



Aktivieren Sie das Scannen Ihrer Datenquellen

Cloud Data Sense

NetApp
December 12, 2022

Inhaltsverzeichnis

- Aktivieren Sie das Scannen Ihrer Datenquellen. 1
 - Erste Schritte mit Cloud Data Sense für Cloud Volumes ONTAP und On-Premises-ONTAP 1
 - Erste Schritte mit Cloud Data Sense für Azure NetApp Files. 7
 - Erste Schritte mit Cloud Data Sense für Amazon FSX für ONTAP 11
 - Erste Schritte mit Cloud Data Sense für Amazon S3 17
- Datenbankschemas werden gescannt. 24
- OneDrive-Konten werden gescannt. 27
- Scannen von SharePoint-Konten. 31
- Google Drive-Konten werden durchsucht 36
- Scannen von Dateifreigaben 38
- Objekt-Storage wird mit S3-Protokoll gescannt 43

Aktivieren Sie das Scannen Ihrer Datenquellen

Erste Schritte mit Cloud Data Sense für Cloud Volumes ONTAP und On-Premises-ONTAP

Führen Sie einige Schritte aus, um Ihren Cloud Volumes ONTAP und Ihre ONTAP Volumes vor Ort mithilfe von Cloud Data Sense zu scannen.

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 Sie die Cloud Data Sense Instanz

["Sinnvolle Implementierung Von Cloud-Daten"](#) Falls noch keine Instanz implementiert wurde.

3

Aktivieren Sie Cloud Data Sense und wählen Sie die zu scannenden Volumes aus

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

4

Zugriff auf Volumes sicherstellen

Jetzt, da Cloud Data Sense aktiviert ist, stellen Sie sicher, dass er auf alle Volumes zugreifen kann.

- Die Cloud Data Sense Instanz benötigt eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP-Subnetz oder On-Prem ONTAP-System.
- Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen aus der Datensense-Instanz zulassen.
- Stellen Sie sicher, dass diese Ports für die Data Sense-Instanz offen sind:
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
- NFS-Volume-Exportrichtlinien müssen den Zugriff aus der Data Sense Instanz zulassen.
- Data Sense benötigt Active Directory-Anmeldeinformationen zum Scannen von CIFS-Volumes.

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

die Anmeldeinformationen an.

5

Verwalten Sie die Volumes, die Sie scannen möchten

Wählen oder deaktivieren Sie die Volumes, die Sie scannen möchten, und Cloud Data Sense startet oder beendet den Scanvorgang.

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"](#).

Bereitstellen der Cloud Data Sense Instanz

Implementieren Sie Cloud-Daten sinnvoll, wenn 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 ["Cloud-Daten sinnvoll in der Cloud implementieren"](#) Oder ["In einer Anlage mit Internetzugang"](#).

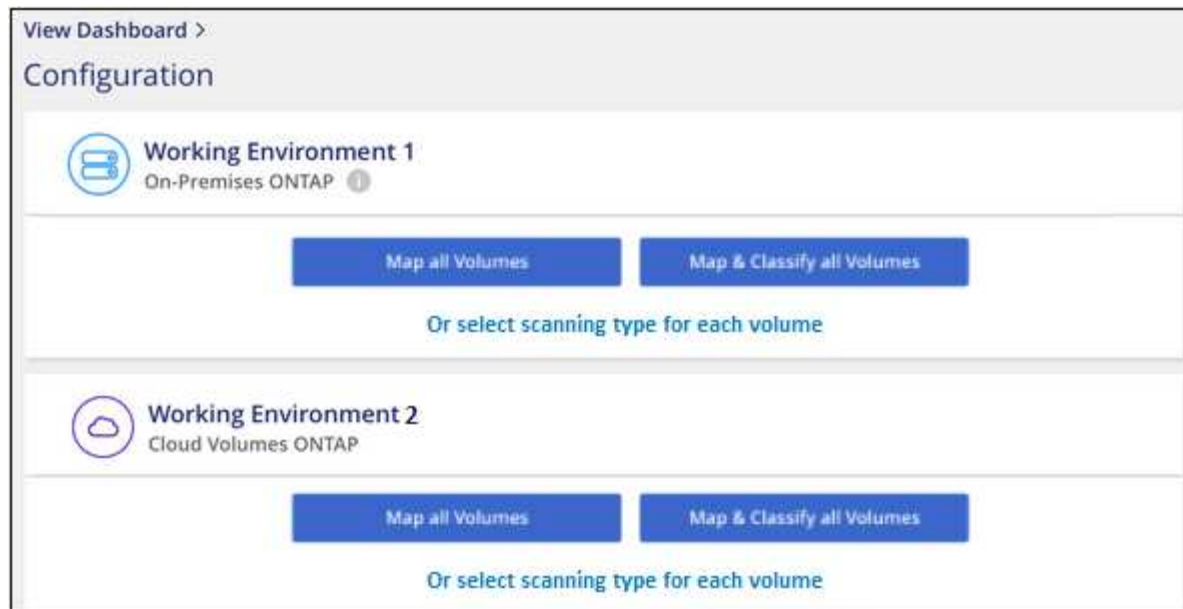
Wenn Sie lokale ONTAP-Systeme scannen, die in einer dunklen Site installiert wurden und über keinen Internetzugang verfügen, müssen Sie sie überprüfen ["Cloud Data Sense implementieren – auf demselben lokalen Standort ohne Internetzugang"](#). Dazu ist auch die Implementierung des BlueXP Connectors am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

Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Cloud-Daten sinnvoll in Ihren Arbeitsumgebungen einsetzen

Sie können Cloud Data Sense auf Cloud Volumes ONTAP Systemen in jedem unterstützten Cloud-Provider und On-Premises 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 **Genehmigen**, damit Data Sense Ihre Volumes scannen kann.

Ergebnis

Cloud Data Sense beginnt mit dem Scannen der Volumes, die Sie in der Arbeitsumgebung ausgewählt haben. Die Ergebnisse werden im Compliance-Dashboard verfügbar sein, sobald Cloud Data Sense die ersten Scans beendet hat. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.

Es wird sichergestellt, dass Cloud Data Sense Zugriff auf Volumes hat

Stellen Sie sicher, dass Cloud Data Sense auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien prüfen. Sie müssen Data Sense mit CIFS Credentials bereitstellen, um auf CIFS Volumes zugreifen zu können.

Schritte

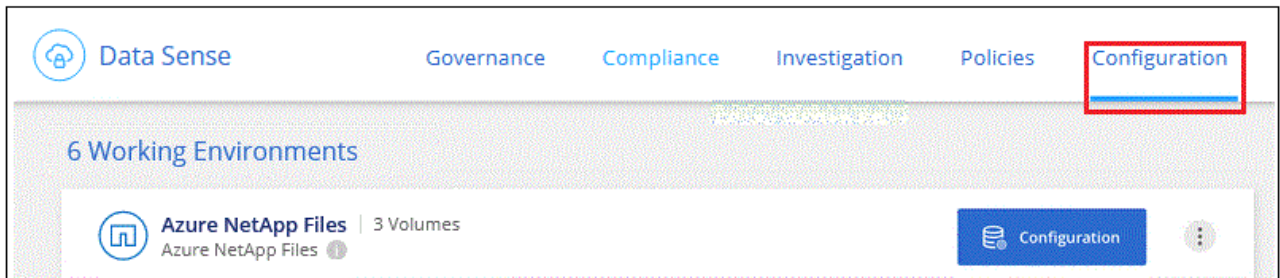
1. Vergewissern Sie sich, dass es eine Netzwerkverbindung zwischen der Cloud Data Sense Instanz und jedem Netzwerk gibt, das Volumes für Cloud Volumes ONTAP oder lokale ONTAP Cluster enthält.
2. Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr aus der Datensense-Instanz zulässt.

Sie können entweder die Sicherheitsgruppe für den Datenverkehr von der IP-Adresse der Instanz Data Sense öffnen oder die Sicherheitsgruppe für den gesamten Datenverkehr im virtuellen Netzwerk öffnen.

3. Stellen Sie sicher, dass die folgenden Ports für die Data Sense-Instanz offen sind:
 - Für NFS – die Ports 111 und 2049.

- Für CIFS – die Ports 139 und 445.

4. Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Sense Instanz enthalten, damit sie auf die Daten auf jedem Volume zugreifen können.
5. Wenn Sie CIFS verwenden, geben Sie Data Sense mit Active Directory Anmeldeinformationen ein, damit CIFS Volumes gescannt werden können.
 - a. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.

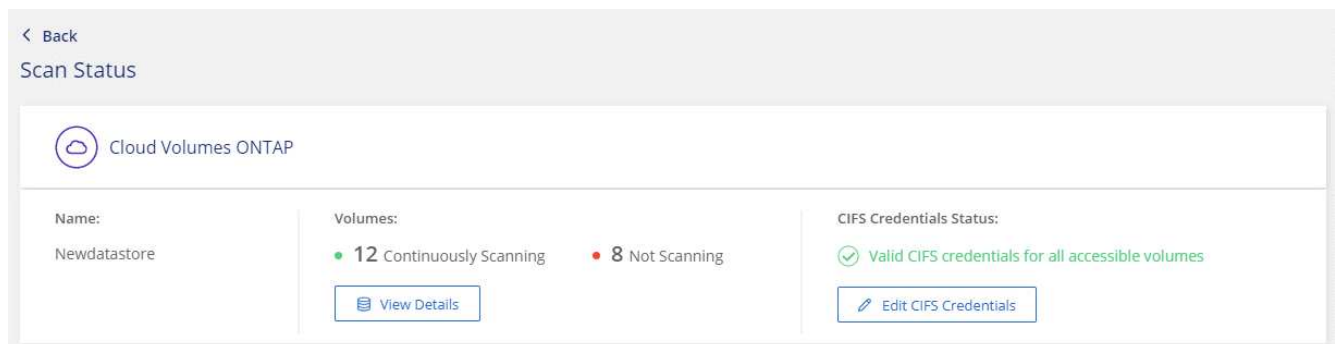


- b. Klicken Sie für jede Arbeitsumgebung auf **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Data Sense für den Zugriff auf CIFS-Volumes auf dem System benötigt.

Die Anmeldedaten können schreibgeschützt sein. Durch die Admin-Berechtigungen wird jedoch sichergestellt, dass Data Sense alle Daten lesen kann, die erhöhte Berechtigungen benötigen. Die Anmeldedaten werden in der Cloud Data Sense Instanz gespeichert.

Wenn Sie sicherstellen möchten, dass Ihre Dateien „letzte Zugriffszeiten“ durch Data Sense Klassifizierungsscans unverändert bleiben, empfehlen wir dem Benutzer die Berechtigung Schreibattribute zu besitzen. 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, von denen Cloud Data Sense aufgrund von Netzwerkverbindungsproblemen zwischen der Data Sense Instanz und dem Volume nicht scannen kann.

cognigoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div> Off Map Map & Classify Custom </div> <div>Learn about the differences →</div> <div>Edit CIFS Credentials</div>				
Scan	Storage Repository (Volume)	Type	Status	Required Action
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	
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

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.

cognigoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div> Off Map Map & Classify Custom </div> <div>Learn about the differences →</div> <div>Edit CIFS Credentials</div>				
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	
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously 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

Standardmäßig werden Datensicherungs-Volumes nicht gescannt, weil sie nicht extern zugänglich sind und Cloud Data Sense nicht auf sie zugreifen kann. 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**.

The screenshot shows the 'Working Environment Name' Configuration page. At the top, it says '22/28 Volumes selected for compliance scan'. There are buttons for 'Enable Access to DP Volumes' (highlighted with a red box) and 'Edit CIFS Credentials'. Below this is a table with columns: Scan, Storage Repository (Volume), Type, Status, and Required Action.

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-Anmeldeinformationen eingegeben haben, damit Cloud Data Sense CIFS-Volumes scannen kann, können Sie diese Anmeldedaten verwenden oder einen anderen Satz von Admin-Anmeldeinformationen angeben.

