



Aktivieren Sie das Scannen Ihrer Datenquellen

BlueXP classification

NetApp
July 25, 2024

Inhalt

- Aktivieren Sie das Scannen Ihrer Datenquellen. 1
 - Erste Schritte mit der BlueXP Klassifizierung für Cloud Volumes ONTAP und lokale ONTAP 1
 - Erste Schritte mit der BlueXP Klassifizierung für Azure NetApp Files 8
 - Erste Schritte mit der BlueXP Klassifizierung für Amazon FSX for ONTAP. 13
- Datenbankschemas scannen. 19
- Scannen von Dateifreigaben 22

Aktivieren Sie das Scannen Ihrer Datenquellen

Erste Schritte mit der BlueXP Klassifizierung für Cloud Volumes ONTAP und lokale ONTAP

Führen Sie ein paar Schritte durch und beginnen Sie mit der Überprüfung Ihrer Cloud Volumes ONTAP und lokalen ONTAP Volumes mithilfe der BlueXP Klassifizierung.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1

Ermitteln Sie die Datenquellen, die Sie scannen möchten

Bevor Sie Volumes scannen können, müssen Sie die Systeme als Arbeitsumgebung in BlueXP hinzufügen:

- Bei Cloud Volumes ONTAP-Systemen sollten diese Arbeitsumgebungen bereits in BlueXP zur Verfügung stehen
- Für On-Premises-ONTAP-Systeme bietet die ["BlueXP muss die ONTAP Cluster ermitteln"](#)

2

Implementieren der BlueXP Klassifizierungsinstanz

["Implementieren Sie die BlueXP Klassifizierung"](#) Falls noch keine Instanz implementiert wurde.

3

Aktivieren Sie die BlueXP Klassifizierung und wählen Sie die zu scannenden Volumes aus

Wählen Sie die Registerkarte **Configuration** und aktivieren Sie Compliance-Scans nach Volumes in bestimmten Arbeitsumgebungen.

4

Zugriff auf Volumes sicherstellen

Nachdem die BlueXP Klassifizierung aktiviert ist, vergewissern Sie sich jetzt, dass sie auf alle Volumes zugreifen kann.

- Die BlueXP Klassifizierungsinstanz benötigt eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder zu jedem lokalen ONTAP System.
- Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen von der BlueXP Klassifizierungsinstanz ermöglichen.
- Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind:
 - Für NFS - die Ports 111 und 2049.
 - Für CIFS - Ports 139 und 445.
- NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.
- Die BlueXP Klassifizierung erfordert Active Directory Zugangsdaten, um CIFS-Volumes zu scannen.

Klicken Sie auf **Compliance > Konfiguration > CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an.

5

Verwalten Sie die Volumes, die Sie scannen möchten

Wählen Sie die Volumes aus, die Sie scannen möchten, oder deaktivieren Sie sie. Die BlueXP Klassifizierung startet bzw. stoppt die Suche.

Ermitteln der Datenquellen, die gescannt werden sollen

Wenn sich die zu scannenden Datenquellen nicht bereits in Ihrer BlueXP-Umgebung befinden, können Sie diese zu diesem Zeitpunkt zur Leinwand hinzufügen.

Ihre Cloud Volumes ONTAP-Systeme sollten bereits auf dem Canvas in BlueXP verfügbar sein. Bei ONTAP Systemen vor Ort ist ein muss erforderlich ["BlueXP ermittelt diese Cluster"](#).

Implementieren der BlueXP Klassifizierungsinstanz

Implementieren Sie die BlueXP Klassifizierung, falls noch keine Instanz implementiert ist.

Wenn Sie Cloud Volumes ONTAP und lokale ONTAP Systeme scannen, die über das Internet zugänglich sind, können Sie diese ausführen ["Implementieren Sie die BlueXP Klassifizierung in der Cloud"](#) Oder ["In einer Anlage mit Internetzugang"](#).

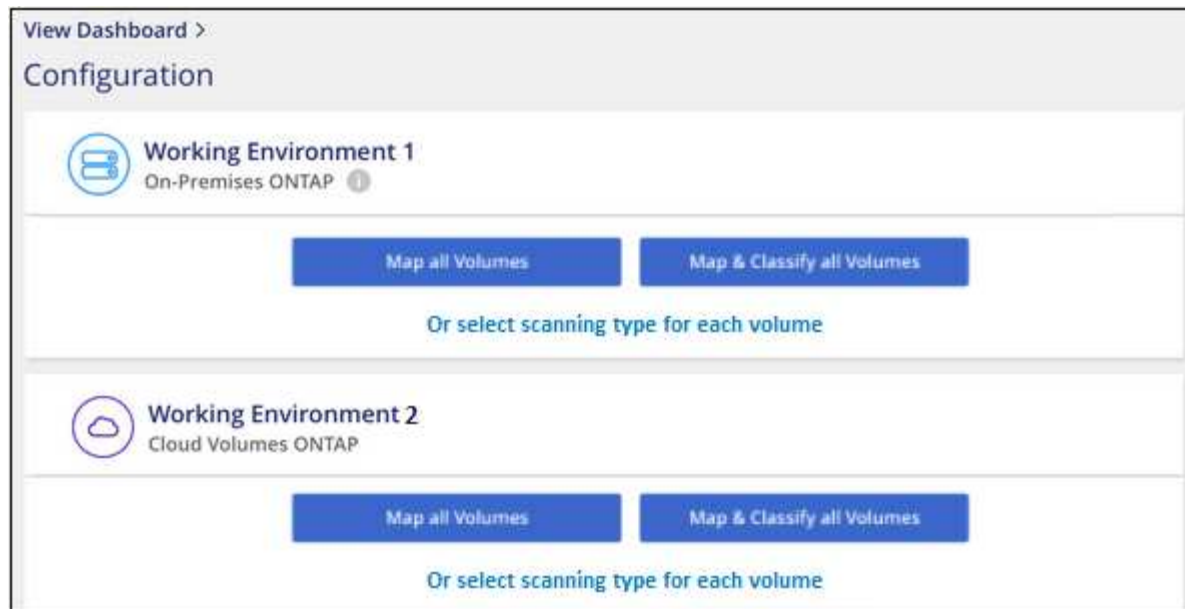
Wenn Sie lokale ONTAP-Systeme scannen, die in einer dunklen Site installiert wurden und über keinen Internetzugang verfügen, müssen Sie sie überprüfen ["Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang"](#). Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Ermöglichen der BlueXP Klassifizierung in Ihren Arbeitsumgebungen

Sie können die BlueXP Klassifizierung auf Cloud Volumes ONTAP Systemen auf jedem unterstützten Cloud-Provider oder auf lokalen ONTAP Clustern aktivieren.

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.



2. Wählen Sie aus, wie die Volumes in den einzelnen Arbeitsumgebungen gescannt werden sollen. ["Hier erfahren Sie mehr über Mapping und Klassifizierungsmessungen"](#):
 - Um alle Volumes zuzuordnen, klicken Sie auf **Alle Volumes zuordnen**.
 - Um alle Bände zu ordnen und zu klassifizieren, klicken Sie auf **Karte & alle Bände klassifizieren**.
 - Um den Scan für jedes Volume anzupassen, klicken Sie auf **oder wählen Sie für jedes Volume** den Scantyp aus, und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

Siehe [Aktivieren und Deaktivieren von Compliance-Scans auf Volumes](#) Entsprechende Details.

3. Klicken Sie im Bestätigungsdiaologfeld auf **approve**, damit die BlueXP Klassifizierung mit dem Scannen Ihrer Volumes beginnt.

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen in der Arbeitsumgebung ausgewählten Volumes. Sobald die ersten Scans durch die BlueXP-Klassifizierung abgeschlossen sind, werden die Ergebnisse im Compliance-Dashboard verfügbar sein. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.



- Wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, scannt das System standardmäßig nicht die Dateien in Ihren Volumes, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, klicken Sie auf **oder wählen Sie den Scantyp für jedes Volume** aus. Die resultierende Seite verfügt über eine Einstellung, die Sie aktivieren können, sodass die BlueXP Klassifizierung die Volumes unabhängig von ihren Berechtigungen scannt.
- Die BlueXP Klassifizierung scannt nur eine Datei-Freigabe unter einem Volume. Wenn Sie mehrere Freigaben in Ihren Volumes haben, müssen Sie diese anderen Freigaben separat als Gruppe „Freigaben“ scannen. ["Weitere Informationen zu dieser BlueXP Klassifizierungsbeschränkung"](#).

