



Einblicke in den Datenschutz

Cloud Manager 3.8

NetApp
March 25, 2024

Inhalt

- Einblicke in den Datenschutz 1
 - Erfahren Sie mehr über Cloud Compliance 1
 - Los geht's 5
 - Mehr Transparenz und Kontrolle über private Daten 28
 - Anzeigen von Compliance-Berichten 42
 - Reaktion auf eine Zugriffsanfrage für betroffene Person 47
 - Deaktivieren Von Cloud Compliance 49
 - Häufig gestellte Fragen zur Cloud Compliance 50

Einblicke in den Datenschutz

Erfahren Sie mehr über Cloud Compliance

Cloud Compliance ist ein Datenschutz- und Compliance-Service für Cloud Manager, der Ihre Volumes, Amazon S3 Buckets und Datenbanken scannt, um die persönlichen und sensiblen Daten zu ermitteln, die sich in diesen Dateien befinden. Mithilfe von künstlicher Intelligenz (KI) hilft Cloud Compliance Unternehmen dabei, den Datenkontext zu verstehen und sensible Daten zu ermitteln.

["Erfahren Sie mehr über Anwendungsfälle für Cloud Compliance"](#).

Funktionen

Cloud Compliance bietet verschiedene Tools, die Sie bei Ihren Compliance-Strategien unterstützen. Cloud Compliance bietet Ihnen:

- Ermitteln von personenbezogenen Daten
- Vielzahl sensibler Daten, je nach DSGVO, CCPA, PCI und HIPAA-Datenschutzvorschriften, identifizieren
- Reagieren Sie auf DSAR (Data Subject Access Requests).

Unterstützte Arbeitsumgebungen und Datenquellen

Cloud Compliance kann Daten aus folgenden Datenquellen scannen:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure
- Azure NetApp Dateien
- Amazon S3
- Datenbanken, die sich überall befinden (die Datenbank muss sich nicht in einer Arbeitsumgebung befinden)

Hinweis: für Azure NetApp Files kann Cloud Compliance alle Volumes scannen, die sich in derselben Region wie Cloud Manager befinden.

Kosten

- Die Kosten für die Verwendung von Cloud Compliance hängen von der Datenmenge ab, die Sie scannen. Zum 7. Oktober 2020 werden die ersten 1 TB der Daten, die Cloud Compliance in einem Cloud Manager-Arbeitsbereich scannt, kostenlos bereitgestellt. Dazu gehören Daten von Cloud Volumes ONTAP Volumes, Azure NetApp Files Volumes, Amazon S3 Buckets und Datenbank-Schemas. Danach ist ein Abonnement für AWS oder Azure Marketplace erforderlich, um mit dem Scannen der Daten fortzufahren. Siehe ["Preisgestaltung"](#) Entsprechende Details.

["Erfahren Sie, wie Sie abonniert werden können"](#).

- Für die Installation von Cloud Compliance ist die Implementierung einer Cloud-Instanz erforderlich, was für den Cloud-Provider, bei dem sie implementiert wird, Gebühren anfallen. Siehe [Der für jeden Cloud-Provider implementierte Instanztyp](#)

- Cloud Compliance erfordert die Implementierung eines Konnektors. Aufgrund anderer Storage-Systeme und Services, die Sie in Cloud Manager verwenden, haben Sie häufig bereits einen Connector. Die Connector-Instanz verursacht Gebühren bei dem Cloud-Provider, wo sie implementiert wird. Siehe "[Für jeden Cloud-Provider implementierte Instanztyp](#)".

Datentransferkosten

Die Datentransferkosten hängen von Ihrer Einrichtung ab. Wenn sich die Cloud Compliance-Instanz und die Datenquelle in derselben Verfügbarkeitszone und Region befinden, entstehen keine Datentransferkosten. Wenn sich die Datenquelle, beispielsweise ein Cloud Volumes ONTAP-Cluster oder S3-Bucket, jedoch in einer *verschiedenen* Verfügbarkeitszone oder -Region befindet, wird Ihr Cloud-Provider für Datentransferkosten berechnet. Weitere Informationen finden Sie unter diesen Links:

- "[AWS: Amazon EC2-Preisgestaltung](#)"
- "[Microsoft Azure: Preisangaben Für Die Bandbreite](#)"

Funktionsweise von Cloud Compliance

Cloud Compliance funktioniert auf hohem Niveau wie folgt:

1. Sie implementieren eine Instanz von Cloud Compliance in Cloud Manager.
2. Sie ermöglichen es in einer oder mehreren Arbeitsumgebungen oder in Ihren Datenbanken.
3. Cloud Compliance scannt die Daten mithilfe eines KI-Learning-Prozesses.
4. In Cloud Manager klicken Sie auf **Compliance** und verwenden Sie das bereitgestellte Dashboard und die Berichterstellungs-Tools, um Ihre Compliance-Bemühungen zu unterstützen.

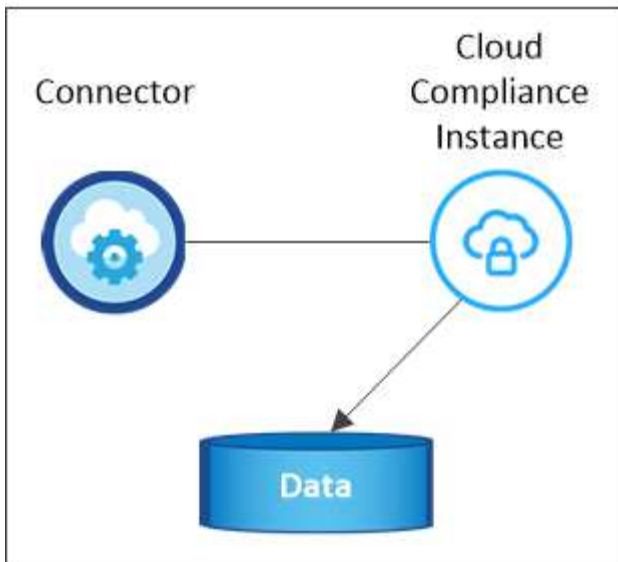
Die Instanz für Cloud Compliance

Wenn Sie Cloud Compliance aktivieren, implementiert Cloud Manager eine Cloud Compliance-Instanz im selben Subnetz wie der Connector. "[Erfahren Sie mehr über Steckverbinder.](#)"



Falls der Connector lokal installiert wird, implementiert er die Cloud Compliance-Instanz in derselben VPC oder vnet wie das erste Cloud Volumes ONTAP-System in der Anfrage.

VPC or VNet



Beachten Sie Folgendes über die Instanz:

- In Azure wird Cloud Compliance auf einer VM mit Standard_D16s_v3 mit einer Festplatte von 512 GB ausgeführt.
- In AWS wird Cloud-Compliance auf einer m5.4xlarge-Instanz mit einer 500-GB-GP2-Festplatte ausgeführt.

In Regionen, in denen m5.4xlarge nicht verfügbar ist, wird Cloud Compliance stattdessen auf einer m4.4xlarge-Instanz ausgeführt.



Das Ändern oder Ändern der Größe des Instanz-/VM-Typs wird nicht unterstützt. Sie müssen die angegebene Größe verwenden.

- Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Pro Connector wird nur eine Cloud-Compliance-Instanz bereitgestellt.
- Die Upgrades der Cloud Compliance-Software sind automatisiert – Sie müssen sich keine Gedanken darüber machen.



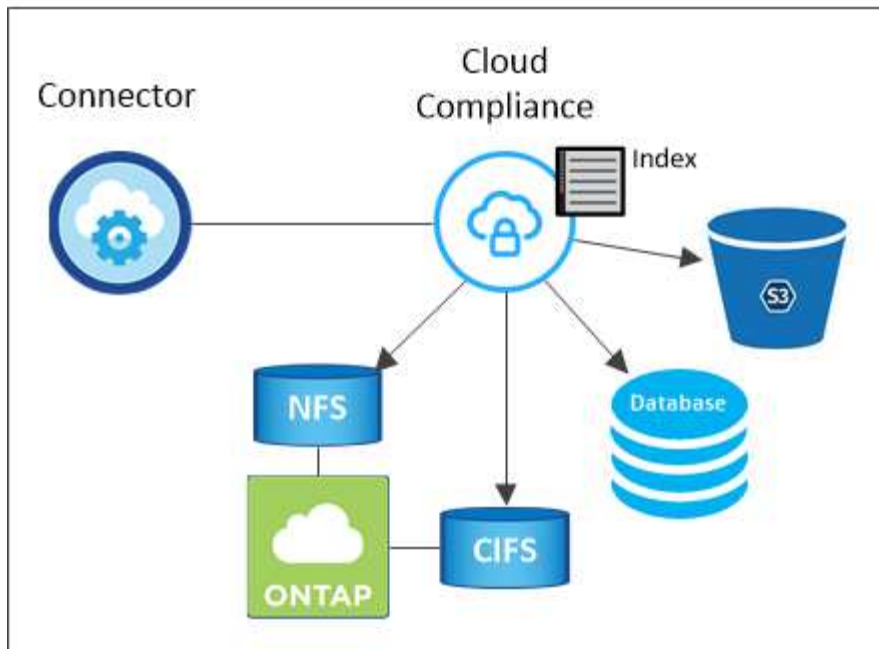
Die Instanz sollte jederzeit ausgeführt werden, da Cloud Compliance die Daten kontinuierlich scannt.

Funktionsweise von Scans

Nachdem Sie Cloud Compliance aktiviert und die Volumes, Buckets oder Datenbankschemata ausgewählt haben, die Sie scannen möchten, wird sofort mit dem Scannen der Daten begonnen, um persönliche und sensible Daten zu identifizieren. Es ordnet Ihre Organisationsdaten zu, kategorisiert jede Datei und identifiziert und extrahiert Entitäten und vordefinierte Muster in den Daten. Das Ergebnis des Scans ist ein Index von persönlichen Daten, sensiblen persönlichen Daten und Datenkategorien.

Cloud Compliance stellt durch das Mounten von NFS- und CIFS-Volumes eine Verbindung zu den Daten wie jedem anderen Client her. NFS Volumes werden automatisch als schreibgeschützt abgerufen und müssen zur Überprüfung von CIFS Volumes Active Directory Anmeldeinformationen bereitstellen.

VPC or VNet



Nach dem ersten Scan scannt Cloud Compliance jedes Volume kontinuierlich, um inkrementelle Änderungen zu erkennen (deshalb ist es wichtig, die Instanz weiterhin zu betreiben).

Sie können Scans im aktivieren und deaktivieren "[Volume-Ebene](#)", Am "[Bucket-Ebene](#)", Und am "[Datenbankschemenebene](#)".

Information, die Cloud Compliance indiziert

Cloud Compliance erfasst, indiziert und weist Kategorien unstrukturierter Daten (Dateien) zu. Cloud Compliance umfasst folgende Daten:

Standard-Metadaten

Cloud Compliance sammelt Standard-Metadaten zu Dateien: Dateityp, Größe, Erstellung, Änderung usw.

Persönliche Daten

Personenbezogene Informationen wie E-Mail-Adressen, Identifikationsnummern oder Kreditkartennummern. "[Weitere Informationen zu personenbezogenen Daten](#)".

Sensible persönliche Daten

Besondere Arten sensibler Daten, wie etwa Gesundheitsdaten, ethnische Herkunft oder politische Ansichten, wie in der DSGVO und anderen Datenschutzvorschriften definiert "[Erfahren Sie mehr über sensible persönliche Daten](#)".

Kategorien

Bei Cloud Compliance werden die gescannten Daten in verschiedene Kategorien unterteilt. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "[Weitere Informationen zu Kategorien](#)".

Name der Entität Anerkennung

Cloud Compliance nutzt KI, um Namen natürlicher Personen aus Dokumenten zu extrahieren. "[Informieren Sie sich über die Reaktion auf Zugriffsanfragen von Betroffenen](#)".

Netzwerkübersicht

Cloud Manager implementiert die Cloud Compliance-Instanz mit einer Sicherheitsgruppe, die eingehende HTTP-Verbindungen von der Connector-Instanz ermöglicht.

Bei der Verwendung von Cloud Manager im SaaS-Modus, wird die Verbindung zu Cloud Manager über HTTPS bedient, und die privaten Daten, die zwischen Ihrem Browser und der Cloud Compliance-Instanz gesendet werden, sind mit End-to-End-Verschlüsselung gesichert, was bedeutet, dass NetApp und Dritte nicht lesen können.

Wenn Sie aus irgendeinem Grund die lokale Benutzeroberfläche anstelle der SaaS-Benutzeroberfläche verwenden müssen, können Sie immer noch ["Greifen Sie auf die lokale UI zu"](#).

Ausgehende Regeln sind vollständig geöffnet. Zum Installieren und Aktualisieren der Cloud Compliance-Software und zum Senden von Nutzungsmetriken ist Internetzugang erforderlich.

Wenn Sie strenge Netzwerkanforderungen erfüllen, ["Informationen zu den Endpunkten, die Cloud Compliance kontaktiert"](#).

Zugriff des Benutzers auf Compliance-Informationen

Jeder Benutzer verfügt über verschiedene Funktionen innerhalb von Cloud Manager und innerhalb von Cloud Compliance:

- **Kontoadministratoren** können Compliance-Einstellungen verwalten und Compliance-Informationen für alle Arbeitsumgebungen anzeigen.
- **Workspace-Administratoren** können Compliance-Einstellungen verwalten und Compliance-Informationen nur für Systeme anzeigen, auf die sie Zugriff haben. Wenn ein Workspace-Administrator nicht auf eine Arbeitsumgebung in Cloud Manager zugreifen kann, werden auf der Registerkarte Compliance keine Compliance-Informationen für die Arbeitsumgebung angezeigt.
- Benutzer mit der Rolle **Cloud Compliance Viewer** können Compliance-Informationen nur anzeigen und Berichte für Systeme erstellen, auf die sie zugreifen können. Diese Benutzer können das Scannen von Volumes, Buckets oder Datenbankschemata nicht aktivieren/deaktivieren.

["Erfahren Sie mehr über die Rollen von Cloud Manager"](#) Und wie ["Benutzer mit bestimmten Rollen hinzufügen"](#).

Los geht's

Implementierung Von Cloud Compliance

Führen Sie einige Schritte durch, um die Cloud Compliance-Instanz in Ihrem Cloud Manager Workspace zu implementieren.

Schnellstart

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

1

Einen Konnektor erstellen

Falls Sie noch keinen Connector haben, erstellen Sie in Azure oder AWS einen Connector. Siehe ["Erstellen eines Konnektors in AWS"](#) Oder ["Erstellen eines Connectors in Azure"](#).

2

Voraussetzungen prüfen

Stellen Sie sicher, dass Ihre Cloud-Umgebung die Voraussetzungen erfüllt, die 16 vCPUs für die Cloud Compliance Instanz, Outbound-Internetzugang zur Instanz, Konnektivität zwischen Connector und Cloud Compliance über Port 80 umfassen kann. [Eine vollständige Liste finden Sie hier](#).

3

Implementierung Von Cloud Compliance

Starten Sie den Installationsassistenten, um die Cloud Compliance-Instanz in Cloud Manager zu implementieren.

4

Abonnieren Sie den Cloud Compliance Service

Die ersten 1 TB an Daten, die Cloud Compliance in Cloud Manager scannt, sind kostenlos. Danach ist ein Abonnement für AWS oder Azure Marketplace erforderlich, um mit dem Scannen der Daten fortzufahren.

Erstellen eines Connectors

Falls Sie noch keinen Connector haben, erstellen Sie in Azure oder AWS einen Connector. Siehe ["Erstellen eines Konnektors in AWS"](#) Oder ["Erstellen eines Connectors in Azure"](#). In den meisten Fällen haben Sie wahrscheinlich einen Connector eingerichtet, bevor Sie Cloud Compliance aktivieren, da die meisten davon ["Für die Funktionen von Cloud Manager ist ein Connector erforderlich"](#), Aber es gibt Fälle, wenn Sie eine Einrichtung jetzt.

Es gibt einige Szenarien, in denen ein Connector in AWS oder Azure für Cloud Compliance verwendet werden muss.

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS oder in AWS S3 Buckets verwenden Sie einen Connector in AWS.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konnektor in Azure.
- Datenbanken können über einen der beiden Connectors gescannt werden.

Wie Sie sehen können, gibt es einige Situationen, in denen Sie verwenden müssen ["Mehrere Anschlüsse"](#).



Wenn Sie Azure NetApp Files scannen möchten, müssen Sie sicherstellen, dass Sie in derselben Region wie die Volumes bereitstellen, die Sie scannen möchten.

Voraussetzungen prüfen

Prüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie Cloud Compliance bereitstellen.

Aktivieren Sie den Outbound-Internetzugang

Cloud Compliance erfordert Outbound-Internetzugang. Wenn Ihr virtuelles Netzwerk einen Proxyserver für den Internetzugriff verwendet, stellen Sie sicher, dass die Cloud Compliance-Instanz über einen ausgehenden Internetzugriff verfügt, um die folgenden Endpunkte zu kontaktieren. Beachten Sie, dass Cloud Manager die Cloud Compliance-Instanz im selben Subnetz wie der Connector bereitstellt.

