



Los geht's

Cloud Data Sense

NetApp
January 09, 2023

Inhaltsverzeichnis

- Los geht's 1
 - Cloud Data Sense nutzen 1
 - Sinnvolle Implementierung Von Cloud-Daten 8
 - Aktivieren Sie das Scannen Ihrer Datenquellen..... 41
 - Integrieren Sie Active Directory in Cloud Data Sense 87
 - Lizenzierung für Cloud Data Sense einrichten..... 90
 - Häufig gestellte Fragen zu Cloud Data Sense..... 96

Los geht's

Cloud Data Sense nutzen

Cloud Data Sense ist ein Data Governance Service für BlueXP (früher Cloud Manager), der On-Premises- und Cloud-Datenquellen Ihres Unternehmens scannt, um Daten zuzuordnen und zu klassifizieren, und private Informationen zu identifizieren. Auf diese Weise reduzieren Sie Sicherheits- und Compliance-Risiken, senken die Storage-Kosten und unterstützen Ihre Datenmigrationsprojekte.

["Hier lernen Sie die Anwendungsfälle für Cloud-Datensinnvoll kennen".](#)

Funktionen

Cloud Data Sense verwendet künstliche Intelligenz (KI), NLP (Natural Language Processing) und Machine Learning (ML), um die von ihm gescannten Inhalte zu verstehen, um Entitäten zu extrahieren und den Inhalt entsprechend zu kategorisieren. Dadurch kann Data Sense folgende Funktionsbereiche bereitstellen.

Einhaltung von Compliance-Vorschriften

Data Sense bietet verschiedene Tools, die Sie bei Ihren Compliance-Bemühungen unterstützen können. Mit Data Sense können Sie:

- Ermitteln von personenbezogenen Daten
- Vielzahl sensibler personenbezogener Daten gemäß den Datenschutzvorschriften des DSGVO, CCPA, PCI und HIPAA ermitteln.
- Reagieren Sie auf Data Subject Access Requests (DSAR) basierend auf Name oder E-Mail-Adresse.
- Identifizieren Sie, ob eindeutige Kennungen aus Ihren Datenbanken in Dateien in anderen Repositories gefunden werden - stellen Sie im Grunde Ihre eigene Liste von „persönlichen Daten“ her, die in Daten-Sense-Scans identifiziert werden.
- Bestimmte Benutzer per E-Mail benachrichtigen, wenn Dateien bestimmte PII enthalten (Sie definieren diese Kriterien mit ["Richtlinien"](#)) So können Sie über einen Aktionsplan entscheiden.

Erhöhte Sicherheit

Der Datensinn kann Daten identifizieren, die potenziell gefährdet sind, wenn sie für kriminelle Zwecke genutzt werden. Mit Data Sense können Sie:

- Ermitteln Sie alle Dateien und Verzeichnisse (Shares und Ordner) mit offenen Berechtigungen, die Ihrem gesamten Unternehmen oder der Öffentlichkeit zugänglich sind.
- Identifizieren Sie sensible Daten, die sich außerhalb des ursprünglichen dedizierten Standorts befinden.
- Einhaltung von Richtlinien zur Datenaufbewahrung.
- Verwenden Sie *Policies*, um das Sicherheitspersonal automatisch über neue Sicherheitsprobleme zu informieren, damit sie sofort reagieren können.
- Fügen Sie benutzerdefinierte Tags zu Dateien hinzu (z. B. „muss verschoben werden“) und weisen Sie einen BlueXP-Benutzer zu, damit diese Person Updates für die Dateien besitzen kann.
- Anzeigen und ändern Sie ["Azure Information Protection \(AIP\)-Etiketten"](#) In Ihren Dateien.

Optimieren Sie die Storage-Auslastung

Data Sense bietet Tools, die Sie bei den Storage-Gesamtbetriebskosten (TCO) unterstützen. Mit Data Sense können Sie:

- Erhöhte Storage-Effizienz durch Identifizierung doppelter oder nicht geschäftlicher Daten. Mit diesen Informationen können Sie entscheiden, ob Sie bestimmte Dateien verschieben oder löschen möchten.
- Löschen Sie Dateien, die unsicher oder zu riskant erscheinen, um in Ihrem Speichersystem zu belassen, oder die Sie als Duplikat identifiziert haben. Mit *Policies* können Dateien, die bestimmten Kriterien entsprechen, automatisch gelöscht werden.
- Sparen Sie Storage-Kosten, indem Sie inaktive Daten ermitteln, die auf kostengünstigeren Objektspeicher verschoben werden können. ["Weitere Informationen zum Tiering von Cloud Volumes ONTAP Systemen"](#). ["Weitere Informationen zum Tiering von lokalen ONTAP Systemen"](#).

Beschleunigte Datenmigration

Mit Daten Sense können Sie Ihre On-Premises-Daten scannen, bevor Sie sie in die Public oder Private Cloud migrieren. Mit Data Sense können Sie:

- Zeigen Sie die Größe der Daten an und ob die Daten vertrauliche Informationen enthalten, bevor Sie sie verschieben.
- Filtern Sie die Quelldaten (basierend auf über 25 Kriterientypen), damit Sie nur die erforderlichen Dateien in das Ziel verschieben können - unnötige Daten werden nicht verschoben.
- Automatisches und unterbrechungsfreies Verschieben, Kopieren oder Synchronisieren nur der erforderlichen Daten in das Cloud-Repository

Unterstützte Datenquellen

Cloud Data Sense kann strukturierte und unstrukturierte Daten aus folgenden Datenquellen scannen und analysieren:

NetApp:

- Cloud Volumes ONTAP (implementiert in AWS, Azure oder GCP)
- On-Premises ONTAP Cluster
- StorageGRID
- Azure NetApp Dateien
- Amazon FSX für ONTAP
- Cloud Volumes Service für Google Cloud
- Kein NetApp:*
- Dell EMC Isilon
- Pure Storage
- Nutanix
- Alle anderen Storage-Anbieter

Wolke:

- Amazon S3

- Azure Blob
- Google Cloud Storage
- OneDrive
- SharePoint Online
- SharePoint On-Premises (SharePoint Server)
- Google Drive

Datenbanken:

- Amazon Relational Database Service (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

Data Sense unterstützt NFS-Versionen 3.x, 4.0 und 4.1 sowie CIFS Versionen 1.x, 2.0, 2.1 und 3.0.