The screenshot shows the 'Provide Active Directory Credentials' dialog box. The option 'Use existing CIFS Scanning Credentials (user1@domain2)' is selected and highlighted with a red box. Below it are fields for 'Active Directory Domain' and 'DNS IP Address'. At the bottom, there are buttons for 'Enable Access to DP Volumes' and 'Cancel'.

The screenshot shows the 'Provide Active Directory Credentials' dialog box. The option 'Use Custom Credentials' is selected and highlighted with a red box. Below it are fields for 'Username', 'Password', 'Active Directory Domain', and 'DNS IP Address'. At the bottom, there are buttons for 'Enable Access to DP Volumes' and 'Cancel'.

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

Ergebnis

Sobald Cloud Data Sense aktiviert ist, erstellt Cloud Data Sense eine NFS-Freigabe von jedem DP-Volume, das zum Scannen aktiviert wurde. Die Exportrichtlinien für die Freigabe erlauben nur den Zugriff aus der Instanz Data Sense.

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 Cloud Data Sense für Azure NetApp Files

In wenigen Schritten zum Einstieg in Cloud Data Sense for Azure NetApp Files.

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 Sie die Cloud Data Sense Instanz

["Implementieren Sie Cloud Data Sense in BlueXP"](#) Falls noch keine Instanz implementiert wurde.

3

Aktivieren Sie Cloud Data Sense 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

Jetzt, da Cloud Data Sense aktiviert ist, stellen Sie sicher, dass er auf alle Volumes zugreifen kann.

- Die Cloud Data Sense Instanz benötigt eine Netzwerkverbindung zu jedem Azure NetApp Files Subnetz.
- Stellen Sie sicher, dass diese Ports für die Data Sense-Instanz offen sind:
 - Für NFS – die Ports 111 und 2049.

- Für CIFS – die Ports 139 und 445.
- NFS-Volume-Exportrichtlinien müssen den Zugriff aus der Data Sense Instanz zulassen.
- Data Sense benötigt Active Directory-Anmeldeinformationen zum Scannen von CIFS-Volumes.

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

5

Verwalten Sie die Volumes, die Sie scannen möchten

Wählen oder deaktivieren Sie die Volumes, die Sie scannen möchten, und Cloud Data Sense startet oder beendet den Scanvorgang.

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"](#).

Bereitstellen der Cloud Data Sense Instanz

["Sinnvolle Implementierung Von Cloud-Daten"](#) Falls noch keine Instanz implementiert wurde.

Beim Scannen von Azure NetApp Files Volumes muss der Einsatz von Datensense in der Cloud stattfinden. Er muss in demselben Bereich wie die Volumes eingesetzt werden, die Sie scannen möchten.

Hinweis: die Bereitstellung von Cloud Data Sense an einem lokalen Speicherort wird derzeit beim Scannen von Azure NetApp Files Volumes nicht unterstützt.

Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Cloud-Daten sinnvoll in Ihren Arbeitsumgebungen einsetzen

Sie können den Einsatz von Cloud-Daten in Ihren Azure NetApp Files Volumes sinnvoll 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 Bestätigungsdialogfeld auf **Genehmigen**, damit Data Sense Ihre Volumes scannen kann.

Ergebnis

Cloud Data Sense beginnt mit dem Scannen der Volumes, die Sie in der Arbeitsumgebung ausgewählt haben. Die Ergebnisse werden im Compliance-Dashboard verfügbar sein, sobald Cloud Data Sense die ersten Scans beendet hat. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.

Es wird sichergestellt, dass Cloud Data Sense Zugriff auf Volumes hat

Stellen Sie sicher, dass Cloud Data Sense auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien prüfen. Sie müssen Data Sense mit CIFS Credentials bereitstellen, um auf CIFS Volumes zugreifen zu können.

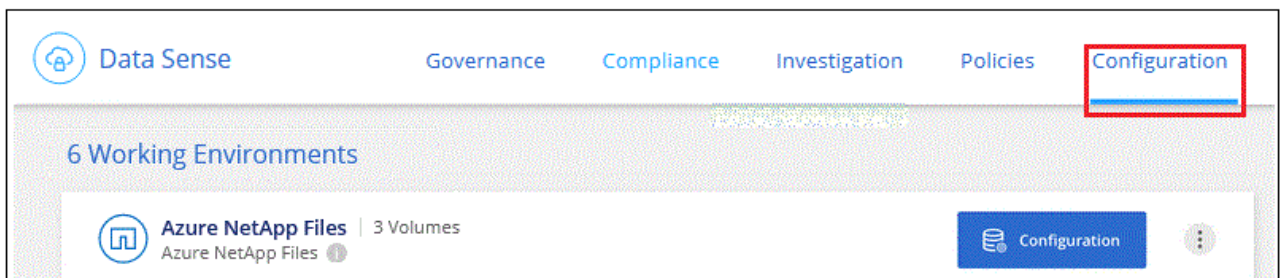
Schritte

1. Stellen Sie sicher, dass es eine Netzwerkverbindung zwischen Cloud Data Sense Instanz und jedem Netzwerk gibt, das Volumes für Azure NetApp Files enthält.



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

2. Stellen Sie sicher, dass die folgenden Ports für die Data Sense-Instanz offen sind:
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
3. Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Sense Instanz enthalten, damit sie auf die Daten auf jedem Volume zugreifen können.
4. Wenn Sie CIFS verwenden, geben Sie Data Sense mit Active Directory Anmeldeinformationen ein, damit CIFS Volumes gescannt werden können.
 - a. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.

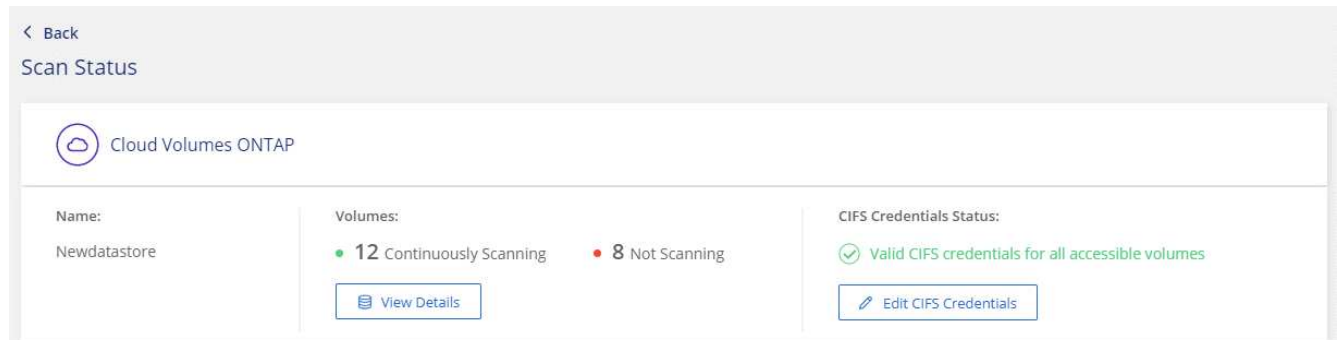


- b. Klicken Sie für jede Arbeitsumgebung auf **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Data Sense für den Zugriff auf CIFS-Volumes auf dem System benötigt.

Die Anmeldedaten können schreibgeschützt sein. Durch die Admin-Berechtigungen wird jedoch sichergestellt, dass Data Sense alle Daten lesen kann, die erhöhte Berechtigungen benötigen. Die Anmeldedaten werden in der Cloud Data Sense Instanz gespeichert.

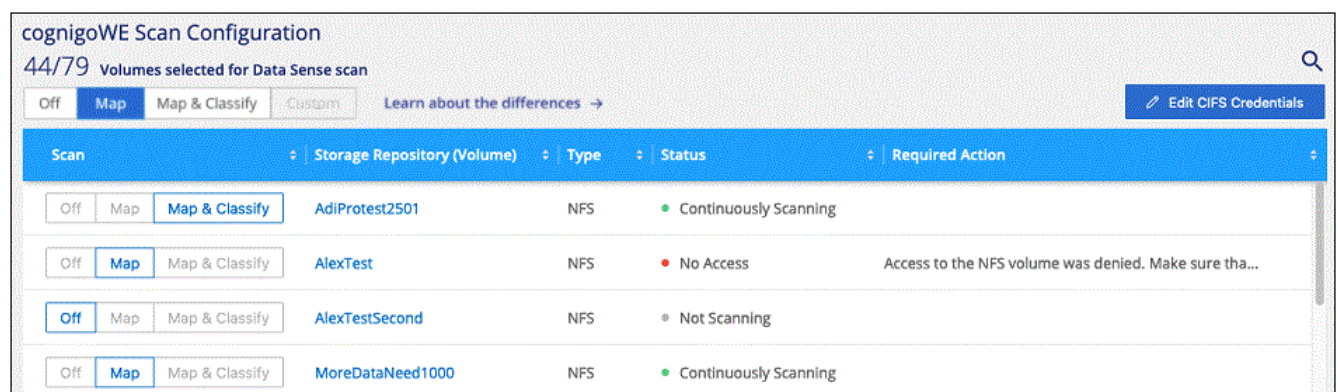
Wenn Sie sicherstellen möchten, dass Ihre Dateien „letzte Zugriffszeiten“ durch Data Sense Klassifizierungsscans unverändert bleiben, empfehlen wir dem Benutzer die Berechtigung Schreibattribute zu besitzen. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete 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, von denen Cloud Data Sense aufgrund von Netzwerkverbindungsproblemen zwischen der Data Sense Instanz und dem Volume nicht scannen kann.



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.

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

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

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	
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously 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 Volumen, 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 Cloud Data Sense für Amazon FSX für ONTAP

Führen Sie einige Schritte durch, um zu beginnen, Amazon FSX für ONTAP-Volume mit Cloud Data Sense zu scannen.

Bevor Sie beginnen

- Für die Implementierung und das Management von Data Sense benötigen Sie einen aktiven Connector in AWS.
- Die Sicherheitsgruppe, die Sie beim Erstellen der Arbeitsumgebung ausgewählt haben, muss Datenverkehr aus der Instanz Cloud Data Sense 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 Sie die Cloud Data Sense Instanz

"[Implementieren Sie Cloud Data Sense in BlueXP](#)" Falls noch keine Instanz implementiert wurde.

3

Aktivieren Sie Cloud Data Sense und wählen Sie die zu scannenden Volumes aus

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

4

Zugriff auf Volumes sicherstellen

Jetzt, da Cloud Data Sense aktiviert ist, stellen Sie sicher, dass er auf alle Volumes zugreifen kann.

- Die Cloud Data Sense Instanz benötigt eine Netzwerkverbindung zu jedem FSX für ONTAP Subnetz.
- Stellen Sie sicher, dass die folgenden Ports für die Data Sense-Instanz geöffnet sind:
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
- NFS-Volume-Exportrichtlinien müssen den Zugriff aus der Data Sense Instanz zulassen.
- Data Sense benötigt Active Directory-Anmeldeinformationen zum Scannen von CIFS-Volumes. + Klicken Sie auf **Compliance** > **Konfiguration** > **CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an.

5

Verwalten Sie die Volumes, die Sie scannen möchten

Wählen oder deaktivieren Sie die Volumes, die Sie scannen möchten, und Cloud Data Sense startet oder beendet den Scanvorgang.

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"](#).

Bereitstellen der Cloud Data Sense Instanz

["Sinnvolle Implementierung Von Cloud-Daten"](#) Falls noch keine Instanz implementiert wurde.

Sie sollten Data Sense im selben AWS Netzwerk einsetzen, wie der Connector für AWS und die FSX Volumes, die Sie scannen möchten.