Endpunkte	Zweck
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Cloud Compliance ermöglicht es, auf Manifeste und Vorlagen zuzugreifen und diese herunterzuladen sowie Protokolle und Kennzahlen zu senden.

Stellen Sie sicher, dass Cloud Manager über die erforderlichen Berechtigungen verfügt

Stellen Sie sicher, dass Cloud Manager über die Berechtigungen zum Implementieren von Ressourcen verfügt und Sicherheitsgruppen für die Instanz Cloud Compliance erstellen kann. Die neuesten Berechtigungen von Cloud Manager finden Sie in ["Die von NetApp bereitgestellten Richtlinien"](#).

Überprüfen Sie Ihre vCPU-Limits

Stellen Sie sicher, dass das vCPU-Limit Ihres Cloud-Providers die Bereitstellung einer Instanz mit 16 Cores ermöglicht. Sie müssen das vCPU-Limit für die entsprechende Instanzfamilie in der Region, in der Cloud Manager ausgeführt wird, überprüfen.

In AWS lautet die Instanzfamilie *On-Demand Standard-Instanzen*. In Azure ist die Instanzfamilie *Standard Dsv3 Family*.

Weitere Informationen zu vCPU-Limits finden Sie im folgenden Dokument:

- ["AWS Dokumentation: Amazon EC2 Service Limits"](#)
- ["Azure Dokumentation: VCPU Kontingente von Virtual Machines"](#)

Stellen Sie sicher, dass Cloud Manager auf Cloud Compliance zugreifen kann

Stellen Sie die Verbindung zwischen dem Connector und der Cloud Compliance-Instanz sicher. Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über Port 80 zu und von der Cloud Compliance-Instanz ermöglichen.

Diese Verbindung ermöglicht die Bereitstellung der Cloud Compliance-Instanz sowie die Anzeige von Informationen auf der Registerkarte Compliance.

Einrichten der Erkennung von Azure NetApp Files

Bevor Sie Volumes für Azure NetApp Files scannen können, ["Cloud Manager muss eingerichtet sein, um die Konfiguration zu ermitteln"](#).

Stellen Sie sicher, dass Cloud-Compliance weiterhin verfügbar ist

Die Cloud Compliance Instanz muss stets zum kontinuierlichen Scannen Ihrer Daten verfügbar sein.

Stellen Sie die Verbindung zwischen Webbrowser und Cloud Compliance sicher

Stellen Sie nach Aktivierung von Cloud Compliance sicher, dass Benutzer von einem Host, der über eine Verbindung zur Cloud Compliance-Instanz verfügt, auf die Cloud Manager-Schnittstelle zugreifen.

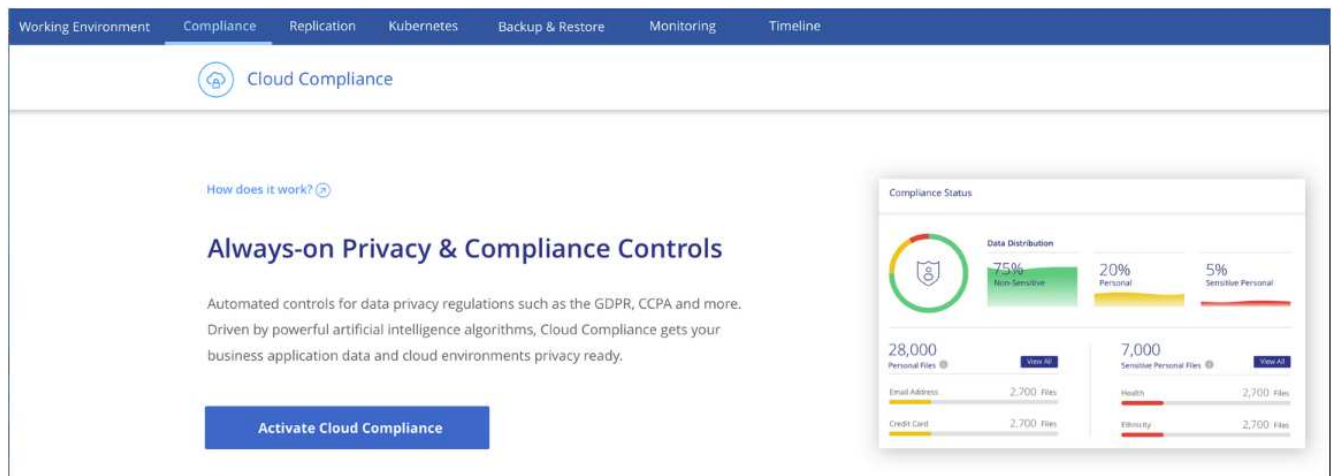
Die Cloud Compliance Instanz verwendet eine private IP-Adresse, um sicherzustellen, dass die indizierten Daten nicht für das Internet verfügbar sind. Daher muss der Webbrowser, den Sie für den Zugriff auf Cloud Manager verwenden, über eine Verbindung zu dieser privaten IP-Adresse verfügen. Die Verbindung kann über eine direkte Verbindung zu AWS oder Azure (z. B. ein VPN) oder von einem Host im selben Netzwerk wie die Cloud-Compliance-Instanz hergestellt werden.

Bereitstellen der Instanz für Cloud-Compliance

Sie implementieren für jede Cloud Manager Instanz eine Instanz von Cloud Compliance.

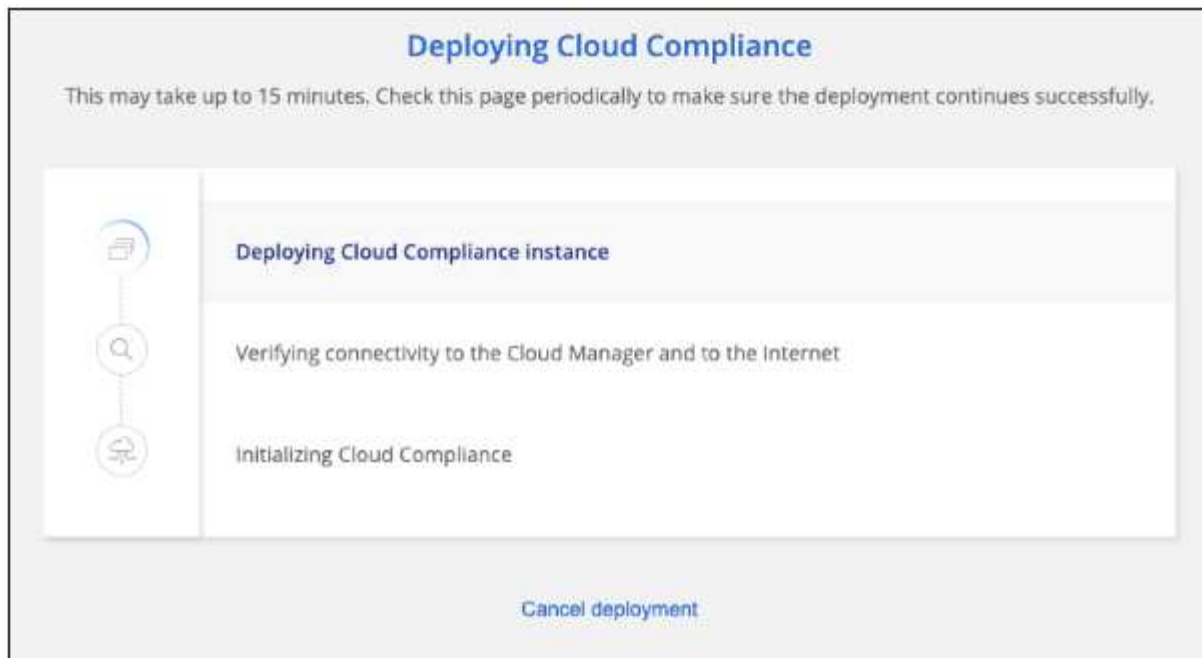
Schritte

1. Klicken Sie in Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie auf **Cloud Compliance aktivieren**, um den Bereitstellungsassistenten zu starten.



The screenshot shows the Azure Cloud Compliance management interface. At the top, there is a navigation bar with tabs for Working Environment, Compliance, Replication, Kubernetes, Backup & Restore, Monitoring, and Timeline. The 'Compliance' tab is selected. Below the navigation bar, the 'Cloud Compliance' section is visible. It includes a 'How does it work?' link and a heading 'Always-on Privacy & Compliance Controls'. The text below the heading states: 'Automated controls for data privacy regulations such as the GDPR, CCPA and more. Driven by powerful artificial intelligence algorithms, Cloud Compliance gets your business application data and cloud environments privacy ready.' A prominent blue button labeled 'Activate Cloud Compliance' is located at the bottom of this section. To the right, a 'Compliance Status' dashboard is displayed. It features a 'Data Distribution' chart with three segments: 75% Non-Sensitive (green), 20% Personal (yellow), and 5% Sensitive Personal (red). Below the chart, there are two main sections: 'Personal Files' (28,000 total) and 'Sensitive Personal Files' (7,000 total). Each section has a 'View All' button and a breakdown of file types: Email Address (2,700 Files), Credit Card (2,700 Files), Health (2,700 Files), and Identity (2,700 Files).

3. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Er wird angehalten und um Informationen gebeten, wenn es zu Problemen kommt.



4. Wenn die Instanz bereitgestellt wird, klicken Sie auf **Weiter zur Konfiguration**, um zur Seite *Scan Configuration* zu gelangen.

Ergebnis

Cloud Manager implementiert die Cloud Compliance-Instanz bei Ihrem Cloud-Provider.

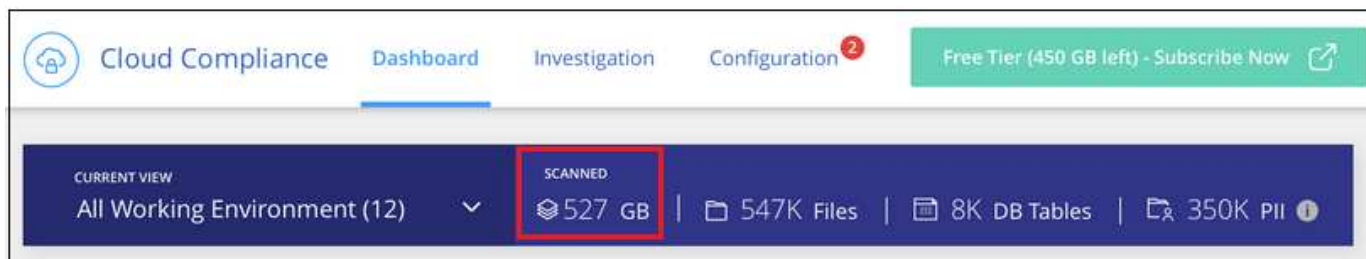
Nächste Schritte

Auf der Seite Scankonfiguration können Sie die Arbeitsumgebungen, Volumes und Buckets auswählen, die Sie auf Compliance überprüfen möchten. Sie können auch eine Verbindung zu einem Datenbankserver herstellen, um bestimmte Datenbankschemas zu scannen. Aktivieren Sie Cloud Compliance für eine dieser Datenquellen.

Abonnieren des Cloud Compliance Service

Es sind die ersten 1 TB an Daten, die Cloud Compliance in einem Cloud Manager Workspace scannt, kostenlos. Danach ist ein Abonnement für AWS oder Azure Marketplace erforderlich, um mit dem Scannen der Daten fortzufahren.

Sie können sich jederzeit für eine Anmeldung anmelden. Die Abrechnung erfolgt erst, wenn die Datenmenge mehr als 1 TB beträgt. Über das Cloud Compliance Dashboard sehen Sie immer die Gesamtdatenmenge an, die gescannt wird. Und die Schaltfläche *Jetzt abonnieren* erleichtert die Anmeldung, wenn Sie bereit sind.



Hinweis: Wenn Sie von Cloud Compliance aufgefordert werden, sich zu abonnieren, aber Sie bereits über ein Azure-Abonnement verfügen, verwenden Sie wahrscheinlich das alte **Cloud Manager**-Abonnement und müssen in das neue **NetApp Cloud Manager**-Abonnement wechseln. Siehe [Änderung im neuen NetApp Cloud Manager Plan in Azure](#) Entsprechende Details.

Schritte

Diese Schritte müssen von einem Benutzer ausgeführt werden, der über die Rolle *Account Admin* verfügt.

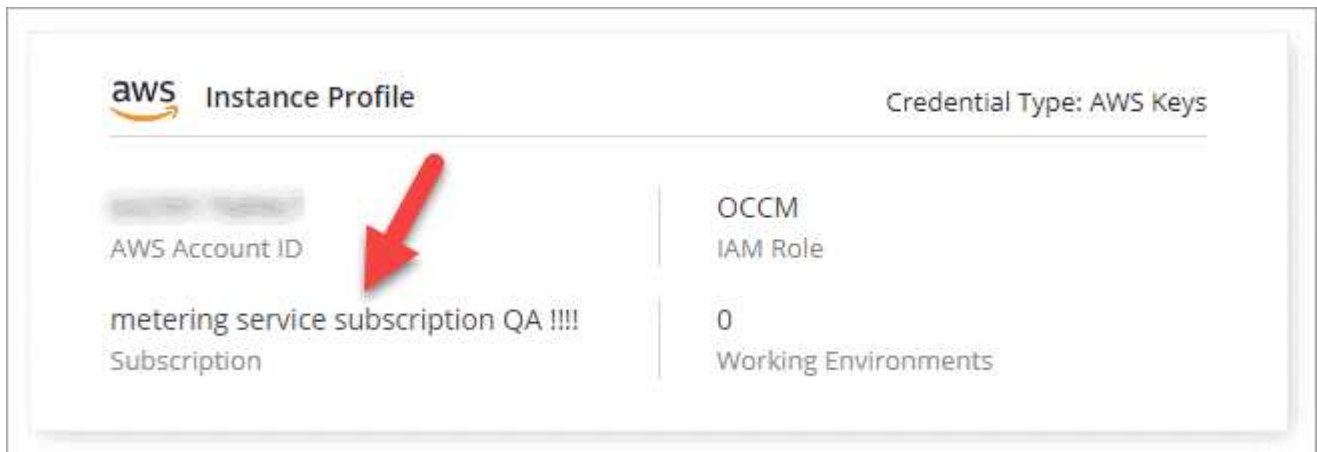
1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



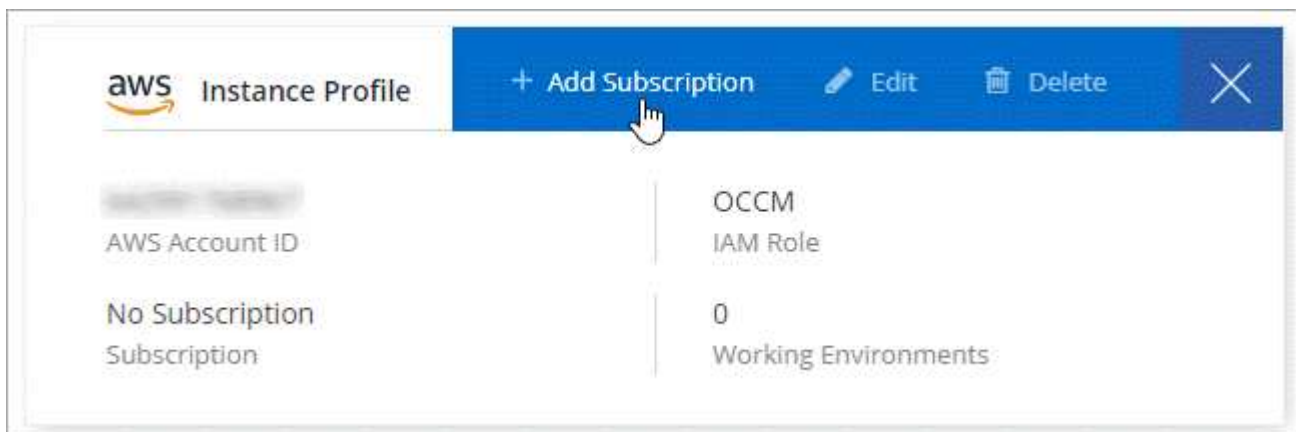
2. Suchen Sie die Zugangsdaten für das AWS Instance Profile oder die Azure Managed Service Identity.

Das Abonnement muss dem Instanzprofil oder der Managed Service Identity hinzugefügt werden. Das Laden funktioniert nicht anders.

Wenn Sie bereits ein Abonnement haben, sind Sie alle eingerichtet – es gibt nichts anderes, was Sie tun müssen.



3. Wenn Sie noch kein Abonnement haben, bewegen Sie den Mauszeiger über die Anmeldeinformationen und klicken Sie auf das Aktionsmenü.
4. Klicken Sie Auf **Abonnement Hinzufügen**.