Kosten

- Die Kosten für die Verwendung von Cloud Data Sense hängen von der Datenmenge ab, die Sie scannen. Die ersten 1 TB an Daten, die Data Sense in einem BlueXP-Arbeitsbereich scannt, sind kostenlos. Dies umfasst alle Daten aus allen Arbeitsumgebungen und Datenquellen. Um mit dem Scannen von Daten nach diesem Zeitpunkt fortzufahren, müssen Sie auf AWS, Azure oder GCP Marketplace oder eine BYOL-Lizenz von NetApp abonnieren. Siehe "[Preisgestaltung](#)" Entsprechende Details.

["Lernen Sie, Cloud Data Sense zu lizenzieren"](#).

- Für die Installation von Cloud Data Sense in der Cloud ist die Implementierung einer Cloud-Instanz erforderlich, was beim Cloud-Provider zu Gebühren führt, wo sie implementiert wird. Siehe [Der für jeden Cloud-Provider implementierte Instanztyp](#). Wenn Sie Daten Sense in einem lokalen System installieren, entstehen Ihnen keine Kosten.
- Für Cloud Data Sense ist die Implementierung eines BlueXP Connectors erforderlich. In vielen Fällen haben Sie bereits einen Connector, weil Sie andere Speicher und Dienste in BlueXP verwenden. Die Connector-Instanz verursacht Gebühren bei dem Cloud-Provider, wo sie implementiert wird. Siehe ["Für jeden Cloud-Provider implementierte Instanztyp"](#). Bei der Installation des Connectors in einem On-Premises-System entstehen keine Kosten.

Datentransferkosten

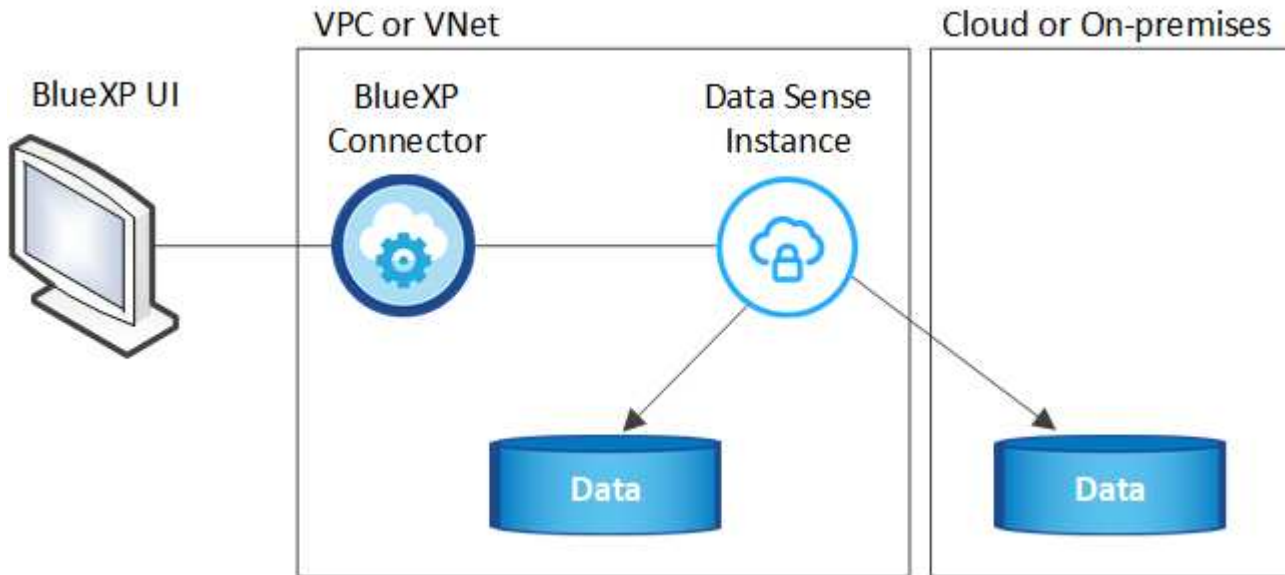
Die Datentransferkosten hängen von Ihrer Einrichtung ab. Wenn sich die Instanz und Datenquelle Cloud Data Sense in derselben Verfügbarkeitszone und Region befinden, entstehen keine Datentransferkosten. Wenn sich die Datenquelle, beispielsweise ein Cloud Volumes ONTAP-System oder S3-Bucket, jedoch in 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"](#)
- ["Google Cloud: Preis für Storage Transfer Service"](#)

Die Instanz Cloud Data Sense

Wenn Sie Data Sense in der Cloud implementieren, stellt BlueXP die Instanz im selben Subnetz wie der Connector bereit. ["Erfahren Sie mehr über Steckverbinder."](#)



Beachten Sie Folgendes über die Standardinstanz:

- In AWS läuft Cloud Data Sense auf einer **"M5.4xlarge-Instanz"** mit einer 500-GB-GP2-Festplatte. Das Betriebssystem-Image ist Amazon Linux 2 (Red hat 7.3.1).

In Regionen, in denen m5.4xlarge nicht verfügbar ist, läuft Data Sense stattdessen auf einer m4.4xlarge-Instanz.

- In Azure wird Cloud Data Sense ausgeführt **"Standard_D16s_v3 VM"** mit einer 512-GB-Festplatte. Das Betriebssystem-Image ist CentOS 7.8.
- In GCP wird Cloud Data Sense ausgeführt **"n2-Standard-16-VM"** mit einer persistenten 512-GB-Standardfestplatte. Das Betriebssystem-Image ist CentOS 7.9.

In Regionen, in denen n2-Standard-16 nicht verfügbar ist, wird Data Sense stattdessen auf einer n2d-Standard-16- oder n1-Standard-16-VM ausgeführt.

- 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 Datensense-Instanz bereitgestellt.
- Upgrades der Software Data Sense sind automatisiert, solange die Instanz einen Internetzugang hat.



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

Verwenden eines kleineren Instanztyps

Sie können Data Sense auf einem System mit weniger CPUs und weniger RAM bereitstellen, aber es gibt einige Einschränkungen beim Einsatz dieser weniger leistungsstarken Systeme.

| Systemgröße | Spezifikationen | Einschränkungen |
|-----------------|--------------------------------|---|
| Groß (Standard) | 16 CPUS, 64 GB RAM, 500 GB SSD | Keine |
| Mittel | 8 CPUS, 32 GB RAM, 200 GB SSD | Langsamer Scan und kann nur bis zu 1 Million Dateien scannen. |
| Klein | 8 CPUS, 16 GB RAM, 100 GB SSD | Die gleichen Einschränkungen wie „Mittel“ und die Möglichkeit, sich zu identifizieren " Namen der Betroffenen " Innerhalb von Dateien ist deaktiviert. |

Wenn Sie Data Sense in der Cloud implementieren, senden Sie eine E-Mail an ng-contact-data-sense@netapp.com, um Hilfe zu erhalten, wenn Sie eines dieser kleineren Systeme verwenden möchten. Wir müssen mit Ihnen zusammenarbeiten, um diese kleineren Cloud-Konfigurationen zu implementieren.