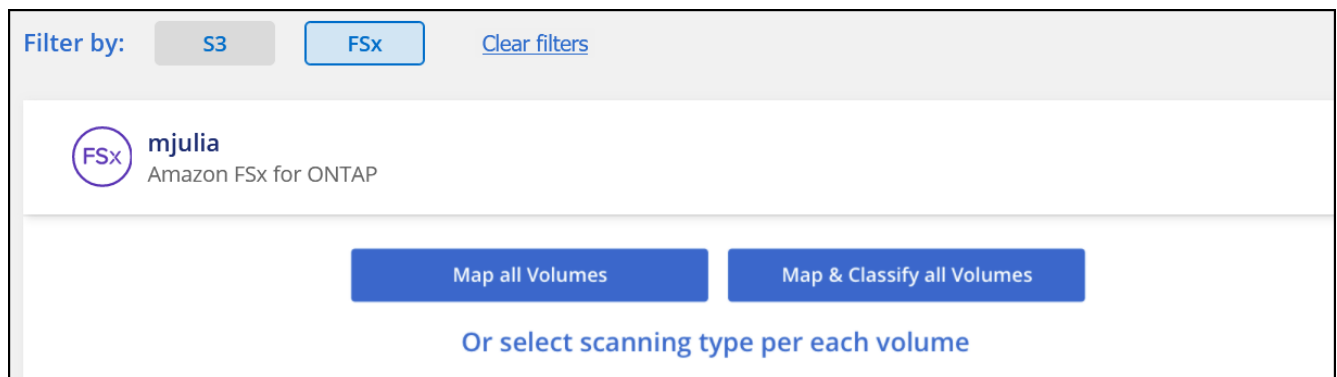
Hinweis: die Bereitstellung von Cloud Data Sense an einem lokalen Speicherort wird derzeit beim Scannen von FSX-Volumes nicht unterstützt.

Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Cloud-Daten sinnvoll in Ihren Arbeitsumgebungen einsetzen

Sie können Cloud Data Sense für FSX für ONTAP Volumes 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 **Genehmigen**, damit Data Sense Ihre Volumes scannen kann.

Ergebnis

Cloud Data Sense beginnt mit dem Scannen der Volumes, die Sie in der Arbeitsumgebung ausgewählt haben. Die Ergebnisse werden im Compliance-Dashboard verfügbar sein, sobald Cloud Data Sense die ersten Scans beendet hat. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.

Es wird sichergestellt, dass Cloud Data Sense Zugriff auf Volumes hat

Stellen Sie sicher, dass Cloud Data Sense auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien prüfen.

Sie müssen Data Sense mit CIFS Credentials bereitstellen, 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 ein Volume Cloud Data Sense aufgrund von Netzwerkverbindungsproblemen zwischen der Data Sense Instanz 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 eine Netzwerkverbindung zwischen Cloud Data Sense Instanz und jedem Netzwerk, das Volumes für FSX für ONTAP enthält, sicher.



Bei FSX für ONTAP kann Cloud Data Sense Volumes nur in derselben Region wie BlueXP scannen.

3. Stellen Sie sicher, dass die folgenden Ports für die Data Sense-Instanz offen sind.
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
4. Sicherstellen, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Sense Instanz enthalten, damit sie auf die Daten auf den einzelnen Volumes zugreifen können.
5. Wenn Sie CIFS verwenden, geben Sie Data Sense mit Active Directory Anmeldeinformationen ein, damit CIFS Volumes gescannt werden können.
 - a. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.
 - b. Klicken Sie für jede Arbeitsumgebung auf **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Data Sense für den Zugriff auf CIFS-Volumes auf dem System benötigt.

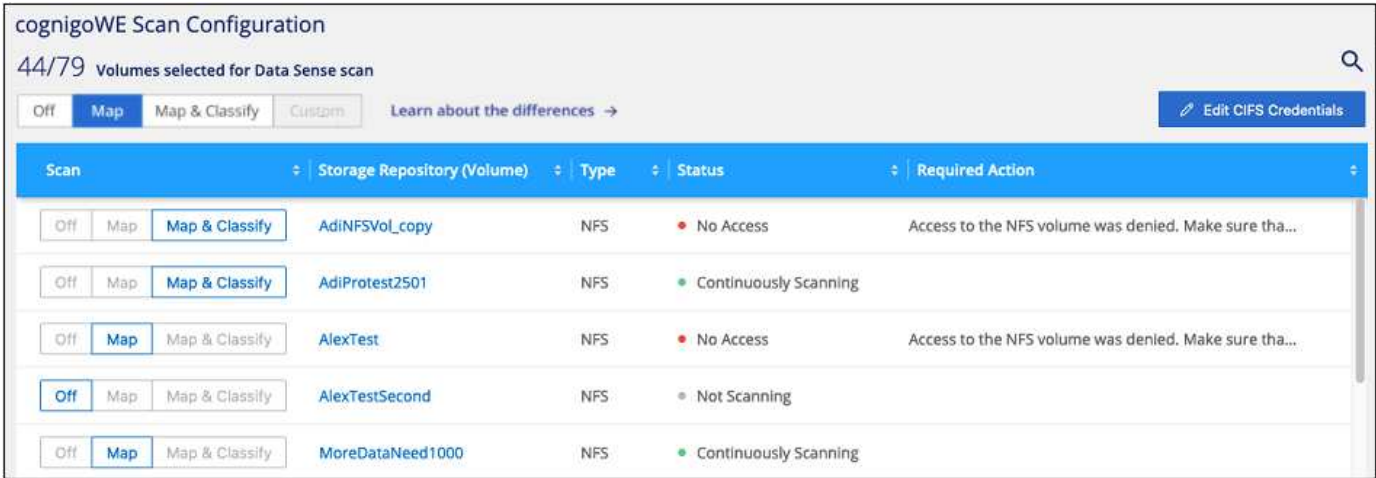
Die Anmeldedaten können schreibgeschützt sein. Durch die Admin-Berechtigungen wird jedoch sichergestellt, dass Data Sense alle Daten lesen kann, die erhöhte Berechtigungen benötigen. Die Anmeldedaten werden in der Cloud Data Sense Instanz gespeichert.

Wenn Sie sicherstellen möchten, dass Ihre Dateien „letzte Zugriffszeiten“ durch Data Sense Klassifizierungsscans unverändert bleiben, empfehlen wir dem Benutzer die Berechtigung Schreibattribute zu besitzen. 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.



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

Standardmäßig werden Datensicherungs-Volumes nicht gescannt, weil sie nicht extern zugänglich sind und Cloud Data Sense nicht auf sie zugreifen kann. 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	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-Anmeldeinformationen eingegeben haben, damit Cloud Data Sense CIFS-Volumes scannen kann, können Sie diese Anmeldedaten verwenden oder einen anderen Satz von Admin-Anmeldeinformationen 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

Sobald Cloud Data Sense aktiviert ist, erstellt Cloud Data Sense eine NFS-Freigabe von jedem DP-Volume, das zum Scannen aktiviert wurde. Die Exportrichtlinien für die Freigabe erlauben nur den Zugriff aus der Instanz Data Sense.

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 Cloud Data Sense für Amazon S3

Cloud Data Sense kann Ihre Amazon S3 Buckets scannen, um die persönlichen und sensiblen Daten zu identifizieren, die sich im S3 Objekt-Storage befinden. Cloud Data Sense kann jeden Bucket im Konto scannen, unabhängig davon, ob er für eine NetApp Lösung erstellt wurde.

Schnellstart

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

1

S3-Anforderungen in Ihrer Cloud-Umgebung einrichten

Stellen Sie sicher, dass Ihre Cloud-Umgebung die Anforderungen für Cloud Data Sense erfüllen kann, einschließlich der Vorbereitung einer IAM-Rolle und der Einrichtung der Konnektivität von Data Sense bis S3. [Eine vollständige Liste finden Sie hier.](#)

2

Implementieren Sie die Cloud Data Sense Instanz

"[Sinnvolle Implementierung Von Cloud-Daten](#)" Falls noch keine Instanz implementiert wurde.

3

Aktivieren Sie Data Sense in Ihrer S3-Arbeitsumgebung

Wählen Sie die Amazon S3-Arbeitsumgebung aus, klicken Sie auf **Aktivieren** und wählen Sie eine IAM-Rolle aus, die die erforderlichen Berechtigungen enthält.

4

Wählen Sie die zu scannenden Buckets aus

Wählen Sie die Buckets aus, die Sie scannen möchten, und Cloud Data Sense beginnt mit dem Scannen.

Überprüfen der S3-Voraussetzungen

Die folgenden Anforderungen gelten insbesondere für das Scannen von S3-Buckets.

