Aktivieren Sie das Scannen Ihrer Datenquellen

NetApp Data Classification

NetApp
February 11, 2026

Inhalt

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

Amazon FSx nach ONTAP -Volumes mit NetApp Data Classification scannen

Führen Sie einige Schritte aus, um Amazon FSx mit NetApp Data Classification nach

ONTAP -Volumes zu scannen.

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.

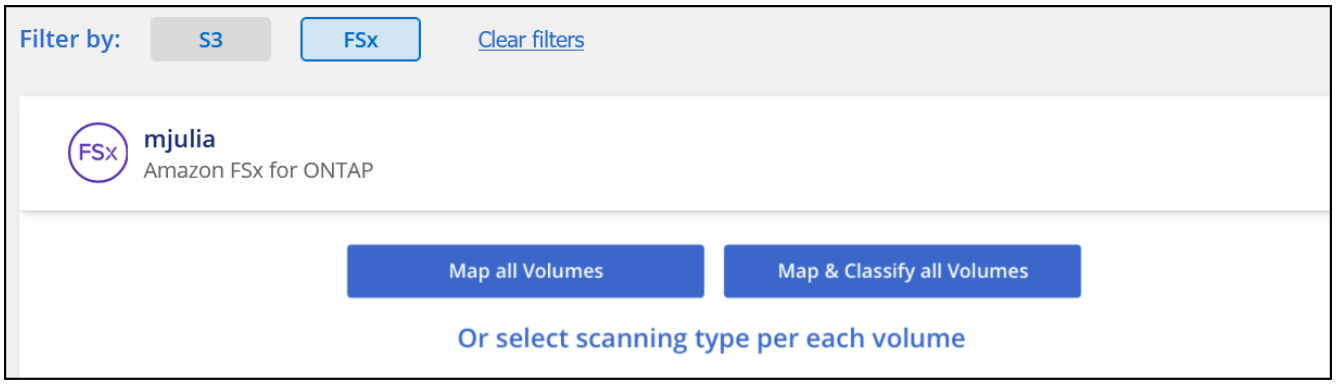
Hinweis: Die Bereitstellung der Datenklassifizierung an einem lokalen Standort wird beim Scannen von FSx-Volumes derzeit nicht unterstützt.

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. Verfolgen Sie den Fortschritt jedes Scans in der Fortschrittsleiste. Sie können mit der Maus über die Fortschrittsleiste 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.

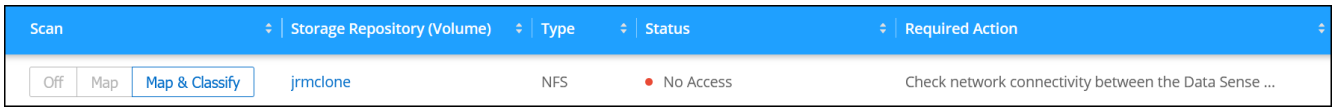
Stellen Sie sicher, dass die Datenklassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien überprüfen.

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.

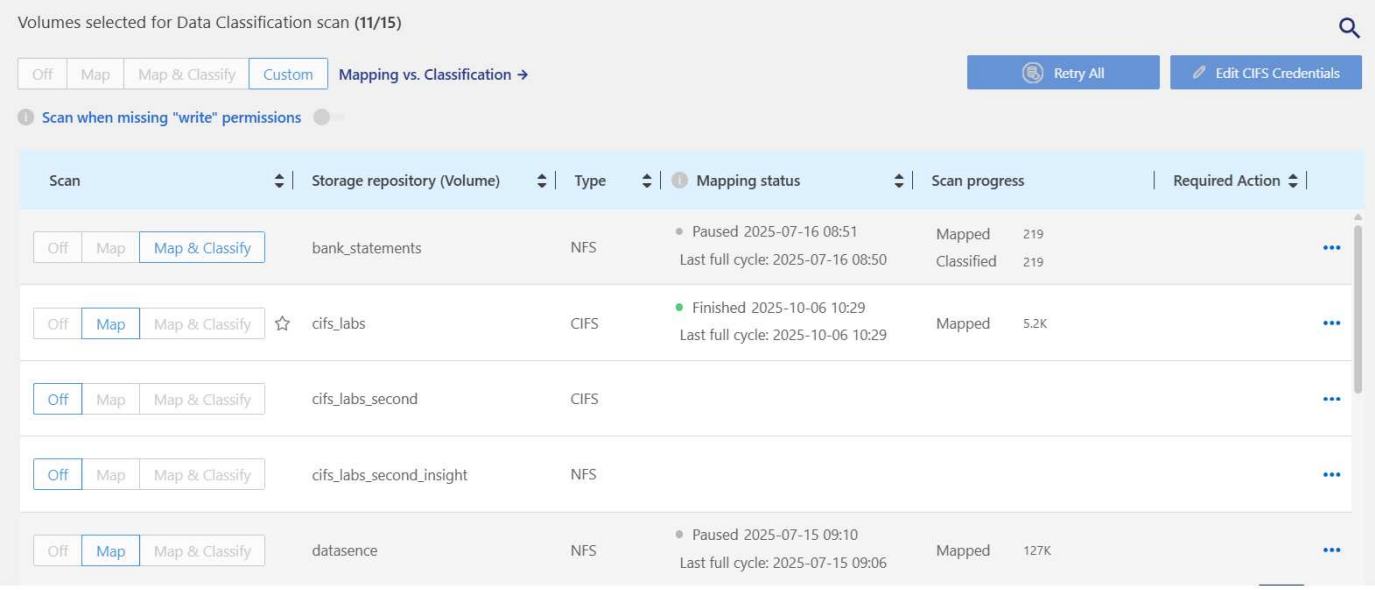
Aktivieren und Deaktivieren von Scans auf Volumes

Sie können Scans auf jedem System jederzeit von der Konfigurationsseite aus starten oder stoppen. Sie können Scans auch von reinen Mapping-Scans auf Mapping- und Klassifizierungs-Scans umstellen und umgekehrt. Es wird empfohlen, alle Volumes in einem System 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** ausgewählt 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 bei fehlenden Schreibberechtigungen** 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".