Verwenden Sie bei der Implementierung von Data Sense vor Ort einfach einen Linux-Host mit den kleineren Spezifikationen. Sie müssen sich nicht an NetApp wenden, um Unterstützung zu erhalten.

Funktionsweise von Cloud Data Sense

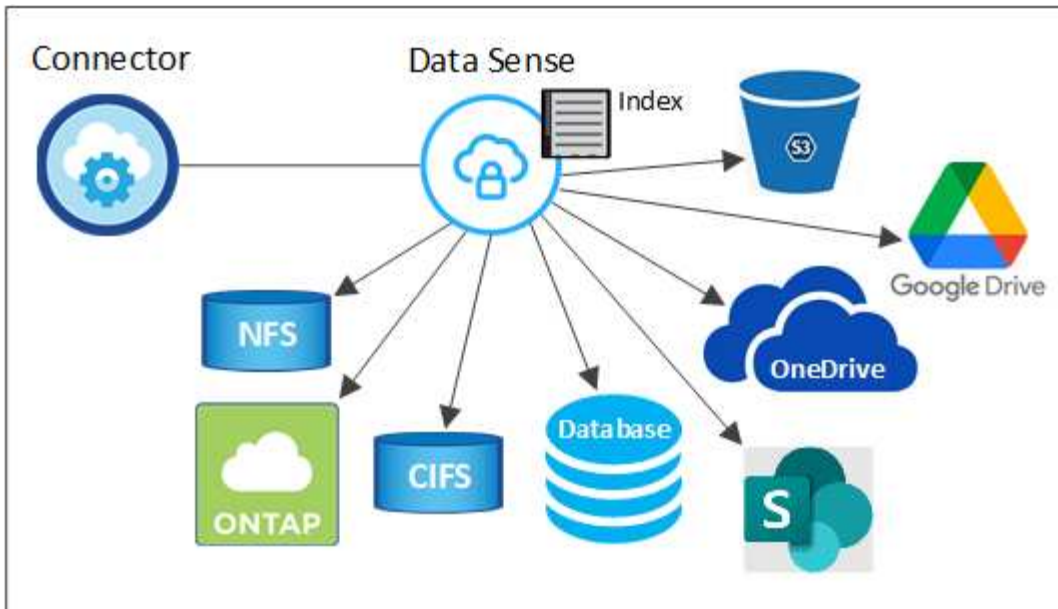
Cloud Data Sense funktioniert auf hoher Ebene wie folgt:

1. Sie stellen eine Instanz von Data Sense in BlueXP bereit.
2. Sie ermöglichen ein hohes Mapping oder tiefes Scannen auf einer oder mehreren Datenquellen.
3. Data Sense scannt die Daten mithilfe eines KI-Lernprozesses.
4. Sie nutzen die bereitgestellten Dashboards und Berichterstellungs-Tools, um Ihre Compliance- und Governance-Bemühungen zu unterstützen.

Funktionsweise von Scans

Nachdem Sie Cloud Data Sense aktiviert und die Volumes, Buckets, Datenbankschemas oder OneDrive oder SharePoint Benutzerdaten 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, Datenkategorien und Dateitypen.

Durch das Mounten von NFS- und CIFS-Volumes stellt der Data Sense 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.



Nach dem ersten Scan scannt Data Sense Ihre Daten kontinuierlich, um inkrementelle Änderungen zu erkennen (deshalb ist es wichtig, die Instanz ausgeführt zu halten).

Sie können Scans auf Volume-Ebene, auf Bucket-Ebene, auf Datenbankschemaebene, auf OneDrive-Benutzerebene und auf SharePoint-Standortebene aktivieren und deaktivieren.

Was ist der Unterschied zwischen Mapping und Classification Scans

Cloud Data Sense ermöglicht es Ihnen, einen allgemeinen Scan mit „Mapping“ für ausgewählte Datenquellen durchzuführen. Das Mapping bietet nur einen Überblick über Ihre Daten auf hoher Ebene, während die Klassifizierung ein tiefes Scannen Ihrer Daten ermöglicht. Das Mapping kann auf Ihren Datenquellen sehr schnell durchgeführt werden, da es nicht auf Dateien zugegriffen wird, um die darin enthaltenen Daten zu sehen.

Viele Benutzer mögen diese Funktionalität, weil sie ihre Daten schnell scannen möchten, um die Datenquellen zu identifizieren, die mehr Forschungsarbeiten benötigen. Sie können dann Scans nur auf die erforderlichen Datenquellen oder Volumes klassifizieren.

In der folgenden Tabelle sind einige Unterschiede aufgeführt:

| Merkmal | Klassifizierung | Zuordnung |
|--|-----------------|-----------|
| Scangeschwindigkeit | Langsam | Schnell |
| Liste der Dateitypen und der genutzten Kapazität | Ja. | Ja. |
| Anzahl der Dateien und genutzte Kapazität | Ja. | Ja. |
| Alter und Größe der Dateien | Ja. | Ja. |
| Fähigkeit, ein auszuführen "Datenzuordnungsbericht" | Ja. | Ja. |
| Datenuntersuchung, um Dateidetails anzuzeigen | Ja. | Nein |
| Suche nach Namen in Dateien | Ja. | Nein |
| Erstellen "Richtlinien" Die benutzerdefinierte Suchergebnisse liefern | Ja. | Nein |

| Merkmal | Klassifizierung | Zuordnung |
|--|-----------------|-----------|
| Kategorisieren Sie Daten mit AIP-Etiketten und Status-Tags | Ja. | Nein |
| Quelldateien kopieren, löschen und verschieben | Ja. | Nein |
| Möglichkeit zur Ausführung anderer Berichte | Ja. | Nein |

Information, die Cloud Data Sense Indizes erstellt

Data Sense erfasst, indiziert und weist Kategorien zu Ihren Daten (Dateien) zu. Die Daten, die Data Sense indiziert werden, umfassen Folgendes:

Standard-Metadaten

Cloud Data Sense erfasst Standard-Metadaten zu Dateien: Dateityp, Größe, Erstellung und Änderung von Daten 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

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

Typen

Cloud Data Sense verwendet die gescannten Daten und werden nach Dateityp unterteilt. "[Erfahren Sie mehr über Typen](#)".

Name der Entität Anerkennung

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

Netzwerkübersicht

BlueXP implementiert die Cloud Data Sense-Instanz mit einer Sicherheitsgruppe, die eingehende HTTP-Verbindungen von der Connector-Instanz ermöglicht.

