst eines Cloud-Anbieters

Technischen Support zu einem Dateidienst eines Cloud-Anbieters, seiner Infrastruktur oder einer Lösung, die den Dienst nutzt, finden Sie in der Dokumentation zu diesem Produkt.

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

Um technischen Support speziell für NetApp und seine Speicherlösungen und Datendienste zu erhalten, verwenden Sie die unten beschriebenen Supportoptionen.

Nutzen Sie Möglichkeiten zur Selbsthilfe

Diese Optionen stehen Ihnen 24 Stunden am Tag, 7 Tage die Woche kostenlos zur Verfügung:

- Dokumentation

  Die NetApp Console Konsolendokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  Durchsuchen Sie die NetApp Wissensdatenbank nach hilfreichen Artikeln zur Problembehebung.

- "Gemeinschaften"

  Treten Sie der NetApp Console Community bei, um aktuelle Diskussionen zu verfolgen oder neue zu starten.

Erstellen Sie einen Fall mit dem NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie nach der Aktivierung des Supports mit einem NetApp -Support-Spezialisten zusammenarbeiten, um alle Probleme zu lösen.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** zu verwenden, müssen Sie zunächst Ihre Anmeldeinformationen für die NetApp -Support-Site mit Ihrem Konsolen-Login verknüpfen. "Erfahren Sie, wie Sie die mit Ihrer

Konsolenanmeldung verknüpften Anmeldeinformationen verwalten." .

- Wenn Sie einen Fall für ein ONTAP -System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer für dieses System verknüpft sein.

Schritte

1. Wählen Sie in der NetApp Console*Hilfe > Support*.
2. Wählen Sie auf der Seite **Ressourcen** unter „Technischer Support“ eine der verfügbaren Optionen aus:

   a. Wählen Sie **Rufen Sie uns an**, wenn Sie mit jemandem telefonieren möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.

   b. Wählen Sie **Fall erstellen**, um ein Ticket bei einem NetApp -Support-Spezialisten zu öffnen:

      - **Dienst**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: * NetApp Console*, wenn es sich speziell um ein technisches Supportproblem mit Workflows oder Funktionen innerhalb der Konsole handelt.
      - **System**: Wählen Sie, falls für den Speicher zutreffend, * Cloud Volumes ONTAP* oder **On-Prem** und dann die zugehörige Arbeitsumgebung aus.