Überprüfung, ob die BlueXP Klassifizierung Zugriff auf Volumes hat

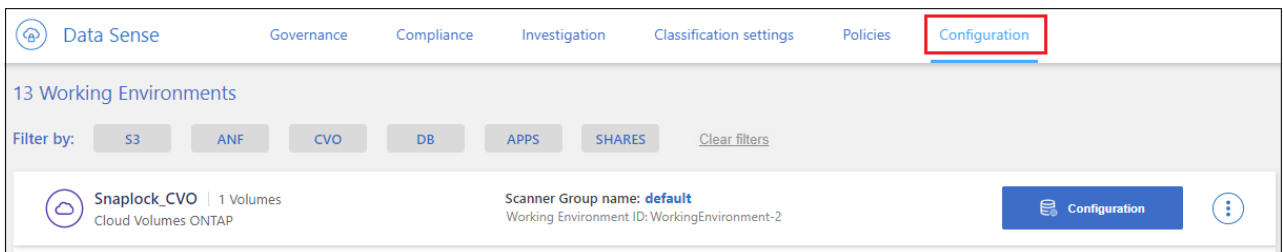
Vergewissern Sie sich, dass die BlueXP Klassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen und Exportrichtlinien prüfen. Sie müssen BlueXP mit CIFS-Anmeldedaten klassifizieren, um auf CIFS Volumes zugreifen zu können.

Schritte

1. Stellen Sie sicher, dass eine Netzwerkverbindung zwischen der BlueXP Klassifizierungsinstanz und jedem Netzwerk, das Volumes für Cloud Volumes ONTAP- oder lokale ONTAP-Cluster umfasst, besteht.
2. Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr von der BlueXP Klassifizierungsinstanz zulässt.

Sie können die Sicherheitsgruppe für Datenverkehr von der IP-Adresse der BlueXP Klassifizierungsinstanz öffnen oder Sie können die Sicherheitsgruppe für den gesamten Datenverkehr innerhalb des virtuellen Netzwerks öffnen.

3. Stellen Sie sicher, dass die folgenden Ports für die BlueXP Klassifizierungsinstanz offen sind:
 - Für NFS - die Ports 111 und 2049.
 - Für CIFS - Ports 139 und 445.
4. Vergewissern Sie sich, dass die Richtlinien für den Export von NFS Volumes die IP-Adresse der BlueXP Klassifizierungsinstanz enthalten, damit sie auf die Daten auf jedem Volume zugreifen können.
5. Wenn Sie CIFS verwenden, bieten Sie BlueXP Klassifizierung mit Active Directory Anmeldeinformationen, um CIFS Volumes zu scannen.
 - a. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.

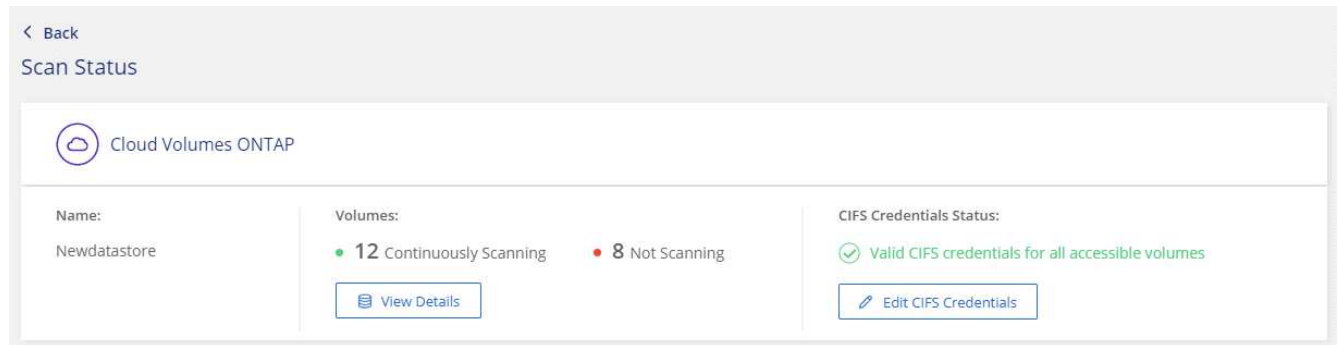


- b. Klicken Sie für jede Arbeitsumgebung auf **Edit CIFS Credentials** und geben Sie den Benutzernamen und das Passwort ein, die die BlueXP Klassifizierung für den Zugriff auf CIFS Volumes auf dem System benötigt.

Die Zugangsdaten können schreibgeschützt sein, aber durch die Angabe von Administratorberechtigungen wird sichergestellt, dass die BlueXP Klassifizierung alle Daten lesen kann, die erhöhte Berechtigungen erfordern. Die Zugangsdaten werden in der BlueXP Klassifizierungsinstanz gespeichert.

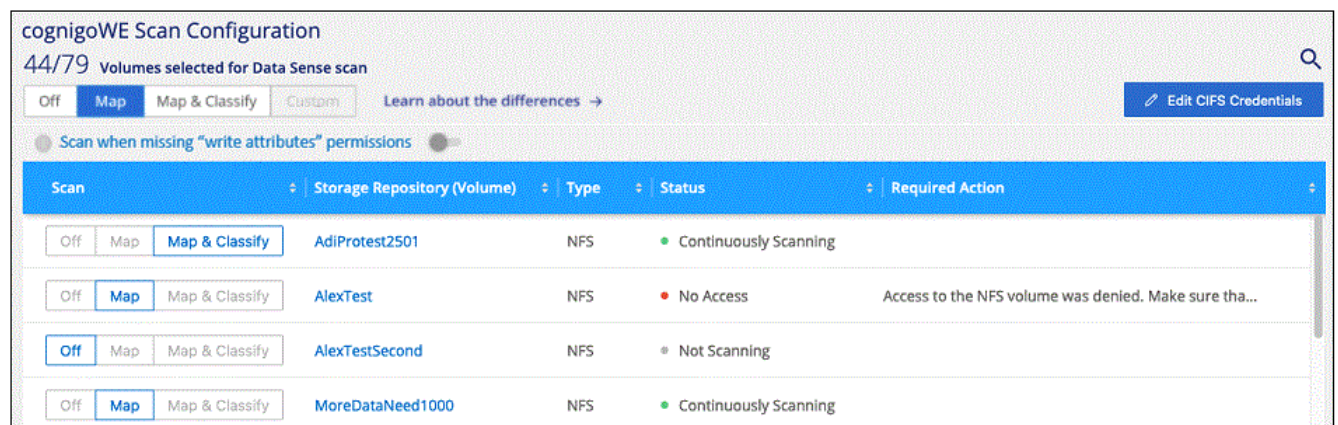
Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

Nach Eingabe der Anmeldedaten sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.



6. Klicken Sie auf der Seite *Configuration* auf **Details anzeigen**, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und eventuelle Fehler zu beheben.

Das folgende Bild zeigt beispielsweise vier Volumes. Eine davon kann aufgrund von Netzwerkverbindungsproblemen zwischen der BlueXP Klassifizierungsinstanz und dem Volume nicht mit der BlueXP Klassifizierung gescannt werden.



Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

Sie können jederzeit auf der Konfigurationsseite Scans oder Scans von nur-Zuordnungen oder Klassifizierungen in einer Arbeitsumgebung starten oder stoppen. Sie können auch von mappingonly Scans zu Mapping- und Klassifizierungsscans und umgekehrt wechseln. Wir empfehlen, alle Volumes zu scannen.

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung 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 EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. ["Weitere Informationen"](#)

cognigoWE Scan Configuration
44/79 Volumes selected for Data Sense scan

Off
Map
Map & Classify
Custom
Learn about the differences →
Edit CIFS Credentials

☐ Scan when missing "write attributes" permissions

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning	
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning	

An:	Tun Sie dies:
Aktivieren von mappinggeschützten Scans auf einem Volume	Klicken Sie im Volumenbereich auf Karte
Aktivieren Sie das vollständige Scannen auf einem Volume	Klicken Sie im Volumenbereich auf Karte & Klassieren
Deaktivieren Sie das Scannen auf einem Volume	Klicken Sie im Volumenbereich auf aus
Aktivieren Sie ausschließlich mappingbare Scans auf allen Volumes	Klicken Sie im Steuerkursbereich auf Karte
Aktivieren Sie das vollständige Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf Karte & Klassieren
Deaktivieren Sie das Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf aus



Neue Volumes, die der Arbeitsumgebung hinzugefügt wurden, werden automatisch nur gescannt, wenn Sie die Einstellung **Karte** oder **Karte & Klassieren** im Steuerkursbereich festgelegt haben. Wenn Sie im Bereich Überschrift auf **Benutzerdefiniert** oder **aus** eingestellt sind, müssen Sie für jedes neue Volumen, das Sie in der Arbeitsumgebung hinzufügen, das Mapping und/oder das vollständige Scannen aktivieren.

Scannen von Datensicherungs-Volumes

Datensicherung-Volumes werden standardmäßig nicht gescannt, da sie nicht extern offengelegt werden und die BlueXP Klassifizierung kann nicht auf sie zugreifen. Es handelt sich dabei um Ziel-Volumes für SnapMirror Vorgänge von einem ONTAP System vor Ort oder von einem Cloud Volumes ONTAP System aus.

Zunächst erkennt die Volume-Liste diese Volumes als *Type DP* mit dem *Status Not Scanning* und der *required Action Enable Access to DP Volumes*.