5. Klicken Sie auf **Abonnement hinzufügen**, klicken Sie auf **Weiter** und befolgen Sie die Schritte.

Im folgenden Video wird gezeigt, wie Sie ein Marketplace-Abonnement zu einem AWS Abonnement

verknüpfen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_aws.mp4 (video)

Im folgenden Video wird gezeigt, wie Sie ein Marketplace-Abonnement zu einem Azure-Abonnement verknüpfen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_azure.mp4 (video)

Änderung beim neuen Cloud Manager Plan in Azure

Cloud Compliance wurde zum Azure Marketplace Abonnement mit dem Namen **NetApp Cloud Manager** zum 7. Oktober 2020 hinzugefügt. Wenn Sie bereits über das ursprüngliche Azure **Cloud Manager**-Abonnement verfügen, können Sie Cloud Compliance nicht nutzen.

Sie müssen diese Schritte ausführen und das neue **NetApp Cloud Manager** Abonnement auswählen und dann das alte **Cloud Manager** Abonnement entfernen.



Wenn Ihr Abonnement auf einem speziellen privaten Angebot ausgestellt wurde, müssen Sie sich an NetApp wenden, damit wir ein neues privates Angebot mit Compliance inbegriffen anbieten können.

Schritte

Diese Schritte ähneln dem Hinzufügen eines neuen Abonnements wie oben beschrieben, variieren jedoch an einigen Stellen.

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Suchen Sie die Anmeldeinformationen für die Azure Managed Service Identity, für die Sie das Abonnement ändern möchten, und zeigen Sie mit dem Mauszeiger über die Anmeldeinformationen, und klicken Sie auf **Associate Subscription**.

Die Details zu Ihrem aktuellen Marketplace-Abonnement werden angezeigt.

3. Klicken Sie auf **Abonnement hinzufügen**, klicken Sie auf **Weiter** und befolgen Sie die Schritte. Sie werden auf das Azure Portal umgeleitet, um das neue Abonnement zu erstellen.
4. Stellen Sie sicher, dass Sie den Plan **NetApp Cloud Manager** für den Zugriff auf Cloud Compliance und nicht **Cloud Manager** wählen.
5. Gehen Sie die Schritte im Video durch, um ein Marketplace-Abonnement für ein Azure-Abonnement zuzuordnen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_azure.mp4 (video)

6. Kehren Sie zu Cloud Manager zurück, wählen Sie das neue Abonnement aus und klicken Sie auf **Associate**.
7. Um zu überprüfen, ob sich Ihr Abonnement geändert hat, bewegen Sie den Mauszeiger über das „i“-Abonnement in der Anmeldeinformationen-Karte.

Jetzt können Sie Ihr altes Abonnement vom Azure Portal abbestellen.

8. Gehen Sie im Azure-Portal zu Software as a Service (SaaS), wählen Sie das Abonnement aus und klicken Sie auf **Abmelden**.

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.



1 Implementieren der Cloud Compliance-Instanz

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



2 Cloud Compliance in Ihren Arbeitsumgebungen

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



3 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.



4 Konfigurieren Sie die Volumes für das Scannen

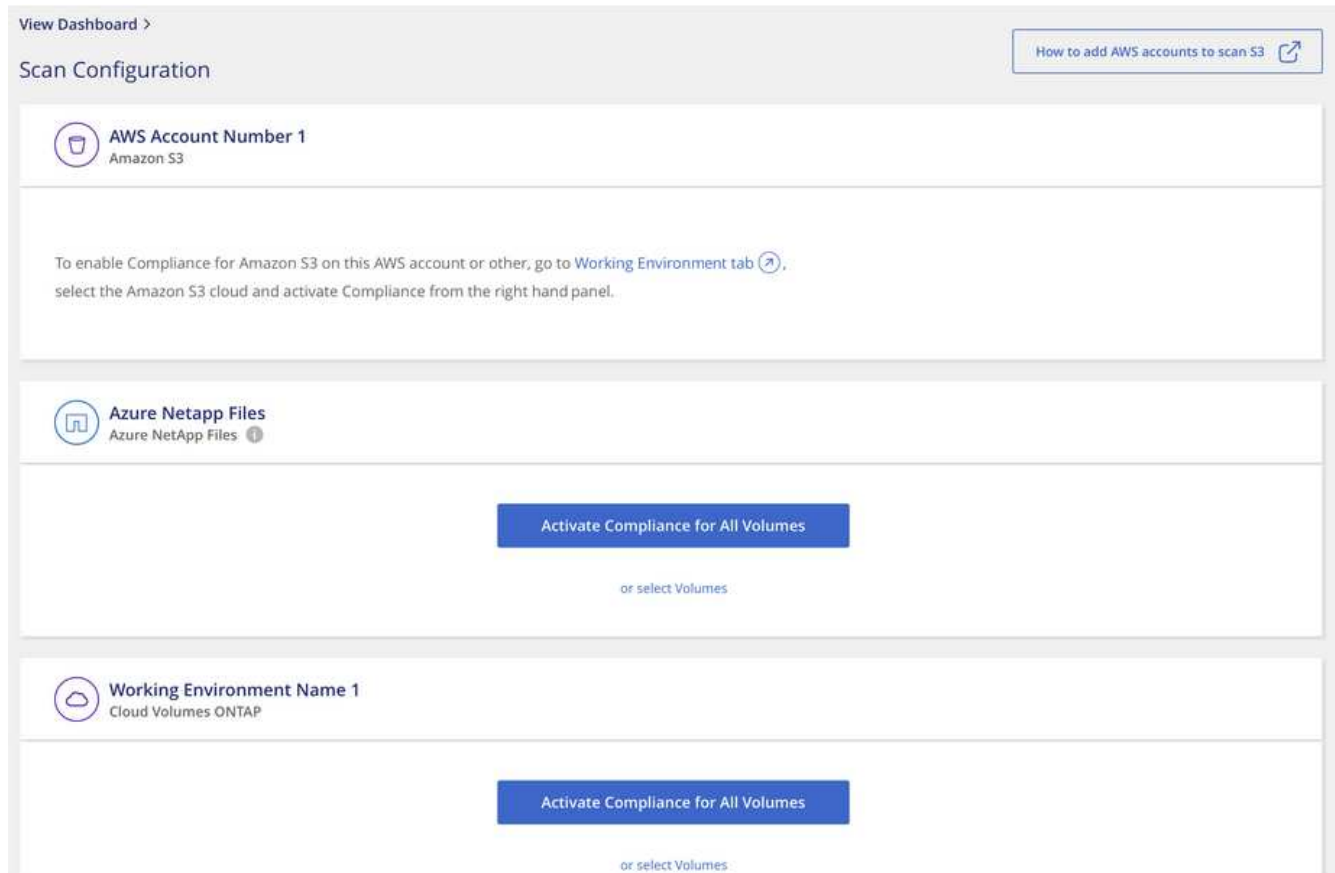
Wählen Sie die Volumes aus, die Sie scannen möchten, und Cloud Compliance beginnt, sie zu scannen.

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.



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.

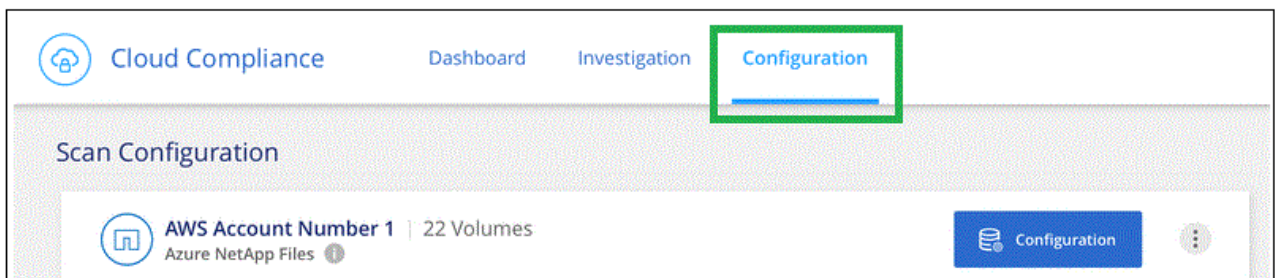


Bei Azure NetApp Files kann Cloud Compliance Volumes nur in derselben Region wie Cloud Manager überprüfen.

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.

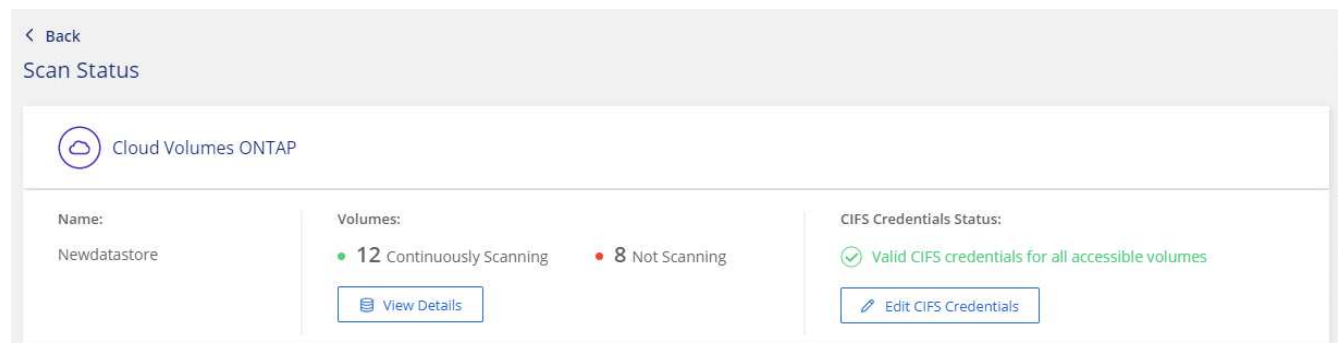
3. Vergewissern Sie sich, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Cloud Compliance-Instanz enthalten, damit sie auf die Daten der einzelnen Volumes zugreifen können.
4. Wenn Sie CIFS verwenden, geben Sie Cloud Compliance mit Active Directory Anmeldedaten ein, damit CIFS Volumes gescannt 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.

Compliance: Activate Compliance for all Volumes | 28/28 Volumes selected for compliance scan

Compliance	Name ↑↓	Protocol ↑↓	Status ↑↓	Required Action ↑↓
<input checked="" type="checkbox"/>	10.160.7.6:/yuval22	NFS	Continuously Scanning	
<input checked="" type="checkbox"/>	10.160.7.6:/yuvalnewtarget	NFS	Continuously Scanning	
<input checked="" type="checkbox"/>	\\10.160.7.6\Danny_share	CIFS	No Access	The CIFS credentials that you provided have expired. Edit the CIFS credential...

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.

Compliance: Activate Compliance for all Volumes | 27/28 Volumes selected for compliance scan

Compliance	Volume Name ↑↓	Status	Required Action
<input type="checkbox"/>	VolumeName1	Not Scanning	Add CIFS Credentials ⓘ
<input type="checkbox"/>	VolumeName2	Continuously Scanning	
<input type="checkbox"/>	VolumeName3	Not Scanning	
<input type="checkbox"/>	VolumeName4	Continuously Scanning	
<input type="checkbox"/>	VolumeName5	Continuously Scanning	

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 Compliance für alle Volumes 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 Compliance für alle Volumes nach rechts

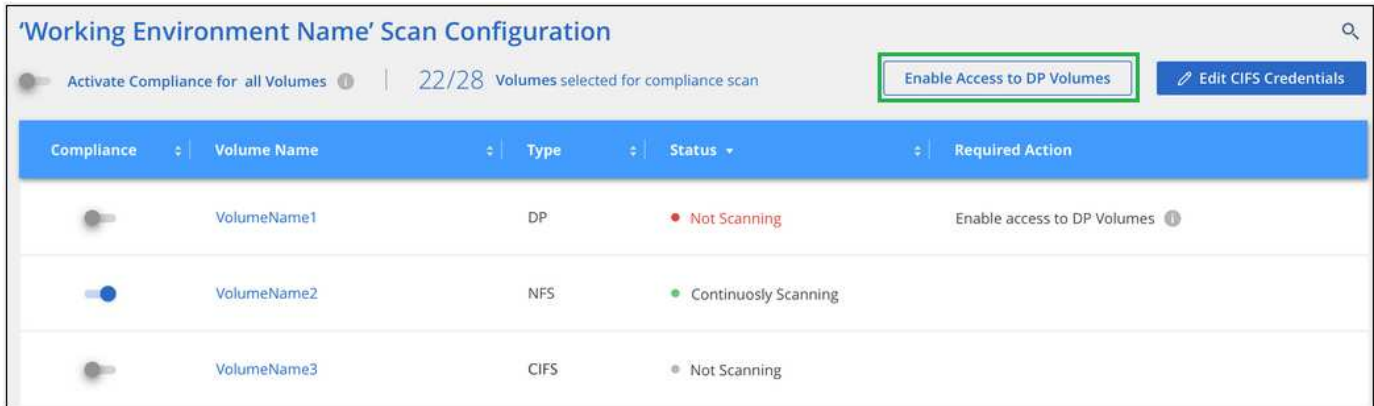


Neue Volumes, die der Arbeitsumgebung hinzugefügt werden, werden nur dann automatisch gescannt, wenn die Einstellung **Compliance für alle Volumes** aktivieren aktiviert ist. Wenn diese Einstellung deaktiviert ist, müssen Sie das Scannen für jedes neue Volumen aktivieren, das Sie in der Arbeitsumgebung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



'Working Environment Name' Scan Configuration

Activate Compliance for all Volumes | 22/28 Volumes selected for compliance scan

Enable Access to DP Volumes | Edit CIFS Credentials

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

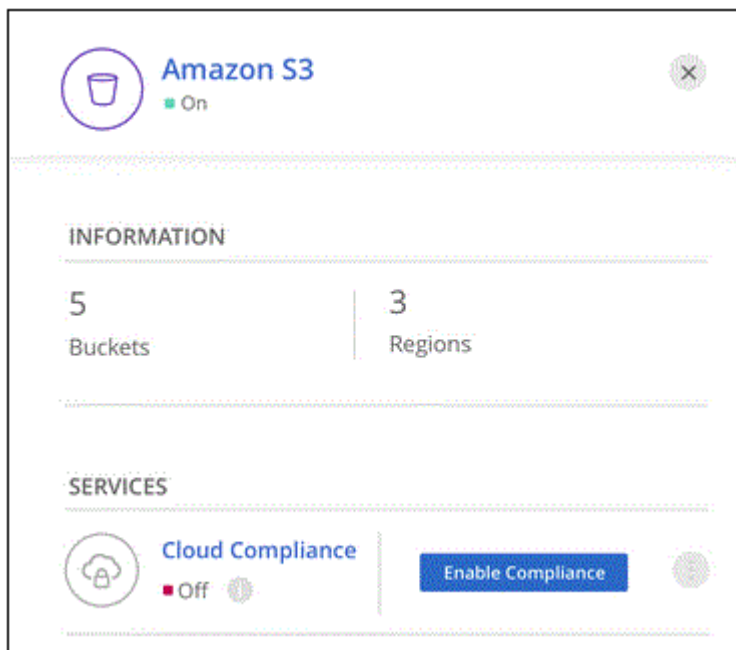
Aktivieren Sie Cloud-Compliance auf Amazon S3, nachdem Sie die Voraussetzungen überprüft haben.

Schritte

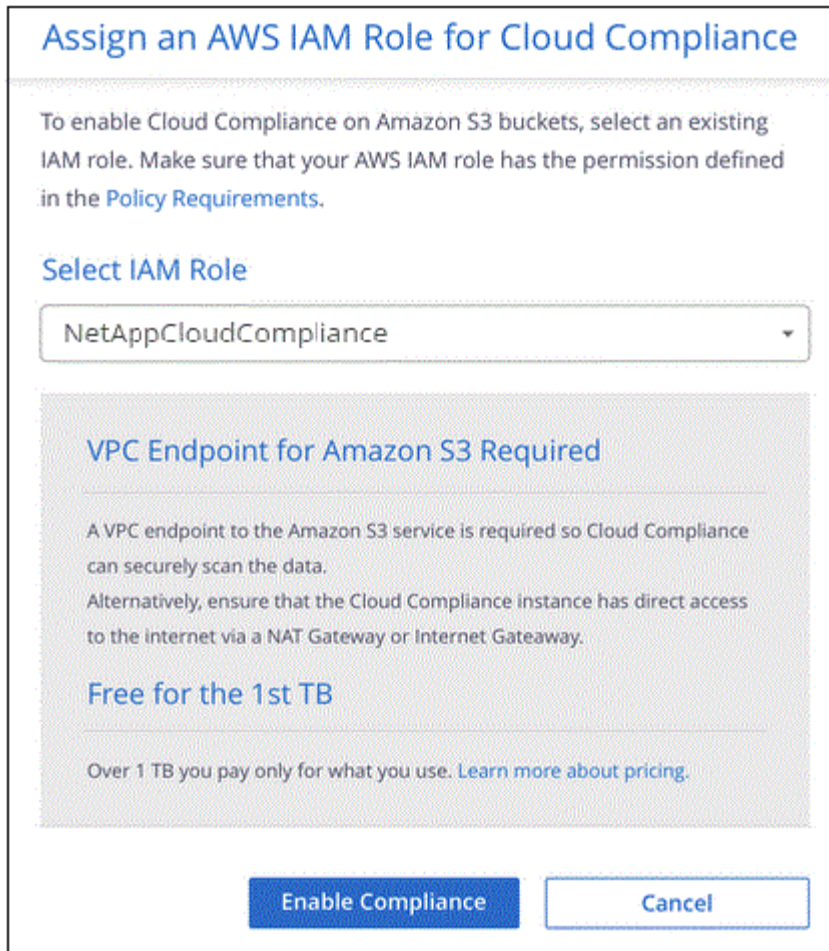
1. Klicken Sie oben im Cloud Manager auf **Arbeitsumgebungen**.
2. Wählen Sie die Amazon S3-Arbeitsumgebung aus.