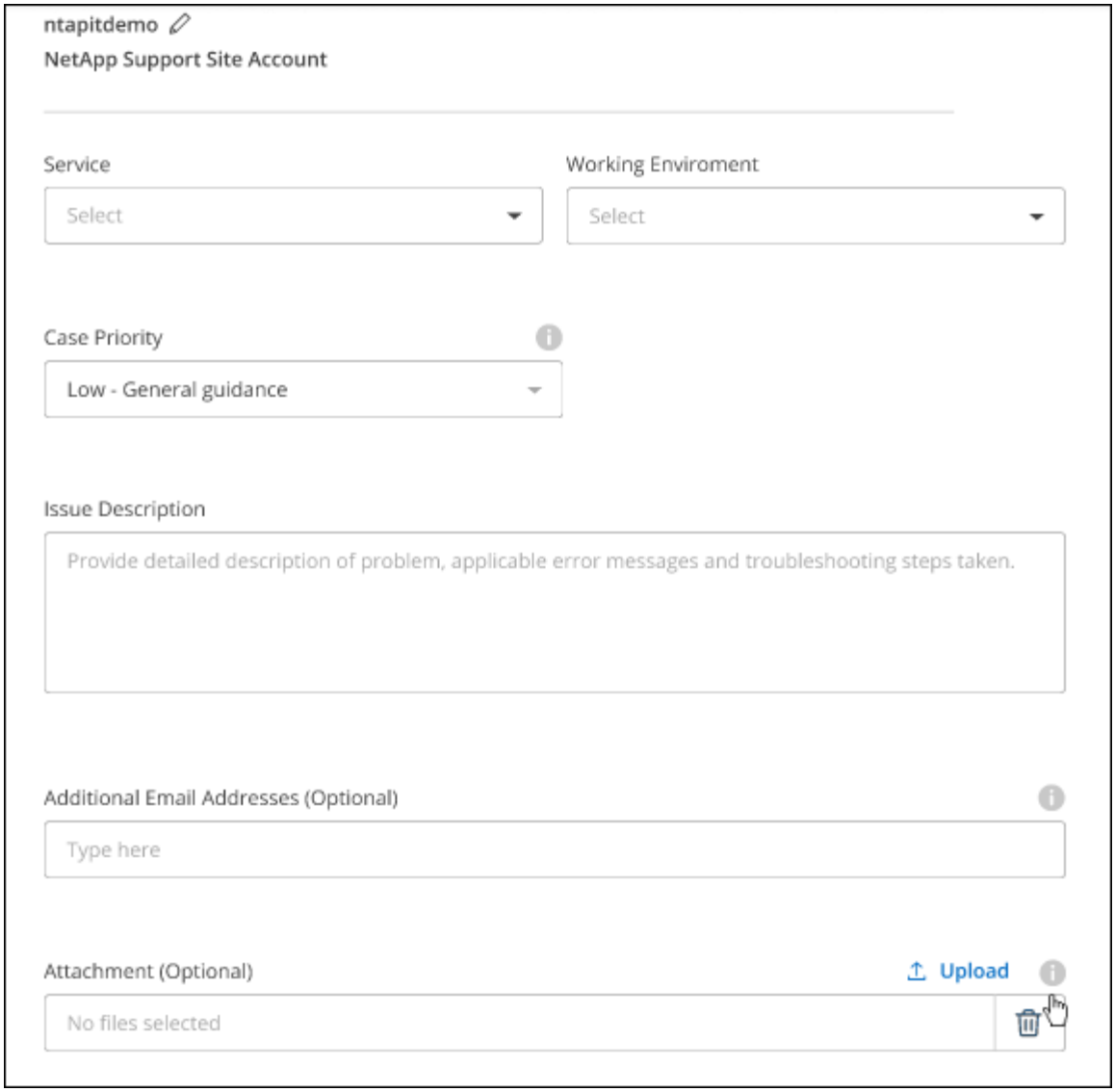
        Die Liste der Systeme liegt im Rahmen der Konsolenorganisation und des Konsolenagenten, den Sie im oberen Banner ausgewählt haben.

      - **Fallpriorität**: Wählen Sie die Priorität für den Fall. Sie kann „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“ sein.

        Um weitere Einzelheiten zu diesen Prioritäten zu erfahren, bewegen Sie die Maus über das Informationssymbol neben dem Feldnamen.

      - **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller zutreffenden Fehlermeldungen oder Schritte zur Fehlerbehebung, die Sie durchgeführt haben.
      - **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderen auf dieses Problem aufmerksam machen möchten.
      - **Anhang (optional)**: Laden Sie bis zu fünf Anhänge hoch, einen nach dem anderen.

        Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nach Abschluss

Es erscheint ein Popup mit Ihrer Support-Fallnummer. Ein NetApp -Support-Spezialist wird Ihren Fall prüfen und sich in Kürze bei Ihnen melden.

Um einen Verlauf Ihrer Supportfälle anzuzeigen, können Sie **Einstellungen > Zeitleiste** auswählen und nach Aktionen mit der Bezeichnung „Supportfall erstellen“ suchen. Über eine Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Beim Versuch, einen Fall zu erstellen, kann es sein, dass die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Dienst zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das damit verknüpfte Unternehmen nicht dasselbe Unternehmen sind, für das die Seriennummer des NetApp Console gilt (d. h. 960xxxx) oder die Seriennummer der Arbeitsumgebung. Sie können auf eine der folgenden Arten Hilfe anfordern:

- Senden Sie einen nicht-technischen Fall an https://mysupport.netapp.com/site/help

Verwalten Sie Ihre Supportfälle

Sie können aktive und gelöste Supportfälle direkt von der Konsole aus anzeigen und verwalten. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpften Fälle verwalten.

Beachten Sie Folgendes:

- Das Fallmanagement-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht links zeigt die Gesamtzahl der Fälle, die in den letzten drei Monaten von dem von Ihnen angegebenen NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht rechts zeigt die Gesamtzahl der in den letzten drei Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto.

  Die Ergebnisse in der Tabelle spiegeln die Fälle wider, die mit der von Ihnen ausgewählten Ansicht in Zusammenhang stehen.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie „Priorität“ und „Status“ filtern. Andere Spalten bieten lediglich Sortierfunktionen.

  Weitere Einzelheiten finden Sie in den folgenden Schritten.
- Auf Einzelfallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Abgeschlossen“ oder „Ausstehend abgeschlossen“ befindet.