Einrichten einer IAM-Rolle für die Cloud Data Sense Instanz

Cloud Data Sense benötigt Berechtigungen, um sich mit den S3 Buckets Ihres Kontos zu verbinden und zu scannen. Richten Sie eine IAM-Rolle ein, die die unten aufgeführten Berechtigungen enthält. BlueXP fordert Sie auf, eine IAM-Rolle auszuwählen, wenn Sie „Data Sense“ in der Amazon S3-Arbeitsumgebung aktivieren.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}

```

Konnektivität von Cloud Data Sense zu Amazon S3

Cloud Data Sense benötigt eine Verbindung zu Amazon S3. Die beste Möglichkeit, eine solche Verbindung bereitzustellen, ist über einen VPC Endpunkt zum S3-Service. Anweisungen hierzu finden Sie unter ["AWS Dokumentation: Erstellen eines Gateway-Endpunkts"](#).

Wenn Sie den VPC-Endpunkt erstellen, müssen Sie die Region, die VPC und die Routing-Tabelle auswählen, die der Cloud Data Sense Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Data Sense keine Verbindung zum S3-Service herstellen.

Informationen zu Problemen finden Sie unter ["AWS Support Knowledge Center: Warum kann ich mich nicht über einen Gateway VPC Endpunkt mit einem S3-Bucket verbinden?"](#)

Eine Alternative besteht darin, die Verbindung über ein NAT Gateway bereitzustellen.



Sie können keinen Proxy verwenden, um über das Internet nach S3 zu gelangen.

Bereitstellen der Cloud Data Sense Instanz

["Implementieren Sie Cloud Data Sense in BlueXP"](#) Falls noch keine Instanz implementiert wurde.

Sie müssen die Instanz mithilfe eines in AWS bereitgestellten Connectors implementieren, damit BlueXP die S3-Buckets in diesem AWS-Konto automatisch erkennt und diese in einer Amazon S3-Arbeitsumgebung anzeigt.

Hinweis: beim Scannen von S3 Buckets wird derzeit nicht die Bereitstellung von Cloud Data Sense an einem lokalen Speicherort unterstützt.

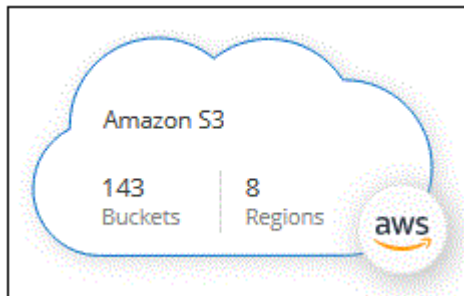
Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Aktivieren von Data Sense in Ihrer S3-Arbeitsumgebung

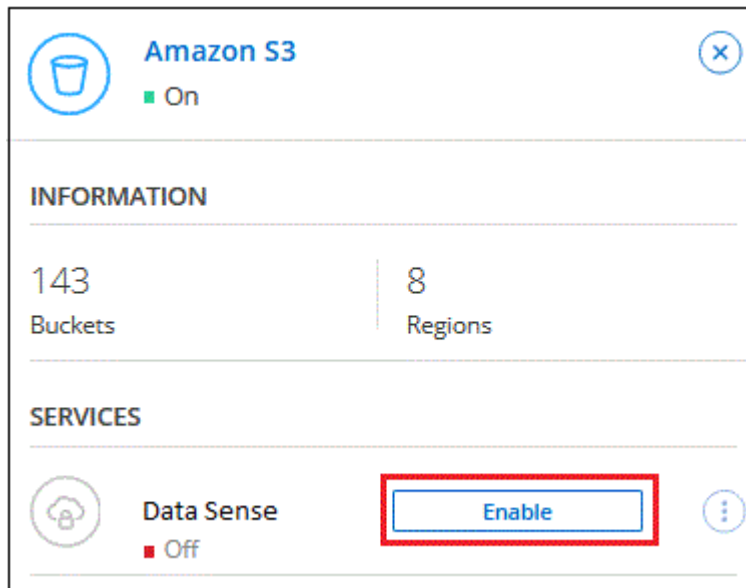
Aktivieren Sie Cloud Data Sense auf Amazon S3, nachdem Sie die Voraussetzungen überprüft haben.

Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Speicherung > Leinwand**.
2. Wählen Sie die Amazon S3-Arbeitsumgebung aus.



3. Klicken Sie im Bereich Datensinn auf der rechten Seite auf **Aktivieren**.



4. Wenn Sie dazu aufgefordert werden, weisen Sie der Cloud Data Sense Instanz eine IAM-Rolle zu [Die erforderlichen Berechtigungen](#).

Assign an AWS IAM Role for Cloud Data Sense

To enable **Cloud Data Sense** on Amazon S3 buckets, select an existing IAM Role. Make sure that your AWS IAM Role has the permission defined in the [Policy Requirements](#).

Select IAM Role

occm

VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so **Data Sense** can securely scan the data.

Alternatively, ensure that the **Data Sense** instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Free for the 1st TB

Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable

Cancel

5. Klicken Sie Auf **Aktivieren**.



Sie können auch Compliance-Scans für eine Arbeitsumgebung über die Konfigurationsseite aktivieren, indem Sie auf die klicken Und wählen Sie **Datensense aktivieren**.

Ergebnis

BlueXP weist der Instanz die IAM-Rolle zu.

Aktivieren und Deaktivieren von Compliance-Scans auf S3-Buckets

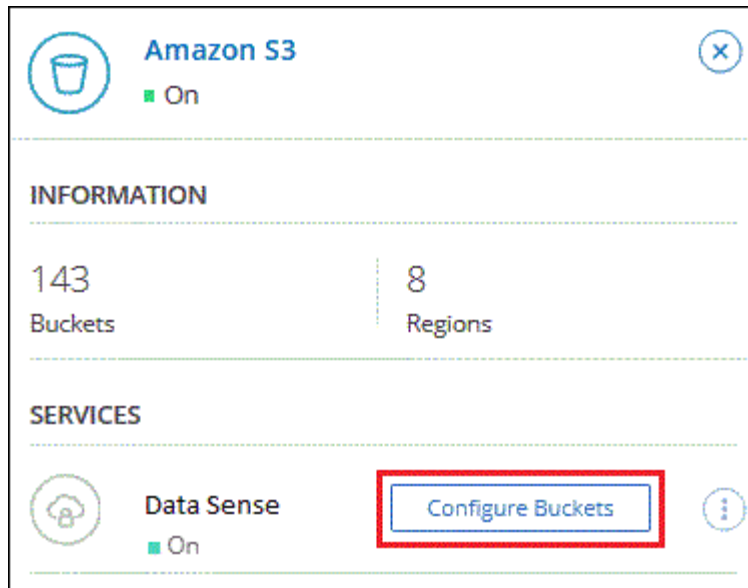
Nachdem BlueXP Cloud Data Sense in Amazon S3 aktiviert hat, müssen im nächsten Schritt die Buckets konfiguriert werden, die gescannt werden sollen.

Wenn BlueXP im AWS Konto ausgeführt wird, das über die S3-Buckets verfügt, die Sie scannen möchten, erkennt es diese Buckets und zeigt sie in einer Amazon S3-Arbeitsumgebung an.

Cloud Data Sense kann es auch [Scannen von S3-Buckets, die in unterschiedlichen AWS Konten vorhanden sind](#).

Schritte

1. Wählen Sie die Amazon S3-Arbeitsumgebung aus.
2. Klicken Sie im rechten Fensterbereich auf **Eimer konfigurieren**.



3. Aktivieren Sie Scans, die nur mappen oder Scans zuordnen und klassifizieren, auf Ihren Buckets.

Amazon S3 Configuration			
15/28 Buckets in Scan Scope.			
Scan	Bucket Name	Status	Required Action
Off Map Map & Classify	BucketName1	● Not Scanning	Add Credentials
Off Map Map & Classify	BucketName2	● Continuously Scanning	
Off Map Map & Classify	BucketName3	● Not Scanning	

An:	Tun Sie dies:
Ermöglichen Sie Mapping-Only-Scans auf einem Bucket	Klicken Sie Auf Karte
Aktivieren vollständiger Scans auf einem Bucket	Klicken Sie Auf Karte & Klassieren
Deaktivieren des Scans auf einem Bucket	Klicken Sie Auf Aus

Ergebnis

Cloud Data Sense beginnt mit dem Scannen der aktivierten S3 Buckets. Wenn Fehler auftreten, werden sie neben der erforderlichen Aktion zur Behebung des Fehlers in der Spalte Status angezeigt.

Scannen von Buckets für weitere AWS Konten

Sie können S3-Buckets scannen, die sich unter einem anderen AWS-Konto befinden, indem Sie über dieses Konto eine Rolle zuweisen, um auf die vorhandene Cloud Data Sense Instanz zuzugreifen.





Schritte

1. Gehen Sie zum AWS Ziel-Konto, in dem Sie S3 Buckets scannen und eine IAM-Rolle erstellen möchten, indem Sie **ein weiteres AWS-Konto** auswählen.

Create role




Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*

- Options**
- ☐ Require external ID (Best practice when a third party will assume this role)
 - ☐ Require MFA 

Gehen Sie wie folgt vor:

- Geben Sie die ID des Kontos ein, auf dem sich die Cloud Data Sense Instanz befindet.
- Ändern Sie die maximale CLI/API-Sitzungsdauer* von 1 Stunde auf 12 Stunden und speichern Sie diese Änderung.
- Hängen Sie die Cloud Data Sense IAM-Richtlinie an. Stellen Sie sicher, dass es über die erforderlichen Berechtigungen verfügt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Gehen Sie zum AWS-Quellkonto, in dem sich die Datensense-Instanz befindet, und wählen Sie die IAM-Rolle aus, die mit der Instanz verbunden ist.
 - a. Ändern Sie die maximale CLI/API-Sitzungsdauer* von 1 Stunde auf 12 Stunden und speichern Sie diese Änderung.
 - b. Klicken Sie auf **Richtlinien anhängen** und dann auf **Richtlinien erstellen**.
 - c. Erstellen Sie eine Richtlinie, die die Aktion „STS:AssumeRole“ enthält, und geben Sie den ARN der Rolle an, die Sie im Zielkonto erstellt haben.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

Das Cloud Data Sense Instanzprofil hat nun Zugriff auf das zusätzliche AWS Konto.

3. Gehen Sie auf die Seite **Amazon S3 Configuration** und das neue AWS-Konto wird angezeigt. Beachten Sie, dass es einige Minuten dauern kann, bis Cloud Data Sense die Arbeitsumgebung des neuen Kontos synchronisiert und diese Informationen anzeigt.



4. Klicken Sie auf **Daten aktivieren Sense & Buckets auswählen** und wählen Sie die Eimer aus, die Sie scannen möchten.

Ergebnis

