



# **Aktivieren Sie das Scannen Ihrer Datenquellen**

Cloud Manager 3.8

NetApp  
March 25, 2024

# Inhalt

- Aktivieren Sie das Scannen Ihrer Datenquellen ..... 1
  - Erste Schritte mit Cloud Compliance für Cloud Volumes ONTAP und Azure NetApp Files ..... 1
  - Erste Schritte mit Cloud Compliance für Amazon S3 ..... 6
- Datenbankschemas werden gescannt ..... 13
- Scannen lokaler ONTAP Daten mit Cloud-Compliance mit SnapMirror ..... 16

# Aktivieren Sie das Scannen Ihrer Datenquellen

## Erste Schritte mit Cloud Compliance für Cloud Volumes ONTAP und Azure NetApp Files

Erste Schritte mit Cloud Compliance für Cloud Volumes ONTAP oder Azure NetApp Files

### Schnellstart

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



#### Implementieren der Cloud Compliance-Instanz

"[Cloud Compliance in Cloud Manager implementieren](#)" Falls noch keine Instanz implementiert wurde.



#### Cloud Compliance in Ihren Arbeitsumgebungen

Klicken Sie auf **Cloud Compliance**, wählen Sie die Registerkarte **Konfiguration** und aktivieren Sie Compliance-Scans für bestimmte Arbeitsumgebungen.



#### Zugriff auf Volumes sicherstellen

Jetzt, wo Cloud Compliance aktiviert ist, stellen Sie sicher, dass die IT auf Volumes zugreifen kann.

- Die Cloud Compliance Instanz benötigt eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP- oder Azure NetApp Files-Subnetz.
- Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen aus der Cloud-Compliance-Instanz zulassen.
- Die NFS-Volume-Exportrichtlinien müssen den Zugriff aus der Cloud Compliance-Instanz zulassen.
- Cloud Compliance benötigt Active Directory-Anmeldeinformationen zum Scannen von CIFS Volumes.

Klicken Sie auf **Cloud Compliance > Scan-Konfiguration > CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an. Die Anmeldedaten können schreibgeschützt sein. Durch Admin-Berechtigungen wird jedoch sichergestellt, dass Cloud Compliance Daten lesen kann, die erhöhte Berechtigungen erfordern.



#### Konfigurieren Sie die Volumes für das Scannen

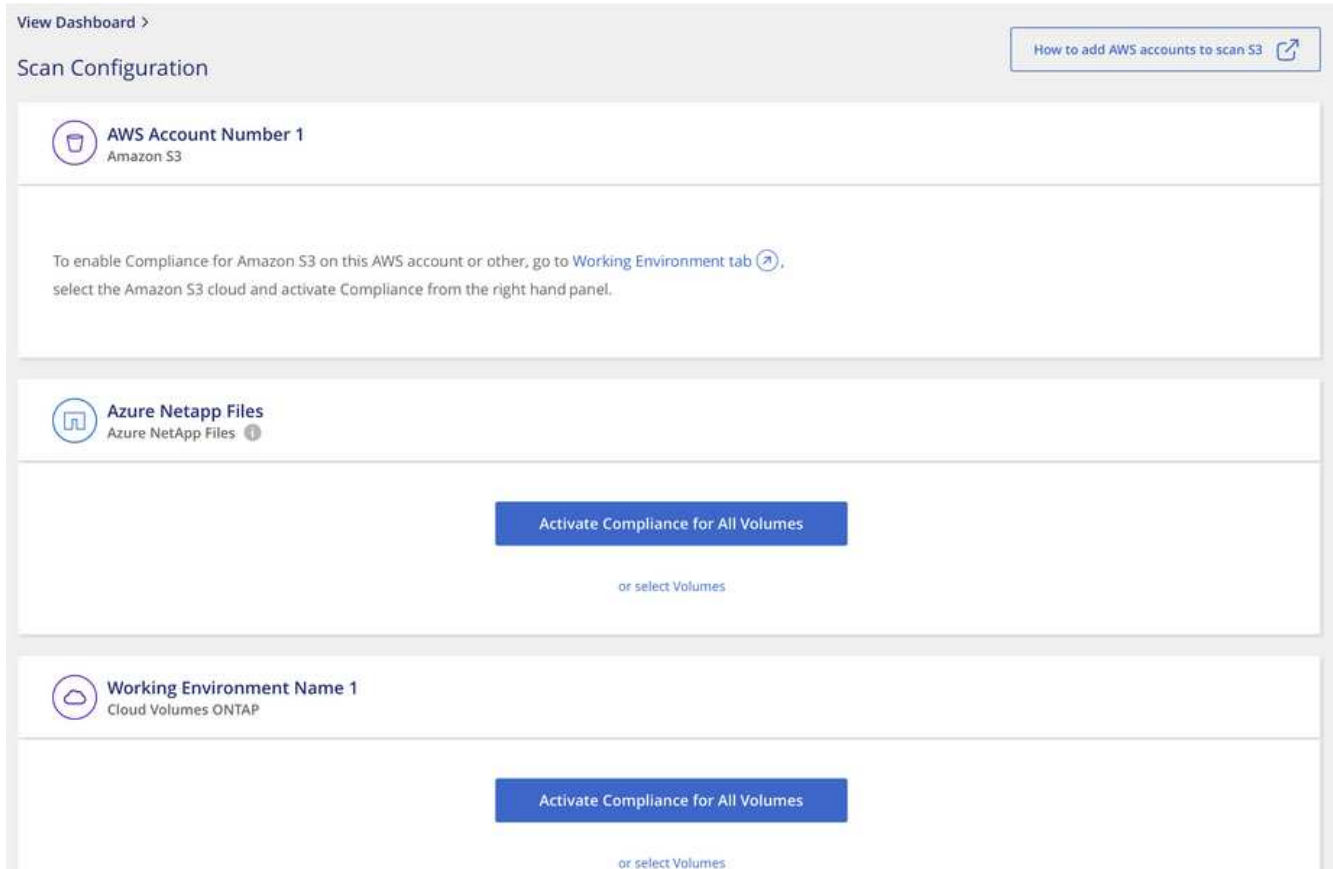
Wählen Sie die Volumes aus, die Sie scannen möchten, und Cloud Compliance beginnt, sie zu scannen.