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

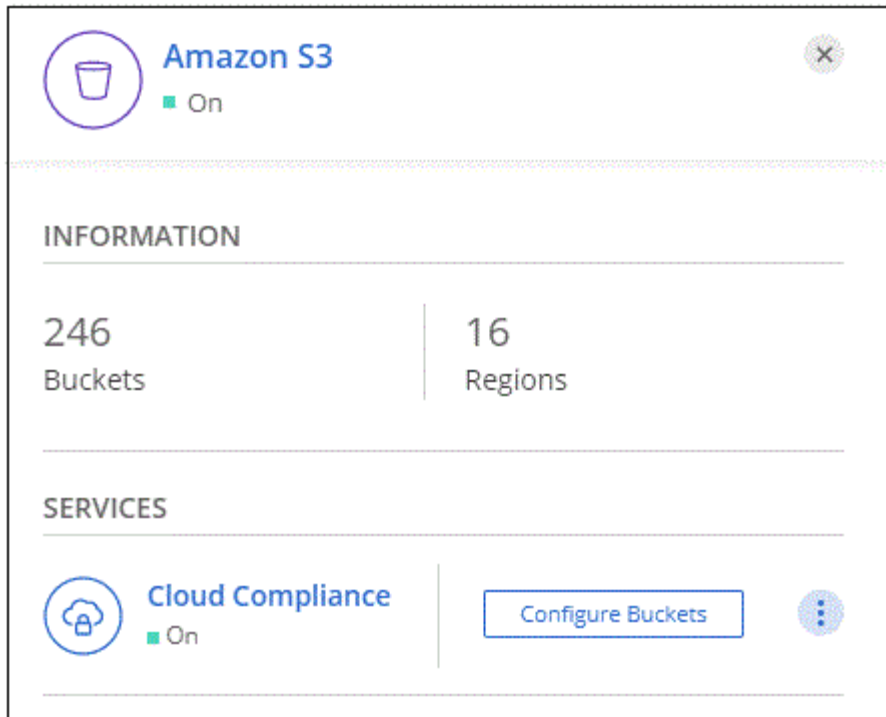
Nachdem Cloud Manager Cloud Compliance in Amazon S3 aktiviert hat, müssen die Buckets konfiguriert werden, die überprüft werden sollen.

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.

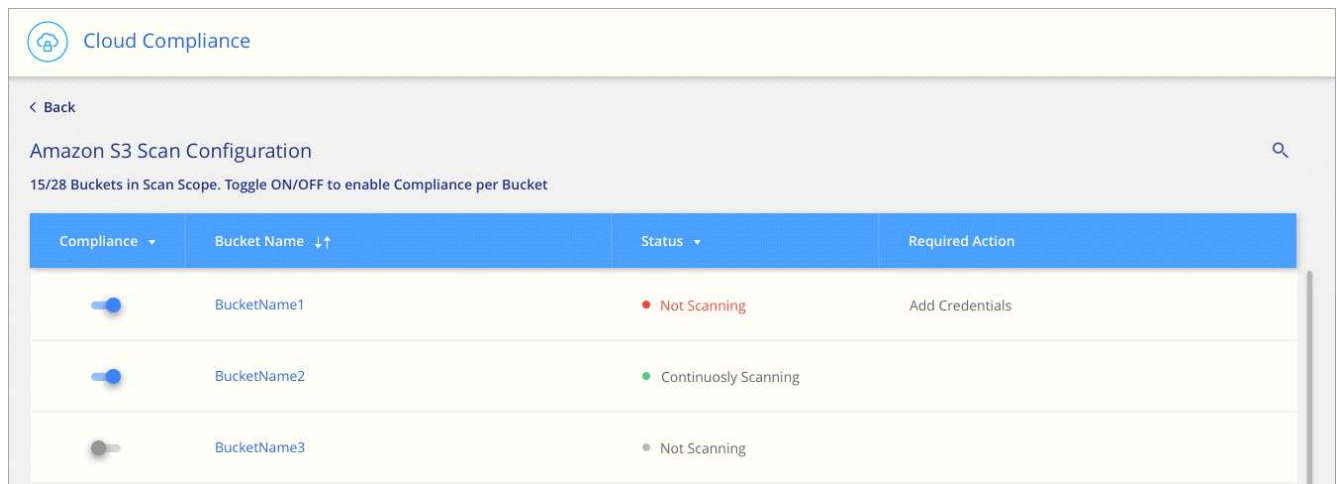
Auch Cloud Compliance kann [Scannen von S3-Buckets, die in unterschiedlichen AWS Konten vorhanden sind](#).

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

 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-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.