Cloud Data Sense beginnt mit dem Scannen der neuen aktivierten S3 Buckets.

Datenbankschemas werden gescannt

Führen Sie einige Schritte durch, um den Scan des Datenbankschemas mit Cloud Data Sense 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 Sie die Cloud Data Sense Instanz

["Sinnvolle Implementierung Von Cloud-Daten"](#) 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

Die folgenden Voraussetzungen prüfen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie Cloud Data Sense aktivieren.

Unterstützte Datenbanken

Cloud Data Sense kann Schemen 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 mit Anbindung an die Cloud Data Sense Instanz kann unabhängig vom gehosteten Speicherort 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 Kennworts ist es wichtig, einen zu wählen, der volle Lese-Berechtigungen für alle Schemas und Tabellen, die Sie scannen möchten. Es wird empfohlen, einen dedizierten Benutzer für das Cloud Data Sense System mit allen erforderlichen Berechtigungen zu erstellen.

Hinweis: für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

Bereitstellen der Cloud Data Sense Instanz

Implementieren Sie Cloud-Daten sinnvoll, wenn noch keine Instanz implementiert ist.

Wenn Sie Datenbankschemas scannen, die über das Internet zugänglich sind, können Sie dies tun "[Cloud-Daten sinnvoll in der Cloud implementieren](#)" Oder "[Implementieren Sie Data Sense in einem lokalen Standort mit Internetzugang](#)".

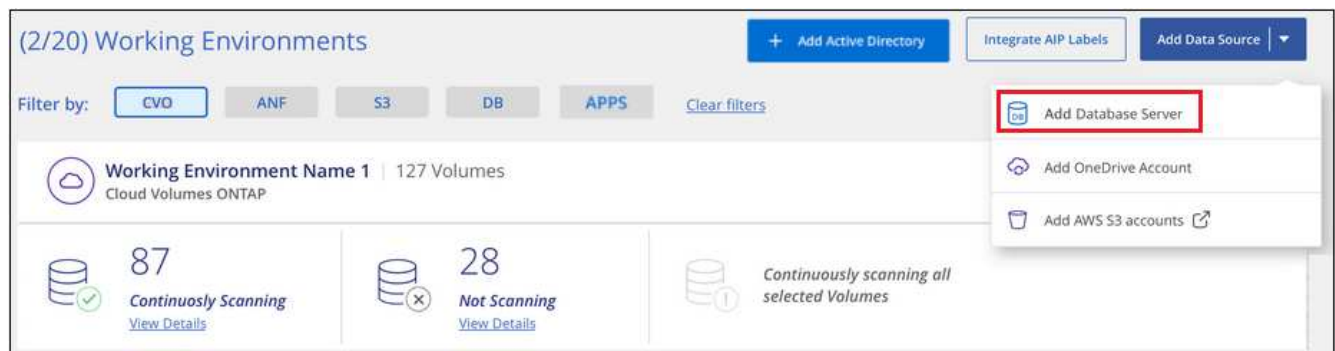
Wenn Sie Datenbankschemas scannen, die in einer dunklen Site installiert wurden, die keinen Internetzugang hat, müssen Sie dies tun "[Cloud Data Sense implementieren – auf demselben lokalen Standort ohne Internetzugang](#)". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des Datenbankservers

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.

- Wählen Sie den Datenbanktyp aus.
- Geben Sie den Port und den Hostnamen oder die IP-Adresse ein, um eine Verbindung zur Datenbank herzustellen.
- Geben Sie für Oracle-Datenbanken den Dienstnamen ein.
- Geben Sie die Anmeldeinformationen ein, damit Cloud Data Sense auf den Server zugreifen kann.
- 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
<input type="text"/>	<input type="text"/>
Port	Service Name
<input type="text"/>	<input type="text"/>

Credentials

Username	Password
<input type="text"/>	<input type="text"/>

Die Datenbank wird zur Liste der Arbeitsumgebungen hinzugefügt.

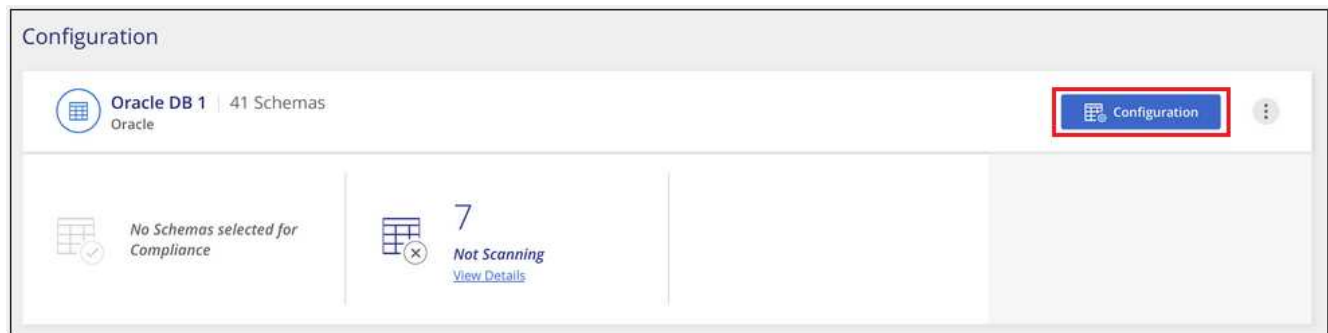
Aktivieren und Deaktivieren von Compliance-Scans auf Datenbankschemas

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

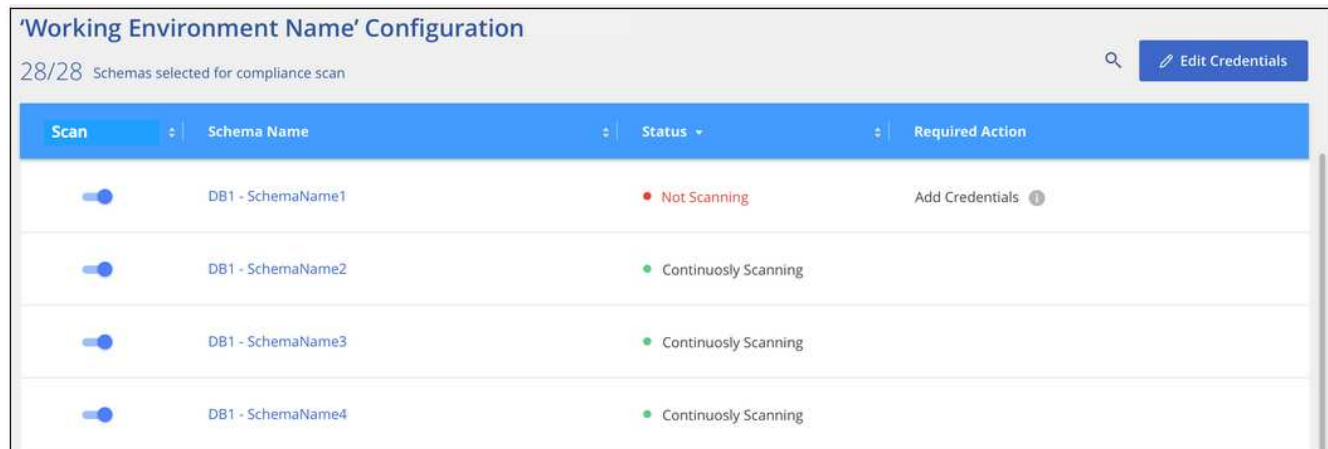


Es besteht keine Möglichkeit, nur mappingbare Scans für Datenbankschemas auszuwählen.

- 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

Cloud Data Sense beginnt mit dem Scannen des von Ihnen aktivierten Datenbankschemas. Wenn Fehler auftreten, werden sie in der Spalte Status angezeigt, neben der erforderlichen Aktion, um den Fehler zu beheben.

OneDrive-Konten werden gescannt

Führen Sie einige Schritte aus, um mit Cloud Data Sense Dateien in OneDrive Ordnern Ihres Benutzers zu scannen.

Schnellstart

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

1

Alle Voraussetzungen für OneDrive prüfen

Stellen Sie sicher, dass Sie über die Administratoranmeldeinformationen verfügen, um sich beim OneDrive-Konto anzumelden.

2

Implementieren Sie die Cloud Data Sense Instanz

"Sinnvolle Implementierung Von Cloud-Daten" Falls noch keine Instanz implementiert wurde.

3

Fügen Sie das OneDrive Konto hinzu

Melden Sie sich bei Verwendung der Admin-Benutzeranmeldeinformationen beim OneDrive-Konto an, auf das Sie zugreifen möchten, damit es als neue Arbeitsumgebung hinzugefügt wird.

4

Fügen Sie die Benutzer hinzu und wählen Sie den Scantyp aus

Fügen Sie die Liste der Benutzer aus dem OneDrive-Konto hinzu, das Sie scannen möchten, und wählen Sie den Scantyp aus. Sie können bis zu 100 Benutzer gleichzeitig hinzufügen.

OneDrive Anforderungen können Sie überprüfen

Die folgenden Voraussetzungen prüfen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie Cloud Data Sense aktivieren.

- Sie müssen über die Admin-Anmeldeinformationen für das OneDrive for Business-Konto verfügen, das Lesezugriff auf die Dateien des Benutzers bietet.
- Für alle Benutzer, deren OneDrive-Ordner Sie scannen möchten, benötigen Sie eine Liste mit den E-Mail-Adressen, die in einer Zeile getrennt sind.

Bereitstellen der Cloud Data Sense Instanz

Implementieren Sie Cloud-Daten sinnvoll, wenn noch keine Instanz implementiert ist.

Der Sinn für Daten kann sein ["In der Cloud implementiert"](#) Oder ["In einer Anlage mit Internetzugang"](#).

Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

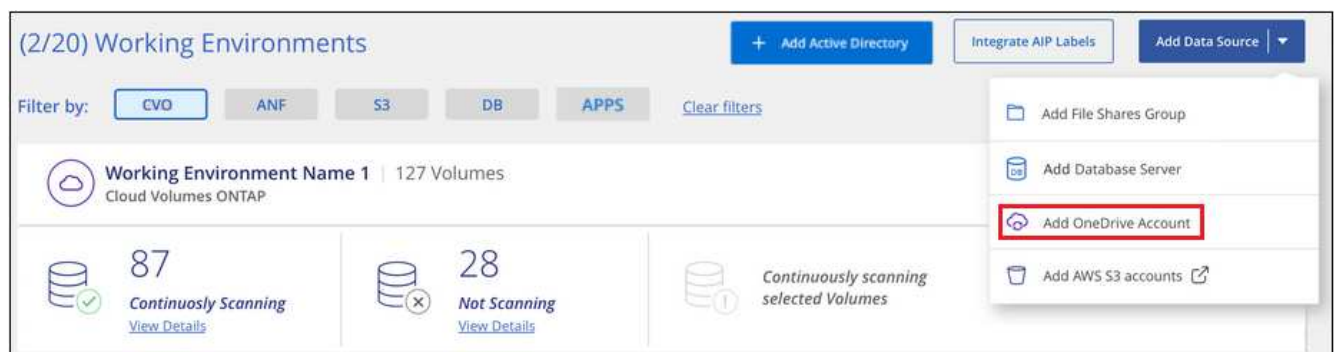
Auch der Datensinn kann sein ["Die Implementierung erfolgt an einem lokalen Standort ohne Internetzugang"](#). Allerdings müssen Sie einen Internetzugang für einige ausgewählte Endpunkte zur Verfügung stellen, um Ihre lokalen OneDrive-Dateien zu scannen. ["Hier finden Sie die Liste der erforderlichen Endpunkte"](#).

Hinzufügen des OneDrive Kontos

Fügen Sie das OneDrive-Konto hinzu, in dem sich die Benutzerdateien befinden.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen > OneDrive Konto hinzufügen**.



2. Klicken Sie im Dialogfeld „OneDrive-Konto hinzufügen“ auf **Anmelden bei OneDrive**.
3. Wählen Sie auf der angezeigten Microsoft-Seite das OneDrive-Konto aus und geben Sie den erforderlichen Admin-Benutzer und das entsprechende Passwort ein. Klicken Sie dann auf **Akzeptieren**, damit Cloud Data Sense Daten aus diesem Konto lesen kann.

Das OneDrive-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

Hinzufügen von OneDrive Benutzern zu Compliance-Scans

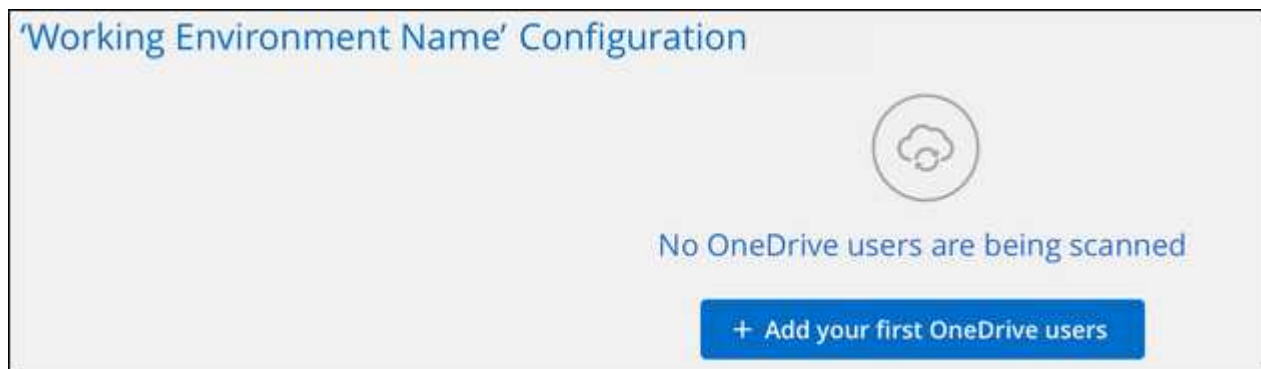
Sie können einzelne OneDrive-Benutzer oder alle OneDrive-Benutzer hinzufügen, damit ihre Dateien nach Cloud Data Sense gescannt werden.

Schritte

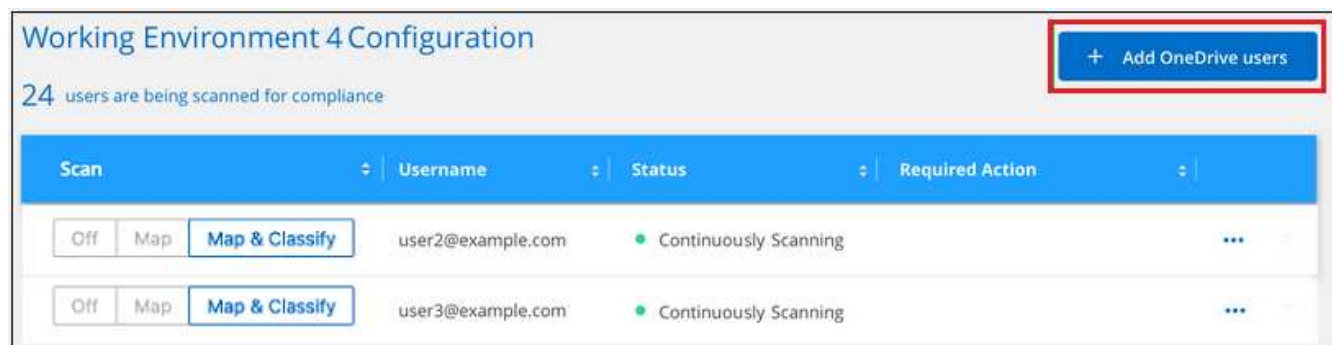
1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Configuration** für das OneDrive-Konto.



2. Wenn dies das erste Mal ist, Benutzer für dieses OneDrive-Konto hinzuzufügen, klicken Sie auf **Fügen Sie Ihre ersten OneDrive-Benutzer**.

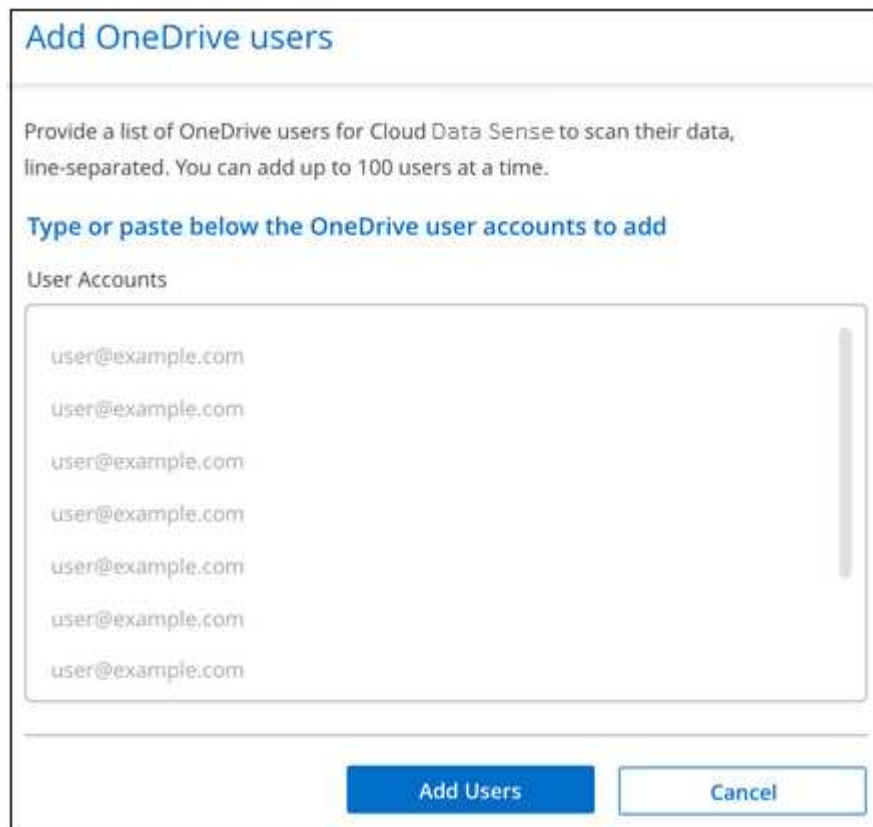


Wenn Sie weitere Benutzer aus einem OneDrive-Konto hinzufügen möchten, klicken Sie auf **OneDrive Users hinzufügen**.



3. Fügen Sie die E-Mail-Adressen für die Benutzer hinzu, deren Dateien Sie scannen möchten - eine E-Mail-

Adresse pro Zeile (bis zu 100 maximal pro Sitzung) - und klicken Sie auf **Benutzer hinzufügen**.



In einem Bestätigungsdialegfeld wird die Anzahl der Benutzer angezeigt, die hinzugefügt wurden.