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 Einstellung für alle Volumes **Benutzerdefiniert** oder **Aus** ist, müssen Sie das Scannen für jedes neue Volume, das Sie hinzufügen, manuell aktivieren.



Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie ein System und dann **Konfiguration**.
3. Um Scans für alle Volumes zu aktivieren oder zu deaktivieren, wählen Sie in der Überschrift über allen Volumes **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus**.

   Um Scans für einzelne Volumes zu aktivieren oder zu deaktivieren, suchen Sie die Volumes in der Liste und wählen Sie dann neben dem Volumenamen **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus** aus.

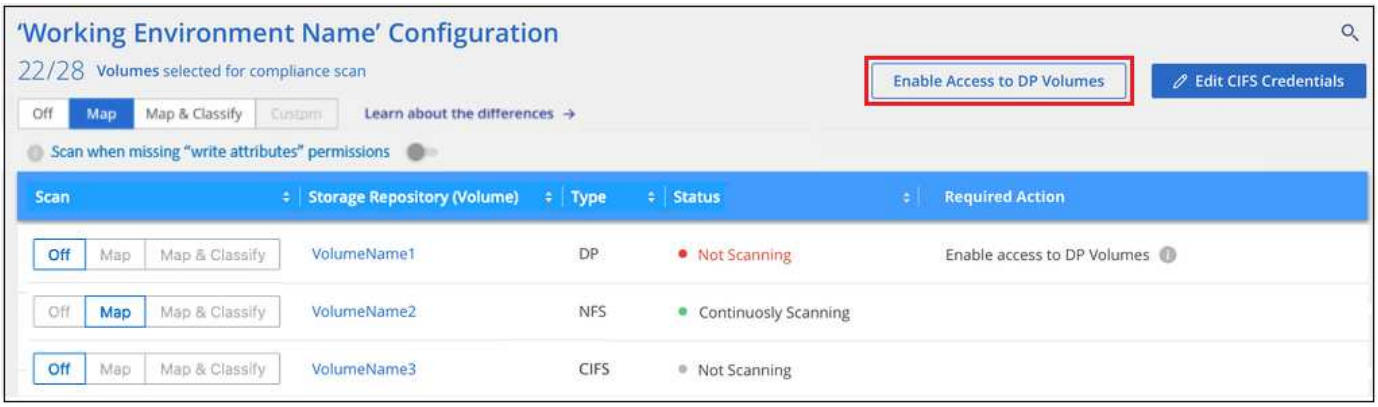
Ergebnis

Wenn Sie das Scannen aktivieren, beginnt die Datenklassifizierung 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 Dauer des Scans hängt von der Datenmenge ab und kann zwischen Minuten und Stunden liegen.

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.

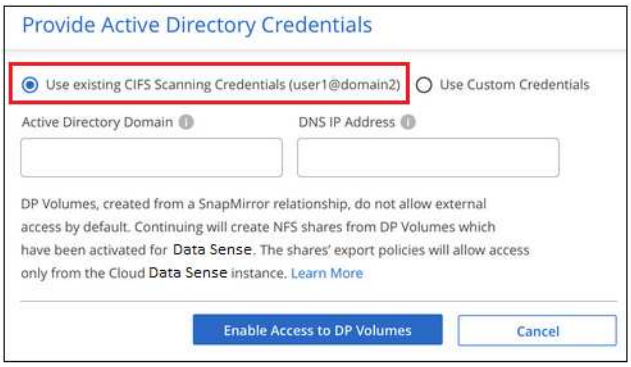
Zunächst werden diese Volumes in der Volumeliste als *Typ* **DP** mit dem *Status* **Nicht scannen** und der *Erforderlichen Aktion* **Zugriff auf DP-Volumes aktivieren** identifiziert.

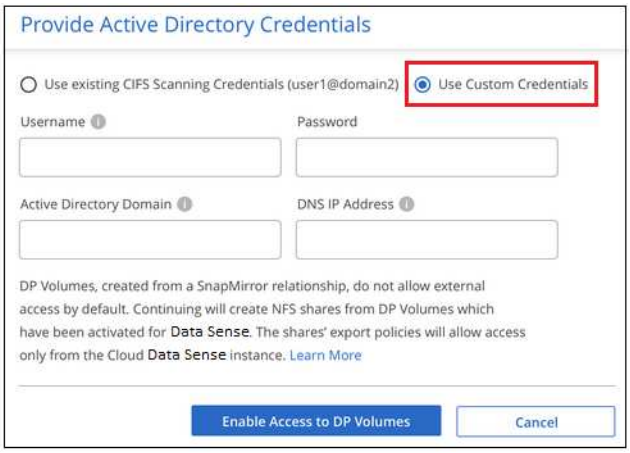


Schritte

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 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 als System in der NetApp Console vorhanden ist,"fügen Sie es auf der Seite „Systeme“ hinzu" .

Bereitstellen der Datenklassifizierungsinstanz

"Datenklassifizierung bereitstellen"wenn noch keine Instanz bereitgestellt ist.