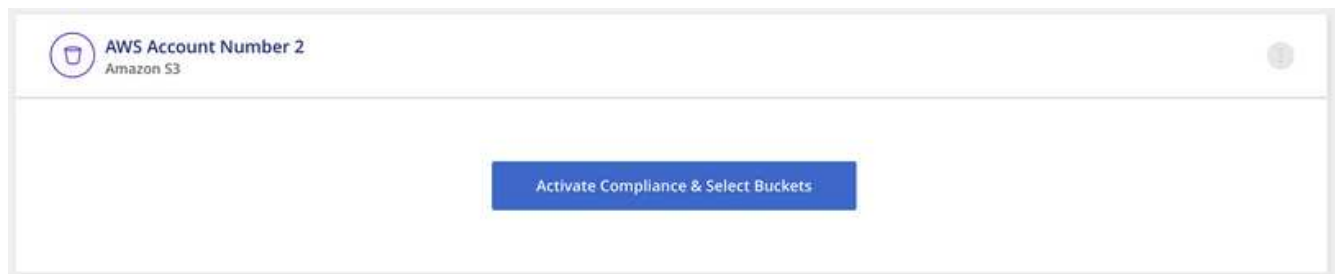

```

{
  "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.

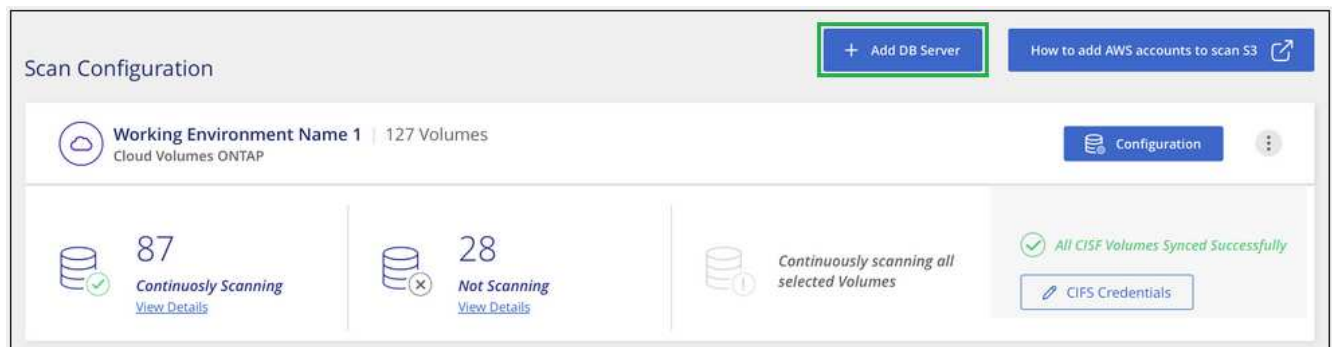
Hinweis: für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

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.

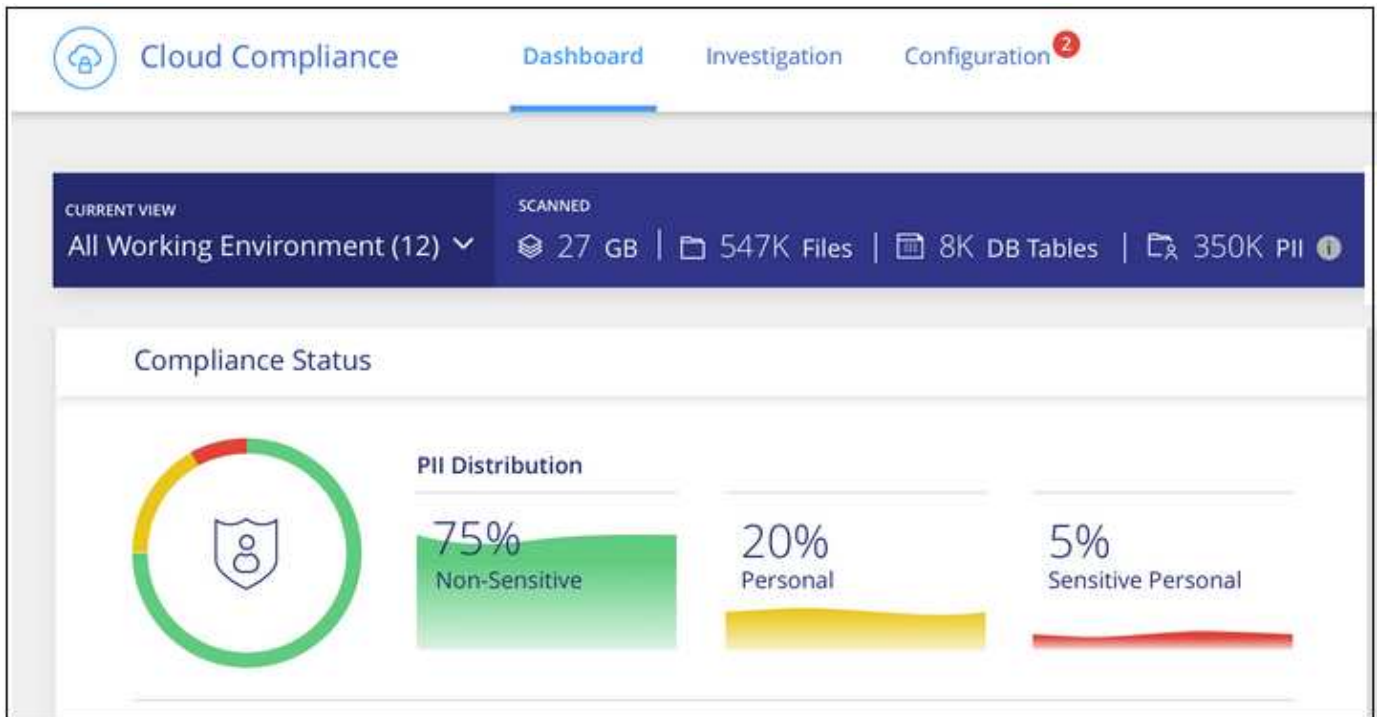
- a. ["Ermitteln des On-Premises-Clusters in Cloud Manager"](#).
 - b. ["Erstellen einer SnapMirror Replizierung zwischen dem lokalen ONTAP Cluster und Cloud Volumes ONTAP aus Cloud Manager"](#).
2. Konfigurieren Sie bei DP-Volumes, die aus SMB-Quell-Volumes erstellt wurden, über die Befehlszeilenschnittstelle 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.

Mehr Transparenz und Kontrolle über private Daten

Mehr Kontrolle über Ihre persönlichen Daten durch die Anzeige von Details zu den personenbezogenen Daten und vertraulichen personenbezogenen Daten in Ihrem Unternehmen. Auch die Kategorien und Dateitypen, die Cloud Compliance in Ihren Daten enthalten ist, können für Sie transparent dargestellt werden.

Standardmäßig werden auf dem Cloud Compliance-Dashboard Compliance-Daten für alle Arbeitsumgebungen und Datenbanken angezeigt.



Wenn Sie Daten nur für einige der Arbeitsumgebungen sehen möchten, [Wählen Sie diese Arbeitsumgebungen aus](#).

Persönliche Daten

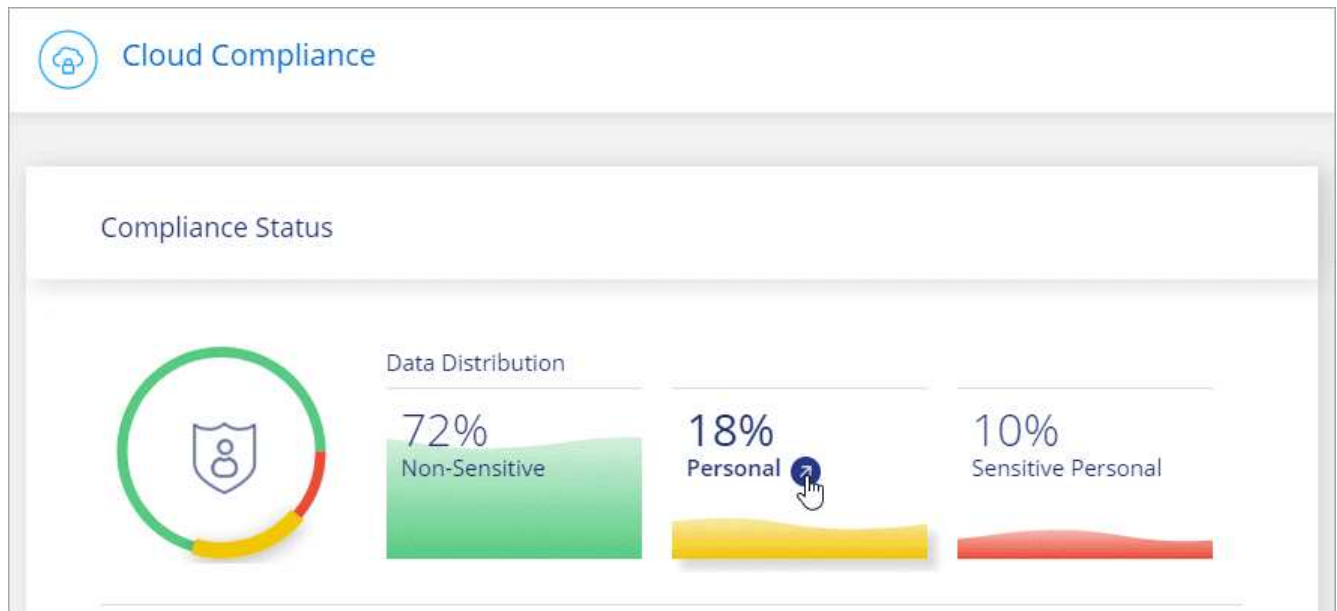
Cloud Compliance identifiziert automatisch bestimmte Wörter, Strings und Muster (Regex) in den Daten. Beispielsweise personenbezogene Daten (Personal Identification Information, PII), Kreditkartennummern, Sozialversicherungsnummern und Kontonummern. [Die vollständige Liste finden Sie hier](#).

Für einige Arten von personenbezogenen Daten verwendet Cloud Compliance die *Proximity-Validierung*, um die Ergebnisse zu validieren. Die Validierung erfolgt, indem ein oder mehrere vordefinierte Schlüsselwörter in der Nähe der gefundenen personenbezogenen Daten gesucht werden. Cloud Compliance identifiziert z. B. eine US-amerikanische Sozialversicherungsnummer (SSN) als SSN, wenn sie neben ihr ein Näherungswort sieht - zum Beispiel *SSN* oder *Sozialversicherung*. [Die Liste unten](#) zeigt an, wann Cloud Compliance die Näherungsüberprüfung verwendet.

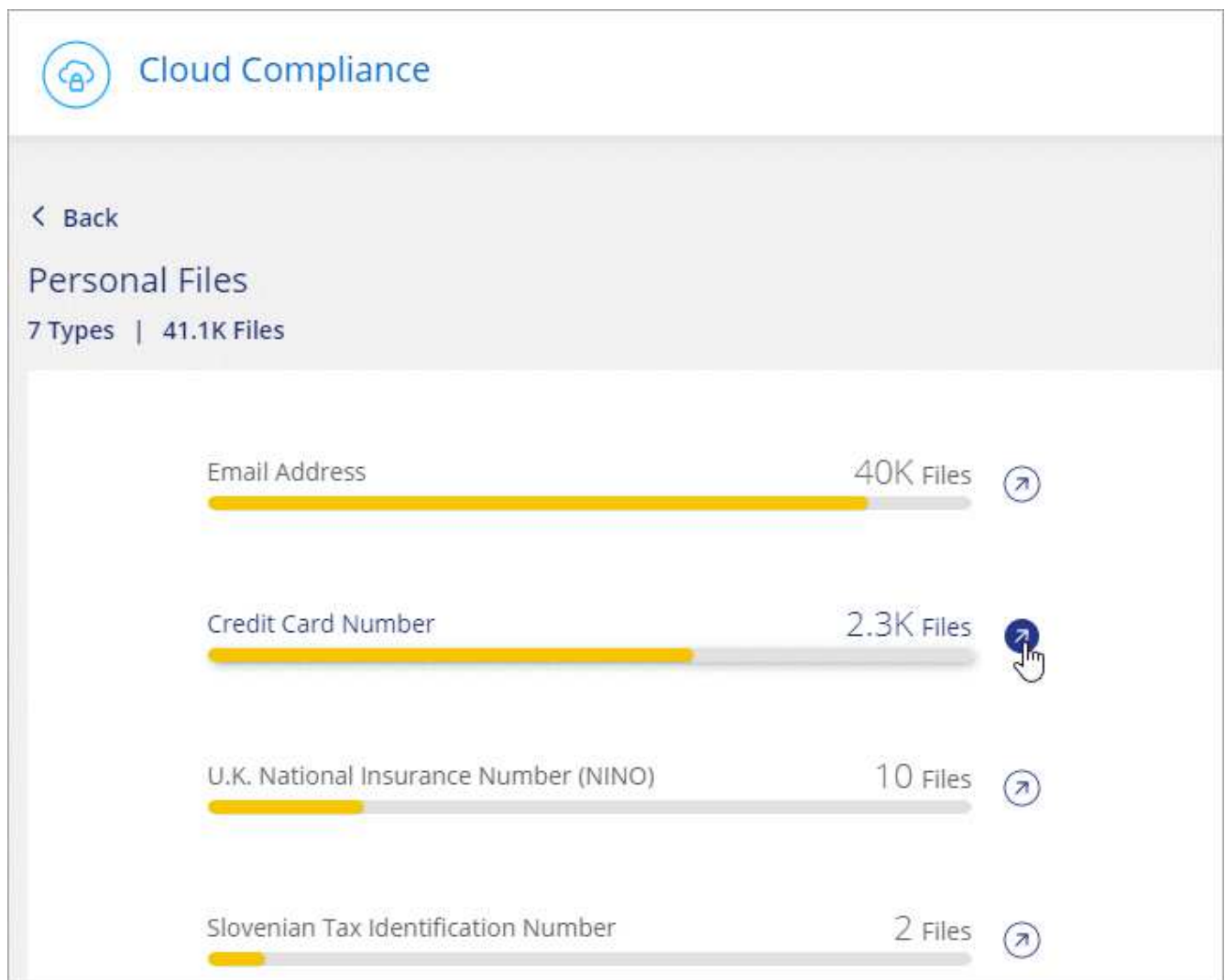
Anzeigen von Dateien mit persönlichen Daten

Schritte

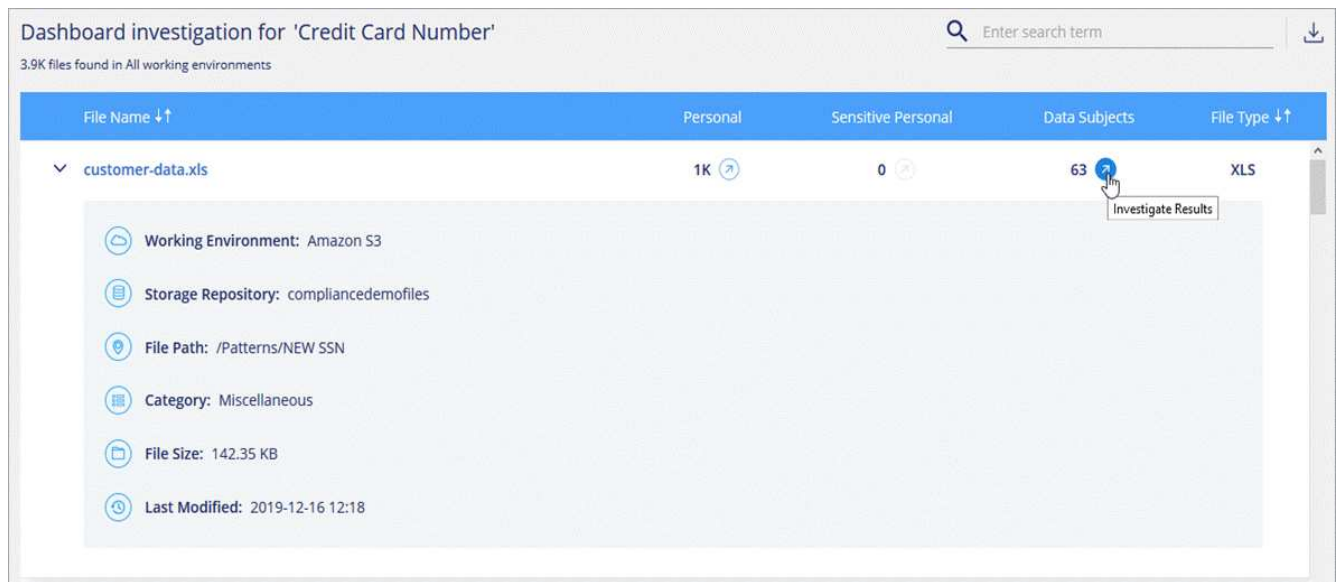
1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance** und klicken Sie auf die Registerkarte **Dashboard**.
2. Um die Angaben zu allen personenbezogenen Daten zu untersuchen, klicken Sie auf das Symbol neben dem Prozentsatz der persönlichen Daten.



- Um die Daten für eine bestimmte Art von personenbezogenen Daten zu untersuchen, klicken Sie auf **Alle anzeigen** und dann auf das Symbol **Ergebnisse untersuchen** für einen bestimmten Typ von personenbezogenen Daten.

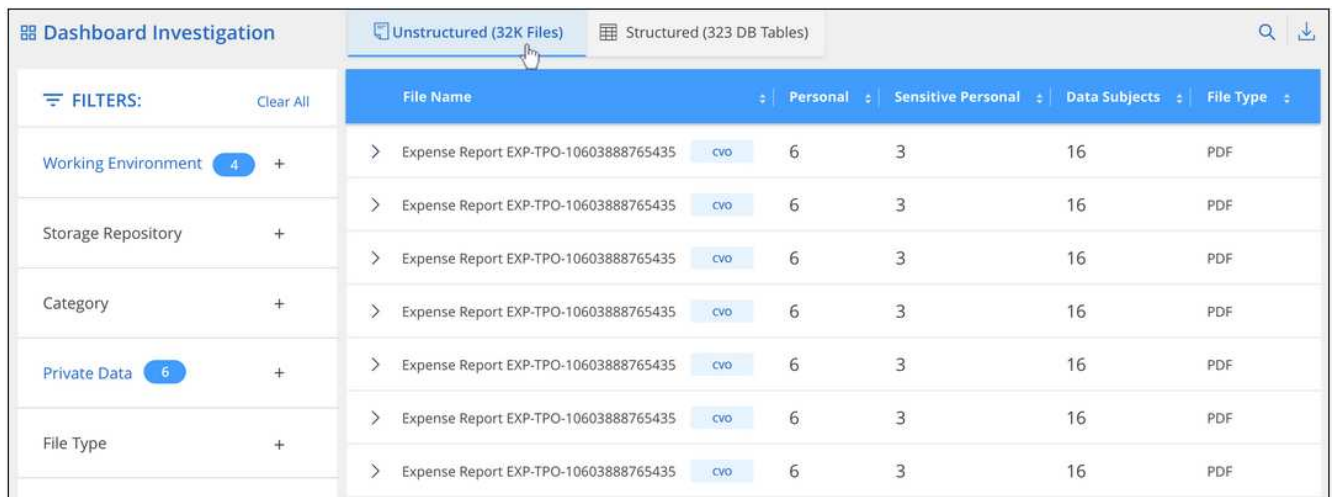


- Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.



- Sie können den Inhalt der Untersuchungsseite auch so filtern, dass nur die Ergebnisse angezeigt werden, die angezeigt werden sollen. Auf den Registerkarten der obersten Ebene können Sie Daten aus Dateien (unstrukturierte Daten) oder aus Datenbanken (strukturierte Daten) anzeigen.

Dann haben Sie Filter für die Arbeitsumgebung, das Storage-Repository, die Kategorie, die privaten Daten, den Dateityp, Datum der letzten Änderung und ob die Berechtigungen des S3-Objekts für den öffentlichen Zugriff zugänglich sind.



Arten personenbezogener Daten

Die in Dateien gefundenen personenbezogenen Daten können allgemeine personenbezogene Daten oder nationale Kennungen sein. In der dritten Spalte wird angegeben, ob Cloud Compliance verwendet wird [Prüfung der Nähe](#) Zum Validieren seiner Ergebnisse für die Kennung.

Typ	Kennung	Näherungsvalidierung?
Allgemein	E-Mail-Adresse	Nein
	Kreditkartennummer	Nein
	IBAN-Nummer (International Bank Account Number)	Nein

Typ	Kennung	Näherungsvalidierung?
Nationale Kennungen	Belgischer Ausweis (Numero National)	Ja.
	Brasilianischer Ausweis (CPF)	Ja.
	Bulgarische ID (UCN)	Ja.
	California Driver's License	Ja.
	Kroatische ID (OIB)	Ja.
	Zypern Steuernummer (TIC)	Ja.
	Tschechische/Slowakische Ausweisnummer	Ja.
	Dänische ID (HLW)	Ja.
	Niederländische ID (BSN)	Ja.
	Estnische ID	Ja.
	Finnische ID (HETU)	Ja.
	Französische Steuernummer (SPI)	Ja.
	Steuernummer (Steuerliche Identifikationsnummer)	Ja.
	Griechische ID	Ja.
	Ungarische Steuernummer	Ja.
	Irish ID (PPS)	Ja.
	Israelische ID	Ja.
	Italienische Steuernummer	Ja.
	Lettischer Ausweis	Ja.
	Litauische ID	Ja.
	Luxemburg-ID	Ja.
	Maltesische ID	Ja.
	Polish ID (PESEL)	Ja.
	Portugiesische Steuernummer (NIF)	Ja.
	Rumänische ID (CNP)	Ja.
	Slowenische ID (EMSO)	Ja.
	Südafrikanischer Ausweis	Ja.
	Spanische Steuernummer	Ja.
	Schwedische ID	Ja.
	GROSSBRITANNIEN ID (NINO)	Ja.
USA Sozialversicherungsnummer (SSN)	Ja.	

Sensible persönliche Daten

Cloud Compliance identifiziert automatisch spezielle Arten von sensiblen personenbezogenen Daten, wie sie in Datenschutzvorschriften wie z. B. definiert sind "[Artikel 9 und 10 der DSGVO](#)". Beispielsweise Informationen über die Gesundheit einer Person, ethnische Herkunft oder sexuelle Orientierung. [Die vollständige Liste finden Sie hier.](#)

Cloud Compliance verwendet künstliche Intelligenz (KI), NLP (Natural Language Processing), maschinelles Lernen (ML) und Cognitive Computing (CC), um die Bedeutung des von ihm gescannten Inhalts zu verstehen, um Entitäten zu extrahieren und entsprechend zu kategorisieren.

Beispielsweise ist eine sensitive DSGVO-Datenkategorie ethnisch Ursprungs. Aufgrund seiner NLP-Fähigkeiten kann Cloud Compliance den Unterschied zwischen einem Satz unterscheiden, der "George ist mexikanisch" (was auf sensible Daten wie in Artikel 9 der DSGVO angegeben), und "George isst mexikanisches Essen".

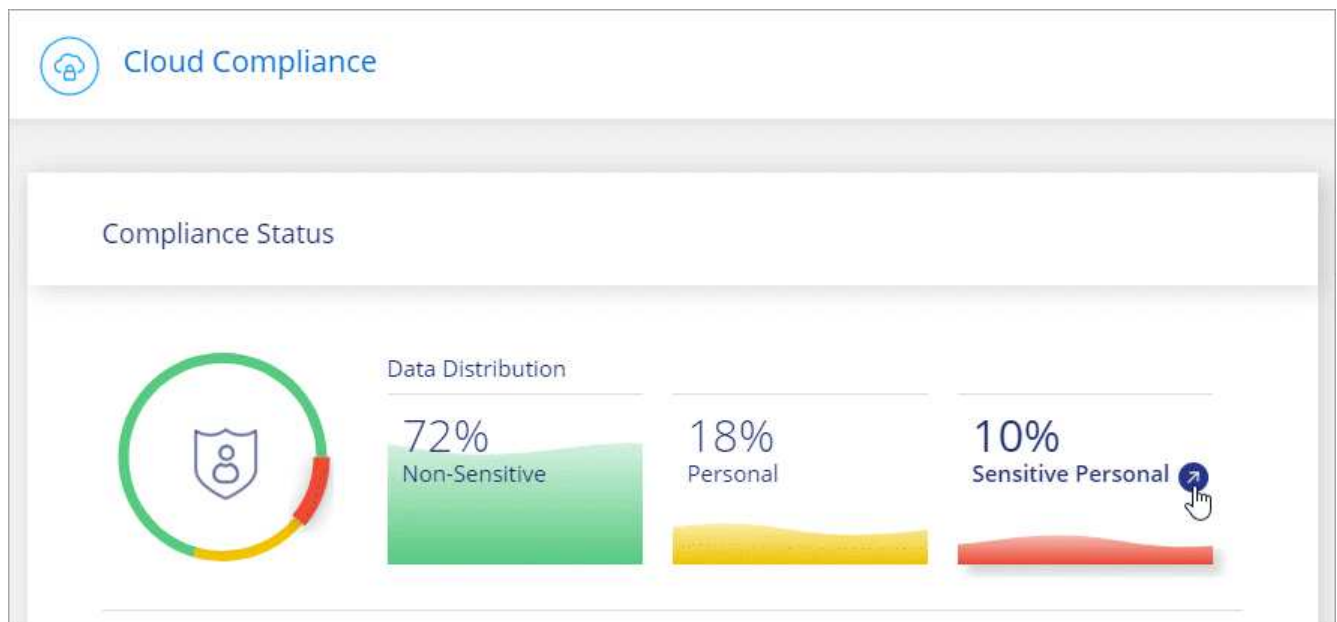


Nur Englisch wird beim Scannen sensibler personenbezogener Daten unterstützt. Support für weitere Sprachen wird später hinzugefügt.

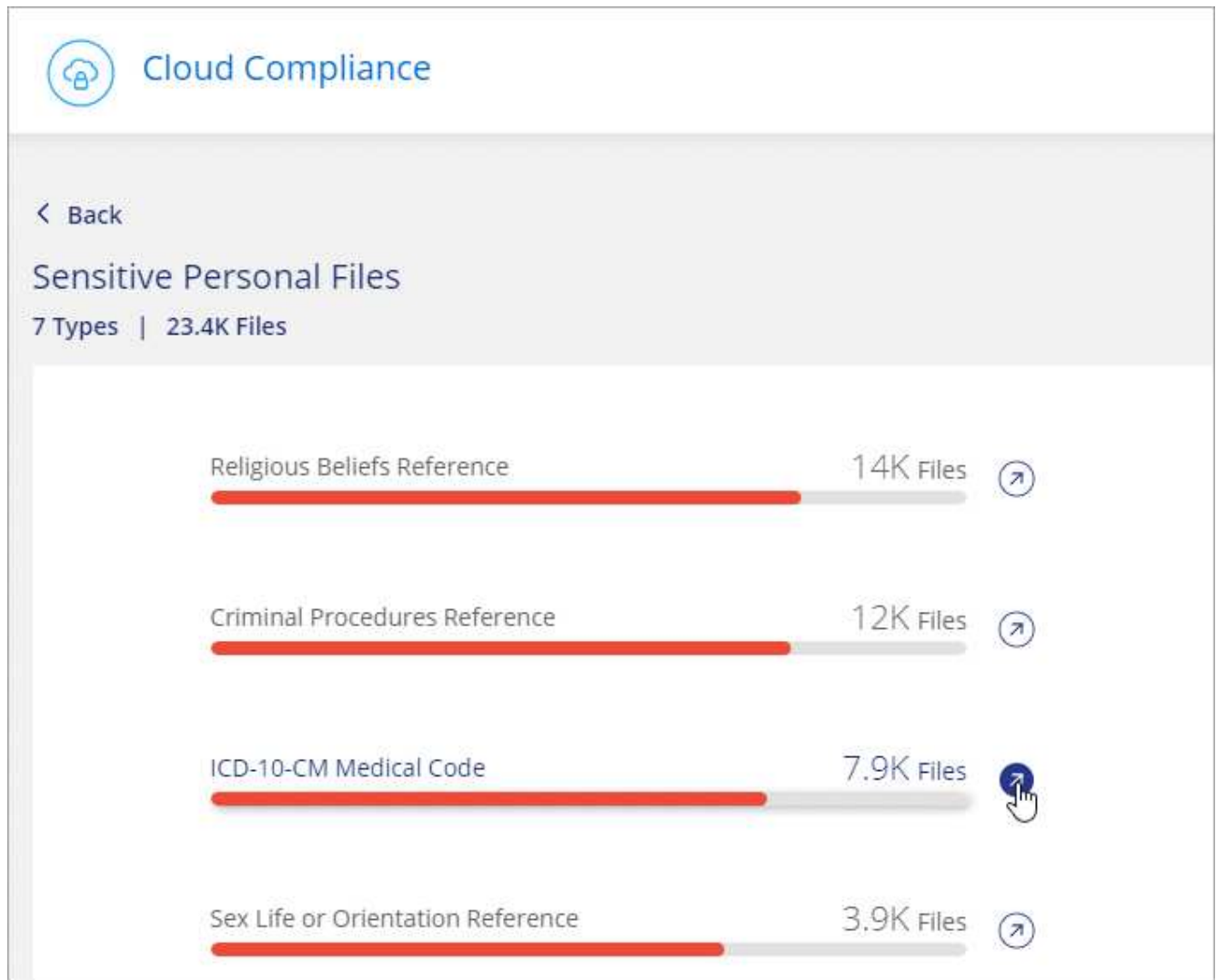
Anzeigen von Dateien mit vertraulichen persönlichen Daten

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Um die Details für alle sensiblen persönlichen Daten zu untersuchen, klicken Sie auf das Symbol neben dem Prozentsatz sensibler personenbezogener Daten.



3. Um die Details für eine bestimmte Art sensibler personenbezogener Daten zu untersuchen, klicken Sie auf **Alle anzeigen** und klicken Sie dann auf das Symbol **Ergebnisse untersuchen** für einen bestimmten Typ sensibler personenbezogener Daten.



4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

Arten sensibler personenbezogener Daten

Folgende sensible personenbezogene Daten, die Cloud Compliance in Dateien finden kann:

Referenz Für Kriminelle Verfahren

Daten zu strafrechtlichen Überzeugungen und Straftaten einer natürlichen Person.

Ethnische Referenz

Daten über die rassische oder ethnische Herkunft einer natürlichen Person.

Systemzustand

Daten über die Gesundheit einer natürlichen Person.

ICD-9-CM-Ärztliche Codes

Codes, die in der Medizin- und Gesundheitsbranche verwendet werden.

ICD-10-CM-Ärztliche Codes

Codes, die in der Medizin- und Gesundheitsbranche verwendet werden.

Philosophische Überzeugungen Referenz

Daten über die philosophischen Überzeugungen einer natürlichen Person.

Religiöse Überzeugungen Referenz

Daten über die religiösen Überzeugungen einer natürlichen Person.

Sexualleben oder Orientierung Referenz

Daten über das Sexualleben einer natürlichen Person oder die sexuelle Orientierung.

Kategorien

Bei Cloud Compliance werden die gescannten Daten in verschiedene Kategorien unterteilt. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. [Siehe die Liste der Kategorien.](#)

Kategorien können Ihnen dabei helfen zu verstehen, was mit Ihren Daten passiert, indem Sie die Arten von Informationen anzeigen, die Sie haben. Beispielsweise kann eine Kategorie wie Lebensläufe oder Mitarbeiterverträge sensible Daten enthalten. Wenn Sie die Ergebnisse untersuchen, können Sie feststellen, dass Mitarbeiterverträge an einem unsicheren Ort gespeichert sind. Sie können das Problem dann beheben.

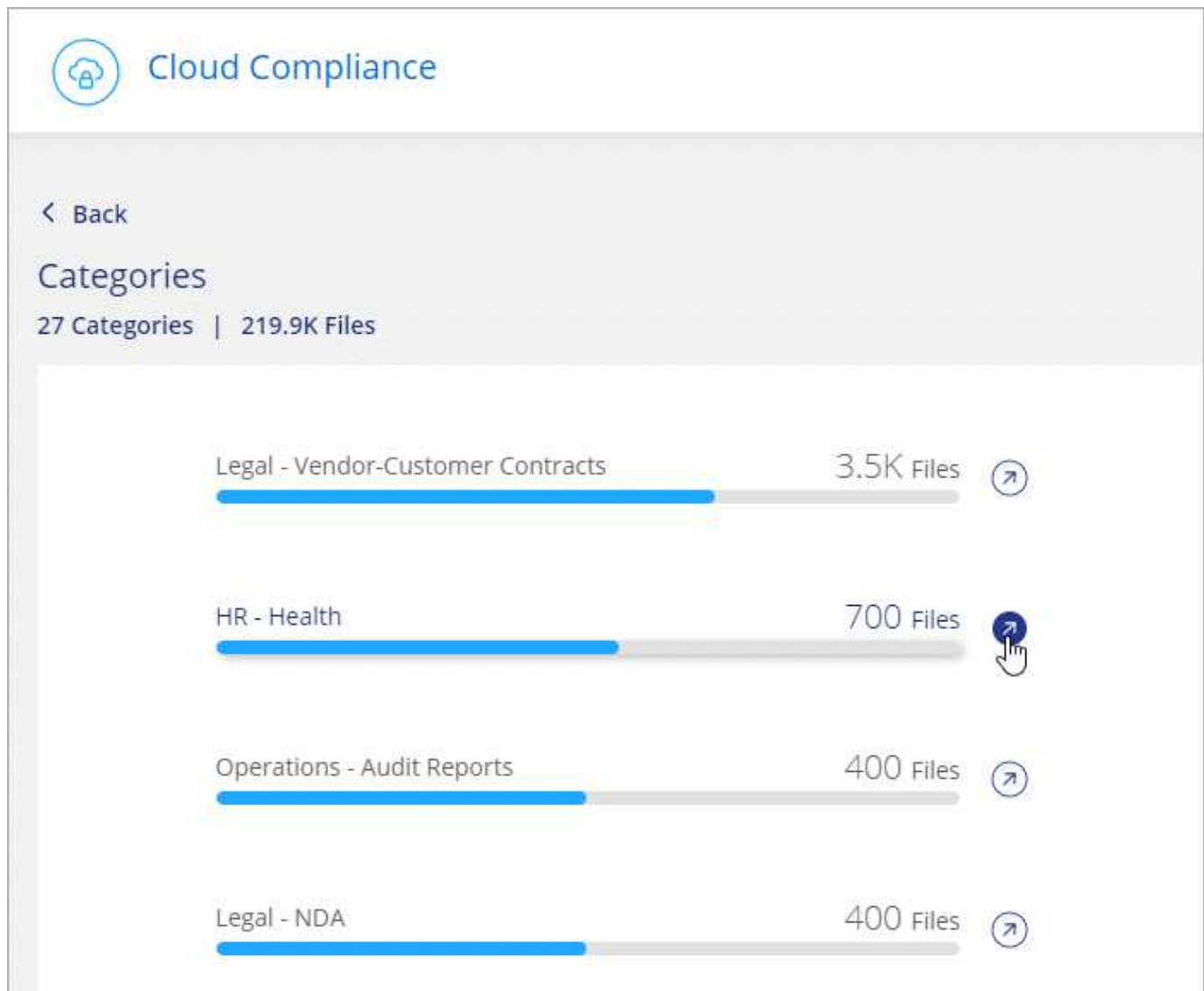


Nur Englisch wird für Kategorien unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Anzeigen von Dateien nach Kategorien

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie auf das Symbol **Ergebnisse untersuchen** für eine der 4 Top-Kategorien direkt im Hauptbildschirm oder klicken Sie auf **Alle anzeigen** und dann auf das Symbol für eine der Kategorien.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

Arten von Kategorien