Schritte

1. Wählen Sie in der NetApp Console*Hilfe > Support*.
2. Wählen Sie **Fallmanagement** und fügen Sie bei entsprechender Aufforderung Ihr NSS-Konto zur Konsole hinzu.

   Auf der Seite **Fallverwaltung** werden offene Fälle angezeigt, die sich auf das NSS-Konto beziehen, das mit Ihrem Konsolenbenutzerkonto verknüpft ist. Dies ist dasselbe NSS-Konto, das oben auf der **NSS-Verwaltungsseite** angezeigt wird.
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:
   - Wählen Sie unter **Fälle der Organisation** die Option **Anzeigen** aus, um alle mit Ihrem Unternehmen verknüpften Fälle anzuzeigen.
   - Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.
   - Filtern Sie den Inhalt der Spalten.
   - Ändern Sie die in der Tabelle angezeigten Spalten, indem Sie und wählen Sie dann die Spalten aus, die Sie anzeigen möchten.
4. Verwalten Sie einen vorhandenen Fall, indem Sie und wählen Sie eine der verfügbaren Optionen aus:
   - **Fall anzeigen**: Alle Details zu einem bestimmten Fall anzeigen.
   - **Fallnotizen aktualisieren**: Geben Sie zusätzliche Details zu Ihrem Problem an oder wählen Sie **Dateien hochladen**, um bis zu fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

- **Fall schließen**: Geben Sie Details zum Grund für das Schließen des Falls an und wählen Sie **Fall schließen** aus.

Häufig gestellte Fragen zur NetApp Data Classification

Diese FAQ können hilfreich sein, wenn Sie nur schnell eine Antwort auf eine Frage suchen.

NetApp Data Classification

Die folgenden Fragen vermitteln ein allgemeines Verständnis der Datenklassifizierung.

Wie funktioniert die Datenklassifizierung?

Die Datenklassifizierung stellt neben Ihrem NetApp Console und Ihren Speichersystemen eine weitere KI-Ebene bereit. Anschließend werden die Daten auf Volumes, Buckets, Datenbanken und anderen Speicherkonten gescannt und die gefundenen Datenerkenntnisse indiziert. Die Datenklassifizierung nutzt sowohl künstliche Intelligenz als auch natürliche Sprachverarbeitung, im Gegensatz zu alternativen Lösungen, die üblicherweise auf regulären Ausdrücken und Mustervergleich basieren.

Bei der Datenklassifizierung wird KI verwendet, um ein kontextuelles Verständnis der Daten für eine genaue Erkennung und Klassifizierung zu ermöglichen. Es wird von KI gesteuert, da es für moderne Datentypen und -skalen konzipiert ist. Es versteht auch den Datenkontext, um eine starke, genaue Entdeckung und Klassifizierung zu ermöglichen.

"Erfahren Sie mehr über die Funktionsweise der Datenklassifizierung" .

Verfügt Data Classification über eine REST-API und funktioniert es mit Tools von Drittanbietern?

Ja, Data Classification verfügt über eine REST-API für die unterstützten Funktionen in der Data Classification-Version, die Teil der Console-Kernplattform ist. Sehen "API-Dokumentation" .

Ist die Datenklassifizierung über die Cloud-Marktplätze verfügbar?

Die Datenklassifizierung ist Teil der Kernfunktionen der NetApp Console , daher müssen Sie für diesen Dienst nicht die Marktplätze verwenden.

Scannen und Analysieren von Datenklassifizierungen

Die folgenden Fragen beziehen sich auf die Scanleistung und Analyse der Datenklassifizierung.

Wie oft scannt die Datenklassifizierung meine Daten?

Während der erste Scan Ihrer Daten etwas Zeit in Anspruch nehmen kann, prüfen nachfolgende Scans nur die inkrementellen Änderungen, wodurch die System-Scan-Zeiten verkürzt werden. Die Datenklassifizierung scannt Ihre Daten kontinuierlich im Round-Robin-Verfahren, jeweils sechs Repositories gleichzeitig, sodass alle geänderten Daten sehr schnell klassifiziert werden.

"Erfahren Sie, wie Scans funktionieren" .

Die Datenklassifizierung scannt Datenbanken nur einmal pro Tag; Datenbanken werden nicht kontinuierlich

gescannt wie andere Datenquellen.