## Bereitstellen der Instanz für Cloud-Compliance

"[Cloud Compliance in Cloud Manager implementieren](#)" Falls noch keine Instanz implementiert wurde.

## Cloud Compliance in Ihren Arbeitsumgebungen

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance** und wählen Sie dann die Registerkarte **Konfiguration** aus.



View Dashboard >

Scan Configuration [How to add AWS accounts to scan S3](#)

**AWS Account Number 1**  
Amazon S3

To enable Compliance for Amazon S3 on this AWS account or other, go to [Working Environment tab](#), select the Amazon S3 cloud and activate Compliance from the right hand panel.

**Azure Netapp Files**  
Azure NetApp Files

**Activate Compliance for All Volumes**  
or select Volumes

**Working Environment Name 1**  
Cloud Volumes ONTAP

**Activate Compliance for All Volumes**  
or select Volumes

2. Um alle Volumes in einer Arbeitsumgebung zu scannen, klicken Sie auf **Compliance für alle Volumes aktivieren**.

Um nur bestimmte Volumes in einer Arbeitsumgebung zu scannen, klicken Sie auf **oder wählen Sie Volumes** und wählen Sie dann die Volumes aus, die Sie scannen möchten.

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

### Ergebnis

Cloud Compliance beginnt mit der Überprüfung der Daten in den einzelnen Arbeitsumgebungen. Die Ergebnisse werden im Compliance-Dashboard verfügbar sein, sobald Cloud Compliance die ersten Scans abgeschlossen hat. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.

## Es wird sichergestellt, dass Cloud Compliance Zugriff auf Volumes hat

Stellen Sie sicher, dass Cloud Compliance auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien prüfen. Cloud Compliance muss über CIFS-Anmeldedaten

bereitgestellt werden, damit der Zugriff auf CIFS Volumes möglich ist.

## Schritte

1. Vergewissern Sie sich, dass eine Netzwerkverbindung zwischen Cloud Compliance-Instanz und jedem Netzwerk besteht, das Volumes für Cloud Volumes ONTAP oder Azure NetApp Files umfasst.

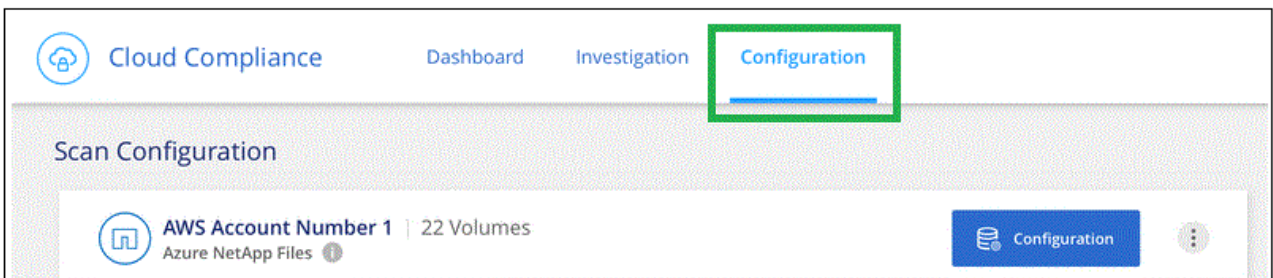


Bei Azure NetApp Files kann Cloud Compliance Volumes nur in derselben Region wie Cloud Manager überprüfen.

2. Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr aus der Cloud-Compliance-Instanz zulässt.