Wenn im Dialogfeld Benutzer aufgeführt werden, die nicht hinzugefügt werden konnten, erfassen Sie diese Informationen, damit Sie das Problem beheben können. In einigen Fällen können Sie den Benutzer mit einer korrigierten E-Mail-Adresse erneut hinzufügen.

4. Ermöglichen Sie Scans, die nur zugeordnet werden können, oder Mapping- und Klassifizierungsprüfungen auf Benutzerdateien.

An:	Tun Sie dies:
Aktivieren Sie mappingonly Scans von Benutzerdateien	Klicken Sie Auf Karte
Aktivieren Sie vollständige Scans von Benutzerdateien	Klicken Sie Auf Karte & Klassieren
Deaktivieren Sie das Scannen von Benutzerdateien	Klicken Sie Auf Aus

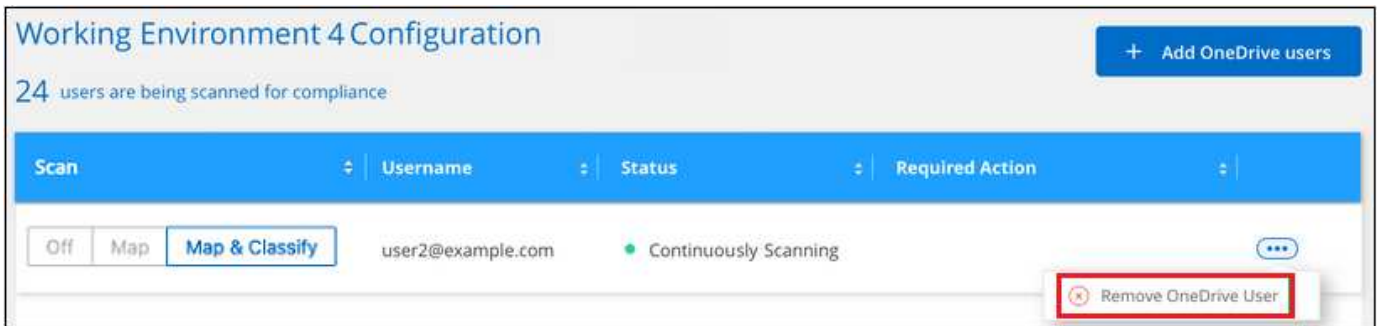
Ergebnis

Cloud Data Sense beginnt mit dem Scannen der Dateien für die Benutzer, die Sie hinzugefügt haben, und die Ergebnisse werden im Dashboard und an anderen Orten angezeigt.

Entfernen eines OneDrive-Benutzers aus Compliance-Scans

Wenn Benutzer das Unternehmen verlassen oder sich ihre E-Mail-Adresse ändert, können Sie einzelne OneDrive Benutzer davon entfernen, dass ihre Dateien jederzeit gescannt werden können. Klicken Sie einfach

auf **OneDrive User entfernen** von der Konfigurationsseite.



Beachten Sie, dass Sie können "[Löschen Sie das gesamte OneDrive-Konto aus Data Sense](#)" Wenn Sie keine Benutzerdaten mehr aus dem OneDrive-Konto scannen möchten.

Scannen von SharePoint-Konten

Führen Sie einige Schritte durch, um mit Cloud Data Sense Dateien in Ihren SharePoint Online- und SharePoint On-Premise-Accounts zu scannen.

Schnellstart

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

1

SharePoint-Voraussetzungen prüfen

Stellen Sie sicher, dass Sie über die Administratoranmeldeinformationen verfügen, um sich beim SharePoint-Konto anzumelden, und dass Sie über die URLs für die SharePoint-Sites verfügen, die Sie scannen möchten.

2

Implementieren Sie die Cloud Data Sense Instanz

["Sinnvolle Implementierung Von Cloud-Daten"](#) Falls noch keine Instanz implementiert wurde.

3

Melden Sie sich beim SharePoint-Konto an

Melden Sie sich mit den Anmeldedaten des Admin-Benutzers beim SharePoint-Konto an, auf das Sie zugreifen möchten, damit es als neue Datenquelle/Arbeitsumgebung hinzugefügt wird.

4

Fügen Sie die URLs der SharePoint-Website zum Scannen hinzu

Fügen Sie die Liste der SharePoint-Website-URLs hinzu, die Sie im SharePoint-Konto scannen möchten, und wählen Sie den Scantyp aus. Sie können bis zu 100 URLs gleichzeitig hinzufügen.

Überprüfung der SharePoint Anforderungen

Prüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie Cloud Data Sense in einem SharePoint Konto aktivieren können.

- Sie müssen über die Admin-Anmeldeinformationen für das SharePoint-Konto verfügen, das Lesezugriff auf alle SharePoint-Sites bietet.
- Für SharePoint vor Ort benötigen Sie auch die URL des SharePoint Servers.
- Für alle zu scannenden Daten benötigen Sie eine Liste der URLs der SharePoint-Website.

Bereitstellen der Cloud Data Sense Instanz

Implementieren Sie Cloud-Daten sinnvoll, wenn noch keine Instanz implementiert ist.

- Für SharePoint Online kann Data Sense verwendet werden ["In der Cloud implementiert"](#) Oder ["An einem lokalen Standort mit Internetzugang installiert"](#).

Auch der Datensinn kann sein ["Die Implementierung erfolgt an einem lokalen Standort ohne Internetzugang"](#). Sie müssen jedoch einige ausgewählte Endpunkte im Internet öffnen, um Ihre SharePoint Online-Dateien zu scannen. ["Hier finden Sie die Liste der erforderlichen Endpunkte"](#).

- Für SharePoint On-Premises-Systeme kann Data Sense installiert werden ["In einer Anlage mit Internetzugang"](#) Oder ["In einem Hotel, das keinen Internetzugang hat"](#).

Wenn Data Sense auf einer Website ohne Internetzugang installiert wird, muss der BlueXP Connector auch ohne Internetzugang auf derselben Website installiert sein. ["Weitere Informationen ."](#)

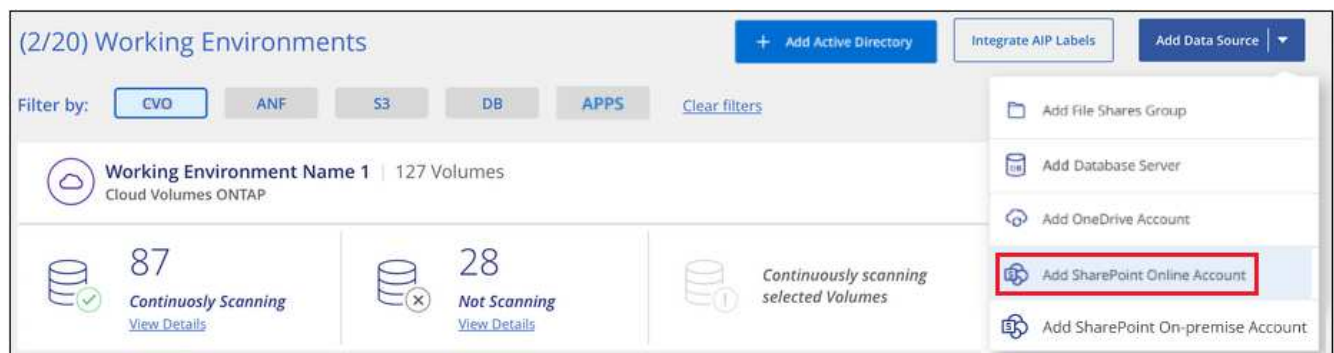
Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen eines SharePoint Online-Kontos

Fügen Sie das SharePoint Online-Konto hinzu, in dem sich die Benutzerdateien befinden.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen > SharePoint Online-Konto hinzufügen**.



2. Klicken Sie im Dialogfeld SharePoint Online-Konto hinzufügen auf **in SharePoint anmelden**.
3. Wählen Sie auf der angezeigten Microsoft-Seite das SharePoint-Konto aus und geben Sie den erforderlichen Admin-Benutzer und das erforderliche Passwort ein. Klicken Sie dann auf **Akzeptieren**, damit Cloud Data Sense Daten aus diesem Konto lesen kann.

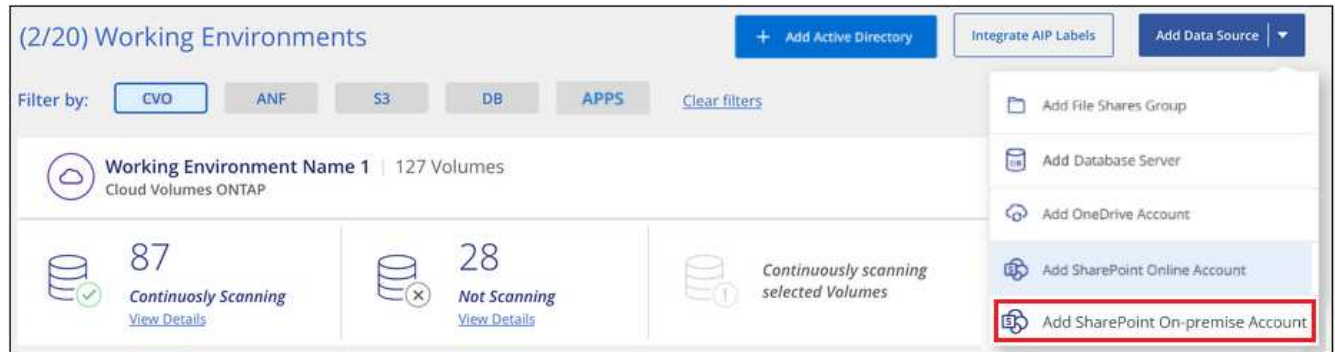
Das SharePoint Online-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

Hinzufügen eines SharePoint-Kontos vor Ort

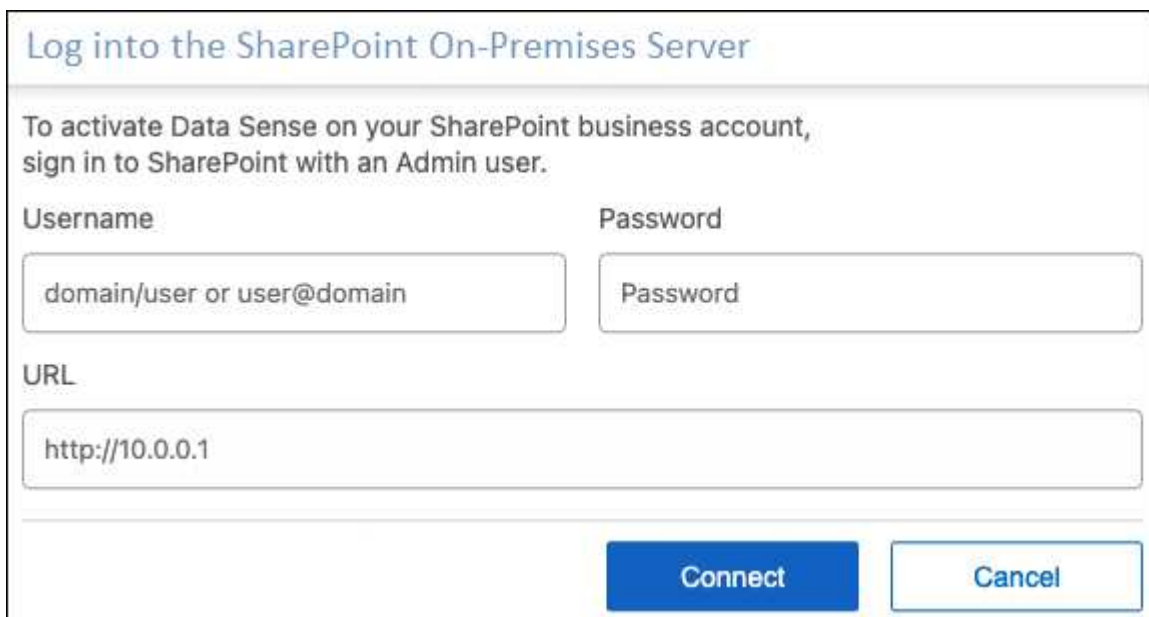
Fügen Sie das SharePoint-On-Premise-Konto hinzu, in dem sich die Benutzerdateien befinden.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen > SharePoint On-Premise-Konto hinzufügen**.



2. Geben Sie im Dialogfeld beim SharePoint-On-Premise-Server anmelden die folgenden Informationen ein:
 - Admin-Benutzer im Format „Domäne/Benutzer“ oder „Benutzer@Domäne“ und „Admin-Passwort“
 - URL des SharePoint Servers

The screenshot shows a dialog box titled 'Log into the SharePoint On-Premises Server'. The text inside says 'To activate Data Sense on your SharePoint business account, sign in to SharePoint with an Admin user.' Below this, there are three input fields: 'Username' with a placeholder 'domain/user or user@domain', 'Password' with a placeholder 'Password', and 'URL' with a placeholder 'http://10.0.0.1'. At the bottom, there are two buttons: 'Connect' and 'Cancel'.

3. Klicken Sie Auf **Verbinden**.

Das On-Premise-Konto SharePoint wird zur Liste der Arbeitsumgebungen hinzugefügt.

Hinzufügen von SharePoint Sites zu Compliance-Scans

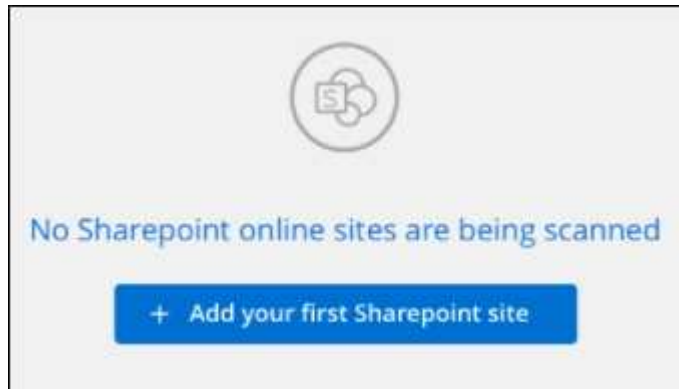
Sie können einzelne SharePoint-Sites oder alle SharePoint-Sites im Konto hinzufügen, damit die zugehörigen Dateien nach Cloud Data Sense gescannt werden. Die Schritte sind die gleichen, wenn SharePoint Online oder SharePoint On-Premise-Websites hinzugefügt werden.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Configuration** für das SharePoint-Konto.



2. Wenn dies das erste Mal ist, Websites für dieses SharePoint-Konto hinzuzufügen, klicken Sie auf **Ihre erste SharePoint-Website hinzufügen**.



Wenn Sie weitere Benutzer von einem SharePoint-Konto hinzufügen, klicken Sie auf **SharePoint-Sites hinzufügen**.



3. Fügen Sie die URLs für die Seiten hinzu, deren Dateien Sie scannen möchten - eine URL pro Zeile (bis zu 100 maximal pro Sitzung) - und klicken Sie auf **Sites hinzufügen**.

In einem Bestätigungsdiaologfeld wird die Anzahl der hinzugefügten Standorte angezeigt.