Bei der Verwendung von BlueXP im SaaS-Modus wird die Verbindung zu BlueXP über HTTPS bedient, und die zwischen Ihrem Browser und der Data Sense Instanz gesendeten privaten Daten sind mit End-to-End-Verschlüsselung gesichert, was bedeutet, dass NetApp und Dritte es nicht lesen können.

Ausgehende Regeln sind vollständig geöffnet. Zur Installation und Aktualisierung der Data Sense Software und zum Senden von Nutzungsmetriken ist Internetzugang erforderlich.

Wenn Sie strenge Netzwerkanforderungen erfüllen, "[Erfahren Sie mehr über die Endpunkte, die Cloud Data Sense-Kontakte haben](#)".

Zugriff des Benutzers auf Compliance-Informationen

Die Rolle, der jedem Benutzer zugewiesen wurde, bietet unterschiedliche Funktionen in BlueXP und in Cloud Data Sense:

- Ein **Account Admin** kann Compliance-Einstellungen verwalten und Compliance-Informationen für alle Arbeitsumgebungen anzeigen.
- Ein **Workspace Admin** kann Compliance-Einstellungen verwalten und Compliance-Informationen nur für Systeme anzeigen, auf die sie Zugriff haben. Wenn ein Workspace-Administrator nicht auf eine Arbeitsumgebung in BlueXP zugreifen kann, werden auf der Registerkarte Data Sense keine Compliance-Informationen für die Arbeitsumgebung angezeigt.
- Benutzer mit der Rolle **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. Diese Benutzer können Dateien auch nicht kopieren, verschieben oder löschen.

["Erfahren Sie mehr über BlueXP-Rollen"](#) Und wie ["Benutzer mit bestimmten Rollen hinzufügen"](#).

Sinnvolle Implementierung Von Cloud-Daten

Cloud-Daten sinnvoll in der Cloud implementieren

Führen Sie einige Schritte durch, um Cloud Data Sense in der Cloud zu implementieren.

Beachten Sie, dass Sie auch können ["Stellen Sie Data Sense auf einem Linux-Host mit Internetzugang bereit"](#). Die Art der Installation ist möglicherweise eine gute Option, wenn Sie lieber On-Premises-ONTAP-Systeme mit einer Data Sense Instanz scannen möchten, die sich auch vor Ort befindet — dies ist jedoch keine Voraussetzung. Die Software funktioniert unabhängig von der gewählten Installationsmethode genau auf die gleiche Weise.

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

Wenn Sie noch keinen Konnektor haben, erstellen Sie jetzt einen Konnektor. Siehe ["Erstellen eines Konnektors in AWS"](#), ["Erstellen eines Connectors in Azure"](#), Oder ["Erstellen eines Konnektors in GCP"](#).

Das können Sie auch ["Stellen Sie den Connector vor Ort bereit"](#) Auf einem Linux-Host in Ihrem Netzwerk oder in der Cloud.

2

Voraussetzungen prüfen

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllen kann. Dazu gehören Outbound-Internetzugang für die Instanz, Konnektivität zwischen Connector und Cloud Data Sense über Port 443 und mehr. [Eine vollständige Liste finden Sie hier](#).

Die Standardkonfiguration benötigt 16 vCPUs für die Cloud Data Sense Instanz. Siehe ["Weitere Details zum Instanztyp"](#).

3

Sinnvolle Implementierung Von Cloud-Daten

Starten Sie den Installationsassistenten, um die Cloud Data Sense Instanz in der Cloud zu implementieren.

4

Abonnieren Sie den Cloud Data Sense Service

Die ersten 1 TB an Daten, die Cloud Data Sense in BlueXP scannt, sind kostenlos. Um die Daten nach diesem Zeitpunkt weiterhin zu scannen, ist ein BlueXP Abonnement über Ihren Cloud-Provider Marketplace oder eine BYOL-Lizenz von NetApp erforderlich.

Einen Konnektor erstellen

Falls Sie noch keinen Connector haben, erstellen Sie bei Ihrem Cloud-Provider einen Connector. Siehe ["Erstellen eines Konnektors in AWS"](#) Oder ["Erstellen eines Connectors in Azure"](#), Oder ["Erstellen eines Konnektors in GCP"](#). In den meisten Fällen werden Sie wahrscheinlich einen Connector eingerichtet haben, bevor Sie versuchen, Cloud Data Sense zu aktivieren, weil die meisten ["Für BlueXP-Funktionen ist ein Connector erforderlich"](#), Aber es gibt Fälle, in denen Sie müssen, um eine Einrichtung jetzt.

Es gibt einige Szenarien, in denen Sie einen Connector verwenden müssen, der bei einem bestimmten Cloud-Provider implementiert wird:

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS, Amazon FSX für ONTAP oder in AWS S3 Buckets wird in AWS ein Connector verwendet.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konnektor in Azure.
 - Bei Azure NetApp Files muss sie in demselben Bereich bereitgestellt werden wie die Volumes, die Sie scannen möchten.
- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP wird ein Connector in GCP verwendet.

On-Prem-ONTAP-Systeme, File Shares anderer Anbieter, generischer S3-Objekt-Storage, Datenbanken, OneDrive-Ordner, SharePoint-Konten und Google Drive-Konten können bei der Verwendung eines dieser Cloud-Connectors gescannt werden.

Beachten Sie, dass Sie auch können ["Stellen Sie den Connector vor Ort bereit"](#) Auf einem Linux-Host in Ihrem Netzwerk oder in der Cloud. Einige Anwender planen, Data Sense On-Prem zu installieren, können auch wählen, den Connector on-Prem zu installieren.

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

Unterstützung für Regierungsregionen

Cloud Data Sense wird unterstützt, wenn der Connector in einer Regierungsregion bereitgestellt wird (AWS GovCloud, Azure Gov oder Azure DoD). Wenn Daten Sense auf diese Weise eingesetzt wird, gelten folgende Einschränkungen:

- OneDrive-Konten, SharePoint-Konten und Google-Laufwerk Konten können nicht gescannt werden.
- Die Funktionalität der Microsoft Azure Information Protection (AIP)-Etiketten kann nicht integriert werden.

Voraussetzungen prüfen

Die folgenden Voraussetzungen prüfen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration

verfügen, bevor Sie Cloud Data Sense in der Cloud implementieren.

Outbound-Internetzugang über Cloud Data Sense aktivieren

Für Cloud Data Sense ist ein Outbound-Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxyserver für den Internetzugriff verwendet, stellen Sie sicher, dass die Datensense-Instanz über Outbound-Internetzugang verfügt, um die folgenden Endpunkte zu kontaktieren. Wenn Daten sinnvoll in der Cloud implementiert werden, befinden sich die Daten im selben Subnetz wie der Connector.