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

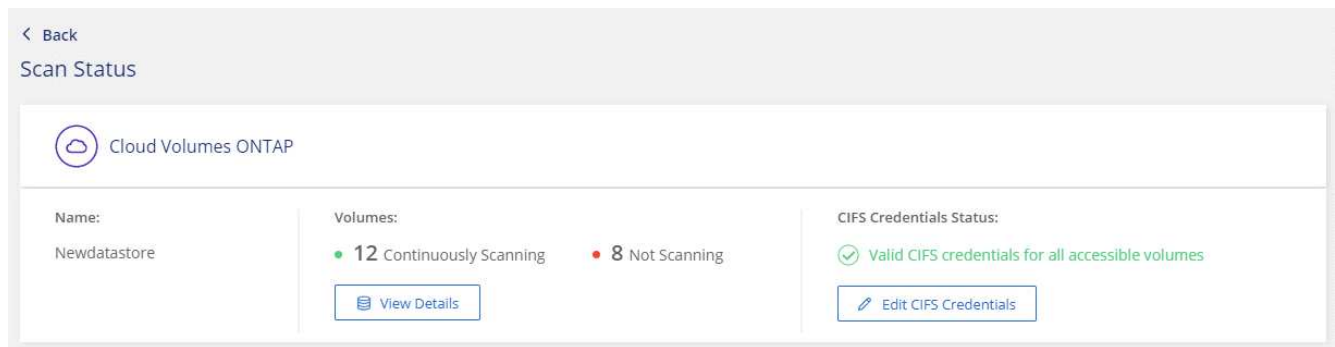
3. Vergewissern Sie sich, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Cloud Compliance-Instanz enthalten, damit sie auf die Daten der einzelnen Volumes zugreifen können.
4. Wenn Sie CIFS verwenden, geben Sie Cloud Compliance mit Active Directory Anmeldedaten ein, damit CIFS Volumes gescannt werden können.
  - a. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
  - b. Klicken Sie auf die Registerkarte **Konfiguration**.



- c. Klicken Sie für jede Arbeitsumgebung auf **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Passwort ein, die Cloud Compliance für den Zugriff auf CIFS-Volumes auf dem System benötigt.

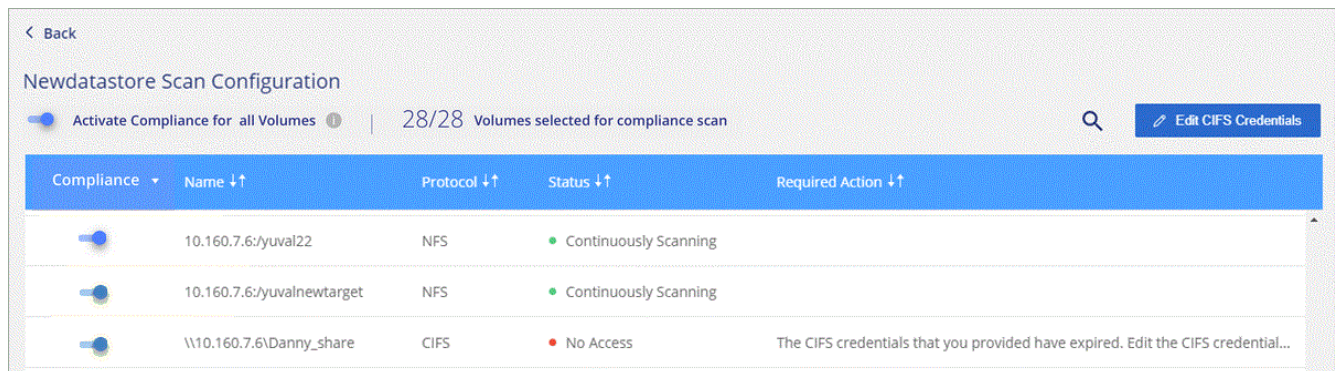
Die Anmeldedaten können schreibgeschützt sein. Durch Admin-Berechtigungen wird jedoch sichergestellt, dass Cloud Compliance Daten lesen kann, die erhöhte Berechtigungen benötigen. Die Anmeldedaten werden in der Instanz Cloud Compliance gespeichert.