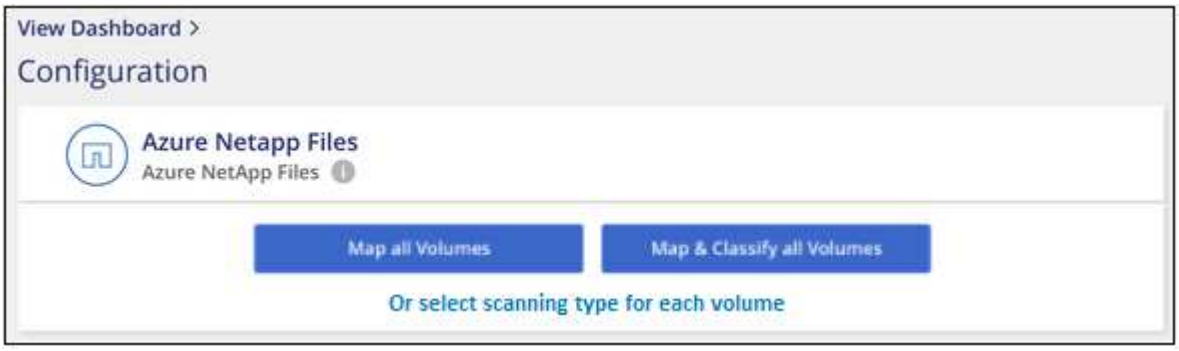
Die Datenklassifizierung muss beim Scannen von Azure NetApp Files Volumes in der Cloud bereitgestellt werden und zwar in derselben Region wie die Volumes, die Sie scannen möchten.

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 oder zuordnen und klassifizieren

möchten.

SehenAktivieren oder Deaktivieren von 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. Die Datenklassifizierung zeigt für jeden Scan einen Fortschrittsbalken an. Sie können 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

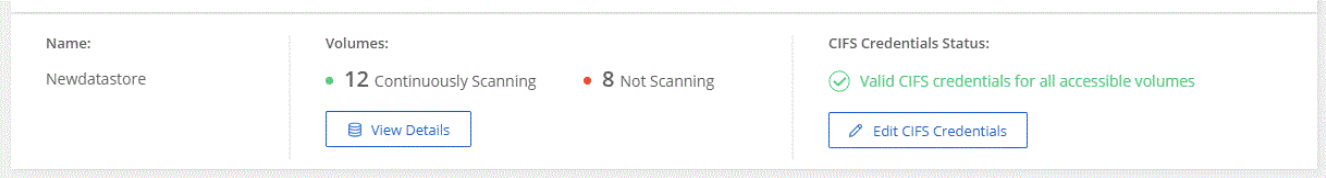
1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.

   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 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. Korrigieren Sie gegebenenfalls alle Fehler, beispielsweise Probleme mit der Netzwerkverbindung.

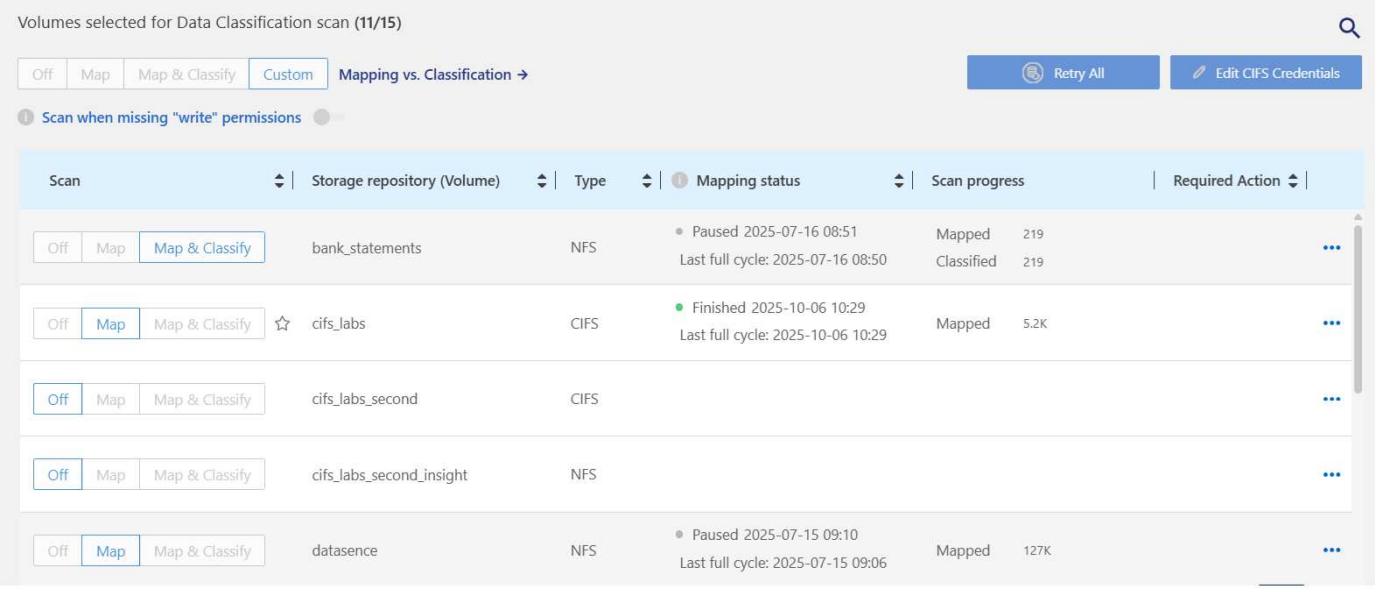
Aktivieren oder Deaktivieren von Scans auf Volumes

Sie können Scans auf jedem System jederzeit von der Konfigurationsseite aus starten oder stoppen. Sie können Scans auch von reinen Mapping-Scans auf Mapping- und Klassifizierungs-Scans umstellen und umgekehrt. Es wird empfohlen, alle Volumes in einem System 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** ausgewählt 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 bei fehlenden Schreibberechtigungen** 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".

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 Einstellung für alle Volumes **Benutzerdefiniert** oder **Aus** ist, müssen Sie das Scannen für jedes neue Volume, das Sie hinzufügen, manuell aktivieren.



Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie ein System und dann **Konfiguration**.
3. Um Scans für alle Volumes zu aktivieren oder zu deaktivieren, wählen Sie in der Überschrift über allen Volumes **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus**.

   Um Scans für einzelne Volumes zu aktivieren oder zu deaktivieren, suchen Sie die Volumes in der Liste und wählen Sie dann neben dem Volumenamen **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus** aus.