'Working Environment Name' Configuration

22/28 Volumes selected for compliance scan

Enable Access to DP Volumes [Edit CIFS Credentials](#)

Off **Map** Map & Classify Custom [Learn about the differences](#) →

☐ Scan when missing "write attributes" permissions ☐

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	VolumeName1	DP	Not Scanning	Enable access to DP Volumes ⓘ
Off Map Map & Classify	VolumeName2	NFS	Continuously Scanning	
Off Map Map & Classify	VolumeName3	CIFS	Not Scanning	

Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

1. Klicken Sie oben auf der Seite auf **Zugriff auf DP-Volumes aktivieren**.
2. Überprüfen Sie die Bestätigungsmeldung und klicken Sie erneut auf **Zugriff auf DP-Volumes**.
 - Volumes, die anfangs als NFS Volumes im ONTAP Quellsystem erstellt wurden, sind aktiviert.
 - Für Volumes, die ursprünglich als CIFS Volumes im Quell-ONTAP System erstellt wurden, müssen Sie die CIFS-Anmeldeinformationen eingeben, um diese DP-Volumes zu scannen. Wenn Sie bereits Active Directory-Anmeldedaten eingegeben haben, sodass die BlueXP Klassifizierung CIFS-Volumes scannen kann, können Sie diese Anmeldedaten verwenden oder einen anderen Satz von Admin-Anmeldedaten angeben.

Provide Active Directory Credentials

☒ Use existing CIFS Scanning Credentials (user1@domain2) ☐ Use Custom Credentials

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for **Data Sense**. The shares' export policies will allow access only from the Cloud **Data Sense** instance. [Learn More](#)

Enable Access to DP Volumes Cancel

Provide Active Directory Credentials

☐ Use existing CIFS Scanning Credentials (user1@domain2) ☒ Use Custom Credentials

Username ⓘ Password

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for **Data Sense**. The shares' export policies will allow access only from the Cloud **Data Sense** instance. [Learn More](#)

Enable Access to DP Volumes Cancel

3. Aktivieren Sie jedes zu scannenden DP-Volume [Auf die gleiche Weise haben Sie andere Volumes aktiviert](#).

Ergebnis

Nach Aktivierung erstellt die BlueXP Klassifizierung von jedem DP-Volume, das zum Scannen aktiviert wurde, eine NFS-Freigabe. Die Richtlinien für den Export von Freigaben sind nur für den Zugriff aus der BlueXP Klassifizierungsinstanz zulässig.

Hinweis: Wenn Sie beim ersten Aktivieren des Zugriffs auf DP-Volumes keine CIFS-Datenschutzvolumes hatten und später noch etwas hinzufügen, erscheint oben auf der Konfigurationsseite die Schaltfläche **Zugriff auf CIFS DP aktivieren**. Klicken Sie auf diese Schaltfläche, und fügen Sie CIFS-Anmeldeinformationen hinzu, um den Zugriff auf diese CIFS-DP-Volumes zu ermöglichen.



Active Directory – Zugangsdaten sind nur in der Storage-VM des ersten CIFS-DP Volumes registriert. Somit werden alle DP-Volumes auf dieser SVM gescannt. Auf allen Volumes, die sich auf anderen SVMs befinden, sind keine Active Directory Anmeldedaten registriert, daher werden diese DP-Volumes nicht gescannt.

Erste Schritte mit der BlueXP Klassifizierung für Azure NetApp Files

Führen Sie einige Schritte für den Einstieg in die BlueXP Klassifizierung für Azure NetApp Files durch.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1

Entdecken Sie die Azure NetApp Files-Systeme, die Sie scannen möchten

Vor dem Scannen von Azure NetApp Files-Volumes ["BlueXP muss eingerichtet sein, um die Konfiguration zu ermitteln"](#).

2

Implementieren der BlueXP Klassifizierungsinstanz

["Implementieren Sie die BlueXP Klassifizierung in BlueXP"](#) Falls noch keine Instanz implementiert wurde.

3

Aktivieren Sie die BlueXP Klassifizierung und wählen Sie die zu scannenden Volumes aus

Klicken Sie auf **Compliance**, wählen Sie die Registerkarte **Konfiguration** und aktivieren Sie Compliance-Scans für Volumes in bestimmten Arbeitsumgebungen.

4

Zugriff auf Volumes sicherstellen

Nachdem die BlueXP Klassifizierung aktiviert ist, vergewissern Sie sich jetzt, dass sie auf alle Volumes zugreifen kann.

- Die BlueXP Klassifizierungsinstanz benötigt eine Netzwerkverbindung zu jedem Azure NetApp Files Subnetz.
- Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind:
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
- NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.
- Die BlueXP Klassifizierung erfordert Active Directory Zugangsdaten, um CIFS-Volumes zu scannen.

Klicken Sie auf **Compliance > Konfiguration > CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an.

Verwalten Sie die Volumes, die Sie scannen möchten

Wählen Sie die Volumes aus, die Sie scannen möchten, oder deaktivieren Sie sie. Die BlueXP Klassifizierung startet bzw. stoppt die Suche.

Ermitteln des Azure NetApp Files-Systems, das Sie scannen möchten

Wenn sich das zu scannenden Azure NetApp Files-System nicht bereits in BlueXP als Arbeitsumgebung befindet, können Sie es zu diesem Zeitpunkt der Arbeitsfläche hinzufügen.

["Erfahren Sie, wie Sie das Azure NetApp Files-System in BlueXP entdecken"](#).

Implementieren der BlueXP Klassifizierungsinstanz

["Implementieren Sie die BlueXP Klassifizierung"](#) Falls noch keine Instanz implementiert wurde.

Die BlueXP Klassifizierung muss bei der Überprüfung von Azure NetApp Files Volumes in der Cloud bereitgestellt werden und muss in derselben Region wie die Volumes bereitgestellt werden, die Sie scannen möchten.

Hinweis: die Implementierung der BlueXP Klassifizierung an einem lokalen Standort wird derzeit beim Scannen von Azure NetApp Files Volumes nicht unterstützt.

Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Ermöglichen der BlueXP Klassifizierung in Ihren Arbeitsumgebungen

Die BlueXP Klassifizierung für Ihre Azure NetApp Files Volumes kann aktiviert werden.

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.



2. Wählen Sie aus, wie die Volumes in den einzelnen Arbeitsumgebungen gescannt werden sollen. ["Hier erfahren Sie mehr über Mapping und Klassifizierungsmessungen"](#):
 - Um alle Volumes zuzuordnen, klicken Sie auf **Alle Volumes zuordnen**.
 - Um alle Bände zu ordnen und zu klassifizieren, klicken Sie auf **Karte & alle Bände klassifizieren**.
 - Um den Scan für jedes Volume anzupassen, klicken Sie auf **oder wählen Sie für jedes Volume** den Scantyp aus, und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

Siehe [Aktivieren und Deaktivieren von Compliance-Scans auf Volumes](#) Entsprechende Details.

3. Klicken Sie im Bestätigungsdialogfeld auf **approve**, damit die BlueXP Klassifizierung mit dem Scannen Ihrer Volumes beginnt.

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen in der Arbeitsumgebung ausgewählten Volumes. Sobald die ersten Scans durch die BlueXP-Klassifizierung abgeschlossen sind, werden die Ergebnisse im Compliance-Dashboard verfügbar sein. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.



- Wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, scannt das System standardmäßig nicht die Dateien in Ihren Volumes, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, klicken Sie auf **oder wählen Sie den Scantyp für jedes Volume** aus. Die resultierende Seite verfügt über eine Einstellung, die Sie aktivieren können, sodass die BlueXP Klassifizierung die Volumes unabhängig von ihren Berechtigungen scannt.
- Die BlueXP Klassifizierung scannt nur eine Datei-Freigabe unter einem Volume. Wenn Sie mehrere Freigaben in Ihren Volumes haben, müssen Sie diese anderen Freigaben separat als Gruppe „Freigaben“ scannen. ["Weitere Informationen zu dieser BlueXP Klassifizierungsbeschränkung"](#).

Überprüfung, ob die BlueXP Klassifizierung Zugriff auf Volumes hat

Vergewissern Sie sich, dass die BlueXP Klassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen und Exportrichtlinien prüfen. Sie müssen BlueXP mit CIFS-Anmeldedaten klassifizieren, um auf CIFS Volumes zugreifen zu können.

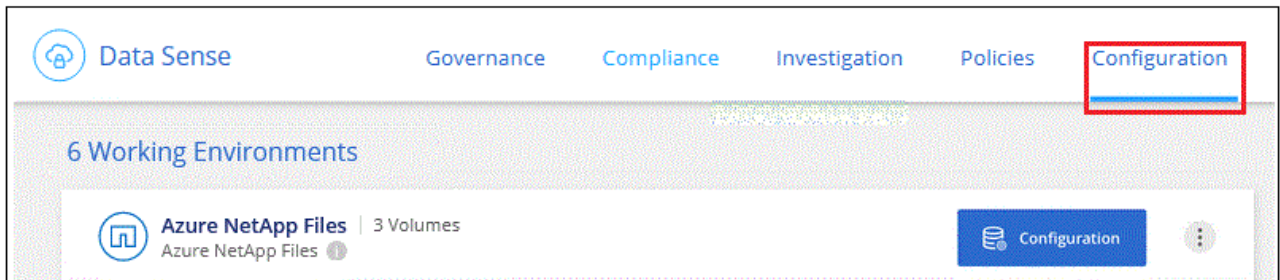
Schritte

1. Stellen Sie sicher, dass eine Netzwerkverbindung zwischen der BlueXP Klassifizierungsinstanz und jedem Netzwerk, das Volumes für Azure NetApp Files umfasst, besteht.