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



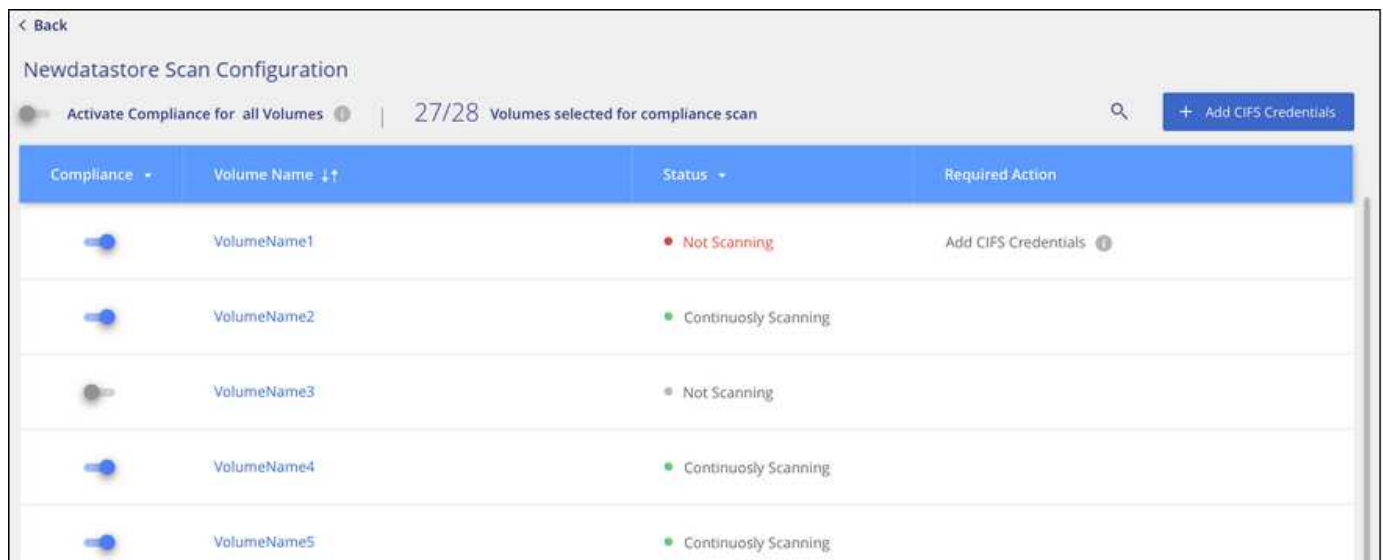
5. Klicken Sie auf der Seite *Scan Configuration* auf **Details anzeigen**, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und eventuelle Fehler zu beheben.

Das folgende Bild zeigt beispielsweise drei Volumes, von denen Cloud Compliance aufgrund von Netzwerkverbindungsproblemen zwischen der Cloud-Compliance-Instanz und dem Volume nicht scannen kann.



## Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

Sie können das Scannen von Volumes in einer Arbeitsumgebung jederzeit über die Seite Scankonfiguration anhalten oder starten. Wir empfehlen, alle Volumes zu scannen.



An:	Tun Sie dies:
Deaktivieren Sie das Scannen nach einem Volume	Bewegen Sie den Lautstärkeregler nach links
Deaktivieren Sie das Scannen für alle Volumes	Bewegen Sie den Schieberegler <b>Compliance für alle Volumes</b> nach links
Aktivieren Sie das Scannen nach einem Volume	Bewegen Sie den Lautstärkeregler nach rechts
Aktivieren Sie das Scannen für alle Volumes	Bewegen Sie den Schieberegler <b>Compliance für alle Volumes</b> nach rechts



Neue Volumes, die der Arbeitsumgebung hinzugefügt werden, werden nur dann automatisch gescannt, wenn die Einstellung **Compliance für alle Volumes** aktivieren aktiviert ist. Wenn diese Einstellung deaktiviert ist, müssen Sie das Scannen für jedes neue Volumen aktivieren, das Sie in der Arbeitsumgebung erstellen.

## Scannen von Datensicherungs-Volumes

Standardmäßig werden Datensicherungs-Volumes nicht gescannt, weil sie nicht extern zugänglich sind und Cloud Compliance nicht darauf zugreifen kann. Diese Volumes sind normalerweise Ziel-Volumes für SnapMirror Vorgänge über ein ONTAP-Cluster vor Ort.

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

The screenshot shows the 'Working Environment Name' Scan Configuration page. At the top, there is a search icon and a button 'Enable Access to DP Volumes' which is highlighted with a green box. Below this, there is a table with the following columns: Compliance, Volume Name, Type, Status, and Required Action. The table contains three rows of data:

Compliance	Volume Name	Type	Status	Required Action
<input type="checkbox"/>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes
<input checked="" type="checkbox"/>	VolumeName2	NFS	Continuously Scanning	
<input type="checkbox"/>	VolumeName3	CIFS	Not Scanning	

### Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

1. Klicken Sie oben auf der Seite auf die Schaltfläche **Zugriff auf DP-Volumes aktivieren**.
2. Aktivieren Sie jedes DP-Volume, das Sie scannen möchten, oder verwenden Sie die Kontrolle **Compliance für alle Volumes aktivieren**, um alle Volumes, einschließlich aller DP-Volumes, zu aktivieren.

Sobald Cloud Compliance aktiviert ist, erstellt jedes DP Volume eine NFS-Freigabe, die für Compliance aktiviert wurde, sodass sie gescannt werden kann. Die Richtlinien für den Share-Export erlauben nur den Zugriff aus der Cloud Compliance-Instanz.



In der Liste der Volumes werden nur Volumes angezeigt, die anfangs als NFS-Volumes im Quell-ONTAP-System erstellt wurden. Quell-Volumes, die zunächst als CIFS erstellt wurden, werden derzeit nicht in Cloud Compliance angezeigt.