Ergebnis

Wenn Sie das Scannen aktivieren, beginnt die Datenklassifizierung 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 Dauer des Scans hängt von der Datenmenge ab und kann zwischen Minuten und Stunden liegen.

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.

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

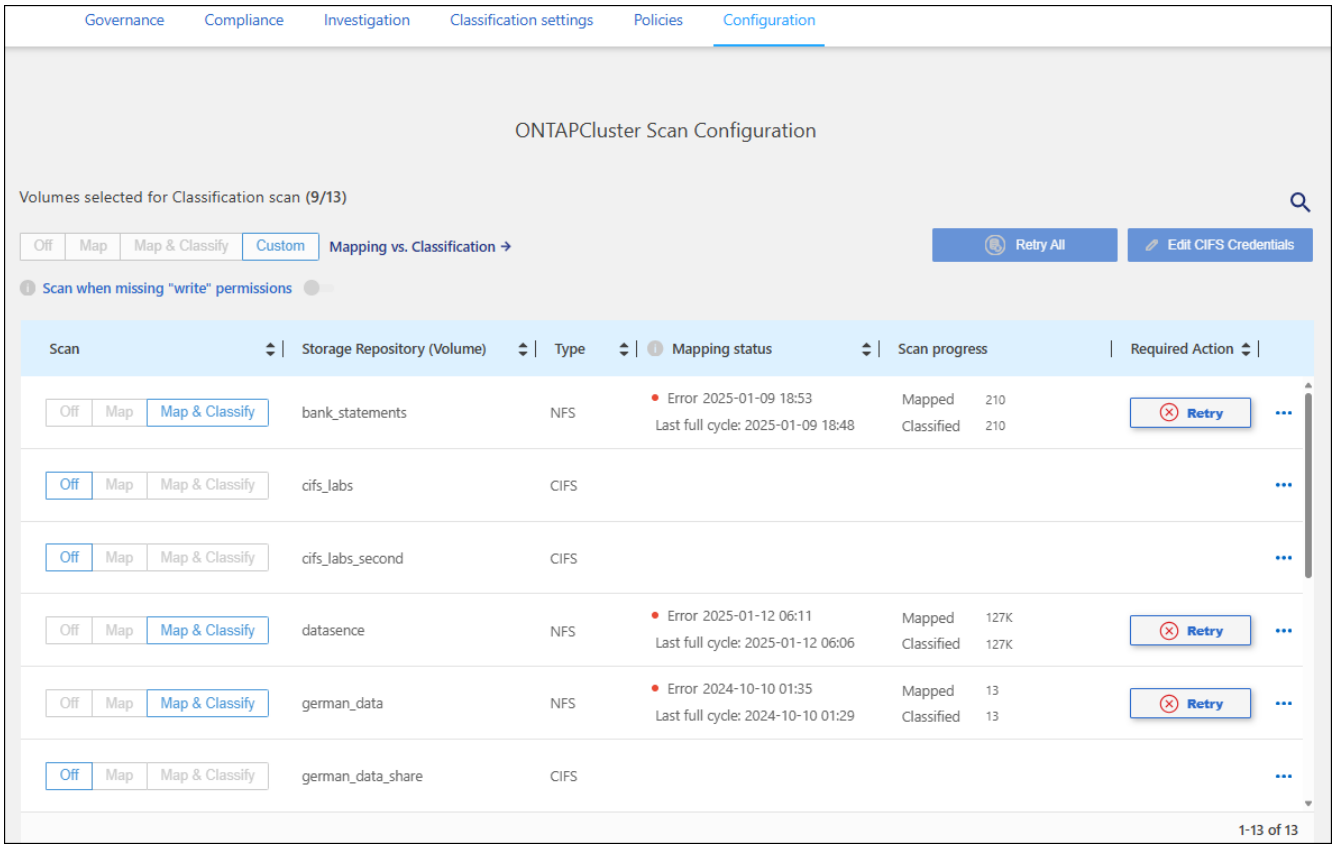
- Stellen Sie sicher, dass zwischen der Data Classification-Instanz und jedem Netzwerk, das Volumes für Cloud Volumes ONTAP oder lokale ONTAP Cluster enthält, eine Netzwerkverbindung besteht.
- Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr von der Data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



2. 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, 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.

Wenn Sie die Anmeldeinformationen korrekt eingegeben haben, bestätigt eine Meldung, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.

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

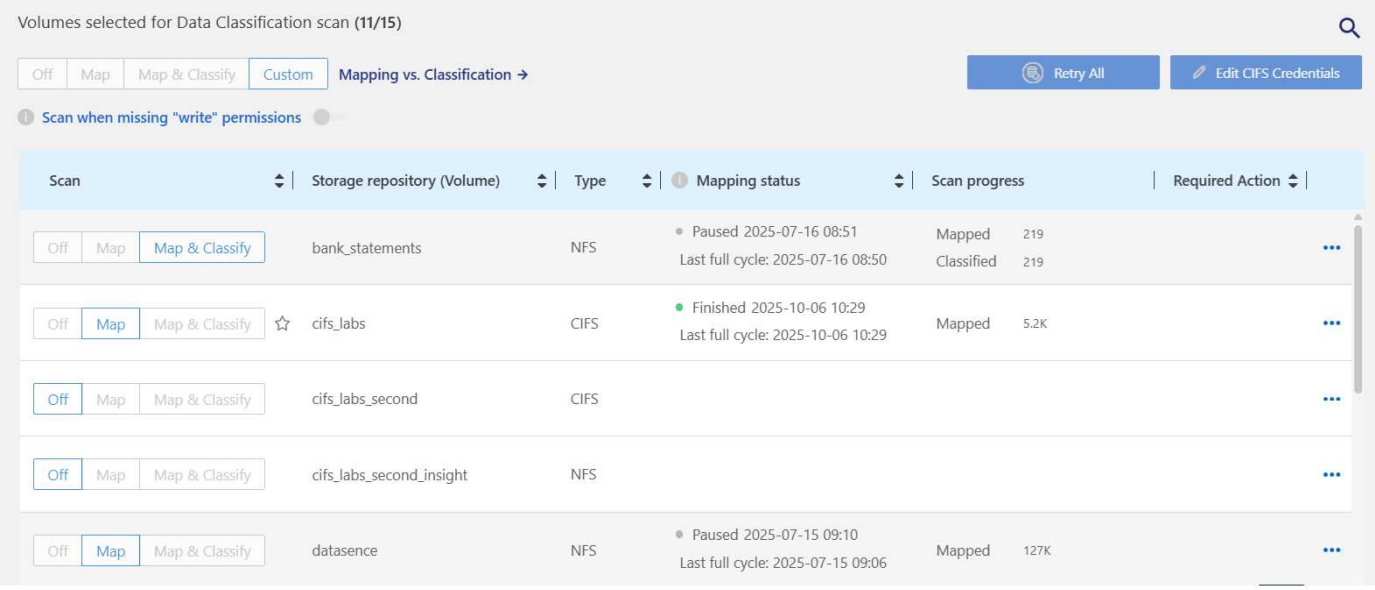
Aktivieren oder Deaktivieren von Scans auf Volumes