Bei Azure NetApp Files kann die BlueXP Klassifizierung nur Volumes scannen, die sich in derselben Region wie BlueXP befinden.

2. Stellen Sie sicher, dass die folgenden Ports für die BlueXP Klassifizierungsinstanz offen sind:
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
3. Vergewissern Sie sich, dass die Richtlinien für den Export von NFS Volumes die IP-Adresse der BlueXP Klassifizierungsinstanz enthalten, damit sie auf die Daten auf jedem Volume zugreifen können.
4. Wenn Sie CIFS verwenden, bieten Sie BlueXP Klassifizierung mit Active Directory Anmeldeinformationen, um CIFS Volumes zu scannen.
 - a. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.

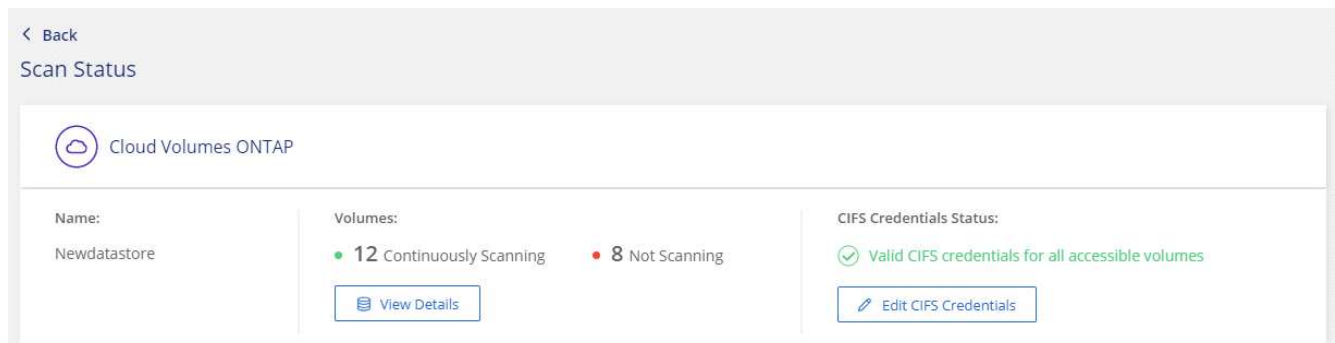


- b. Klicken Sie für jede Arbeitsumgebung auf **Edit CIFS Credentials** und geben Sie den Benutzernamen und das Passwort ein, die die BlueXP Klassifizierung für den Zugriff auf CIFS Volumes auf dem System benötigt.

Die Zugangsdaten können schreibgeschützt sein, aber durch die Angabe von Administratorberechtigungen wird sichergestellt, dass die BlueXP Klassifizierung alle Daten lesen kann, die erhöhte Berechtigungen erfordern. Die Zugangsdaten werden in der BlueXP Klassifizierungsinstanz gespeichert.

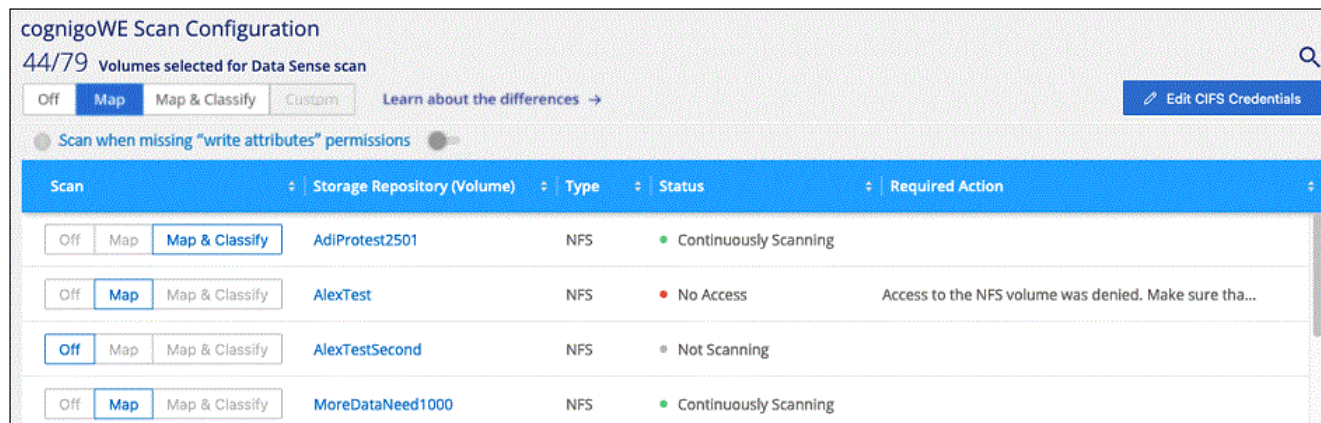
Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

Nach Eingabe der Anmeldedaten sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.



5. Klicken Sie auf der Seite *Configuration* auf **Details anzeigen**, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und eventuelle Fehler zu beheben.

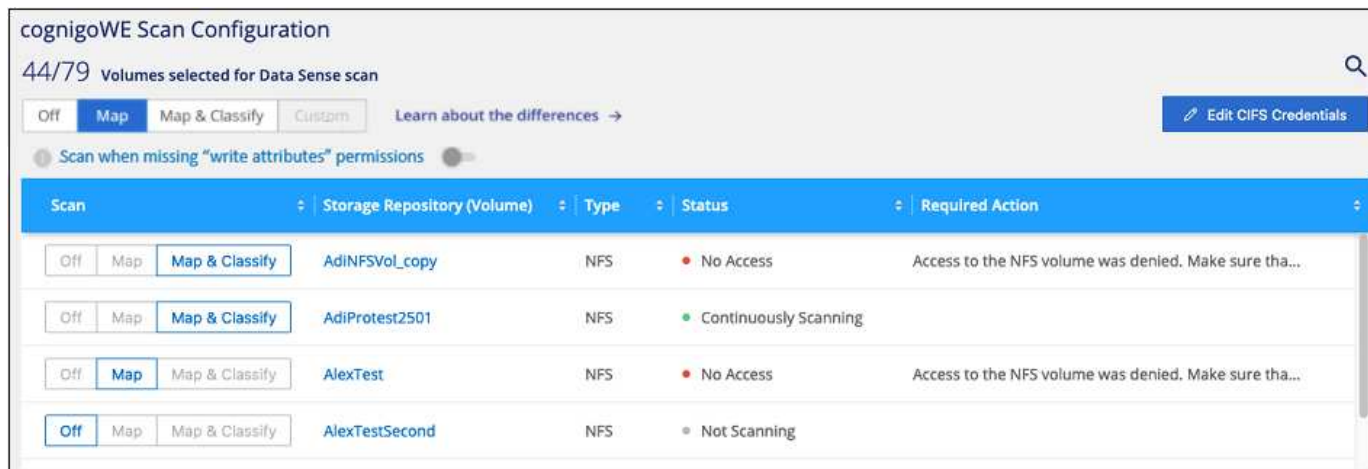
Das folgende Bild zeigt beispielsweise vier Volumes. Eine davon kann aufgrund von Netzwerkverbindungsproblemen zwischen der BlueXP Klassifizierungsinstanz und dem Volume nicht mit der BlueXP Klassifizierung gescannt werden.



Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

Sie können jederzeit auf der Konfigurationsseite Scans oder Scans von nur-Zuordnungen oder Klassifizierungen in einer Arbeitsumgebung starten oder stoppen. Sie können auch von mappingonly Scans zu Mapping- und Klassifizierungsscans und umgekehrt wechseln. Wir empfehlen, alle Volumes zu scannen.

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung 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 EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. ["Weitere Informationen"](#).



An:	Tun Sie dies:
Aktivieren von mappinggeschützten Scans auf einem Volume	Klicken Sie im Volumenbereich auf Karte
Aktivieren Sie das vollständige Scannen auf einem Volume	Klicken Sie im Volumenbereich auf Karte & Klassieren
Deaktivieren Sie das Scannen auf einem Volume	Klicken Sie im Volumenbereich auf aus
Aktivieren Sie ausschließlich mappingbare Scans auf allen Volumes	Klicken Sie im Steuerkursbereich auf Karte

An:	Tun Sie dies:
Aktivieren Sie das vollständige Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf Karte & Klassieren
Deaktivieren Sie das Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf aus



Neue Volumes, die der Arbeitsumgebung hinzugefügt wurden, werden automatisch nur gescannt, wenn Sie die Einstellung **Karte** oder **Karte & Klassieren** im Steuerkursbereich festgelegt haben. Wenn Sie im Bereich Überschrift auf **Benutzerdefiniert** oder **aus** eingestellt sind, müssen Sie für jedes neue Volumen, das Sie in der Arbeitsumgebung hinzufügen, das Mapping und/oder das vollständige Scannen aktivieren.