## Erste Schritte mit Cloud Compliance für Amazon S3

Cloud Compliance kann Ihre Amazon S3 Buckets scannen, um die persönlichen und sensiblen Daten zu identifizieren, die sich im S3 Objekt-Storage befinden. Cloud Compliance kann jeden Bucket auf dem 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.



#### S3-Anforderungen in Ihrer Cloud-Umgebung einrichten

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



#### Implementieren der Cloud Compliance-Instanz

"[Cloud Compliance in Cloud Manager implementieren](#)" Falls noch keine Instanz implementiert wurde.



#### Aktivieren Sie Compliance in Ihrer S3-Arbeitsumgebung

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



#### Wählen Sie die zu scannenden Buckets aus

Wählen Sie die Buckets aus, die Sie scannen möchten, und Cloud Compliance 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 Compliance-Instanz

Cloud Compliance 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. Cloud Manager fordert Sie auf, eine IAM-Rolle auszuwählen, wenn Sie Cloud Compliance in der Amazon S3-Arbeitsumgebung aktivieren.



```

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

```

### Bereitstellung der Konnektivität von Cloud Compliance zu Amazon S3

Cloud Compliance 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, sollten Sie die Region, die VPC und die Routing-Tabelle auswählen, die der Cloud Compliance-Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Cloud Compliance 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 Instanz für Cloud-Compliance

["Cloud Compliance in Cloud Manager implementieren"](#) Falls noch keine Instanz implementiert wurde.

Sie müssen die Instanz in einem AWS Connector implementieren, damit Cloud Manager die S3-Buckets in diesem AWS-Konto automatisch erkennt und in einer Amazon S3-Arbeitsumgebung angezeigt wird.

## Aktivierung von Compliance in Ihrer S3-Arbeitsumgebung

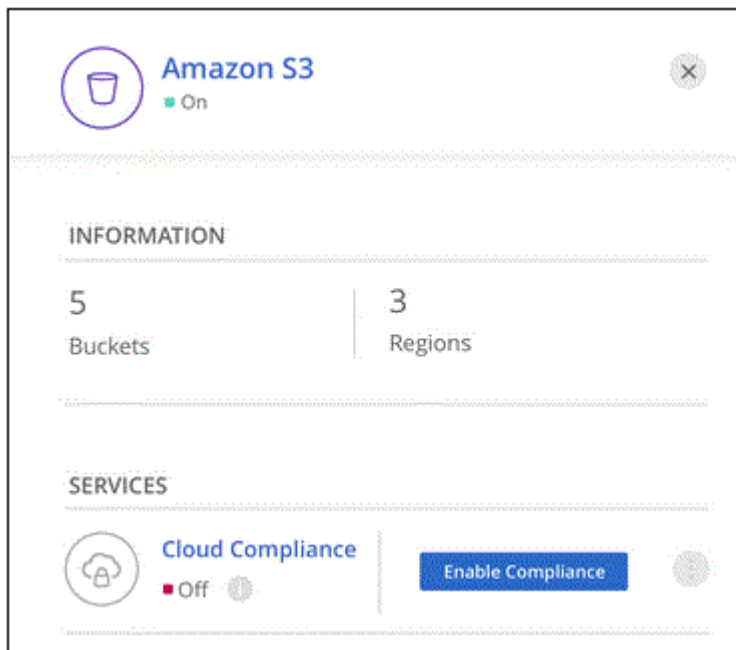
Aktivieren Sie Cloud-Compliance auf Amazon S3, nachdem Sie die Voraussetzungen überprüft haben.

### Schritte

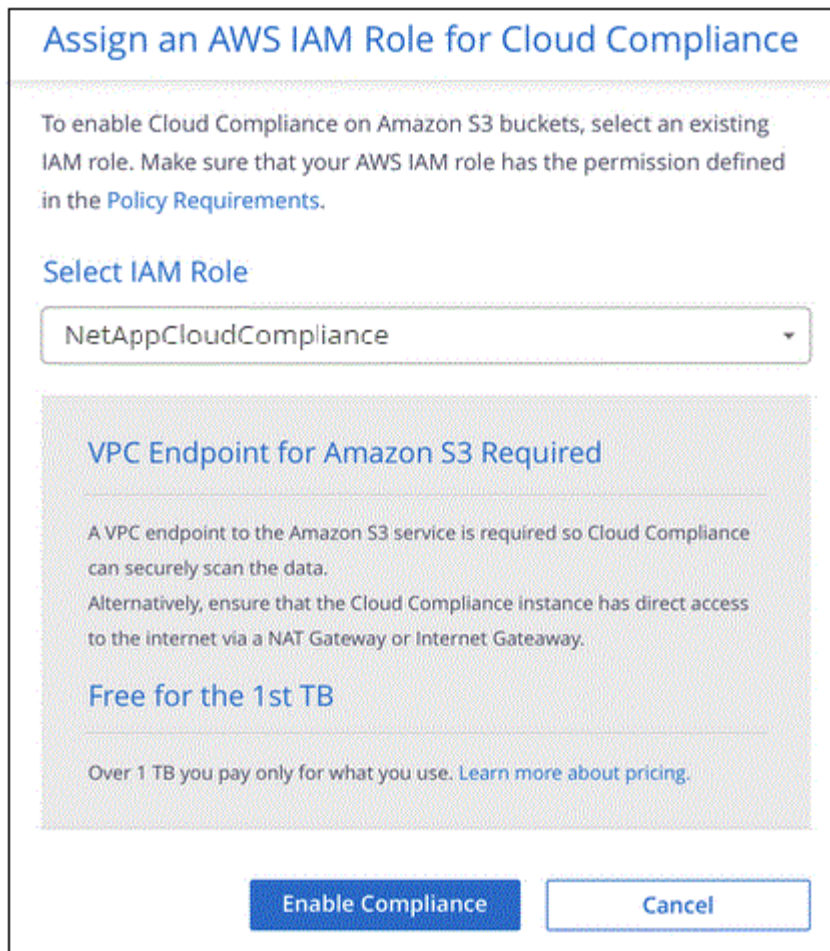
1. Klicken Sie oben im Cloud Manager auf **Arbeitsumgebungen**.
2. Wählen Sie die Amazon S3-Arbeitsumgebung aus.