Datenscans haben nur einen vernachlässigbaren Einfluss auf Ihre Speichersysteme und Ihre Daten.

Variiert die Scanleistung?

Die Scanleistung kann je nach Netzwerkbandbreite und durchschnittlicher Dateigröße in Ihrer Umgebung variieren. Es kann auch von den Größenmerkmalen des Hostsystems abhängen (entweder in der Cloud oder vor Ort). Siehe "Die Datenklassifizierungsinstanz" Und "Bereitstellen der Datenklassifizierung" für weitere Informationen.

Beim erstmaligen Hinzufügen neuer Datenquellen können Sie auch festlegen, dass anstelle eines vollständigen „Klassifizierungs“-Scans (Map & Classify) nur ein „Mapping“-Scan (Mapping only) durchgeführt wird. Das Mapping Ihrer Datenquellen kann sehr schnell durchgeführt werden, da zum Anzeigen der darin enthaltenen Daten kein Zugriff auf Dateien erforderlich ist. "Sehen Sie den Unterschied zwischen einem Mapping- und einem Klassifizierungsscan" .

Kann ich meine Daten mithilfe der Datenklassifizierung durchsuchen?

Die Datenklassifizierung bietet umfangreiche Suchfunktionen, die die Suche nach einer bestimmten Datei oder einem bestimmten Datenelement in allen verbundenen Quellen vereinfachen. Durch die Datenklassifizierung können Benutzer tiefer suchen als nur das, was die Metadaten widerspiegeln. Es handelt sich um einen sprachunabhängigen Dienst, der die Dateien auch lesen und eine Vielzahl sensibler Datentypen wie Namen und IDs analysieren kann. Beispielsweise können Benutzer sowohl strukturierte als auch unstrukturierte Datenspeicher durchsuchen, um Daten zu finden, die möglicherweise unter Verstoß gegen die Unternehmensrichtlinien aus Datenbanken in Benutzerdateien gelangt sind. Suchvorgänge können für später gespeichert werden und es können Richtlinien erstellt werden, um in einer festgelegten Häufigkeit nach Ergebnissen zu suchen und entsprechende Maßnahmen zu ergreifen.

Sobald die gewünschten Dateien gefunden wurden, können Merkmale aufgelistet werden, darunter Tags, Systemkonto, Bucket, Dateipfad, Kategorie (aus der Klassifizierung), Dateigröße, letzte Änderung, Berechtigungsstatus, Duplikate, Vertraulichkeitsstufe, persönliche Daten, vertrauliche Datentypen innerhalb der Datei, Eigentümer, Dateityp, Dateigröße, Erstellungszeit, Datei-Hash, ob die Daten jemandem zugewiesen wurden, der ihre Aufmerksamkeit sucht, und mehr. Um nicht relevante Merkmale auszusortieren, können Filter angewendet werden.

Die Datenklassifizierung verfügt außerdem über eine rollenbasierte Zugriffskontrolle (RBAC), um das Verschieben oder Löschen von Dateien zu ermöglichen, sofern die entsprechenden Berechtigungen vorhanden sind. Wenn die richtigen Berechtigungen nicht vorhanden sind, können die Aufgaben jemandem in der Organisation zugewiesen werden, der über die richtigen Berechtigungen verfügt.

Datenklassifizierungsverwaltung und Datenschutz

Die folgenden Fragen bieten Informationen zur Verwaltung der Datenklassifizierung und der Datenschutzeinstellungen.

Wie aktiviere oder deaktiviere ich die Datenklassifizierung?

Zuerst müssen Sie eine Instanz der Datenklassifizierung in der Konsole oder auf einem lokalen System bereitstellen. Sobald die Instanz ausgeführt wird, können Sie den Dienst auf vorhandenen Systemen, Datenbanken und anderen Datenquellen über die Registerkarte **Konfiguration** oder durch Auswahl eines bestimmten Systems aktivieren. "Erfahren Sie, wie Sie loslegen können" .

Das Aktivieren der Datenklassifizierung für eine Datenquelle führt zu einem sofortigen ersten Scan. Die Scanergebnisse werden kurz darauf angezeigt.

Sie können die Datenklassifizierung beim Scannen einzelner Systeme, Datenbanken oder Dateifreigabegruppen auf der Seite „Datenklassifizierungskonfiguration“ deaktivieren. Sehen "Datenquellen aus der Datenklassifizierung entfernen" .