Erste Schritte mit der BlueXP Klassifizierung für Amazon FSX für ONTAP

Führen Sie ein paar Schritte durch, um zu beginnen, Amazon FSX für ONTAP Volumes mit BlueXP Klassifizierung zu scannen.

Bevor Sie beginnen

- Sie benötigen einen aktiven Connector in AWS für die Implementierung und das Management der BlueXP Klassifizierung.
- Die beim Erstellen der Arbeitsumgebung ausgewählte Sicherheitsgruppe muss Datenverkehr von der BlueXP Klassifizierungsinstanz zulassen. Sie können die zugehörige Sicherheitsgruppe mithilfe der ENI finden, die mit dem FSX für ONTAP-Dateisystem verbunden ist, und es mit der AWS-Verwaltungskonsolle bearbeiten.

["AWS Sicherheitsgruppen für Linux Instanzen"](#)

["AWS Sicherheitsgruppen für Windows Instanzen"](#)

["Elastische AWS Netzwerkschnittstellen \(ENI\)"](#)

Schnellstart

Führen Sie die folgenden Schritte aus, oder scrollen Sie nach unten, um weitere Informationen zu erhalten.

1

Entdecken Sie die FSX für ONTAP-Dateisysteme, die Sie scannen möchten

Bevor Sie FSX für ONTAP Volumes scannen können, ["Sie benötigen eine FSX-Arbeitsumgebung mit konfigurierten Volumes"](#).

2

Implementieren der BlueXP Klassifizierungsinstanz

["Implementieren Sie die BlueXP Klassifizierung in BlueXP"](#) Falls noch keine Instanz implementiert wurde.

3

Aktivieren Sie die BlueXP Klassifizierung und wählen Sie die zu scannenden Volumes aus

Wählen Sie die Registerkarte **Configuration** und aktivieren Sie Compliance-Scans nach Volumes in bestimmten Arbeitsumgebungen.

4

Zugriff auf Volumes sicherstellen

Nachdem die BlueXP Klassifizierung aktiviert ist, vergewissern Sie sich jetzt, dass sie auf alle Volumes zugreifen kann.

- Die BlueXP Klassifizierungsinstanz benötigt eine Netzwerkverbindung zu jedem FSX for ONTAP Subnetz.
- Stellen Sie sicher, dass die folgenden Ports für die BlueXP Klassifizierungsinstanz offen sind:
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
- NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.
- Die BlueXP Klassifizierung erfordert Active Directory Zugangsdaten, um CIFS-Volumes zu scannen. + Klicken Sie auf **Compliance > Konfiguration > CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an.

5

Verwalten Sie die Volumes, die Sie scannen möchten

Wählen Sie die Volumes aus, die Sie scannen möchten, oder deaktivieren Sie sie. Die BlueXP Klassifizierung startet bzw. stoppt ihre Suche.

Erkennung des FSX für ONTAP-Dateisystems, das Sie scannen möchten

Wenn das Dateisystem FSX für ONTAP, das Sie scannen möchten, nicht bereits in BlueXP als Arbeitsumgebung vorhanden ist, können Sie es zu diesem Zeitpunkt der Arbeitsfläche hinzufügen.

["Lesen Sie, wie Sie das Dateisystem FSX für ONTAP in BlueXP erkennen oder erstellen"](#).

Implementieren der BlueXP Klassifizierungsinstanz

["Implementieren Sie die BlueXP Klassifizierung"](#) Falls noch keine Instanz implementiert wurde.

Sie sollten die BlueXP Klassifizierung im selben AWS-Netzwerk implementieren wie der Connector für AWS und die FSX Volumes, die Sie scannen möchten.

Hinweis: die Implementierung der BlueXP Klassifizierung an einem lokalen Standort wird derzeit beim Scannen von FSX Volumes nicht unterstützt.

Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Ermöglichen der BlueXP Klassifizierung in Ihren Arbeitsumgebungen

Sie können die BlueXP Klassifizierung für FSX for ONTAP Volumes aktivieren.


1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.

Filter by:

S3

FSx

[Clear filters](#)


mjulia
Amazon FSx for ONTAP

Map all Volumes

Map & Classify all Volumes

Or select scanning type per each volume

- Wählen Sie aus, wie die Volumes in den einzelnen Arbeitsumgebungen gescannt werden sollen. "[Hier erfahren Sie mehr über Mapping und Klassifizierungsmessungen](#)":
 - Um alle Volumes zuzuordnen, klicken Sie auf **Alle Volumes zuordnen**.
 - Um alle Bände zu ordnen und zu klassifizieren, klicken Sie auf **Karte & alle Bände klassifizieren**.
 - Um den Scan für jedes Volume anzupassen, klicken Sie auf **oder wählen Sie für jedes Volume** den Scantyp aus, und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

Siehe [Aktivieren und Deaktivieren von Compliance-Scans auf Volumes](#) Entsprechende Details.

- Klicken Sie im Bestätigungsdialogfeld auf **approve**, damit die BlueXP Klassifizierung mit dem Scannen Ihrer Volumes beginnt.

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen in der Arbeitsumgebung ausgewählten Volumes. Sobald die ersten Scans durch die BlueXP-Klassifizierung abgeschlossen sind, werden die Ergebnisse im Compliance-Dashboard verfügbar sein. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.



- Wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, scannt das System standardmäßig nicht die Dateien in Ihren Volumes, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, klicken Sie auf **oder wählen Sie den Scantyp für jedes Volume** aus. Die resultierende Seite verfügt über eine Einstellung, die Sie aktivieren können, sodass die BlueXP Klassifizierung die Volumes unabhängig von ihren Berechtigungen scannt.
- Die BlueXP Klassifizierung scannt nur eine Datei-Freigabe unter einem Volume. Wenn Sie mehrere Freigaben in Ihren Volumes haben, müssen Sie diese anderen Freigaben separat als Gruppe „Freigaben“ scannen. "[Weitere Informationen zu dieser BlueXP Klassifizierungsbeschränkung](#)".

Überprüfung, ob die BlueXP Klassifizierung Zugriff auf Volumes hat

Sorgen Sie dafür, dass die BlueXP Klassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen und Exportrichtlinien prüfen.

Sie müssen BlueXP mit CIFS-Anmeldedaten klassifizieren, um auf CIFS Volumes zugreifen zu können.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf **Details anzeigen**, um den Status zu überprüfen und Fehler zu beheben.

Das folgende Bild zeigt beispielsweise, dass eine Klassifizierung von Volume BlueXP aufgrund von Netzwerkverbindungsproblemen zwischen der BlueXP Klassifizierungsinstanz und dem Volume nicht scannen kann.

Scan	Storage Repository (Volume)	Type	Status	Required Action
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	jrmclone	NFS	● No Access	Check network connectivity between the Data Sense ...

2. Stellen Sie sicher, dass zwischen der BlueXP Klassifizierungsinstanz und jedem Netzwerk, das Volumes für FSX für ONTAP umfasst, eine Netzwerkverbindung besteht.



Bei FSX for ONTAP kann die BlueXP Klassifizierung Volumes nur in derselben Region wie BlueXP scannen.

3. Stellen Sie sicher, dass die folgenden Ports für die BlueXP Klassifizierungsinstanz offen sind.
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
4. Vergewissern Sie sich, dass die Richtlinien für den Export von NFS Volumes die IP-Adresse der BlueXP Klassifizierungsinstanz enthalten, damit sie auf die Daten auf jedem Volume zugreifen können.
5. Wenn Sie CIFS verwenden, bieten Sie BlueXP Klassifizierung mit Active Directory Anmeldeinformationen, um CIFS Volumes zu scannen.
 - a. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.
 - b. Klicken Sie für jede Arbeitsumgebung auf **Edit CIFS Credentials** und geben Sie den Benutzernamen und das Passwort ein, die die BlueXP Klassifizierung für den Zugriff auf CIFS Volumes auf dem System benötigt.

Die Zugangsdaten können schreibgeschützt sein, aber durch die Angabe von Administratorberechtigungen wird sichergestellt, dass die BlueXP Klassifizierung alle Daten lesen kann, die erhöhte Berechtigungen erfordern. Die Zugangsdaten werden in der BlueXP Klassifizierungsinstanz gespeichert.

Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

Nach Eingabe der Anmeldedaten sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.

Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

Sie können jederzeit auf der Konfigurationsseite Scans oder Scans von nur-Zuordnungen oder Klassifizierungen in einer Arbeitsumgebung starten oder stoppen. Sie können auch von mappingonly Scans zu Mapping- und Klassifizierungsscans und umgekehrt wechseln. Wir empfehlen, alle Volumes zu scannen.