Sie können Scans auf jedem System jederzeit von der Konfigurationsseite aus starten oder stoppen. Sie können Scans auch von reinen Mapping-Scans auf Mapping- und Klassifizierungs-Scans umstellen und umgekehrt. Es wird empfohlen, alle Volumes in einem System 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** ausgewählt 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 bei fehlenden Schreibberechtigungen** 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".

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 Einstellung für alle Volumes **Benutzerdefiniert** oder **Aus** ist, müssen Sie das Scannen für jedes neue Volume, das Sie hinzufügen, manuell aktivieren.



Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie ein System und dann **Konfiguration**.
3. Um Scans für alle Volumes zu aktivieren oder zu deaktivieren, wählen Sie in der Überschrift über allen Volumes **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus**.

   Um Scans für einzelne Volumes zu aktivieren oder zu deaktivieren, suchen Sie die Volumes in der Liste und wählen Sie dann neben dem Volumenamen **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus** aus.

Ergebnis

Wenn Sie das Scannen aktivieren, beginnt die Datenklassifizierung 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 Dauer des Scans hängt von der Datenmenge ab und kann zwischen Minuten und Stunden liegen.

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" .

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" .

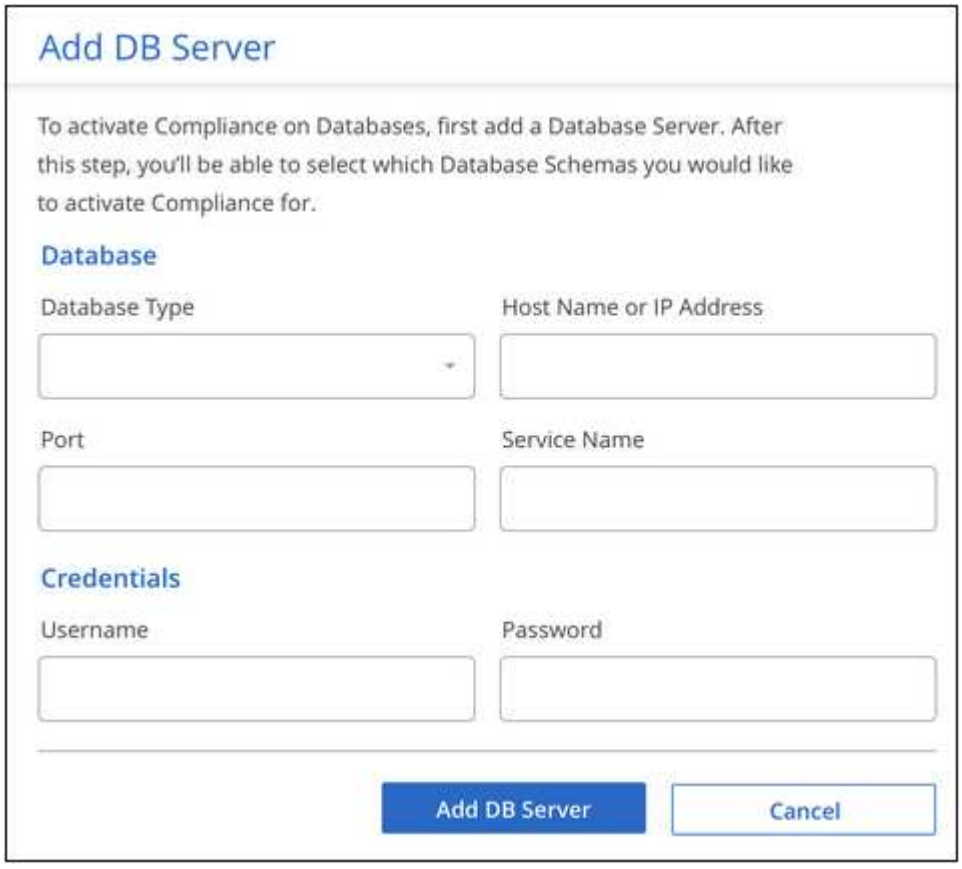
Wenn Sie Datenbankschemata scannen, die in einer Dark Site ohne Internetzugang installiert wurden, müssen Sie"Stellen Sie die Datenklassifizierung am selben lokalen Standort bereit, der keinen Internetzugang hat" . Dies erfordert auch, dass der Konsolenagent am selben lokalen Standort bereitgestellt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