Wenn im Dialogfeld keine Sites aufgeführt sind, die nicht hinzugefügt werden konnten, erfassen Sie diese Informationen, damit Sie das Problem beheben können. In einigen Fällen können Sie die Site mit einer korrigierten URL erneut hinzufügen.

4. Ermöglichen Sie auf den Dateien auf den SharePoint-Sites Mapping- und Klassifizierungscans.

An:	Tun Sie dies:
Aktivieren Sie Mapping-Only-Scans auf Dateien	Klicken Sie Auf Karte
Aktivieren Sie vollständige Scans auf Dateien	Klicken Sie Auf Karte & Klassieren
Deaktivieren Sie das Scannen von Dateien	Klicken Sie Auf Aus

Ergebnis

Cloud Data Sense beginnt mit dem Scannen der Dateien in den hinzugefügten SharePoint-Sites und die Ergebnisse werden im Dashboard und an anderen Speicherorten angezeigt.

Entfernen einer SharePoint-Website aus Compliance-Scans

Wenn Sie eine SharePoint-Site in der Zukunft entfernen oder sich entscheiden, keine Dateien auf einer SharePoint-Site zu scannen, können Sie einzelne SharePoint-Sites davon entfernen, dass ihre Dateien jederzeit gescannt werden. Klicken Sie einfach auf **SharePoint-Website entfernen** von der Konfigurationsseite.

Scan	Site URL	Status	Required Action
Off Map Map & Classify	Site URL	Continuously Scanning	...
Off Map Map & Classify	Site URL	Continuously Scanning	Remove SharePoint Site

Beachten Sie, dass Sie können "[Löschen Sie das gesamte SharePoint-Konto aus Data Sense](#)" Wenn Sie keine Benutzerdaten mehr vom SharePoint-Konto scannen möchten.

Google Drive-Konten werden durchsucht

Führen Sie einige Schritte aus, um das Scannen von Benutzerdateien in Ihren Google Drive-Konten mit Cloud Data Sense zu starten.

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 Google Drive

Stellen Sie sicher, dass Sie über die Administratoranmeldeinformationen verfügen, um sich beim Google Drive-Konto anzumelden.

2

Sinnvolle Implementierung Von Cloud-Daten

["Sinnvolle Implementierung Von Cloud-Daten"](#) Falls noch keine Instanz implementiert wurde.

3

Melden Sie sich beim Google Drive-Konto an

Wenn Sie Admin-Benutzeranmeldeinformationen verwenden, melden Sie sich beim Google Drive-Konto an, auf das Sie zugreifen möchten, damit es als neue Datenquelle hinzugefügt wird.

4

Wählen Sie den Scantyp für die Benutzerdateien aus

Wählen Sie den Scantyp aus, den Sie für die Benutzerdateien durchführen möchten; Zuordnen oder Zuordnen und Klassifizieren.

Überprüfen der Google-Laufwerksanforderungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie Cloud Data Sense auf einem Google Drive-Konto aktivieren können.

- Sie müssen über die Admin-Anmeldeinformationen für das Google Drive-Konto verfügen, das Lesezugriff auf die Dateien des Benutzers bietet

Aktuelle Einschränkungen

Die folgenden Data Sense-Funktionen werden derzeit nicht von Google Drive-Dateien unterstützt:

- Beim Anzeigen von Dateien auf der Seite „Datenuntersuchung“ sind die Aktionen in der Schaltflächenleiste nicht aktiv. Sie können keine Dateien kopieren, verschieben, löschen usw..
- Berechtigungen können nicht innerhalb von Dateien in Google Drive identifiziert werden, daher werden auf der Untersuchungsseite keine Berechtigungsinformationen angezeigt.

Cloud Data Sense Implementieren

Implementieren Sie Cloud-Daten sinnvoll, wenn noch keine Instanz implementiert ist.

Der Sinn für Daten kann sein ["In der Cloud implementiert"](#) Oder ["In einer Anlage mit Internetzugang"](#).

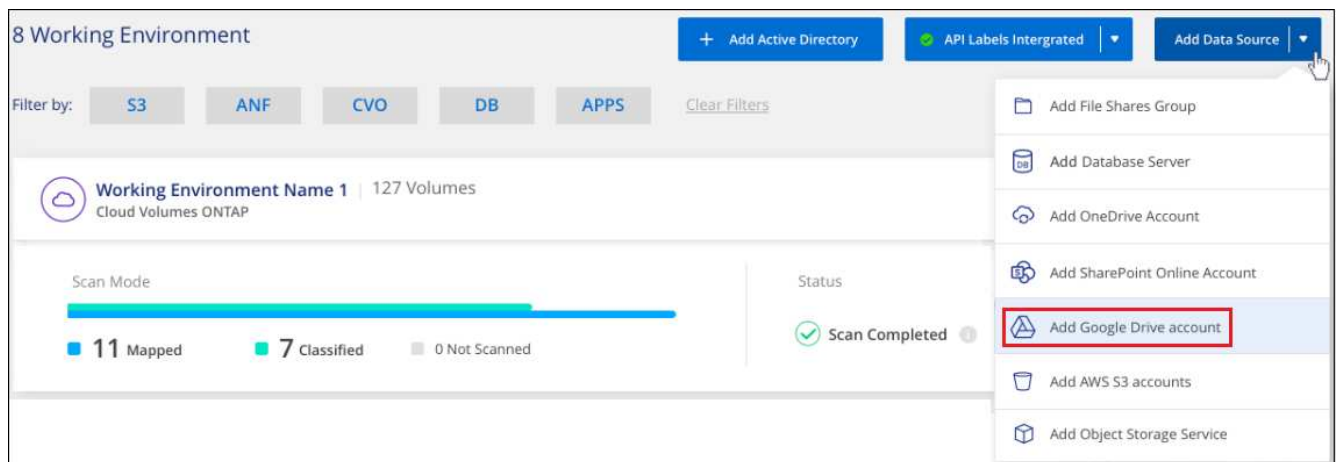
Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des Google Drive-Kontos

Fügen Sie das Google Drive-Konto hinzu, in dem sich die Benutzerdateien befinden. Wenn Sie Dateien von mehreren Benutzern scannen möchten, müssen Sie diesen Schritt für jeden Benutzer ausführen.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen > Google Drive Account hinzufügen**.



2. Klicken Sie im Dialogfeld „Google Drive Account hinzufügen“ auf **beim Google Drive** anmelden.
3. Wählen Sie auf der angezeigten Google-Seite das Google Drive-Konto aus und geben Sie den erforderlichen Admin-Benutzer und das Passwort ein. Klicken Sie dann auf **Akzeptieren**, damit Cloud Data Sense Daten aus diesem Konto lesen kann.

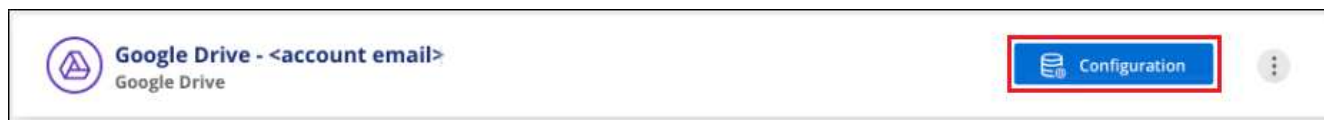
Das Google Drive-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

Auswählen des Scantyps für Benutzerdaten

Wählen Sie die Art des Scans aus, die Cloud Data Sense für die Daten des Benutzers ausführen soll.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Konfiguration** für das Google Drive-Konto.



2. Aktivieren Sie mapping-only Scans oder Mapping- und Klassifizierungsscans auf den Dateien im Google Drive-Konto.



An:	Tun Sie dies:
Aktivieren Sie Mapping-Only-Scans auf Dateien	Klicken Sie Auf Karte
Aktivieren Sie vollständige Scans auf Dateien	Klicken Sie Auf Karte & Klassieren
Deaktivieren Sie das Scannen von Dateien	Klicken Sie Auf Aus

Ergebnis

Cloud Data Sense beginnt mit dem Scannen der Dateien im Google Drive-Konto, das Sie hinzugefügt haben, und die Ergebnisse werden im Dashboard und an anderen Orten angezeigt.

Entfernen eines Google Drive-Kontos aus Compliance-Scans

Da nur die Google Drive-Dateien eines einzigen Benutzers Teil eines einzigen Google Drive-Kontos sind, wenn Sie die Suche von Dateien von einem Benutzer Google Drive-Konto beenden möchten, dann sollten Sie ["Löschen Sie das Google Drive-Konto aus Data Sense"](#).

Scannen von Dateifreigaben

Führen Sie einige Schritte durch, um die direkten Scans von NFS- oder CIFS-Dateifreigaben anderer Anbieter mit Cloud Data Sense zu starten. Diese Dateifreigaben können lokal oder in der Cloud gespeichert werden.

Schnellstart

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



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 Sie die Cloud Data Sense Instanz

["Sinnvolle Implementierung Von Cloud-Daten"](#) 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 hinzu und wählen Sie die zu scannenden Freigaben aus

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

Die folgenden Voraussetzungen prüfen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie Cloud Data Sense aktivieren.

- Die Shares können überall gehostet werden, auch in der Cloud oder vor Ort. Es handelt sich dabei um File Shares, die auf Storage-Systemen anderer Anbieter residieren.
- Es muss eine Netzwerkverbindung zwischen der Instanz Data Sense und den Freigaben bestehen.
- Stellen Sie sicher, dass diese Ports für die Data Sense-Instanz offen sind:
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
- 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.
- Stellen Sie für CIFS-Freigaben (SMB) sicher, dass Sie über Active Directory-Anmeldeinformationen verfügen, die Lesezugriff auf die Freigaben bieten. Administratorberechtigungen sind bevorzugte Zugangsdaten für den Fall, dass Cloud Data Sense Daten scannen muss, die erhöhte Berechtigungen erfordern.