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung 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 EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. ["Weitere Informationen"](#).

cognigoWE Scan Configuration

44/79 Volumes selected for Data Sense scan

OffMapMap & ClassifyCustom

Learn about the differences →

Edit CIFS Credentials

☐ Scan when missing "write attributes" permissions

Scan	Storage Repository (Volume)	Type	Status	Required Action
<div>OffMapMap & Classify</div>	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>OffMapMap & Classify</div>	AdiProtest2501	NFS	Continuously Scanning	
<div>OffMapMap & Classify</div>	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>OffMapMap & Classify</div>	AlexTestSecond	NFS	Not Scanning	

An:	Tun Sie dies:
Aktivieren von mappinggeschützten Scans auf einem Volume	Klicken Sie im Volumenbereich auf Karte
Aktivieren Sie das vollständige Scannen auf einem Volume	Klicken Sie im Volumenbereich auf Karte & Klassieren
Deaktivieren Sie das Scannen auf einem Volume	Klicken Sie im Volumenbereich auf aus
Aktivieren Sie ausschließlich mappingbare Scans auf allen Volumes	Klicken Sie im Steuerkursbereich auf Karte
Aktivieren Sie das vollständige Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf Karte & Klassieren
Deaktivieren Sie das Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf aus



Neue Volumes, die der Arbeitsumgebung hinzugefügt wurden, werden automatisch nur gescannt, wenn Sie die Einstellung **Karte** oder **Karte & Klassieren** im Steuerkursbereich festgelegt haben. Wenn Sie im Bereich Überschrift auf **Benutzerdefiniert** oder **aus** eingestellt sind, müssen Sie für jedes neue Volumen, das Sie in der Arbeitsumgebung hinzufügen, das Mapping und/oder das vollständige Scannen aktivieren.

Scannen von Datensicherungs-Volumes

Datensicherung-Volumes werden standardmäßig nicht gescannt, da sie nicht extern offengelegt werden und die BlueXP Klassifizierung kann nicht auf sie zugreifen. Dies sind die Ziel-Volumes für SnapMirror Vorgänge von einem FSX für ONTAP Filesystem.

Zunächst erkennt die Volume-Liste diese Volumes als *Type DP* mit dem *Status Not Scanning* und der *required Action Enable Access to DP Volumes*.

'Working Environment Name' Configuration

22/28 Volumes selected for compliance scan

Enable Access to DP Volumes [Edit CIFS Credentials](#)

Off **Map** Map & Classify Custom [Learn about the differences](#) →

Scan when missing "write attributes" permissions ☐

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	VolumeName1	DP	Not Scanning	Enable access to DP Volumes ⓘ
Off Map Map & Classify	VolumeName2	NFS	Continuously Scanning	
Off Map Map & Classify	VolumeName3	CIFS	Not Scanning	

Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

1. Klicken Sie oben auf der Seite auf **Zugriff auf DP-Volumes aktivieren**.
2. Überprüfen Sie die Bestätigungsmeldung und klicken Sie erneut auf **Zugriff auf DP-Volumes**.
 - Volumes, die ursprünglich als NFS-Volumes im Quell-FSX für ONTAP erstellt wurden, sind aktiviert.
 - Für Volumes, die ursprünglich als CIFS Volumes im Quell-FSX für ONTAP erstellt wurden, müssen Sie CIFS-Anmeldeinformationen eingeben, um diese DP-Volumes zu scannen. Wenn Sie bereits Active Directory-Anmeldedaten eingegeben haben, sodass die BlueXP Klassifizierung CIFS-Volumes scannen kann, können Sie diese Anmeldedaten verwenden oder einen anderen Satz von Admin-Anmeldedaten angeben.

Provide Active Directory Credentials

☒ Use existing CIFS Scanning Credentials (user1@domain2) ☐ Use Custom Credentials

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for **Data Sense**. The shares' export policies will allow access only from the Cloud **Data Sense** instance. [Learn More](#)

Enable Access to DP Volumes Cancel

Provide Active Directory Credentials

☐ Use existing CIFS Scanning Credentials (user1@domain2) ☒ Use Custom Credentials

Username ⓘ Password

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for **Data Sense**. The shares' export policies will allow access only from the Cloud **Data Sense** instance. [Learn More](#)

Enable Access to DP Volumes Cancel

3. Aktivieren Sie jedes zu scannenden DP-Volume [Auf die gleiche Weise haben Sie andere Volumes aktiviert](#).

Ergebnis

Nach Aktivierung erstellt die BlueXP Klassifizierung von jedem DP-Volume, das zum Scannen aktiviert wurde, eine NFS-Freigabe. Die Richtlinien für den Export von Freigaben sind nur für den Zugriff aus der BlueXP Klassifizierungsinstanz zulässig.

Hinweis: Wenn Sie beim ersten Aktivieren des Zugriffs auf DP-Volumes keine CIFS-Datenschutzvolumes hatten und später noch etwas hinzufügen, erscheint oben auf der Konfigurationsseite die Schaltfläche **Zugriff auf CIFS DP aktivieren**. Klicken Sie auf diese Schaltfläche, und fügen Sie CIFS-Anmeldeinformationen hinzu, um den Zugriff auf diese CIFS-DP-Volumes zu ermöglichen.



Active Directory – Zugangsdaten sind nur in der Storage-VM des ersten CIFS-DP Volumes registriert. Somit werden alle DP-Volumes auf dieser SVM gescannt. Auf allen Volumes, die sich auf anderen SVMs befinden, sind keine Active Directory Anmeldedaten registriert, daher werden diese DP-Volumes nicht gescannt.

Datenbankschemas scannen

Führen Sie ein paar Schritte durch, um mit dem Scannen Ihrer Datenbankschemas mit der BlueXP Klassifizierung zu beginnen.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1

Datenbankvoraussetzungen prüfen

Stellen Sie sicher, dass Ihre Datenbank unterstützt wird und dass Sie über die erforderlichen Informationen verfügen, um eine Verbindung zur Datenbank herzustellen.

2

Implementieren der BlueXP Klassifizierungsinstanz

["Implementieren Sie die BlueXP Klassifizierung"](#) Falls noch keine Instanz implementiert wurde.

3

Fügen Sie den Datenbankserver hinzu

Fügen Sie den Datenbankserver hinzu, auf den Sie zugreifen möchten.

4

Wählen Sie die Schemas aus

Wählen Sie die Schemata aus, die Sie scannen möchten.

Voraussetzungen prüfen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass eine unterstützte Konfiguration vorhanden ist, bevor Sie die BlueXP Klassifizierung aktivieren.

Unterstützte Datenbanken

Die BlueXP Klassifizierung kann Schemata aus den folgenden Datenbanken scannen:

- Amazon Relational Database Service (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL

- SAP HANA
- SQL Server (MSSQL)



Die Statistik-Sammelfunktion *muss in der Datenbank aktiviert sein.

Datenbankanforderungen erfüllt

Jede Datenbank, die mit der BlueXP Klassifizierungsinstanz verbunden ist, kann unabhängig vom Hosting gescannt werden. Sie benötigen lediglich die folgenden Informationen, um eine Verbindung zur Datenbank herzustellen:

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

Bei der Auswahl eines Benutzernamens und Passworts ist es wichtig, einen zu wählen, der über vollständige Leseberechtigungen für alle Schemas und Tabellen verfügt, die Sie scannen möchten. Wir empfehlen, einen dedizierten Benutzer für das BlueXP Klassifizierungssystem mit allen erforderlichen Berechtigungen zu erstellen.

Hinweis: für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

Implementieren der BlueXP Klassifizierungsinstanz

Implementieren Sie die BlueXP Klassifizierung, falls noch keine Instanz implementiert ist.

Wenn Sie Datenbankschemas scannen, die über das Internet zugänglich sind, können Sie dies tun ["Implementieren Sie die BlueXP Klassifizierung in der Cloud"](#) Oder ["Implementieren Sie die BlueXP Klassifizierung an einem lokalen Standort mit Internetzugang"](#).

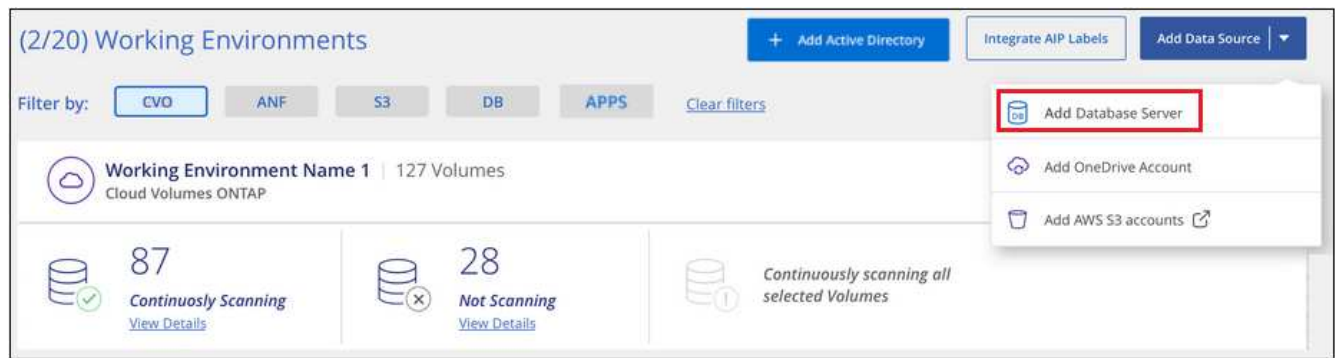
Wenn Sie Datenbankschemas scannen, die in einer dunklen Site installiert wurden, die keinen Internetzugang hat, müssen Sie dies tun ["Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang"](#). Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Fügen Sie den Datenbankserver hinzu

Fügen Sie den Datenbankserver dort hinzu, wo sich die Schemas befinden.