Um die Datenklassifizierungsinstanz vollständig zu entfernen, entfernen Sie die Datenklassifizierungsinstanz manuell aus dem Portal oder vom lokalen Standort Ihres Cloud-Anbieters.

Kann der Dienst das Scannen von Daten in bestimmten Verzeichnissen ausschließen?

Ja. Wenn Sie möchten, dass die Datenklassifizierung das Scannen von Daten ausschließt, die sich in bestimmten Datenquellenverzeichnissen befinden, können Sie diese Liste der Klassifizierungs-Engine bereitstellen. Nachdem Sie diese Änderung angewendet haben, schließt die Datenklassifizierung das Scannen von Daten in den angegebenen Verzeichnissen aus. "Mehr erfahren" .

Werden Snapshots, die sich auf ONTAP Volumes befinden, gescannt?

Nein. Die Datenklassifizierung scannt keine Snapshots, da der Inhalt mit dem Inhalt im Volume identisch ist.

Was passiert, wenn auf Ihren ONTAP Volumes Data Tiering aktiviert ist?

Wenn die Datenklassifizierung Volumes mit Cold Data scannt, die mithilfe von Nur-Mapping-Scans in Objektspeichern abgelegt sind, scannt sie alle Daten – Daten auf lokalen Festplatten und Cold Data, die in Objektspeichern abgelegt sind. Dies gilt auch für Nicht- NetApp -Produkte, die Tiering implementieren.

Der reine Mapping-Scan erwärmt die kalten Daten nicht – sie bleiben kalt und verbleiben im Objektspeicher. Wenn Sie hingegen den Map & Classify-Scan durchführen, können einige Konfigurationen die kalten Daten aufheizen.

Arten von Quellsystemen und Datentypen

Die folgenden Fragen beziehen sich auf die Speichertypen, die gescannt werden können, und die Datentypen, die gescannt werden.

Gibt es Einschränkungen bei der Entsendung in eine Regierungsregion?

Die Datenklassifizierung wird unterstützt, wenn der Konsolenagent in einer Regierungsregion (AWS GovCloud, Azure Gov oder Azure DoD) bereitgestellt wird – auch als „Eingeschränkter Modus“ bezeichnet.

Welche Datenquellen kann ich scannen, wenn ich Data Classification auf einer Site ohne Internetzugang installiere?

Der private BlueXP Modus (alte BlueXP -Schnittstelle) wird normalerweise in lokalen Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, darunter AWS Secret Cloud, AWS Top Secret Cloud und Azure IL6. NetApp unterstützt diese Umgebungen weiterhin mit der alten BlueXP Schnittstelle. Die Dokumentation zum privaten Modus in der alten BlueXP Schnittstelle finden Sie unter"PDF-Dokumentation für den privaten Modus von BlueXP" .

Die Datenklassifizierung kann nur Daten aus Datenquellen scannen, die sich lokal am Standort vor Ort befinden. Derzeit kann die Datenklassifizierung die folgenden lokalen Datenquellen im „Privatmodus“ – auch als „dunkle“ Site bezeichnet – scannen:

- On-Premises- ONTAP -Systeme
- Datenbankschemata
- Objektspeicher, der das Simple Storage Service (S3)-Protokoll verwendet

Welche Dateitypen werden unterstützt?

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`

Welche Arten von Daten und Metadaten werden durch die Datenklassifizierung erfasst?

Mit der Datenklassifizierung können Sie einen allgemeinen „Mapping“-Scan oder einen vollständigen „Klassifizierungs“-Scan Ihrer Datenquellen ausführen. Die Zuordnung bietet lediglich einen allgemeinen Überblick über Ihre Daten, während die Klassifizierung eine gründliche Überprüfung Ihrer Daten ermöglicht. Das Mapping Ihrer Datenquellen kann sehr schnell durchgeführt werden, da zum Anzeigen der darin enthaltenen Daten kein Zugriff auf Dateien erforderlich ist.

- **Datenzuordnungsscan (nur Zuordnungsscan)**: Die Datenklassifizierung scannt nur die Metadaten. Dies ist nützlich für die allgemeine Datenverwaltung und -steuerung, die schnelle Projektplanung, sehr große Grundstücke und die Priorisierung. Die Datenzuordnung basiert auf Metadaten und gilt als **schneller** Scan.