3. Klicken Sie im rechten Fensterbereich auf **Compliance aktivieren**.




4. Weisen Sie bei der entsprechenden Aufforderung der Cloud Compliance-Instanz eine IAM-Rolle zu [Die erforderlichen Berechtigungen](#).



5. Klicken Sie Auf **Compliance Aktivieren**.



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

### Ergebnis

Cloud Manager weist der Instanz die IAM-Rolle zu.

## Aktivieren und Deaktivieren von Compliance-Scans auf S3-Buckets

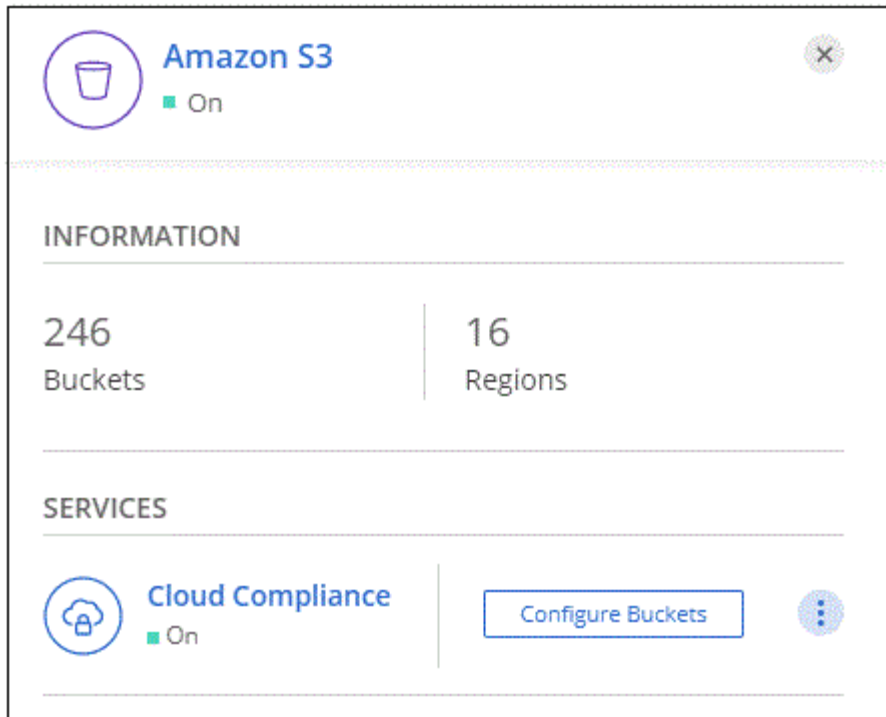
Nachdem Cloud Manager Cloud Compliance in Amazon S3 aktiviert hat, müssen die Buckets konfiguriert werden, die überprüft werden sollen.

Wenn Cloud Manager 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.