Je nachdem, ob Sie Cloud Data Sense in AWS, Azure oder GCP implementieren, können Sie die unten stehende Tabelle durchlesen.

Erforderliche Endpunkte für AWS Implementierungen:

| Endpunkte | Zweck |
|--|--|
| https://api.blueexp.netapp.com | Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts |
| https://netapp-cloud-account.auth0.com https://auth0.com | Kommunikation mit der BlueXP-Website zur zentralen 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 https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com | Cloud Data Sense kann auf Manifeste und Vorlagen zugreifen und diese herunterladen sowie Protokolle und Kennzahlen senden. |

Erforderliche Endpunkte für Azure- und GCP-Bereitstellungen:

| Endpunkte | Zweck |
|--|---|
| https://api.blueexp.netapp.com | Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts |
| https://netapp-cloud-account.auth0.com https://auth0.com | Kommunikation mit der BlueXP-Website zur zentralen Benutzerauthentifizierung. |
| https://support.compliance.api.blueexp.netapp.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, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden. |

| Endpunkte | Zweck |
|---|---|
| https://support.compliance.api.bluexp.netapp.com/ | Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen. |

Stellen Sie sicher, dass BlueXP über die erforderlichen Berechtigungen verfügt

Stellen Sie sicher, dass BlueXP über die Berechtigungen zum Bereitstellen von Ressourcen verfügt und Sicherheitsgruppen für die Cloud Data Sense Instanz erstellt. Die neuesten BlueXP-Berechtigungen 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 jeweilige Instanzfamilie in der Region, in der BlueXP ausgeführt wird, überprüfen. ["Siehe die erforderlichen Instanztypen"](#).

Weitere Informationen zu vCPU Limits finden Sie in den folgenden Links:

- ["AWS Dokumentation: Amazon EC2 Service Quotas"](#)
- ["Azure Dokumentation: VCPU Kontingente von Virtual Machines"](#)
- ["Google Cloud Dokumentation: Ressourcenkontingente"](#)

Beachten Sie, dass Sie Daten Sense auf einem System mit weniger CPUs und weniger RAM implementieren können, es gibt jedoch Einschränkungen bei der Verwendung dieser Systeme. Siehe ["Verwenden eines kleineren Instanztyps"](#) Entsprechende Details.

Stellen Sie sicher, dass der BlueXP Connector auf Cloud Data Sense zugreifen kann

Stellen Sie die Verbindung zwischen dem Connector und der Cloud Data Sense Instanz sicher. Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über Port 443 zu und aus der Instanz Data Sense zulassen. Diese Verbindung ermöglicht die Bereitstellung der Data Sense-Instanz und ermöglicht die Anzeige von Informationen auf den Registerkarten Compliance und Governance. Cloud Data Sense wird in Regierungsregionen in AWS und Azure unterstützt.

Für AWS und AWS GovCloud Implementierungen sind zusätzliche Regeln für ein- und ausgehende Sicherheitsgruppen erforderlich. Siehe ["Regeln für den Connector in AWS"](#) Entsprechende Details.

Für die Implementierung von Azure und Azure Government sind zusätzliche Regeln für ein- und ausgehende Sicherheitsgruppen erforderlich. Siehe ["Regeln für den Connector in Azure"](#) Entsprechende Details.

Sorgen Sie dafür, dass Cloud Data Sense ausgeführt wird

Die Cloud Data Sense Instanz muss kontinuierlich ausgeführt werden, um Ihre Daten kontinuierlich zu scannen.

Stellen Sie sicher, dass Webbrowser mit Cloud Data Sense verbunden ist

Wenn Cloud Data Sense aktiviert ist, stellen Sie sicher, dass Benutzer von einem Host, der über eine Verbindung zur Data Sense Instanz verfügt, auf die BlueXP-Schnittstelle zugreifen.

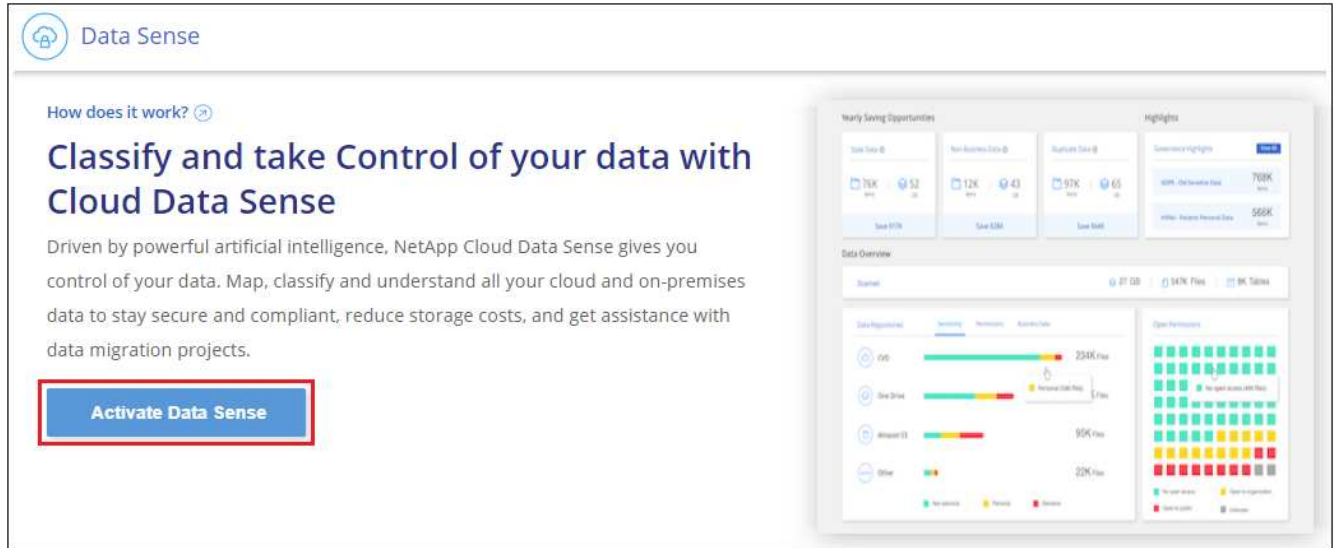
Die Instanz Data Sense verwendet eine private IP-Adresse, um sicherzustellen, dass die indizierten Daten nicht für das Internet verfügbar sind. Daher muss der Webbrowser, den Sie für den Zugriff auf BlueXP verwenden, über eine Verbindung mit dieser privaten IP-Adresse verfügen. Die Verbindung kann über eine direkte Verbindung zu Ihrem Cloud-Provider (z. B. einem VPN) oder von einem Host im selben Netzwerk wie die Data Sense Instanz erfolgen.