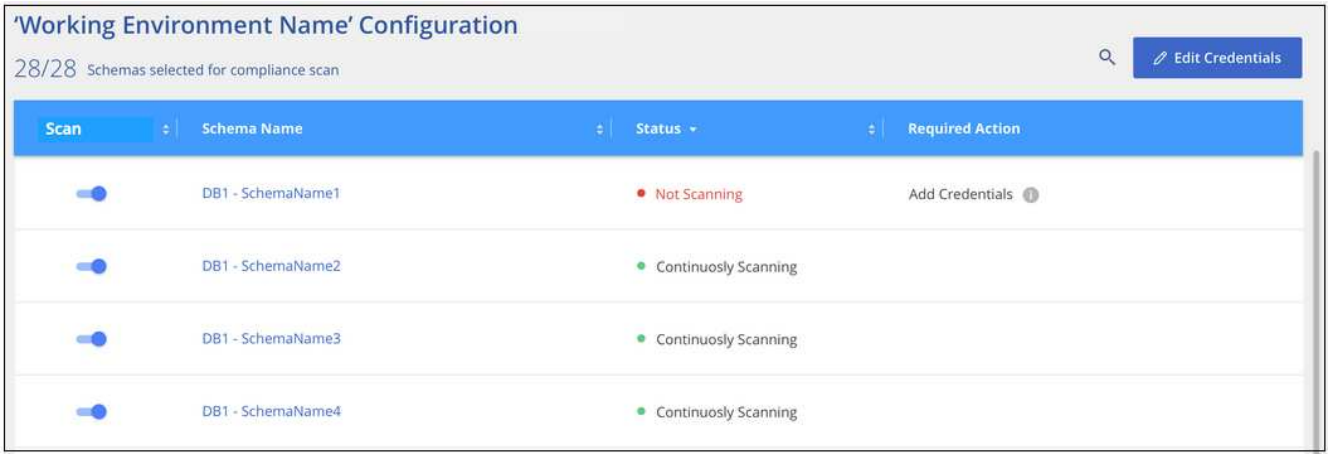
Aktivieren und Deaktivieren von Scans für Datenbankschemata

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 den erforderlichen Maßnahmen 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.

Google Cloud NetApp Volumes mit NetApp Data Classification scannen

NetApp Data Classification unterstützt Google Cloud NetApp Volumes als System. Erfahren Sie, wie Sie Ihr Google Cloud NetApp Volumes -System scannen.

Ermitteln Sie das Google Cloud NetApp Volumes -System, das Sie scannen möchten

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

Bereitstellen der Datenklassifizierungsinstanz

"Datenklassifizierung bereitstellen"wenn noch keine Instanz bereitgestellt ist.

Beim Scannen von Google Cloud NetApp Volumes muss die Datenklassifizierung 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 Google Cloud NetApp Volumes derzeit nicht unterstützt.

Aktivieren Sie die Datenklassifizierung in Ihren Systemen

Sie können die Datenklassifizierung auf Ihrem Google Cloud NetApp Volumes -System 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 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: einige Minuten bis einige Stunden. Sie können den Fortschritt des ersten Scans im Abschnitt **Systemkonfiguration** des Menüs **Konfiguration** verfolgen. Die Datenklassifizierung zeigt für jeden Scan einen Fortschrittsbalken an. 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. Für CIFS-Volumes müssen Sie die Datenklassifizierung mit CIFS-Anmeldeinformationen bereitstellen.

Bei Google Cloud NetApp Volumes 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 Google Cloud NetApp Volumes 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

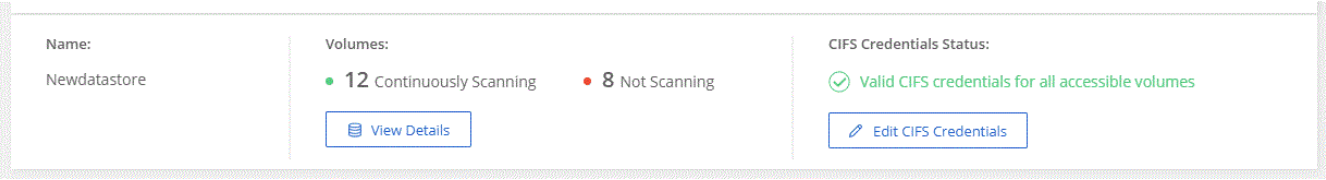
1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.

   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.

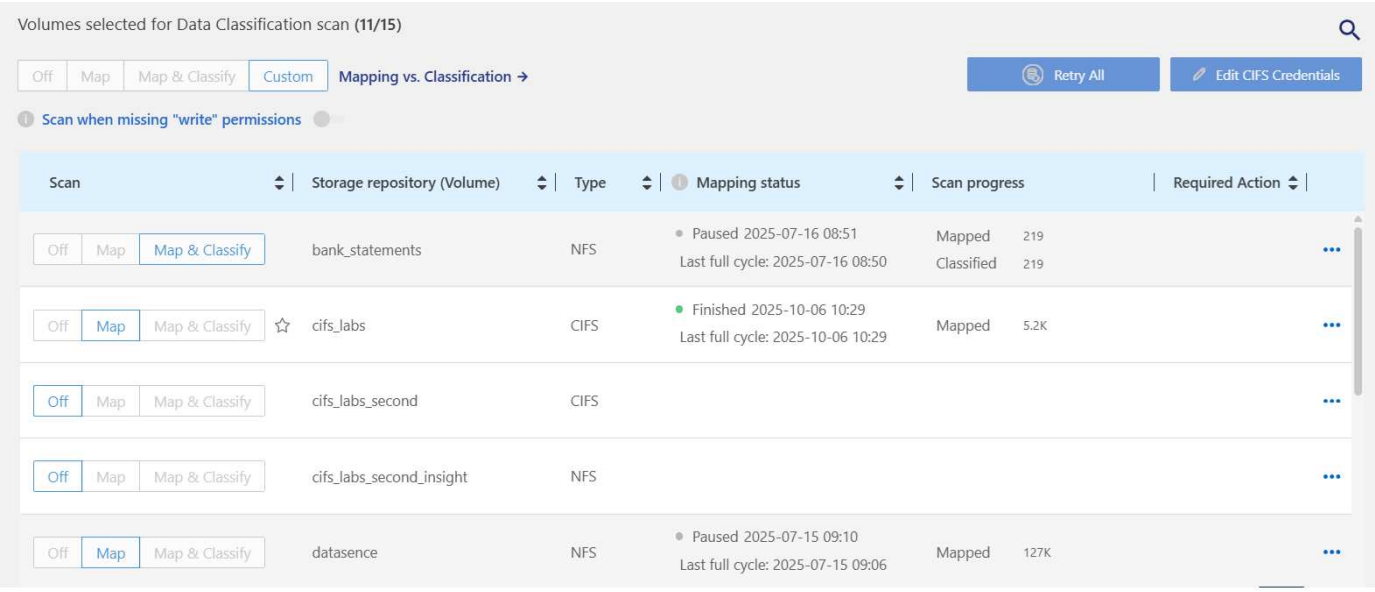
Aktivieren und Deaktivieren von Scans auf Volumes