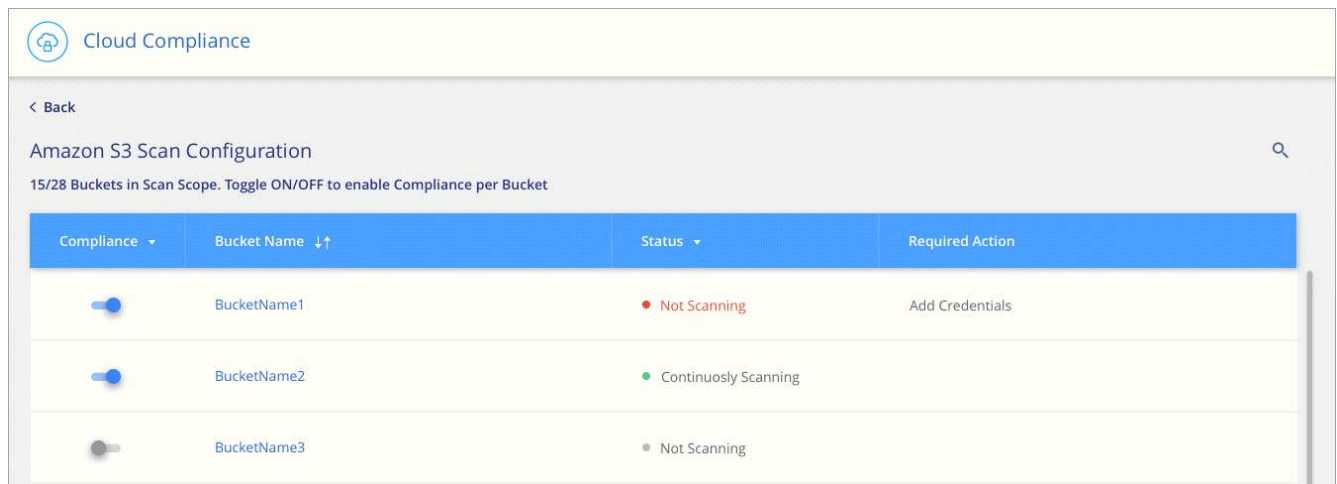
Auch Cloud Compliance kann [Scannen von S3-Buckets, die in unterschiedlichen AWS Konten vorhanden sind](#).

### Schritte

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



3. Aktivieren Sie Compliance in den Buckets, die Sie scannen möchten.



### Ergebnis

Cloud Compliance 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 von diesem Konto eine Rolle zuweisen, um auf die vorhandene Cloud-Compliance-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

 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> 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-Compliance-Instanz befindet.
- Ändern Sie die maximale CLI/API-Sitzungsdauer\* von 1 Stunde auf 12 Stunden und speichern Sie diese Änderung.
- Hängen Sie die Cloud Compliance 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:HeadBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Wechseln Sie zum AWS Quellkonto, in dem sich die Cloud Compliance 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“ und den ARN der Rolle umfasst, die Sie im Zielkonto erstellt haben.