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen > Datenbank-Server hinzufügen**.



2. Geben Sie die erforderlichen Informationen ein, um den Datenbankserver zu identifizieren.
 - 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 Dienstenamen ein.
 - d. Geben Sie die Zugangsdaten ein, damit die BlueXP Klassifizierung auf den Server zugreifen kann.
 - e. Klicken Sie auf **DB-Server hinzufügen**.

Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

Database

Database Type

Host Name or IP Address

Port

Service Name

Credentials

Username

Password

Add DB Server

Cancel

Die Datenbank wird zur Liste der Arbeitsumgebungen hinzugefügt.

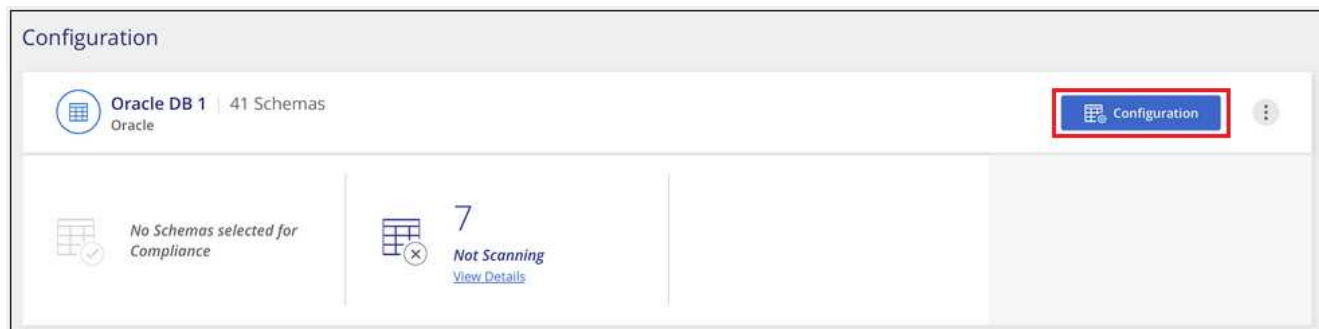
Aktivieren und deaktivieren Sie Compliance-Scans für Datenbankschemas

Sie können jederzeit das vollständige Scannen Ihrer Schemas anhalten oder starten.

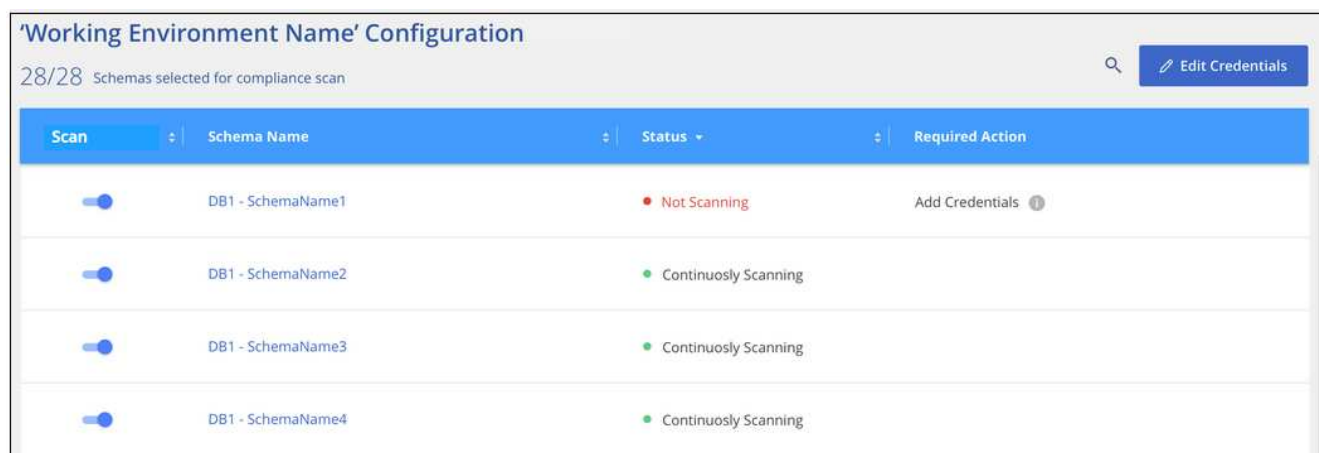


Es besteht keine Möglichkeit, nur mappingbare Scans für Datenbankschemas auszuwählen.

1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Configuration** für die zu konfigurierende Datenbank.



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



Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen aktivierten Datenbankschemas. Wenn Fehler auftreten, werden sie neben der erforderlichen Aktion zur Behebung des Fehlers in der Spalte Status angezeigt.

Die BlueXP Klassifizierung scannt Ihre Datenbanken einmal pro Tag – Datenbanken werden nicht wie andere Datenquellen fortlaufend gescannt.

Scannen von Dateifreigaben

Führen Sie einige Schritte aus, um mit dem Scannen von NFS- oder CIFS-Dateifreigaben aus Google Cloud NetApp Volumes und älteren NetApp 7-Mode-Systemen zu beginnen. Diese Dateifreigaben können lokal oder in der Cloud gespeichert werden.



Das Scannen von Daten aus nicht-NetApp-Dateifreigaben wird in der Kernversion der BlueXP Klassifizierung nicht unterstützt.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1

Prüfen Sie die Voraussetzungen für die Dateifreigabe

Stellen Sie für CIFS-Freigaben (SMB) sicher, dass Sie über Anmeldeinformationen für den Zugriff auf Freigaben verfügen.

2

Implementieren der BlueXP Klassifizierungsinstanz

["Implementieren Sie die BlueXP Klassifizierung"](#) Falls noch keine Instanz implementiert wurde.

3

Erstellen Sie eine Gruppe, um die Dateifreigaben zu halten

Die Gruppe ist ein Container für die Dateifreigaben, die Sie scannen möchten, und er wird als Name der Arbeitsumgebung für diese Dateifreigaben verwendet.

4

Fügen Sie die Dateifreigaben der Gruppe hinzu

Fügen Sie die Liste der zu scannenden Dateifreigaben hinzu und wählen Sie den Scantyp aus. Sie können bis zu 100 Dateifreigaben gleichzeitig hinzufügen.

Prüfen der Anforderungen für die Dateifreigabe

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass eine unterstützte Konfiguration vorhanden ist, bevor Sie die BlueXP Klassifizierung aktivieren.

- Die Shares können überall gehostet werden, auch in der Cloud oder vor Ort. CIFS-Freigaben von älteren NetApp 7-Mode Storage-Systemen können als Dateifreigaben gescannt werden.

Beachten Sie, dass die BlueXP Klassifizierung keine Berechtigungen oder die „Zeit des letzten Zugriffs“ aus 7-Mode Systemen extrahieren kann. Aufgrund eines bekannten Problems zwischen einigen Linux-Versionen und CIFS-Freigaben auf 7-Mode-Systemen müssen Sie die Freigabe zudem so konfigurieren, dass nur SMB v1 mit aktivierter NTLM-Authentifizierung verwendet wird.

- Zwischen der BlueXP Klassifizierungsinstanz und den Freigaben muss eine Netzwerkverbindung bestehen.
- Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind:
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
- Sie können eine DFS-Freigabe (Distributed File System) als reguläre CIFS-Freigabe hinzufügen. Da die BlueXP Klassifizierung jedoch nicht bewusst ist, dass die Freigabe auf mehreren Servern/Volumes basiert, erhalten Sie möglicherweise Berechtigungen oder Verbindungsfehler bezüglich der Freigabe, wenn die Nachricht sich wirklich nur auf einen der Ordner/Freigaben bezieht, die sich auf einem anderen Server/Volume befinden.
- Stellen Sie für CIFS-Freigaben (SMB) sicher, dass Sie über Active Directory-Anmeldeinformationen

verfügen, die Lesezugriff auf die Freigaben bieten. Anmeldedaten als Administrator sind bevorzugt, wenn die BlueXP Klassifizierung alle Daten scannt, die erhöhte Berechtigungen erfordern.

Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

- Sie benötigen die Liste der Freigaben, die Sie im Format hinzufügen möchten
<host_name>:/<share_path>. Sie können die Freigaben einzeln eingeben oder eine Liste der Dateien, die Sie scannen möchten, mit einer Zeile angeben.

Implementieren der BlueXP Klassifizierungsinstanz

Implementieren Sie die BlueXP Klassifizierung, falls noch keine Instanz implementiert ist.

Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

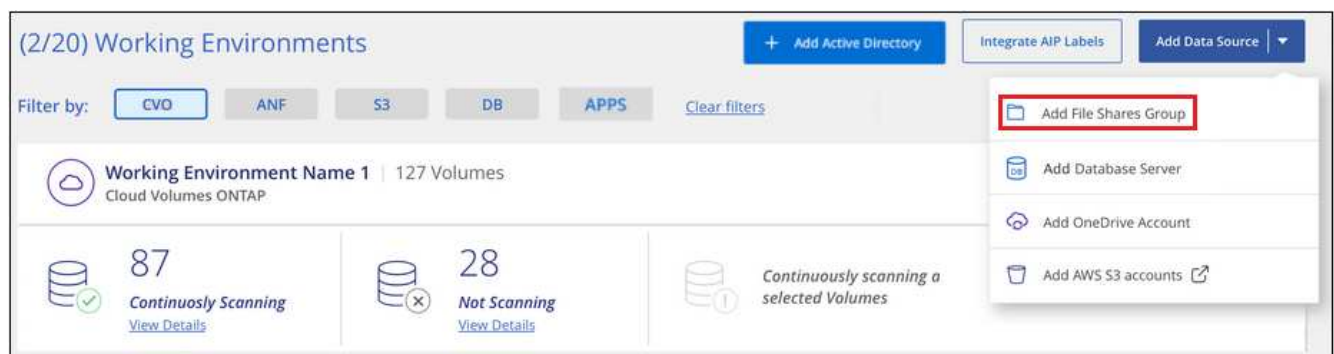
Erstellen der Gruppe für die Dateifreigaben

Sie müssen eine „Gruppe“ von Dateifreigaben für Dateien hinzufügen, bevor Sie Ihre Dateifreigaben hinzufügen können. Die Gruppe ist ein Container für die zu scannenden Dateifreigaben, und der Gruppenname wird als Name der Arbeitsumgebung für diese Dateifreigaben verwendet.

Sie können NFS- und CIFS-Freigaben in einer Gruppe kombinieren. Allerdings müssen alle CIFS-Dateifreigaben in einer Gruppe dieselben Active Directory-Anmeldedaten verwenden. Wenn Sie CIFS-Freigaben hinzufügen möchten, die unterschiedliche Anmeldedaten verwenden, müssen Sie für jeden eindeutigen Satz von Anmeldeinformationen eine separate Gruppe erstellen.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen > Datei-Shares-Gruppe hinzufügen**.



2. Geben Sie im Dialogfeld „Gruppe Dateien hinzufügen“ den Namen für die Gruppe der Freigaben ein, und klicken Sie auf **Weiter**.

Die neue File Shares-Gruppe wird der Liste der Arbeitsumgebungen hinzugefügt.

Hinzufügen von Dateifreigaben zu einer Gruppe

Sie fügen der Dateifreigaben-Gruppe Dateifreigaben hinzu, damit die Dateien in diesen Freigaben durch die BlueXP-Klassifizierung gescannt werden. Sie fügen die Freigaben im Format hinzu

<host_name>:/<share_path>.

Sie können einzelne Dateifreigaben hinzufügen, oder Sie können eine Liste der Dateien, die Sie scannen möchten, mit einer Zeile eingeben. Sie können bis zu 100 Shares gleichzeitig hinzufügen.

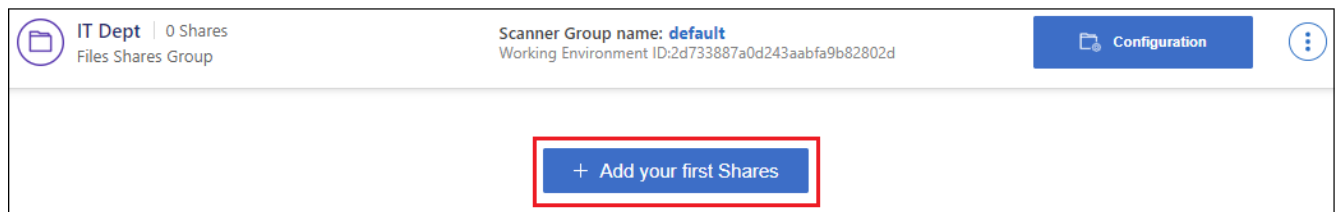
Wenn Sie in einer einzelnen Gruppe sowohl NFS- als auch CIFS-Freigaben hinzufügen, müssen Sie diesen Prozess zweimal durchlaufen: Sobald Sie NFS-Freigaben hinzufügen, und dann erneut CIFS-Freigaben hinzufügen.

Schritte

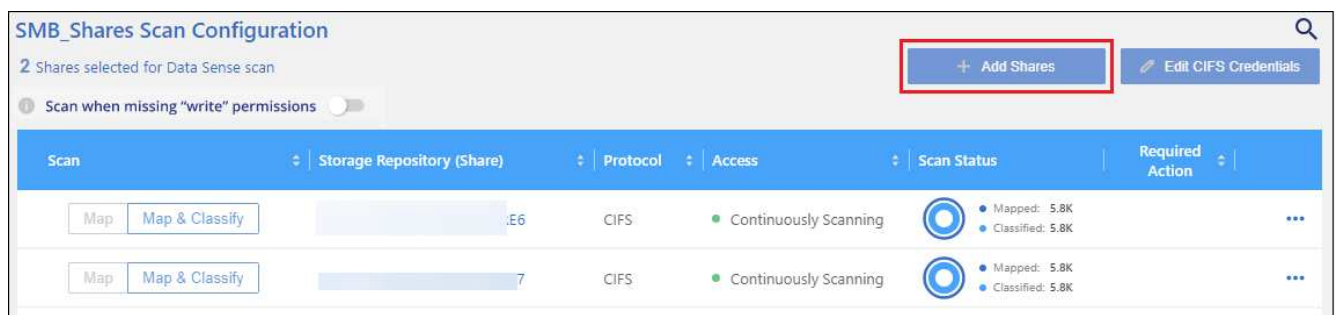
1. Klicken Sie auf der Seite *Working Environments* auf die Schaltfläche **Konfiguration** für die File Shares Group.



2. Wenn dies das erste Mal ist, um Dateifreigaben für diese File Shares-Gruppe hinzuzufügen, klicken Sie auf **erste Shares hinzufügen**.



Wenn Sie einer vorhandenen Gruppe File Shares hinzufügen, klicken Sie auf **Add Shares**.



3. Wählen Sie das Protokoll für die File Shares aus, die Sie hinzufügen, fügen Sie die File Shares hinzu, die Sie scannen möchten - eine Dateifreigabe pro Zeile - und klicken Sie auf **Weiter**.

Beim Hinzufügen von CIFS (SMB)-Freigaben müssen Sie die Active Directory-Anmeldeinformationen eingeben, die Lesezugriff auf die Freigaben bieten. Anmeldedaten für Admin werden bevorzugt.

Ein Bestätigungsdiaologfeld zeigt die Anzahl der hinzugefügten Freigaben an.

Wenn im Dialogfeld Freigaben aufgeführt werden, die nicht hinzugefügt werden konnten, erfassen Sie diese Informationen, damit Sie das Problem beheben können. In einigen Fällen können Sie die Freigabe mit einem korrigierten Hostnamen oder Freigabennamen erneut hinzufügen.

4. Aktivieren Sie für jede Dateifreigabe nur mappingbare Scans oder Mappings und Klassifizierungen.

An:	Tun Sie dies:
Aktivieren Sie Mapping-Only-Scans auf File Shares	Klicken Sie Auf Karte
Vollständige Scans auf Dateifreigaben ermöglichen	Klicken Sie Auf Karte & Klassieren
Deaktivieren Sie das Scannen von Dateifreigaben	Klicken Sie Auf Aus

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung 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 EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. ["Weitere Informationen ."](#)

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der Dateien in den von Ihnen hinzugefügten Dateifreigaben. Die Ergebnisse werden im Dashboard und an anderen Orten angezeigt.

Entfernen einer Dateifreigabe aus Compliance-Scans

Wenn Sie bestimmte Dateifreigaben nicht mehr scannen müssen, können Sie einzelne Dateifreigaben jederzeit aus dem Scannen ihrer Dateien entfernen. Klicken Sie einfach auf der Konfigurationsseite auf **Share**

entfernen.

Working Environment 2 Configuration

+ Add Shares

Edit CIFS Credentials

2/22 Shares selected for compliance scan

Scan	Share name	Protocol	Status	Required Action
<div>OffMapMap & Classify</div>	Sharepath1	NFS	<div>Not Scanning</div>	<div>Add new credentials</div> <div>Remove Share</div>

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.