Implementieren Sie Daten sinnvoll in der Cloud

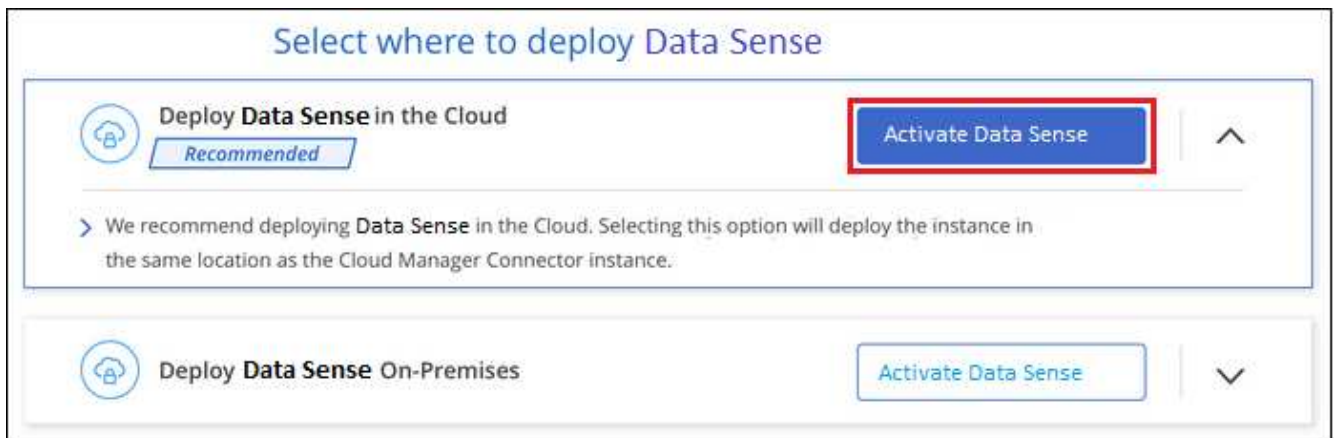
Führen Sie diese Schritte aus, um eine Instanz von Cloud Data Sense in der Cloud zu implementieren.

Schritte

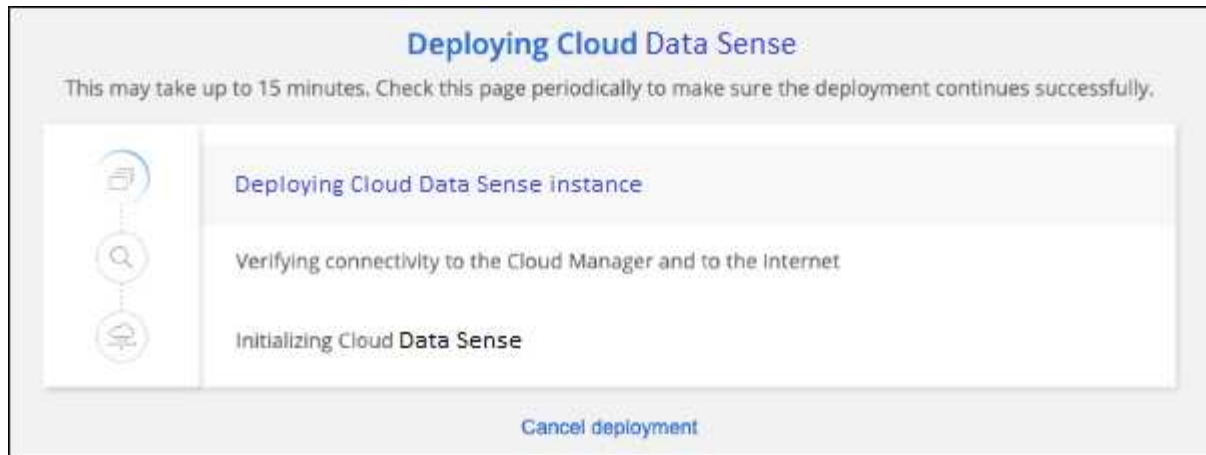
1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung**.
2. Klicken Sie Auf **Datensense Aktivieren**.



3. Klicken Sie auf **Activate Data Sense**, um den Assistenten zur Cloud-Bereitstellung zu starten.



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



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

Ergebnis

BlueXP implementiert die Cloud Data Sense Instanz bei Ihrem Cloud-Provider.

Nächste Schritte

Auf der Seite Konfiguration können Sie die Datenquellen auswählen, die Sie scannen möchten.

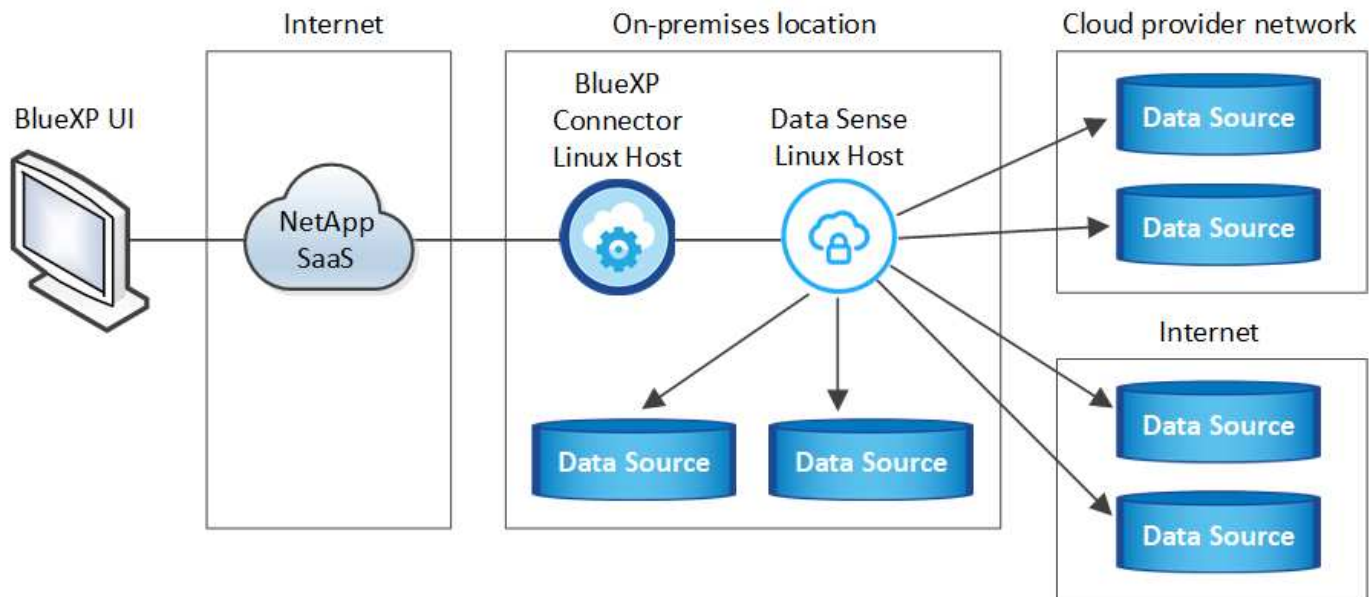
Das können Sie auch "[Lizenzierung für Cloud Data Sense einrichten](#)" Derzeit. Sie werden erst berechnet, wenn die Datenmenge mehr als 1 TB beträgt.