  Nach einem schnellen Scan können Sie einen Datenzuordnungsbericht erstellen. Dieser Bericht bietet eine Übersicht über die in Ihren Unternehmensdatenquellen gespeicherten Daten und unterstützt Sie bei Entscheidungen zu Ressourcennutzung, Migration, Sicherung, Sicherheit und Compliance-Prozessen.

- **Tiefenscan zur Datenklassifizierung (Map & Classify-Scan)**: Die Datenklassifizierung scannt Daten mithilfe von Standardprotokollen und schreibgeschützter Berechtigung in Ihren gesamten Umgebungen. Ausgewählte Dateien werden geöffnet und auf vertrauliche geschäftsbezogene Daten, private Informationen und Probleme im Zusammenhang mit Ransomware gescannt.

  Nach einem vollständigen Scan stehen Ihnen zahlreiche zusätzliche Datenklassifizierungsfunktionen zur Verfügung, die Sie auf Ihre Daten anwenden können, z. B. das Anzeigen und Verfeinern von Daten auf der Seite „Datenuntersuchung“, die Suche nach Namen in Dateien, das Kopieren, Verschieben und Löschen von Quelldateien und vieles mehr.

Die Datenklassifizierung erfasst Metadaten wie Dateiname, Berechtigungen, Erstellungszeit, letzter Zugriff und letzte Änderung. Dies umfasst alle Metadaten, die auf der Seite „Datenuntersuchungsdetails“ und in den Datenuntersuchungsberichten angezeigt werden.

Durch die Datenklassifizierung können viele Arten privater Daten identifiziert werden, beispielsweise personenbezogene Daten (PII) und sensible personenbezogene Daten (SPII). Einzelheiten zu privaten Daten finden Sie unterKategorien privater Daten, die von der Datenklassifizierung gescannt werden .

Kann ich die Datenklassifizierungsinformationen auf bestimmte Benutzer beschränken?

Ja, die Datenklassifizierung ist vollständig in die NetApp Console integriert. Benutzer der NetApp Console können nur Informationen zu den Systemen sehen, zu deren Anzeige sie gemäß ihren Berechtigungen berechtigt sind.

Wenn Sie außerdem bestimmten Benutzern nur das Anzeigen der Scanergebnisse zur Datenklassifizierung gestatten möchten, ohne dass sie die Datenklassifizierungseinstellungen verwalten können, können Sie diesen Benutzern die Rolle „Klassifizierungsbetrachter“ (bei Verwendung der NetApp Console im Standardmodus) oder die Rolle „Compliance-Betrachter“ (bei Verwendung der NetApp Console im eingeschränkten Modus) zuweisen. "Mehr erfahren" .

Kann jeder auf die privaten Daten zugreifen, die zwischen meinem Browser und Data Classification gesendet werden?

Nein. Die privaten Daten, die zwischen Ihrem Browser und der Datenklassifizierungsinstanz gesendet werden, sind durch eine End-to-End-Verschlüsselung mit TLS 1.2 gesichert, was bedeutet, dass sie weder von NetApp noch von NetApp Parteien gelesen werden können. Data Classification gibt keine Daten oder Ergebnisse an NetApp weiter, es sei denn, Sie fordern den Zugriff an und genehmigen ihn.

Die gescannten Daten bleiben in Ihrer Umgebung.

Wie wird mit sensiblen Daten umgegangen?

NetApp hat keinen Zugriff auf vertrauliche Daten und zeigt diese nicht in der Benutzeroberfläche an. Sensible Daten werden maskiert, bei Kreditkarteninformationen werden beispielsweise die letzten vier Ziffern angezeigt.

Wo werden die Daten gespeichert?

Die Scanergebnisse werden in Elasticsearch in Ihrer Datenklassifizierungsinstanz gespeichert.

Wie erfolgt der Zugriff auf die Daten?

Die Datenklassifizierung greift über API-Aufrufe auf in Elasticsearch gespeicherte Daten zu, die eine Authentifizierung erfordern und mit AES-128 verschlüsselt sind. Für den direkten Zugriff auf Elasticsearch ist Root-Zugriff erforderlich.

Lizenzen und Kosten

Die folgende Frage bezieht sich auf die Lizenzierung und die Kosten für die Nutzung der Datenklassifizierung.

Wie viel kostet die Datenklassifizierung?

Die Datenklassifizierung ist eine Kernfunktion der NetApp Console . Es wird nichts berechnet.