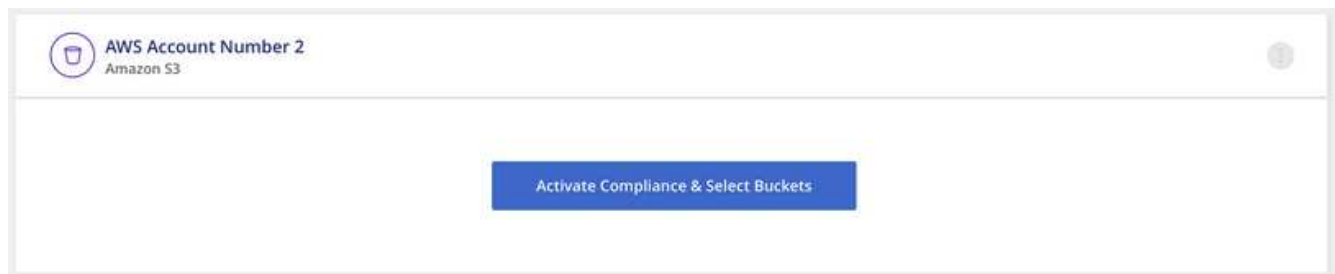
```

{
  "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 Instanzprofil für Cloud Compliance hat nun Zugriff auf das zusätzliche AWS Konto.

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



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

### Ergebnis

Cloud Compliance beginnt mit dem Scannen der neuen aktivierten S3-Buckets.

# Datenbankschemas werden gescannt

Führen Sie einige Schritte durch, um den Scan des Datenbankschemas mit Cloud Compliance zu beginnen.

## Schnellstart

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



### Datenbankvoraussetzungen prüfen

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



### Implementieren der Cloud Compliance-Instanz

"[Cloud Compliance in Cloud Manager implementieren](#)" Falls noch keine Instanz implementiert wurde.



### Fügen Sie den Datenbankserver hinzu

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



### 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 Compliance aktivieren.

### Unterstützte Datenbanken

Cloud Compliance kann Schemen aus den folgenden Datenbanken scannen:

- MongoDB
- 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 Compliance-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 Compliance-System mit allen erforderlichen Berechtigungen zu erstellen.

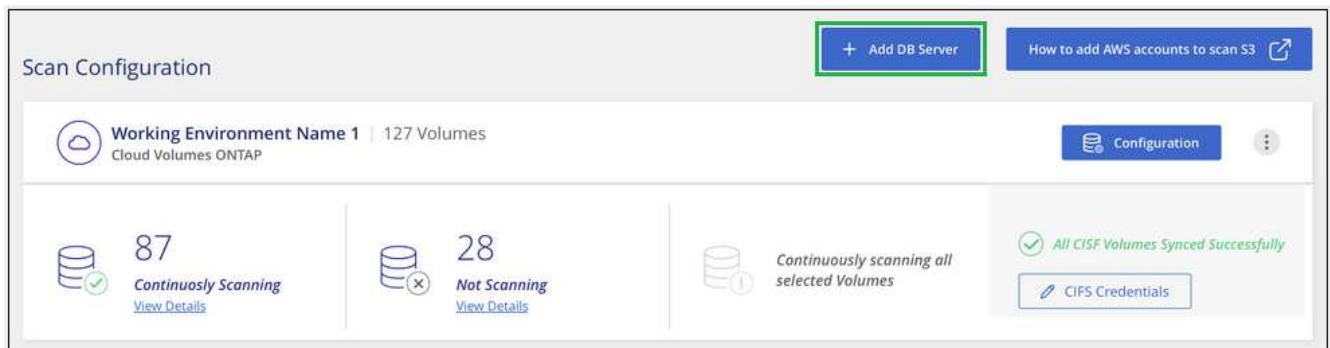
**Hinweis:** für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

## Hinzufügen des Datenbankservers

Dieser muss unbedingt vorhanden sein "[Bereits eine Instanz von Cloud Compliance in Cloud Manager implementiert](#)".

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

1. Klicken Sie auf der Seite *Scan Configuration* auf die Schaltfläche **DB 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 Dienstnamen ein.
  - d. Geben Sie die Anmeldeinformationen ein, damit Cloud Compliance 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

Die Datenbank wird der Liste der Arbeitsverzeichnisse hinzugefügt.

## Aktivieren und Deaktivieren von Compliance-Scans auf Datenbankschemas

Sie können die Scanschemata jederzeit anhalten oder starten.

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

Scan Configuration

Oracle DB 1 | 41 Schemas  
Oracle

No Schemas selected for Compliance

7 Not Scanning  
[View Details](#)

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


'Working Environment Name' Scan Configuration			
Compliance	Schema Name	Status	Required Action
<input checked="" type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials
<input checked="" type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

## Ergebnis

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

## Entfernen einer Datenbank aus Cloud Manager

Wenn Sie eine bestimmte Datenbank nicht mehr scannen möchten, können Sie sie über die Cloud Manager Schnittstelle löschen und alle Scans anhalten.

Klicken Sie auf der Seite *Scan Configuration* auf . Klicken Sie in der Zeile der Datenbank auf **DB Server entfernen**.



## Scannen lokaler ONTAP Daten mit Cloud-Compliance mit SnapMirror

Sie können Ihre lokalen ONTAP-Daten mit Cloud-Compliance scannen, indem Sie die On-Premises-NFS- oder CIFS-Daten in eine Cloud Volumes ONTAP Arbeitsumgebung replizieren und damit Compliance sicherstellen. Das Scannen der Daten direkt aus einer lokalen ONTAP-Arbeitsumgebung wird nicht unterstützt.

Dieser muss unbedingt vorhanden sein "[Bereits eine Instanz von Cloud Compliance in Cloud Manager implementiert](#)".

### Schritte

1. Erstellen Sie in Cloud Manager eine SnapMirror Beziehung zwischen dem lokalen ONTAP Cluster und Cloud Volumes ONTAP.
  - a. ["Ermitteln des On-Premises-Clusters in Cloud Manager"](#).
  - b. ["Erstellen einer SnapMirror Replizierung zwischen dem lokalen ONTAP Cluster und Cloud Volumes ONTAP aus Cloud Manager"](#).
2. Konfigurieren Sie bei DP-Volumes, die aus SMB-Quell-Volumes erstellt wurden, über die Befehlszeilenschnittstelle von ONTAP die SMB-Ziel-Volumes für den Datenzugriff. (Dies ist für NFS-Volumes nicht erforderlich, da der Datenzugriff automatisch über Cloud-Compliance aktiviert wird.)
  - a. ["SMB-Freigabe auf dem Ziel-Volume erstellen"](#).
  - b. ["Wenden Sie die entsprechenden ACLs auf die SMB-Freigabe am Ziel-Volume an"](#).
3. Aktivieren Sie über Cloud Manager Cloud Compliance in der Cloud Volumes ONTAP Arbeitsumgebung, die die SnapMirror Daten enthält:
  - a. Klicken Sie Auf **Arbeitsumgebungen**.
  - b. Wählen Sie die Arbeitsumgebung aus, die die SnapMirror Daten enthält, und klicken Sie auf **Compliance aktivieren**.  
  
["Klicken Sie hier, wenn Sie Hilfe bei der Aktivierung von Cloud-Compliance auf einem Cloud Volumes ONTAP System benötigen"](#).
  - c. Klicken Sie oben auf der Seite *Scan Configuration* auf die Schaltfläche **Zugriff auf DP-Volumes** aktivieren.
  - d. Aktivieren Sie jedes DP-Volume, das Sie scannen möchten, oder verwenden Sie die Kontrolle **Compliance für alle Volumes aktivieren**, um alle Volumes, einschließlich aller DP-Volumes, zu aktivieren.

Siehe ["Scannen von Datensicherungs-Volumes"](#) Weitere Informationen zum Scannen von DP-Volumes.

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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.