Implementieren Sie Cloud Data Sense auf einem Linux-Host mit Internetzugang

Führen Sie einige Schritte durch, um Cloud Data Sense auf einem Linux-Host in Ihrem Netzwerk oder einem Linux-Host in der Cloud mit Internetzugang zu implementieren.

Die On-Premises-Installation kann eine gute Option sein, wenn Sie lieber lokale ONTAP-Systeme mit einer Data Sense Instanz scannen möchten, die sich auch vor Ort befindet - dies ist jedoch keine Voraussetzung. Die Software funktioniert unabhängig von der gewählten Installationsmethode genau auf die gleiche Weise.

Die typische lokale Installation hat die folgenden Komponenten und Anschlüsse.



Bei sehr großen Konfigurationen, bei denen Sie Petabyte an Daten scannen, können Sie mehrere Hosts einschließen, um zusätzliche Verarbeitungsleistung zu schaffen. Bei der Verwendung mehrerer Hostsysteme wird das primäre System als Manager-Node bezeichnet, und die zusätzlichen Systeme, die eine zusätzliche Prozessorleistung bieten, heißen Scanner-Knoten.

Beachten Sie, dass Sie auch können ["Implementieren Sie Data Sense auf einem lokalen Standort, der keinen Internetzugang hat"](#) Für vollständig sichere Standorte.

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, ["Stellen Sie den Connector vor Ort bereit"](#) Auf einem Linux-Host in Ihrem Netzwerk oder in der Cloud.

Sie können auch einen Connector mit Ihrem Cloud-Provider erstellen. Siehe ["Erstellen eines Konnektors in AWS"](#), ["Erstellen eines Connectors in Azure"](#), Oder ["Erstellen eines Konnektors in GCP"](#).

2

Voraussetzungen prüfen

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllen kann. Dazu gehören Outbound-Internetzugang für die Instanz, Konnektivität zwischen Connector und Cloud Data Sense über Port 443 und mehr. [Eine vollständige Liste finden Sie hier.](#)

Außerdem benötigen Sie ein Linux-System, das die erfüllt [Erfüllt](#).

3

Laden Sie Cloud Data Sense herunter und implementieren Sie es

Laden Sie die Cloud Data Sense Software von der NetApp Support Site herunter, und kopieren Sie die Installer-Datei auf den Linux-Host, den Sie verwenden möchten. Starten Sie dann den Installationsassistenten,

und befolgen Sie die Anweisungen zur Bereitstellung der Data Sense-Instanz.

4

Abonnieren Sie den Cloud Data Sense Service

Die ersten 1 TB an Daten, die Cloud Data Sense in BlueXP scannt, sind kostenlos. Um die Daten nach diesem Zeitpunkt weiterhin zu scannen, benötigen Sie ein Abonnement für Ihren Cloud-Provider Marketplace oder eine BYOL-Lizenz von NetApp.

Einen Konnektor erstellen

Bevor Sie Data Sense installieren und verwenden können, ist ein BlueXP Connector erforderlich. In den meisten Fällen haben Sie wahrscheinlich einen Connector eingerichtet, bevor Sie versuchen, Cloud Data Sense zu aktivieren, da die meisten ["Für BlueXP-Funktionen ist ein Connector erforderlich"](#), Aber es gibt Fälle, in denen Sie müssen, um eine Einrichtung jetzt.

Informationen zum Erstellen einer Lösung in Ihrer Cloud-Provider-Umgebung finden Sie unter ["Erstellen eines Konnektors in AWS"](#), ["Erstellen eines Connectors in Azure"](#), Oder ["Erstellen eines Konnektors in GCP"](#).

Es gibt einige Szenarien, in denen Sie einen Connector verwenden müssen, der bei einem bestimmten Cloud-Provider implementiert wird:

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS, Amazon FSX für ONTAP oder in AWS S3 Buckets wird in AWS ein Connector verwendet.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konnektor in Azure.

Bei Azure NetApp Files muss sie in demselben Bereich bereitgestellt werden wie die Volumes, die Sie scannen möchten.

- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP verwenden Sie einen Connector in GCP.

On-Prem ONTAP Systeme, File Shares anderer Anbieter, generischer S3 Objekt-Storage, Datenbanken, OneDrive Ordner, SharePoint Konten und Google Drive Konten können über jeden dieser Cloud Connectors gescannt werden.

Beachten Sie, dass Sie auch können ["Stellen Sie den Connector vor Ort bereit"](#) Auf einem Linux-Host in Ihrem Netzwerk oder in der Cloud. Einige Anwender planen, Data Sense On-Prem zu installieren, können auch wählen, den Connector on-Prem zu installieren.

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

Bei der Installation von Data Sense benötigen Sie die IP-Adresse oder den Hostnamen des Connector-Systems. Diese Informationen erhalten Sie, wenn Sie den Connector in Ihrem Haus installiert haben. Wenn der Connector in der Cloud bereitgestellt wird, finden Sie diese Informationen in der BlueXP-Konsole: Klicken Sie auf das Hilfesymbol, wählen Sie **Support** und klicken Sie auf **BlueXP Connector**.

Bereiten Sie das Linux-Hostsystem vor

Data Sense Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Softwareanforderungen usw. erfüllt. Der Linux-Host kann sich in Ihrem Netzwerk oder in der Cloud befinden. Data Sense wird auf einem Host, der für andere Anwendungen freigegeben ist, nicht unterstützt - der Host muss ein dedizierter Host sein.

Sorgen Sie dafür, dass Cloud Data Sense ausgeführt wird. Die Cloud Data Sense Maschine muss

kontinuierlich ausgeführt werden, um Ihre Daten kontinuierlich zu scannen.