Sie können Scans auf jedem System jederzeit von der Konfigurationsseite aus starten oder stoppen. Sie können Scans auch von reinen Mapping-Scans auf Mapping- und Klassifizierungs-Scans umstellen und umgekehrt. Es wird empfohlen, alle Volumes in einem System 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** ausgewählt 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 bei fehlenden Schreibberechtigungen** 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".

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 Einstellung für alle Volumes **Benutzerdefiniert** oder **Aus** ist, müssen Sie das Scannen für jedes neue Volume, das Sie hinzufügen, manuell aktivieren.



Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie ein System und dann **Konfiguration**.
3. Um Scans für alle Volumes zu aktivieren oder zu deaktivieren, wählen Sie in der Überschrift über allen Volumes **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus**.

   Um Scans für einzelne Volumes zu aktivieren oder zu deaktivieren, suchen Sie die Volumes in der Liste und wählen Sie dann neben dem Volumenamen **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus** aus.

Ergebnis

Wenn Sie das Scannen aktivieren, beginnt die Datenklassifizierung 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 Dauer des Scans hängt von der Datenmenge ab und kann zwischen Minuten und Stunden liegen.

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.

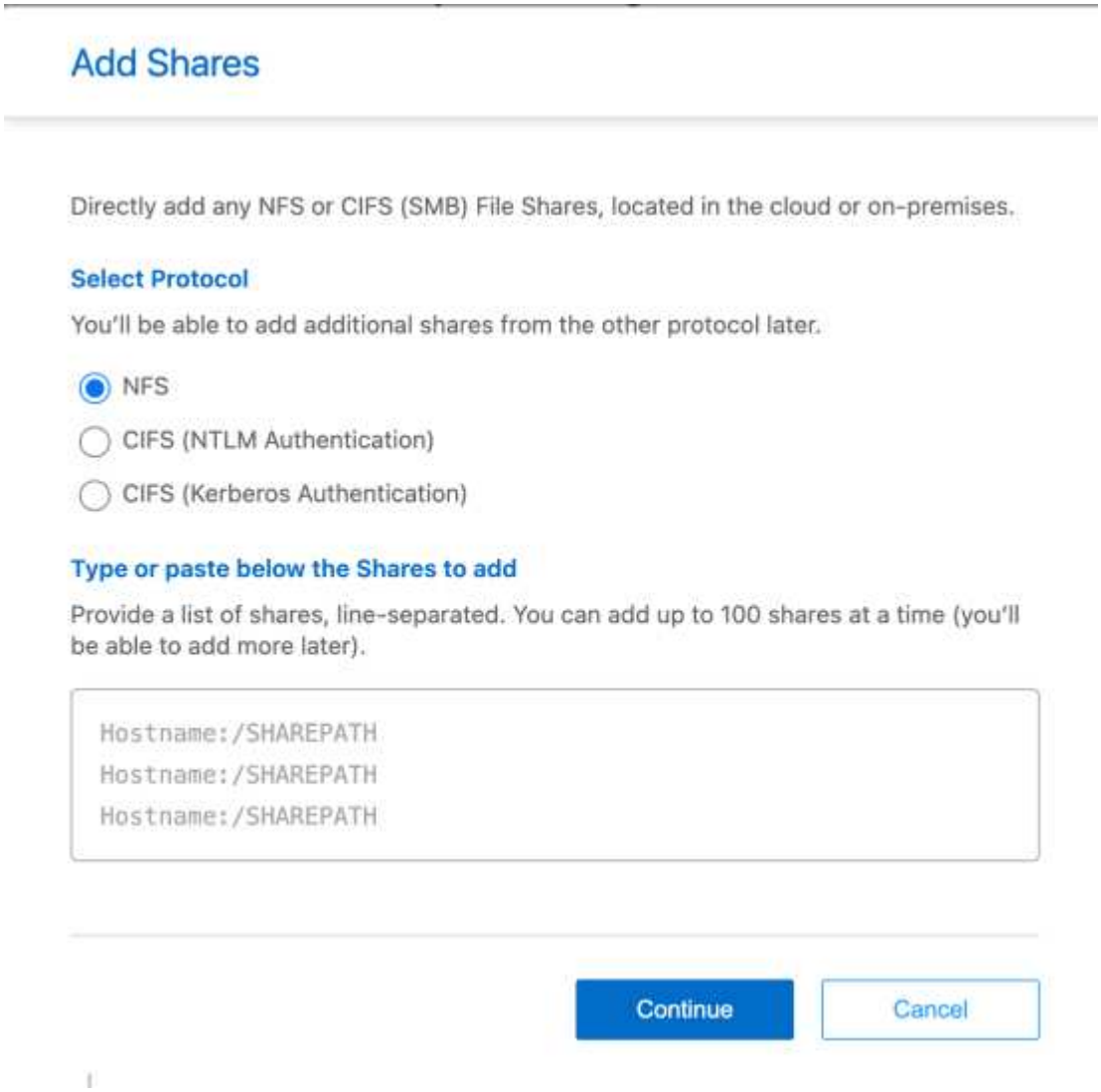
Erstellen einer Dateifreigabegruppe

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.