Cloud Compliance kategorisiert Ihre Daten wie folgt:

Finanzen

- Bilanz
- Bestellungen
- Rechnungen
- Vierteljährliche Berichte

HR

- Background-Checks
- Vergütungspläne
- Mitarbeiterverträge

- Mitarbeiterbewertung
- Systemzustand
- Wird Fortgesetzt

Legal

- NDAs
- Verträge zwischen Anbietern und Kunden

Marketing

- Kampagnen
- Konferenzen

Betrieb

- Audit-Berichte

Vertrieb

- Aufträge

Services

- RFI
- AUSSCHREIBUNG
- SOW
- Schulung

Unterstützung

- Reklamationen und Tickets

Metadatenkategorien

- Applikationsdaten
- Archivdateien
- Audio
- Daten Von Business-Applikationen
- CAD-Dateien
- Codieren
- Datenbank- und Indexdateien
- Design-Dateien
- E-Mail-Anwendungsdaten
- Ausführbare Dateien
- Daten Aus Finanzapplikationen
- Daten Der Integritätsanwendungen
- Bilder
- Protokolle
- Verschiedene Dokumente

- Diverse Präsentationen
- Verschiedene Tabellenkalkulationen
- Videos

Dateitypen

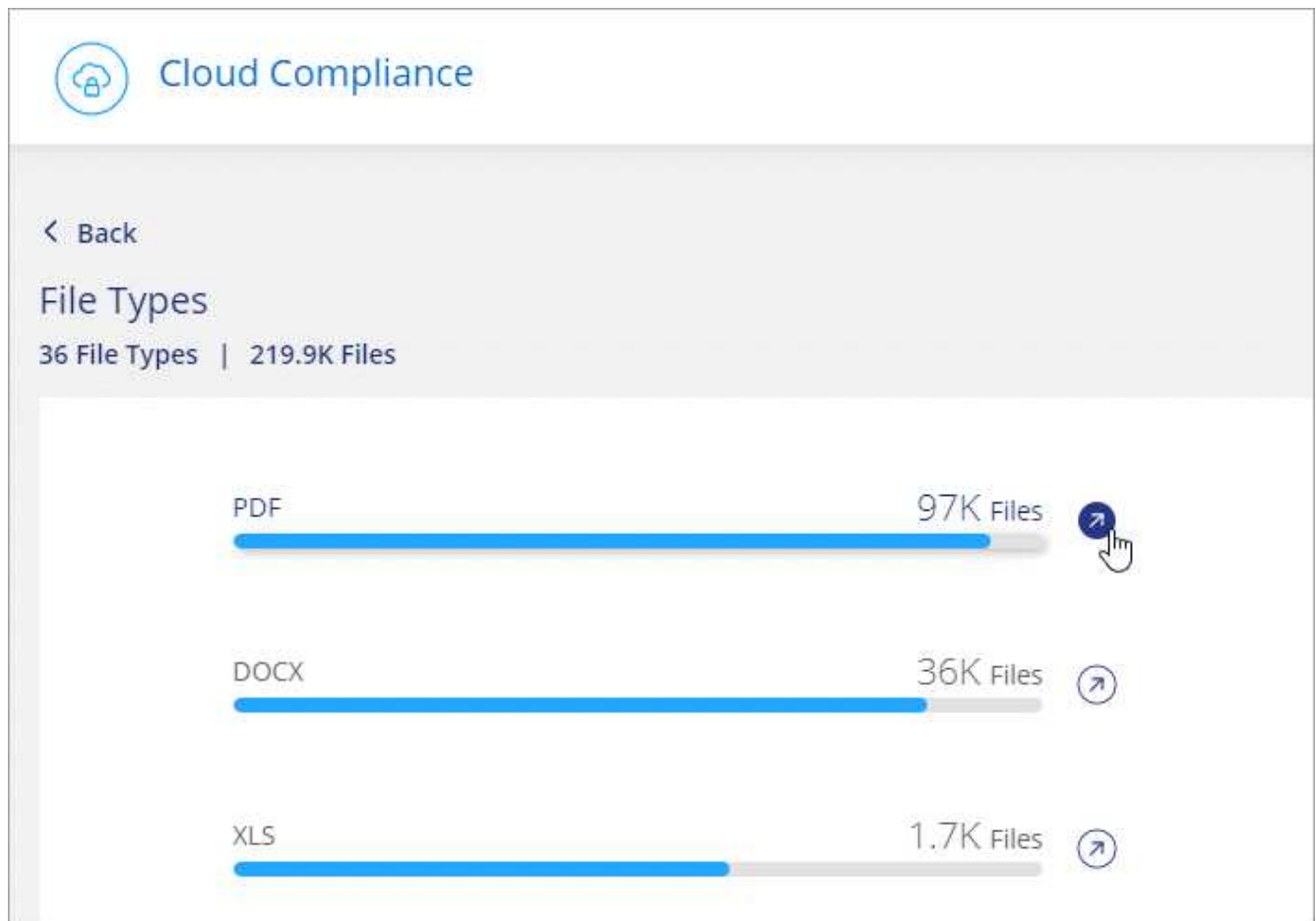
Cloud Compliance greift die gescannten Daten auf und legt sie nach Dateityp fest. Die Überprüfung Ihrer Dateitypen kann Ihnen helfen, Ihre sensiblen Daten zu kontrollieren, da Sie möglicherweise feststellen können, dass bestimmte Dateitypen nicht richtig gespeichert sind. [Siehe die Liste der Dateitypen.](#)

Sie können beispielsweise CAD-Dateien speichern, die sehr sensible Informationen über Ihr Unternehmen enthalten. Wenn diese nicht gesichert sind, können Sie die Kontrolle über vertrauliche Daten übernehmen, indem Sie Berechtigungen beschränken oder Dateien an einen anderen Speicherort verschieben.

Anzeigen von Dateitypen

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie auf das Symbol **Ergebnisse untersuchen** für einen der 4 wichtigsten Dateitypen direkt vom Hauptbildschirm aus, oder klicken Sie auf **Alle anzeigen** und dann auf das Symbol für einen der Dateitypen.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die

Dateiliste herunter.

Dateitypen

Cloud Compliance scannt alle Dateien nach Informationen zu Kategorien und Metadaten und zeigt alle Dateitypen im Abschnitt Dateitypen im Dashboard an.

Wenn aber Cloud Compliance personenbezogene Daten (PII) erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF UND .JSON.

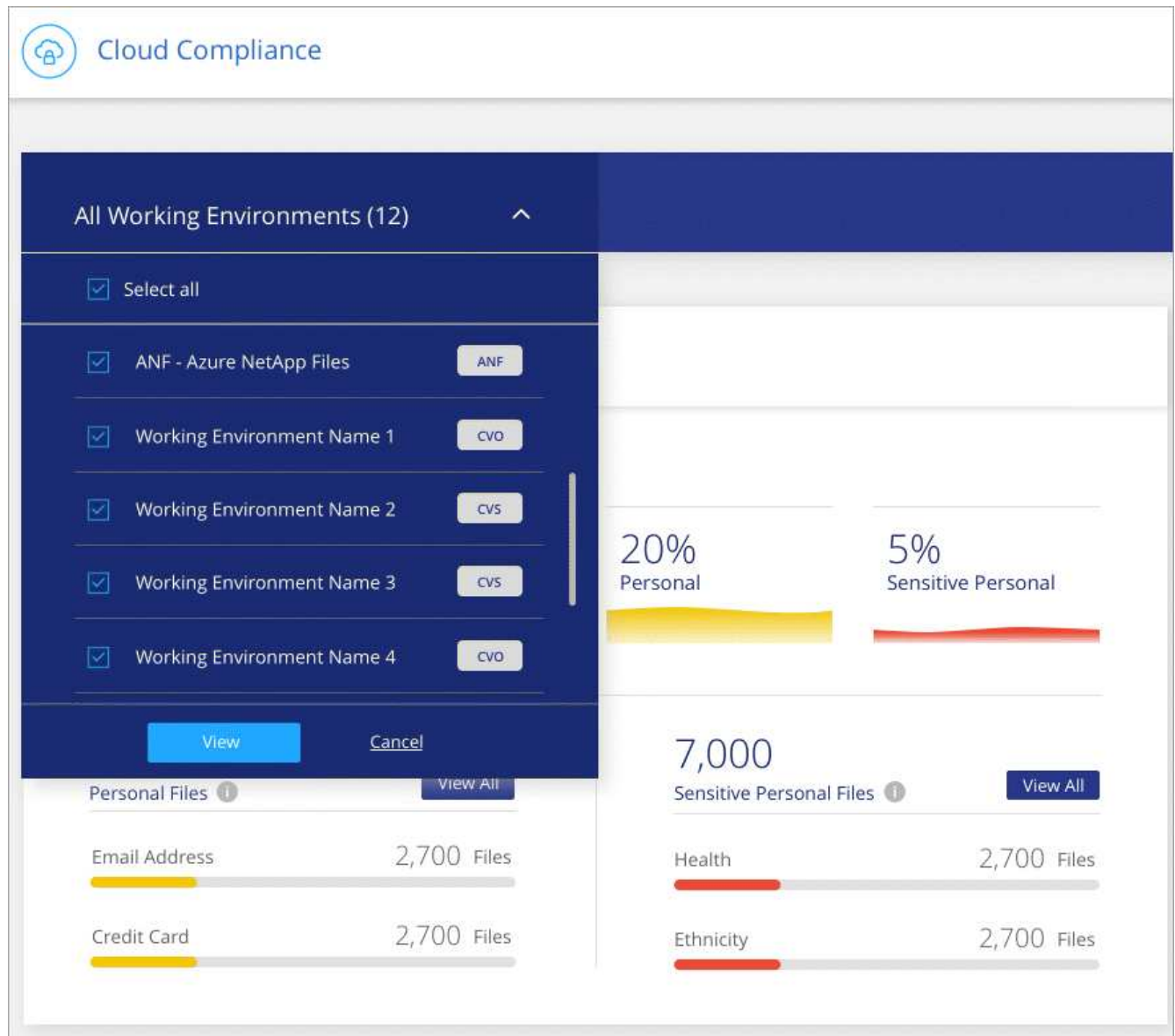
Anzeigen von Daten aus bestimmten Arbeitsumgebungen

Sie können die Inhalte des Cloud Compliance Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur für bestimmte Arbeitsumgebungen anzuzeigen.

Wenn Sie das Dashboard filtern, wird durch Cloud Compliance die Compliance-Daten und -Berichte genau den von Ihnen ausgewählten Arbeitsumgebungen beschrieben.

Schritte

1. Klicken Sie auf das Dropdown-Menü Filter, wählen Sie die Arbeitsumgebungen aus, für die Sie Daten anzeigen möchten, und klicken Sie auf **Ansicht**.



Genauigkeit der gefundenen Informationen

NetApp kann keine Garantie für 100 % Genauigkeit der persönlichen Daten und für sensible personenbezogene Daten, die Cloud Compliance identifiziert hat, geben. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Auf der Grundlage unserer Tests zeigt die folgende Tabelle die Richtigkeit der Informationen, die Cloud Compliance findet. Wir brechen es durch *Precision* und *Recall* ab:

Präzision

Die Wahrscheinlichkeit, dass das, was Cloud Compliance findet, korrekt identifiziert wurde. Beispielsweise bedeutet eine Datengenauigkeit von 90% für personenbezogene Daten, dass 9 von 10 Dateien, die als personenbezogene Daten identifiziert werden, tatsächlich personenbezogene Daten enthalten. 1 von 10 Dateien wäre falsch positiv.

Rückruf

Die Wahrscheinlichkeit, dass Cloud Compliance die entsprechenden Daten findet. Beispielsweise bedeutet eine Rückrufquote von 70 % für personenbezogene Daten, dass Cloud Compliance 7 von 10 Dateien

identifizieren kann, die tatsächlich personenbezogene Daten in Ihrem Unternehmen enthalten. Cloud Compliance würde 30% der Daten vermissen und wird nicht im Dashboard erscheinen.

Cloud Compliance gibt es in einer Version mit kontrollierter Verfügbarkeit und wir verbessern kontinuierlich die Genauigkeit unserer Ergebnisse. Diese Verbesserungen werden in zukünftigen Versionen der Cloud-Compliance automatisch verfügbar sein.

Typ	Präzision	Rückruf
Personenbezogene Daten - Allgemeines	90 % - 95 %	60 % - 80 %
Persönliche Daten – Länderkennungen	30 % - 60 %	40 % - 60 %
Sensible persönliche Daten	80 % - 95 %	20 % - 30 %
Kategorien	90 % - 97 %	60 % - 80 %

Was ist in jedem Datei Liste Bericht enthalten (CSV-Datei)

Auf jeder Untersuchungsseite können Sie Dateilisten (im CSV-Format) mit Details zu den identifizierten Dateien herunterladen. Wenn es mehr als 10,000 Ergebnisse gibt, werden nur die Top 10,000 in der Liste angezeigt.

Jede Dateiliste enthält die folgenden Informationen:

- Dateiname
- Positionstyp
- Arbeitsumgebung
- Storage Repository
- Protokoll
- Dateipfad
- Dateityp
- Kategorie
- Persönliche Angaben
- Sensible persönliche Daten
- Löscherkennung Datum

Ein Löscherkennungsdatum gibt das Datum an, an dem die Datei gelöscht oder verschoben wurde. So können Sie feststellen, wann sensible Dateien verschoben wurden. Gelöschte Dateien sind nicht Teil der Anzahl der Dateinummern, die im Dashboard oder auf der Untersuchungsseite angezeigt wird. Die Dateien werden nur in den CSV-Berichten angezeigt.

Anzeigen von Compliance-Berichten

Cloud Compliance stellt Berichte bereit, anhand deren Sie den Status des Datenschutzprogramms Ihres Unternehmens besser verstehen können.

Standardmäßig werden auf dem Cloud Compliance-Dashboard Compliance-Daten für alle Arbeitsumgebungen und Datenbanken angezeigt. Wenn Sie Berichte anzeigen möchten, die Daten nur für einige Arbeitsumgebungen enthalten, [Wählen Sie diese Arbeitsumgebungen aus](#).



NetApp kann keine Garantie für 100 % Genauigkeit der persönlichen Daten und für sensible personenbezogene Daten, die Cloud Compliance identifiziert hat, geben. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Datenschutzrisiko-Assessment-Bericht

Der Datenschutzrisiko-Assessment-Bericht bietet einen Überblick über den Datenschutzrisikostatus Ihres Unternehmens, wie dies durch Datenschutzvorschriften wie DSGVO und CCPA erforderlich ist. Der Bericht enthält die folgenden Informationen:

Compliance-Status

A **Schweregrad** Und die Verteilung von Daten, ganz gleich, ob es sich um unempfindliche, personenbezogene oder sensible Daten handelt.

Assessment-Übersicht

Eine Aufschlüsselung der gefundenen Arten von personenbezogenen Daten sowie der Kategorien von Daten.

Betroffene in dieser Beurteilung

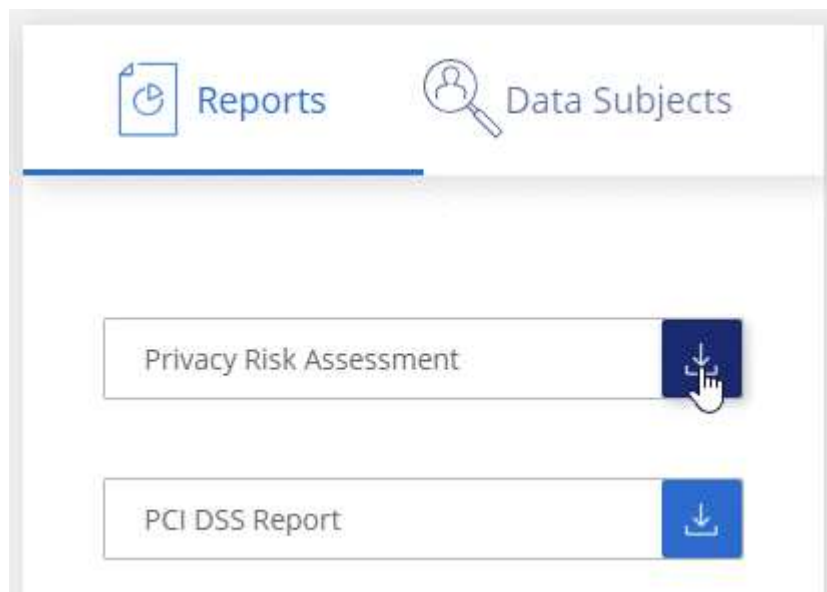
Die Anzahl der Personen, nach Ort, für die nationale Kennungen gefunden wurden.

Generieren des Datenschutzrisikobewertungsberichts

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie unter **Reports** auf das Download-Symbol neben **Privacy Risk Assessment**.



Ergebnis

Cloud Compliance generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Schweregrad

Cloud Compliance berechnet den Schweregrad für den Privacy Risk Assessment-Bericht auf der Grundlage von drei Variablen:

- Der Prozentsatz der personenbezogenen Daten aus allen Daten.
- Der Prozentsatz sensibler personenbezogener Daten aus allen Daten.
- Der Prozentsatz der Dateien, die betroffene Daten enthalten, die durch nationale Kennungen wie nationale IDs, Sozialversicherungsnummern und Steuerkennzahlen bestimmt werden.

Die folgende Logik dient zur Ermittlung der Punktzahl:

Schweregrad	Logik
0	Alle drei Variablen sind genau 0%
1	Eine der Variablen ist größer als 0 %
2	Eine der Variablen ist größer als 3%
3	Zwei der Variablen sind größer als 3%
4	Drei der Variablen sind größer als 3 %
5	Eine der Variablen ist größer als 6%
6	Zwei der Variablen sind größer als 6%
7	Drei der Variablen sind größer als 6 %
8	Eine der Variablen ist größer als 15%
9	Zwei der Variablen sind größer als 15%
10	Drei der Variablen sind größer als 15 %

PCI DSS-Bericht

Der PCI DSS-Bericht (Payment Card Industry Data Security Standard) hilft Ihnen bei der Identifizierung der Verteilung von Kreditkarteninformationen über Ihre Dateien hinweg. Der Bericht enthält die folgenden Informationen:

Überblick

Wie viele Dateien enthalten Kreditkarteninformationen und in welchen Arbeitsumgebungen.

Verschlüsselung

Der Prozentsatz der Dateien, die Kreditkartendaten in verschlüsselten oder nicht verschlüsselten Arbeitsumgebungen enthalten. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Schutz Vor Ransomware

Der Prozentsatz von Dateien mit Kreditkarteninformationen, die in Arbeitsumgebungen gespeichert sind, für die der Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Aufbewahrung