Wenn Sie sicherstellen möchten, dass Ihre Dateien „letzte Zugriffszeiten“ durch Data Sense Klassifizierungsscans unverändert bleiben, empfehlen wir dem Benutzer die Berechtigung Schreibattribute zu besitzen. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

Bereitstellen der Cloud Data Sense Instanz

Implementieren Sie Cloud-Daten sinnvoll, wenn noch keine Instanz implementiert ist.

Wenn Sie nicht-NetApp NFS- oder CIFS-File Shares scannen, die über das Internet zugänglich sind, können Sie sie ausführen ["Cloud-Daten sinnvoll in der Cloud implementieren"](#) Oder ["Implementieren Sie Data Sense in einem lokalen Standort mit Internetzugang"](#).

Wenn Sie nicht-NetApp NFS- oder CIFS-File Shares scannen, die in einer dunklen Site installiert wurden und über keinen Internetzugang verfügen, müssen Sie sie verwenden "[Cloud Data Sense implementieren – auf demselben lokalen Standort ohne Internetzugang](#)". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

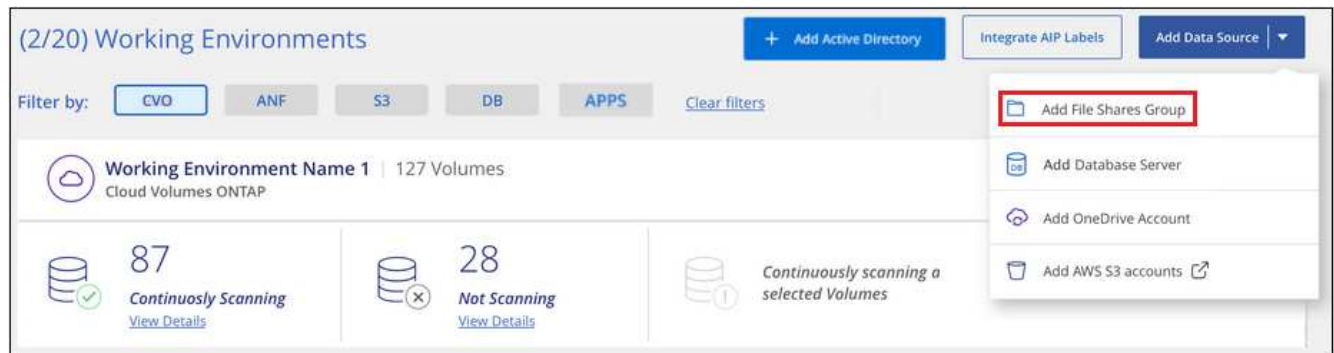
Erstellen der Gruppe für die Dateifreigaben

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 File Shares-Gruppe Dateifreigaben hinzu, damit die Dateien in diesen Freigaben nach Cloud Data Sense 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

Ergebnis

Cloud Data Sense beginnt mit dem Scannen der Dateien in den hinzugefügten Dateifreigaben und die Ergebnisse werden im Dashboard und an anderen Speicherorten 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**.



Objekt-Storage wird mit S3-Protokoll gescannt

Führen Sie einige Schritte durch, um Daten direkt im Objekt-Storage mit Cloud Data Sense zu scannen. Data Sense kann Daten von jedem Objekt-Storage-Service scannen, der das Simple Storage Service (S3)-Protokoll verwendet. Dazu zählen NetApp StorageGRID, IBM Cloud Object Store, Azure Blob (mit Minio), Linode, B2 Cloud Storage und Amazon S3.

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 den Objekt-Storage

Es muss die Endpunkt-URL vorhanden sein, um eine Verbindung mit dem Objekt-Storage-Service herzustellen.

Sie benötigen den Zugriffsschlüssel und den geheimen Schlüssel vom Objekt-Storage-Provider, damit Cloud Data Sense auf die Buckets zugreifen kann.

2

Implementieren Sie die Cloud Data Sense Instanz

["Sinnvolle Implementierung Von Cloud-Daten"](#) Falls noch keine Instanz implementiert wurde.

3

Fügen Sie den Objekt-Storage-Service hinzu

Fügen Sie den Objekt-Storage-Service Cloud Data Sense hinzu.

4

Wählen Sie die zu scannenden Buckets aus

Wählen Sie die Buckets aus, die Sie scannen möchten, und Cloud Data Sense beginnt mit dem Scannen.

Überprüfung der Objekt-Storage-Anforderungen

Die folgenden Voraussetzungen prüfen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie Cloud Data Sense aktivieren.

- Es muss die Endpunkt-URL vorhanden sein, um eine Verbindung mit dem Objekt-Storage-Service herzustellen.
- Sie benötigen den Zugriffsschlüssel und den geheimen Schlüssel vom Objekt-Storage-Provider, damit Data Sense auf die Buckets zugreifen kann.
- Für die Unterstützung für Azure Blob müssen Sie den verwenden ["Minio Service"](#).

Bereitstellen der Cloud Data Sense Instanz

Implementieren Sie Cloud-Daten sinnvoll, wenn noch keine Instanz implementiert ist.

Wenn Sie Daten aus dem S3-Objektspeicher scannen, auf den über das Internet zugegriffen werden kann, ist die entsprechende Möglichkeit möglich ["Cloud-Daten sinnvoll in der Cloud implementieren"](#) Oder ["Implementieren Sie Data Sense in einem lokalen Standort mit Internetzugang"](#).

Wenn Sie Daten vom S3 Objekt-Storage scannen, der auf einem dunklen Standort ohne Internetzugang installiert wurde, müssen Sie sie überprüfen ["Cloud Data Sense implementieren – auf demselben lokalen Standort ohne Internetzugang"](#). Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

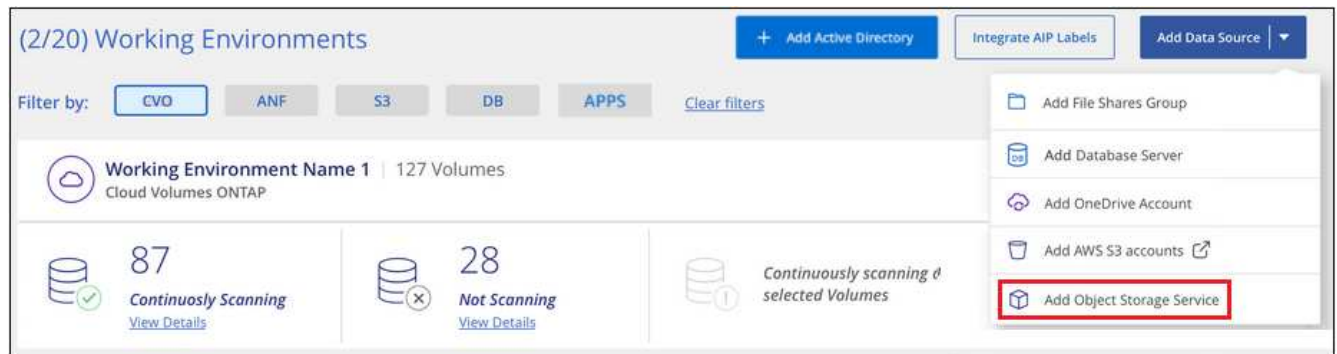
Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des Objekt-Storage-Service zu Cloud Data Sense

Fügen Sie den Objekt-Storage-Service hinzu.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen > Objekt-Storage-Service hinzufügen**.



2. Geben Sie im Dialogfeld Add Object Storage Service die Details für den Objekt-Speicherdienst ein und klicken Sie auf **Continue**.
 - a. Geben Sie den Namen ein, den Sie für die Arbeitsumgebung verwenden möchten. Dieser Name sollte den Namen des Objektspeicherdienstes widerspiegeln, mit dem Sie eine Verbindung herstellen.
 - b. Geben Sie die Endpunkt-URL ein, um auf den Objekt-Storage-Service zuzugreifen.
 - c. Geben Sie den Zugriffsschlüssel und den geheimen Schlüssel ein, damit Cloud Data Sense auf die Buckets im Objekt-Storage zugreifen kann.

Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKD0574NDJG86795"/>	<input type="password" value="....."/>

Ergebnis

Der neue Objekt-Speicherdienst wird der Liste der Arbeitsumgebungen hinzugefügt.

Aktivieren und Deaktivieren von Compliance-Scans an Objekt-Storage-Buckets

Nachdem Sie Cloud Data Sense in Ihrem Objekt-Storage-Service aktiviert haben, konfigurieren Sie als nächstes die Buckets, die gescannt werden sollen. Data Sense erkennt diese Buckets und zeigt sie in der von Ihnen erstellten Arbeitsumgebung an.

Schritte

1. Klicken Sie auf der Konfigurationsseite in der Arbeitsumgebung Object Storage Service auf **Konfiguration**.

(1/20) Working Environments

Filter by: CVO ANF S3 DB APPS **OB.STG** [Clear filters](#)

Rstor Integrated | 41 Buckets

Configuration

23 Continuously Scanning [View Details](#)

All Buckets selected for Compliance

Continuously scanning all selected Buckets

2. Aktivieren Sie Scans, die nur mappen oder Scans zuordnen und klassifizieren, auf Ihren Buckets.

Rstor Integrated Configuration
3/55 Buckets selected for Compliance scan

Scan	Storage Repository (Bucket) ↓↑	Status ↓↑	Required Action ↓↑
<div>Off</div> <div>Map</div> <div>Map & Classify</div>	logs-759995470648-us-east-1	● Not Scanning	
<div>Off</div> <div>Map</div> <div>Map & Classify</div>	logs-759995470648-us-west-2	● Not Scanning	
<div>Off</div> <div>Map</div> <div>Map & Classify</div>	carstock	● Continuously Scanning	

An:	Tun Sie dies:
Ermöglichen Sie Mapping-Only-Scans auf einem Bucket	Klicken Sie Auf Karte
Aktivieren vollständiger Scans auf einem Bucket	Klicken Sie Auf Karte & Klassieren
Deaktivieren des Scans auf einem Bucket	Klicken Sie Auf Aus

Ergebnis

Cloud Data Sense beginnt mit dem Scannen der aktivierten Buckets. Wenn Fehler auftreten, werden sie neben der erforderlichen Aktion zur Behebung des Fehlers in der Spalte Status angezeigt.

Copyright-Informationen

Copyright © 2022 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, BEISPIELHAFT 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.