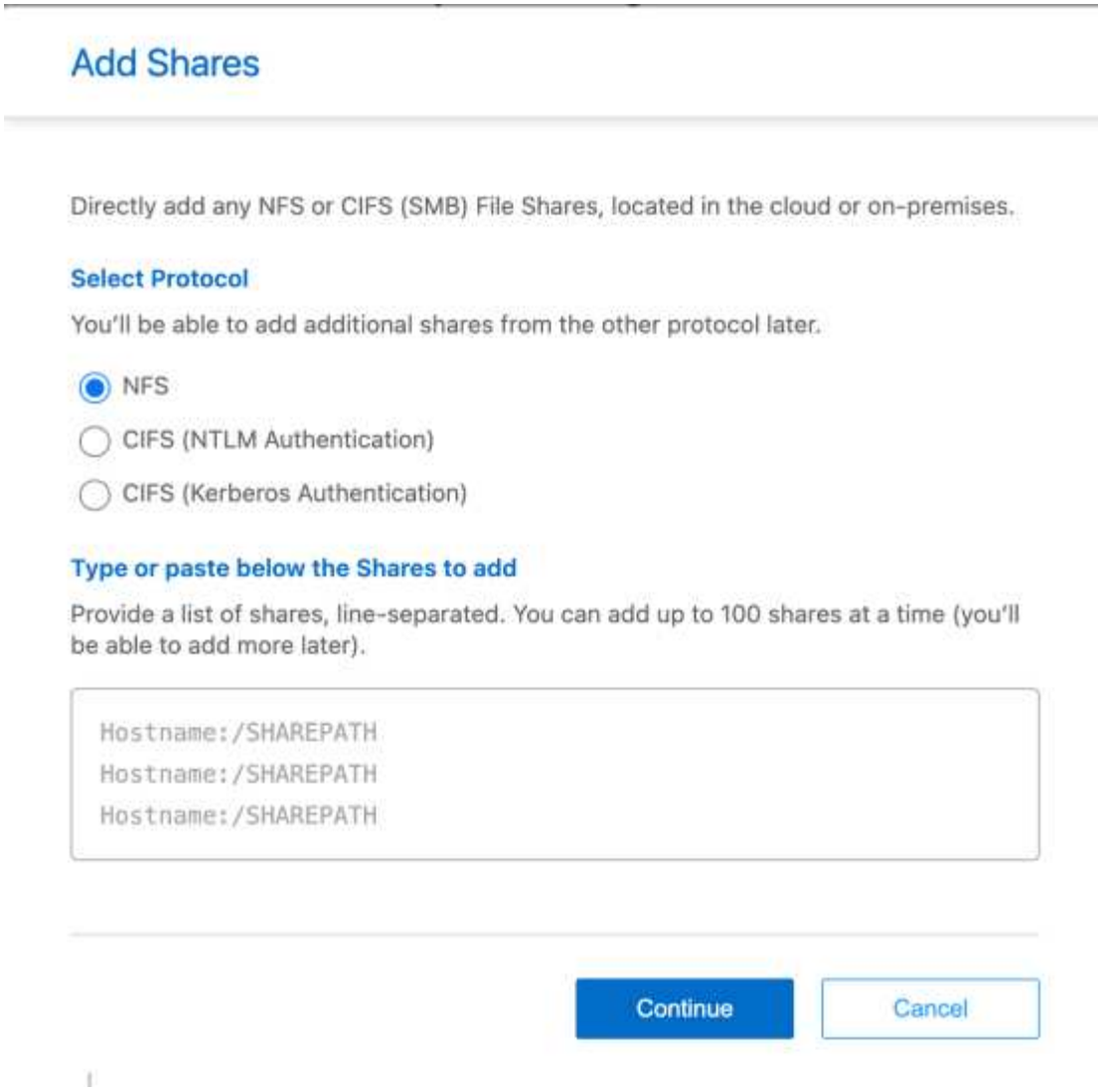
Bearbeiten Sie die CIFS-Protokollkonfiguration

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 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 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.

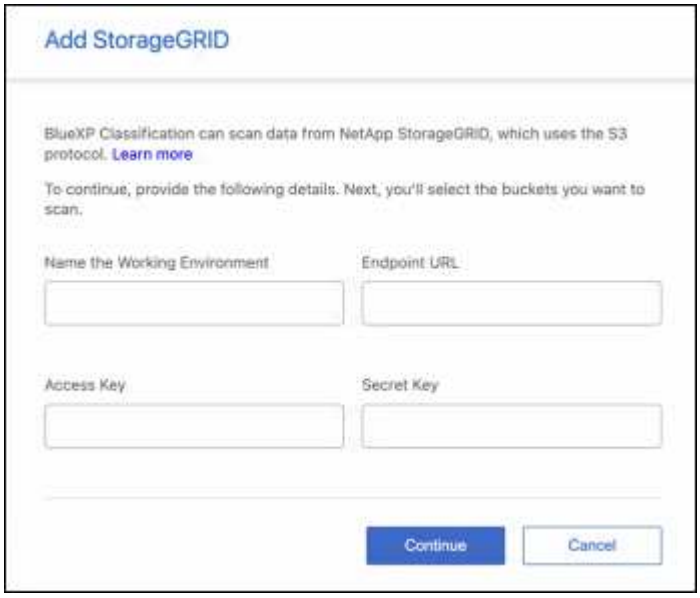
Fügen Sie den StorageGRID -Dienst zur Datenklassifizierung hinzu

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 Scans auf 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.