Der Zeitrahmen, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, weil Sie Ihre Kreditkartendaten nicht länger aufbewahren sollten, als Sie sie bearbeiten müssen.

Verteilung der Kreditkarteninformationen

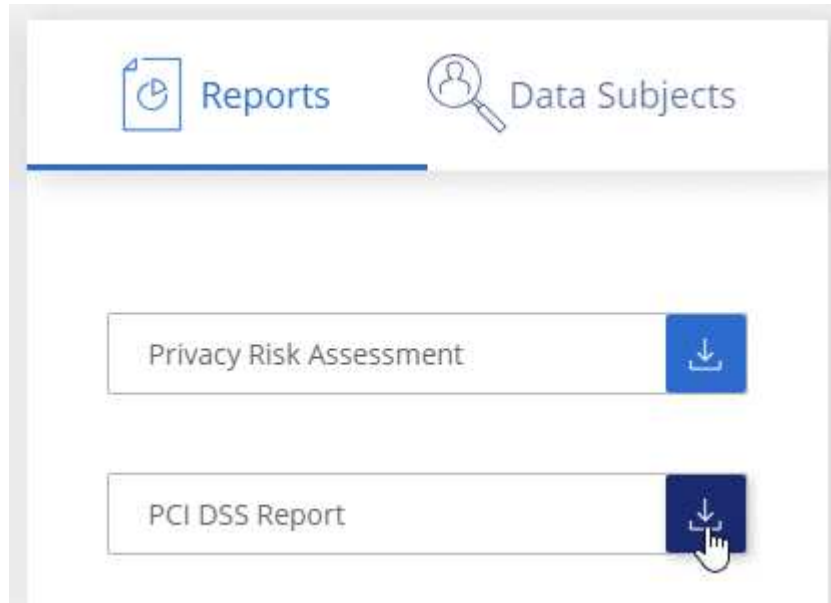
Die Arbeitsumgebungen, in denen Kreditkartendaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

PCI DSS-Bericht wird erstellt

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie unter **Reports** auf das Download-Symbol neben **PCI DSS Report**.



Ergebnis

Cloud Compliance generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

HIPAA-Bericht

Der HIPAA-Bericht (Health Insurance Portability and Accountability Act) hilft Ihnen bei der Identifizierung von Dateien, die Gesundheitsdaten enthalten. Es wurde entwickelt, um die Anforderung Ihres Unternehmens zu unterstützen, die HIPAA-Datenschutzgesetze einzuhalten. Die von Cloud Compliance gesucht werden, umfasst:

- Zustandsreferenzmuster
- ICD-10 CM medizinischer Code
- ICD-9 CM medizinischer Code
- HR – Kategorie Gesundheit
- Datenkategorie für Gesundheitsanwendungen

Der Bericht enthält die folgenden Informationen:

Überblick

Wie viele Dateien enthalten Gesundheitsinformationen und in welchen Arbeitsumgebungen.

Verschlüsselung

Der Prozentsatz der Dateien, die Gesundheitsinformationen in verschlüsselten oder nicht verschlüsselten Arbeitsumgebungen enthalten. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Schutz Vor Ransomware

Der Prozentsatz von Dateien mit Gesundheitsinformationen in Arbeitsumgebungen, in denen Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Aufbewahrung

Der Zeitrahmen, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, weil Sie Gesundheitsinformationen nicht länger aufbewahren sollten, als Sie sie verarbeiten müssen.

Verteilung von Gesundheitsinformationen

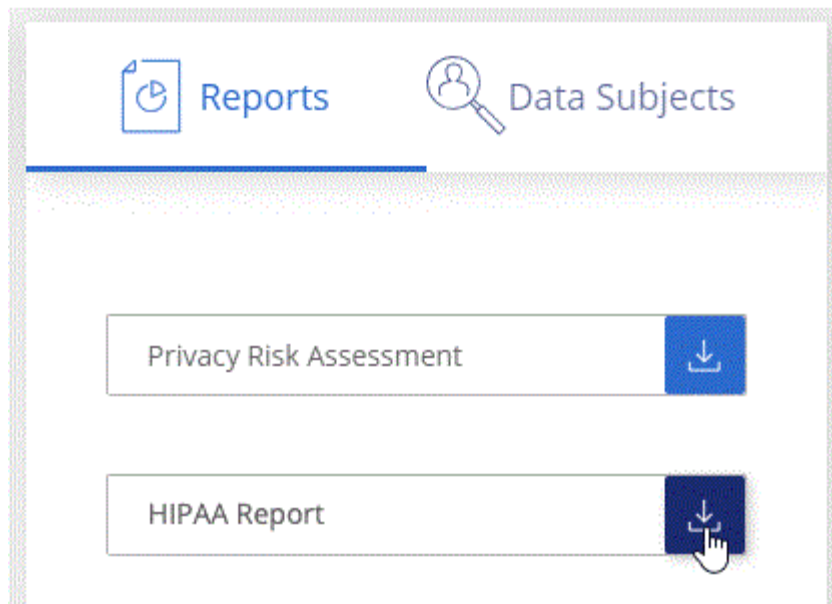
In den Arbeitsumgebungen, in denen die Gesundheitsdaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

HIPAA-Bericht wird erstellt

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie unter **Reports** auf das Download-Symbol neben **HIPAA Report**.



Ergebnis

Cloud Compliance generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Auswählen der Arbeitsumgebungen für Berichte

Sie können die Inhalte des Cloud Compliance Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur für bestimmte Arbeitsumgebungen anzuzeigen.

Wenn Sie das Dashboard filtern, wird durch Cloud Compliance die Compliance-Daten und -Berichte genau den von Ihnen ausgewählten Arbeitsumgebungen beschrieben.

Schritte

1. Klicken Sie auf das Dropdown-Menü Filter, wählen Sie die Arbeitsumgebungen aus, für die Sie Daten anzeigen möchten, und klicken Sie auf **Ansicht**.

The screenshot shows the 'Cloud Compliance' dashboard. A filter menu is open, displaying 'All Working Environments (12)'. The menu includes a 'Select all' option and a list of environments: 'ANF - Azure NetApp Files', 'Working Environment Name 1', 'Working Environment Name 2', 'Working Environment Name 3', and 'Working Environment Name 4'. Each environment has a checkbox and a small button with its identifier (ANF, CVO, CVS, CVS, CVO). At the bottom of the menu are 'View' and 'Cancel' buttons. The main dashboard area shows summary statistics: '20% Personal' and '5% Sensitive Personal' with corresponding progress bars. Below this, there are two sections: 'Personal Files' (7,000 total) and 'Sensitive Personal Files' (7,000 total). Each section has a 'View All' button and a list of categories with file counts and progress bars: 'Email Address' (2,700 Files), 'Credit Card' (2,700 Files), 'Health' (2,700 Files), and 'Ethnicity' (2,700 Files).

Reaktion auf eine Zugriffsanfrage für betroffene Person

Reagieren Sie auf eine DSAR (Data Subject Access Request), indem Sie nach dem vollständigen Namen oder der bekannten Kennung (z. B. einer E-Mail-Adresse) eines Studienteilnehmers suchen und dann einen Bericht herunterladen. Der Bericht soll Ihrem

Unternehmen helfen, die Vorgaben der DSGVO oder ähnlicher Datenschutzgesetze einzuhalten.



NetApp kann keine Garantie für 100 % Genauigkeit der persönlichen Daten und für sensible personenbezogene Daten, die Cloud Compliance identifiziert hat, geben. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Was ist ein Antrag auf Zugang für betroffene Person?

Datenschutzvorschriften wie die Europäische DSGVO erteilen Betroffenen (wie Kunden oder Mitarbeitern) das Recht, auf ihre personenbezogenen Daten zuzugreifen. Wenn eine betroffene Person diese Informationen anfordert, wird dies als DSAR (Zugriffsanfrage für betroffene Person) bezeichnet. Unternehmen sind verpflichtet, auf diese Anfragen „ohne unzumutbare Verzögerung“ und spätestens innerhalb eines Monats nach Eingang zu reagieren.

Wie kann Cloud Compliance Ihnen helfen, auf einen DSAR zu reagieren?

Wenn Sie eine Suche des Betroffenen durchführen, findet Cloud Compliance alle Dateien, die den Namen oder die Kennung der betreffenden Person enthalten. Cloud Compliance prüft die neuesten vorindizierten Daten auf den Namen oder die Kennung. Es wird kein neuer Scan gestartet.

Nachdem die Suche abgeschlossen ist, können Sie die Liste der Dateien für einen Bericht für die Anforderung von Datensubjekten herunterladen. Der Bericht sammelt Erkenntnisse aus den Daten und stellt die Daten zu rechtlichen Bedingungen bereit, die Sie an die Person zurücksenden können.

Suchen nach Betroffenen und Herunterladen von Berichten

Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen, und laden Sie dann einen Dateilistenbericht oder einen DSAR-Bericht herunter. Suchen Sie nach "[Alle persönlichen Informationstypen](#)".

Nur Englisch wird bei der Suche nach den Namen von Betroffenen unterstützt. Support für weitere Sprachen wird später hinzugefügt.

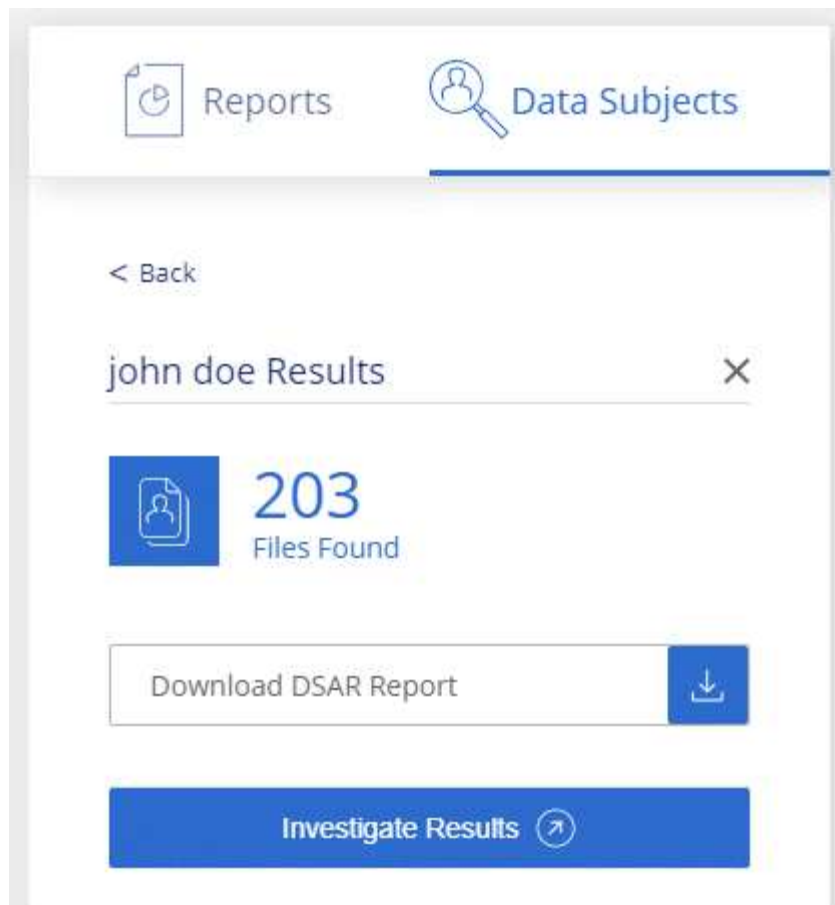


Die Suche nach Betroffenen wird derzeit in Datenbanken nicht unterstützt.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie Auf **Data Subjects**.
3. Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen.

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



4. Wählen Sie eine der folgenden Optionen:

- **Download DSAR Report:** Eine formelle Antwort auf die Zugriffsanfrage, die Sie an den Betroffenen senden können. Dieser Bericht enthält automatisch generierte Informationen auf der Grundlage von Daten, die Cloud Compliance dem Betroffenen zur Verfügung stellte und für die Nutzung als Vorlage konzipiert wurde. Füllen Sie das Formular aus und überprüfen Sie es intern, bevor Sie es an den Betroffenen senden.
- **Ergebnisse untersuchen:** Eine Seite, auf der Sie die Daten untersuchen können, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern und die Dateiliste herunterladen.



Wenn es mehr als 10,000 Ergebnisse gibt, werden nur die Top 10,000 in der Dateiliste angezeigt.

Deaktivieren Von Cloud Compliance


Wenn Sie benötigen, können Sie verhindern, dass Cloud Compliance eine oder mehrere Arbeitsumgebungen oder Datenbanken scannt. Sie können auch die Cloud Compliance-Instanz löschen, wenn Sie Cloud Compliance nicht mehr in Ihrer Arbeitsumgebung verwenden möchten.

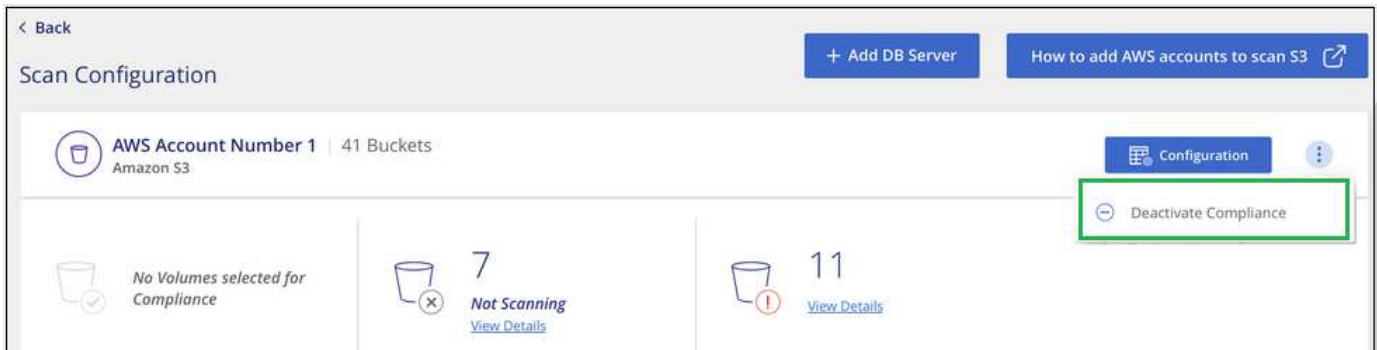
Deaktivieren von Compliance-Scans für eine Arbeitsumgebung

Wenn Sie Scans deaktivieren, scannt Cloud Compliance die Daten auf dem System nicht mehr und entfernt alle indizierten Compliance-Einblicke aus der Cloud Compliance Instanz (die Daten aus der Arbeitsumgebung

oder der Datenbank selbst werden nicht gelöscht).

Schritte

Klicken Sie auf der Seite *Scan Configuration* auf  Klicken Sie in der Zeile für die Arbeitsumgebung auf **Compliance deaktivieren**.



Sie können bei der Auswahl der Arbeitsumgebung auch die Compliance-Scans für eine Arbeitsumgebung im Fenster „Services“ deaktivieren.

Löschen der Cloud-Compliance-Instanz

Sie können die Cloud Compliance-Instanz löschen, wenn Sie Cloud Compliance nicht mehr verwenden möchten. Durch das Löschen der Instanz werden auch die zugehörigen Festplatten gelöscht, auf denen sich die indizierten Daten befinden.

Schritt

1. Gehen Sie zur Konsole Ihres Cloud-Providers und löschen Sie die Instanz für Cloud Compliance.

Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Häufig gestellte Fragen zur Cloud Compliance

Diese FAQ kann Ihnen helfen, wenn Sie nur eine schnelle Antwort auf eine Frage suchen.

Was ist Cloud Compliance?

Cloud Compliance ist ein Cloud-Angebot, das künstliche Intelligenz (KI) nutzt, um Unternehmen dabei zu unterstützen, den Datenkontext zu verstehen und sensible Daten in ihren Azure NetApp Files Konfigurationen zu identifizieren, Cloud Volumes ONTAP-Systeme in AWS oder Azure, Amazon S3 Buckets und Datenbanken zu hosten.