Bereitstellung des Konsolenagenten

Die folgenden Fragen beziehen sich auf den Konsolenagenten.

Was ist der Konsolenagent?

Der Konsolenagent ist eine Software, die auf einer Compute-Instanz entweder innerhalb Ihres Cloud-Kontos oder vor Ort ausgeführt wird und es der NetApp Console ermöglicht, Cloud-Ressourcen sicher zu verwalten. Sie müssen einen Konsolenagenten bereitstellen, um die Datenklassifizierung zu verwenden.

Wo muss der Konsolenagent installiert werden?

Beim Scannen von Daten muss der NetApp Console -Agent an den folgenden Speicherorten installiert werden:

- Für Cloud Volumes ONTAP in AWS oder Amazon FSx für ONTAP: Der Konsolenagent befindet sich in AWS.
- Für Cloud Volumes ONTAP in Azure oder in Azure NetApp Files: Der Konsolenagent befindet sich in Azure.
- Für Cloud Volumes ONTAP in GCP: Der Konsolenagent befindet sich in GCP.
- Für lokale ONTAP -Systeme: Der Konsolenagent befindet sich vor Ort.

Wenn Sie Daten an diesen Standorten haben, müssen Sie möglicherweise "mehrere Konsolenagenten" .

Benötigt die Datenklassifizierung Zugriff auf Anmeldeinformationen?

Die Datenklassifizierung selbst ruft keine Speicheranmeldeinformationen ab. Stattdessen werden sie im Konsolenagenten gespeichert.

Bei der Datenklassifizierung werden Anmeldeinformationen der Datenebene verwendet, beispielsweise CIFS-Anmeldeinformationen, um Freigaben vor dem Scannen bereitzustellen.

Verwendet die Kommunikation zwischen dem Dienst und dem Konsolenagenten HTTP?

Ja, die Datenklassifizierung kommuniziert über HTTP mit dem Konsolenagenten.

Bereitstellung der Datenklassifizierung

Die folgenden Fragen beziehen sich auf die separate Instanz der Datenklassifizierung.

Welche Bereitstellungsmodelle unterstützt die Datenklassifizierung?

Mit der NetApp Console kann der Benutzer Systeme praktisch überall scannen und Berichte dazu erstellen, einschließlich On-Premises-, Cloud- und Hybridumgebungen. Die Datenklassifizierung wird normalerweise mithilfe eines SaaS-Modells bereitgestellt, bei dem der Dienst über die Konsolenschnittstelle aktiviert wird und keine Hardware- oder Softwareinstallation erfordert. Auch in diesem Click-and-Run-Bereitstellungsmodus kann die Datenverwaltung unabhängig davon erfolgen, ob sich die Datenspeicher vor Ort oder in der öffentlichen Cloud befinden.

Welcher Instanz- oder VM-Typ wird für die Datenklassifizierung benötigt?

Wann"in der Cloud bereitgestellt" :

- In AWS läuft die Datenklassifizierung auf einer m6i.4xlarge-Instanz mit einer 500-GiB-GP2-Festplatte. Sie können während der Bereitstellung einen kleineren Instanztyp auswählen.

- In Azure wird die Datenklassifizierung auf einer Standard_D16s_v3-VM mit einer 500-GiB-Festplatte ausgeführt.
- In GCP läuft die Datenklassifizierung auf einer n2-standard-16-VM mit einer persistenten Standardfestplatte mit 500 GiB.

"Erfahren Sie mehr über die Funktionsweise der Datenklassifizierung" .

Kann ich die Datenklassifizierung auf meinem eigenen Host bereitstellen?

Ja. Sie können die Datenklassifizierungssoftware auf einem Linux-Host mit Internetzugang in Ihrem Netzwerk oder in der Cloud installieren. Alles funktioniert gleich und Sie verwalten Ihre Scan-Konfiguration und -Ergebnisse weiterhin über die Konsole. Sehen"Bereitstellen der Datenklassifizierung vor Ort" für Systemanforderungen und Installationsdetails.

Was ist mit sicheren Websites ohne Internetzugang?

Ja, das wird auch unterstützt. Du kannst"Bereitstellen der Datenklassifizierung an einem lokalen Standort ohne Internetzugang" für absolut sichere Websites.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

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

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

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

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

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

Datenschutzrichtlinie

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

Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

- "Hinweis zur NetApp Console"
- "Hinweis zur NetApp Data Classification"