Cloud Compliance bietet vordefinierte Parameter (wie z. B. sensible Informationstypen und Kategorien), um neue Compliance-Anforderungen für Datenschutz und -Sensibilität wie DSGVO, CCPA, HIPAA usw. zu erfüllen.

Warum sollte ich Cloud-Compliance verwenden?

Cloud Compliance bietet Ihnen mehr Möglichkeiten für die Nutzung von Daten:

- Einhaltung von Daten-Compliance- und Datenschutzvorschriften
- Einhaltung von Richtlinien zur Datenaufbewahrung.
- Das Auffinden und Reporting von Daten zu bestimmten Daten als Antwort auf Betroffene kann ganz nach Bedarf auf DSGVO, CCPA, HIPAA und anderen Datenschutzvorschriften erfolgen.

Was sind die gängigsten Anwendungsfälle für Cloud Compliance?

- Ermitteln von personenbezogenen Daten
- Identifizieren Sie einen breiten Umfang sensibler Daten, wie sie im Sinne der DSGVO- und CCPA-Datenschutzvorschriften erforderlich sind.
- Einhaltung neuer und anstehender Datenschutzvorschriften

["Erfahren Sie mehr über die Anwendungsfälle für Cloud Compliance"](#).

Welche Datentypen können mit Cloud Compliance gescannt werden?

Cloud Compliance unterstützt die Überprüfung unstrukturierter Daten über die von Cloud Volumes ONTAP und Azure NetApp Files gemanagten NFS- und CIFS-Protokolle. Cloud Compliance kann auch Daten scannen, die in Amazon S3 Buckets gespeichert sind.

Außerdem können mit Cloud Compliance Datenbanken gescannt werden, die sich an einem beliebigen Ort befinden - sie müssen nicht von Cloud Manager gemanagt werden.

["Lesen Sie, wie Scans funktionieren"](#).

Welche Cloud-Provider werden unterstützt?

Cloud Compliance arbeitet als Teil von Cloud Manager und unterstützt derzeit AWS und Azure. Dadurch erhält Ihr Unternehmen Transparenz im Hinblick auf den Datenschutz bei verschiedenen Cloud-Providern. Demnächst wird auch Support für die Google Cloud Platform (GCP) verfügbar sein.

Wie erhalte ich Zugriff auf Cloud Compliance?

Cloud Compliance wird über Cloud Manager betrieben und gemanagt. Sie können Cloud Compliance-Funktionen über die Registerkarte **Compliance** in Cloud Manager aufrufen.

Wie funktioniert Cloud Compliance?

Cloud Compliance implementiert gemeinsam mit Ihrem Cloud Manager System und Ihren Storage-Systemen eine weitere Schicht künstlicher Intelligenz. Anschließend werden die Daten auf Volumes, Buckets und Datenbanken überprüft und die gefundenen Dateneinblicke indiziert.

["Funktionsweise von Cloud Compliance"](#).

Wie viel kostet Cloud Compliance?

Die Kosten für die Verwendung von Cloud Compliance hängen von der Datenmenge ab, die Sie scannen. Es sind die ersten 1 TB an Daten, die Cloud Compliance in einem Cloud Manager Workspace scannt, kostenlos.

Danach ist ein Abonnement für AWS oder Azure Marketplace erforderlich, um mit dem Scannen der Daten fortzufahren. Siehe ["Preisgestaltung"](#) Entsprechende Details.

Wie oft scannt Cloud Compliance meine Daten?

Da sich die Daten häufig ändern, scannt Cloud Compliance Ihre Daten kontinuierlich, ohne Auswirkungen auf Ihre Daten. Während der erste Scan Ihrer Daten länger dauern kann, scannen nachfolgende Scans nur die inkrementellen Änderungen, was die Dauer des Systemscans verkürzt.

["Lesen Sie, wie Scans funktionieren"](#).

Bietet Cloud Compliance Berichte an?

Ja. Die von Cloud Compliance angebotenen Informationen können für andere Beteiligte in Ihrem Unternehmen relevant sein. So können Sie Berichte erstellen und Einblicke erhalten.

Für Cloud Compliance stehen folgende Berichte zur Verfügung:

Datenschutzrisiko-Assessment-Bericht

Bietet Einblicke in den Datenschutz und eine Bewertung des Datenschutzrisikos. ["Weitere Informationen ."](#)

Bericht für Anforderung von Datenfachzugriff

Ermöglicht Ihnen, einen Bericht aller Dateien zu extrahieren, die Informationen über den spezifischen Namen oder die persönliche Kennung eines Betroffenen enthalten. ["Weitere Informationen ."](#)

PCI DSS-Bericht

Unterstützt Sie bei der Identifizierung der Verteilung von Kreditkarteninformationen über Ihre Dateien. ["Weitere Informationen ."](#)

HIPAA-Bericht

Hilft Ihnen dabei, die Verteilung von Gesundheitsinformationen über Ihre Dateien hinweg zu identifizieren. ["Weitere Informationen ."](#)

Berichte zu einem bestimmten Informationstyp

Es stehen Berichte zur Verfügung, die Details zu den identifizierten Dateien enthalten, die personenbezogene Daten und sensible personenbezogene Daten enthalten. Sie können auch Dateien nach Kategorie und Dateityp aufgeschlüsselt sehen. ["Weitere Informationen ."](#)

Welcher Instanztyp oder VM ist für Cloud Compliance erforderlich?

- In Azure wird Cloud Compliance auf einer VM mit Standard_D16s_v3 mit einer Festplatte von 512 GB ausgeführt.
- In AWS wird Cloud-Compliance auf einer m5.4xlarge-Instanz mit einer 500-GB-GP2-Festplatte ausgeführt.

In Regionen, in denen m5.4xlarge nicht verfügbar ist, wird Cloud Compliance stattdessen auf einer m4.4xlarge-Instanz ausgeführt.



Das Ändern oder Ändern der Größe des Instanz-/VM-Typs wird nicht unterstützt. Es muss die angegebene Standardgröße verwendet werden.

["Funktionsweise von Cloud Compliance"](#).

Ist die Scanleistung unterschiedlich?

Die Scan-Performance kann je nach Netzwerkbandbreite und durchschnittlicher Dateigröße in der Cloud-Umgebung variieren.

Welche Dateitypen werden unterstützt?

Cloud Compliance scannt alle Dateien nach Informationen zu Kategorien und Metadaten und zeigt alle Dateitypen im Abschnitt Dateitypen im Dashboard an.

Wenn Cloud Compliance personenbezogene Daten (PII) erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF UND .JSON.

Wie kann ich Cloud-Compliance aktivieren?

Zunächst müssen Sie eine Instanz von Cloud Compliance in Cloud Manager implementieren. Sobald die Instanz ausgeführt wurde, können Sie sie auf bestehenden Arbeitsumgebungen und Datenbanken über die Registerkarte **Compliance** oder durch Auswahl einer bestimmten Arbeitsumgebung aktivieren.

["Erste Schritte"](#).



Durch die Aktivierung von Cloud Compliance wird ein sofortiger anfänglicher Scan durchgeführt. Ergebnisse der Compliance werden kurz danach angezeigt.

Wie deaktiviere ich Cloud Compliance?

Sie können Cloud-Compliance auf der Seite Arbeitsumgebung deaktivieren, nachdem Sie eine individuelle Arbeitsumgebung ausgewählt haben.

["Weitere Informationen ."](#)



Wenn Sie die Cloud Compliance-Instanz vollständig entfernen möchten, können Sie die Cloud Compliance-Instanz manuell aus dem Portal Ihres Cloud-Providers entfernen.

Was geschieht, wenn das Daten-Tiering auf Cloud Volumes ONTAP aktiviert ist?

Es ist sinnvoll, Cloud-Compliance auf einem Cloud Volumes ONTAP System zu aktivieren, das kalte Daten auf Objekt-Storage absichert. Wenn das Daten-Tiering aktiviert ist, scannt Cloud Compliance alle Daten auf Festplatten, die sich auf kalten Daten befinden, die in Objekt-Storage verschoben werden.

Der Compliance-Scan erhitzt die nicht kalten Daten – es bleibt kalt und führt zu Objekt-Storage.

Kann ich Cloud Compliance verwenden, um den lokalen ONTAP Storage zu scannen?

Das Scannen der Daten direkt aus einer lokalen ONTAP-Arbeitsumgebung wird nicht unterstützt. Sie können Ihre lokalen ONTAP-Daten jedoch scannen, indem Sie die On-Premises-NFS- oder CIFS-Daten in eine Cloud Volumes ONTAP Arbeitsumgebung replizieren und anschließend die Compliance für diese Volumes aktivieren. Wir planen, Cloud Compliance durch zusätzliche Cloud-Angebote wie Cloud Volumes Service zu unterstützen.

["Weitere Informationen ."](#)

Kann Cloud Compliance Benachrichtigungen an mein Unternehmen senden?

Nein, aber Sie können Statusberichte herunterladen, die Sie intern in Ihrem Unternehmen teilen können.

Kann ich den Service an die Bedürfnisse meiner Organisation anpassen?

Cloud Compliance bietet sofortige Einblicke in Ihre Daten. Diese Erkenntnisse können extrahiert und für die Bedürfnisse Ihres Unternehmens verwendet werden.

Kann ich die Daten zur Cloud Compliance auf bestimmte Benutzer begrenzen?

Ja, Cloud Compliance ist vollständig in Cloud Manager integriert. Cloud Manager-Benutzer können nur Informationen für die Arbeitsumgebungen anzeigen, die sie entsprechend ihren Arbeitsbereichsberechtigungen anzeigen können.

Wenn Sie bestimmten Benutzern die Möglichkeit geben möchten, die Ergebnisse des Cloud-Compliance-Scans einfach anzuzeigen, ohne Cloud-Compliance-Einstellungen verwalten zu können, können Sie diesen Benutzern die Rolle „*Cloud Compliance Viewer*“ zuweisen.

["Weitere Informationen ."](#)

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.