- **Betriebssystem:** Red hat Enterprise Linux oder CentOS Versionen 8.0 bis 8.7
 - Version 7.8 oder 7.9 kann verwendet werden, aber die Linux-Kernel-Version muss 4.0 oder höher sein
 - Das Betriebssystem muss in der Lage sein, die Docker-Engine zu installieren
- **Disk:** SSD mit 500 gib erhältlich auf /, oder
 - 100 gib verfügbar auf /opt
 - 400 gib verfügbar auf /var
 - 5 gib auf /tmp
- **RAM:** 64 GB (Swap-Speicher muss auf dem Host deaktiviert sein)
- **CPU:** 16 Kerne

Beachten Sie, dass Sie Daten Sense auf einem System mit weniger CPUs und weniger RAM implementieren können, es gibt jedoch Einschränkungen bei der Verwendung dieser Systeme. Siehe ["Verwenden eines kleineren Instanztyps"](#) Entsprechende Details.

- **Red hat Subscription Management:** Ein Red hat Enterprise Linux System muss mit Red hat Subscription Management registriert werden. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositories zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.
- **Zusätzliche Software:** Sie müssen die folgende Software auf dem Host installieren, bevor Sie Data Sense installieren:
 - Docker Engine Version 19 oder höher. ["Installationsanweisungen anzeigen"](#).
 - Python 3 Version 3.6 oder höher. ["Installationsanweisungen anzeigen"](#).
- **Firewalld Überlegungen:** Wenn Sie planen zu verwenden `firewalld`, Wir empfehlen, dass Sie es aktivieren, bevor Sie Data Sense installieren. Führen Sie die folgenden Befehle zum Konfigurieren aus `firewalld` Damit es mit Data Sense kompatibel ist:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Wenn Sie planen, zusätzliche Data Sense Hosts zu verwenden, fügen Sie diese Regeln zu Ihrem Primärsystem zu diesem Zeitpunkt hinzu:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Wenn Sie aktivieren `firewalld` Nach der Installation von Data Sense müssen Sie den Docker neu starten.



Die IP-Adresse des Data Sense Hostsystems kann nach der Installation nicht geändert werden.

Outbound-Internetzugang über Cloud Data Sense aktivieren

Für Cloud Data Sense ist ein Outbound-Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxyserver für den Internetzugriff verwendet, stellen Sie sicher, dass die Datensense-Instanz über Outbound-Internetzugang verfügt, um die folgenden Endpunkte zu kontaktieren.

| Endpunkte | Zweck |
|--|---|
| https://api.bluexp.netapp.com | Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts |
| https://netapp-cloud-account.auth0.com https://auth0.com | Kommunikation mit der BlueXP-Website zur zentralen Benutzerauthentifizierung. |
| https://support.compliance.api.bluexp.netapp.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, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden. |
| https://support.compliance.api.bluexp.netapp.com/ | Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen. |
| https://github.com/docker https://download.docker.com http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm | Enthält die für die Installation erforderlichen Pakete. |

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

Sie müssen sicherstellen, dass alle erforderlichen Ports für die Kommunikation zwischen Connector, Data Sense, Active Directory und Ihren Datenquellen offen sind.

| Verbindungstyp | Ports | Beschreibung |
|-------------------------|------------------------------|---|
| Connector <> Data Sense | 8080 (TCP), 443 (TCP) und 80 | Die Firewall- oder Routing-Regeln für den Connector müssen ein- und ausgehenden Datenverkehr über Port 443 zu und aus der Instanz Data Sense ermöglichen. Stellen Sie sicher, dass Port 8080 geöffnet ist, damit Sie den Installationsfortschritt in BlueXP sehen können. |

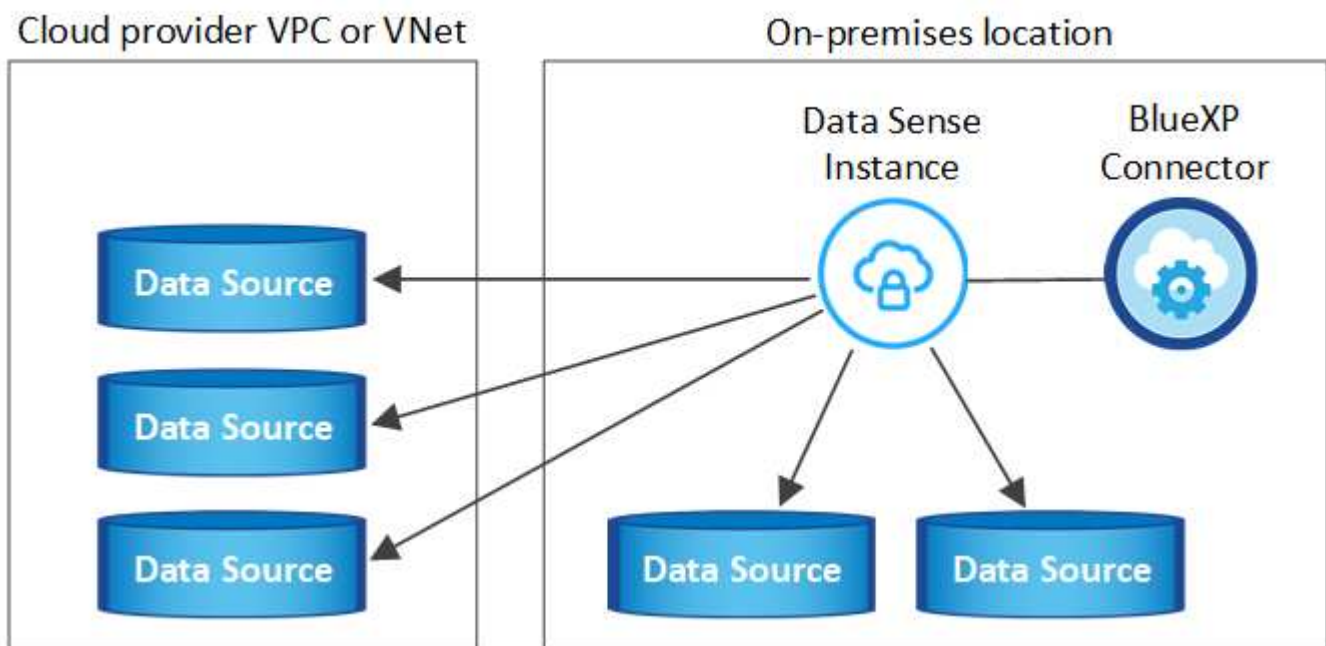
| Verbindungstyp | Ports | Beschreibung |
|----------------------------------|--|---|
| Connector <> ONTAP-Cluster (NAS) | 443 (TCP) | <p>BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen:</p> <ul style="list-style-type: none"> • Der Connector-Host muss ausgehenden HTTPS-Zugriff über Port 443 ermöglichen. Wenn sich der Connector in der Cloud befindet, ist die gesamte ausgehende Kommunikation durch vordefinierte Firewall- oder Routingregeln zulässig. • Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen. Die standardmäßige "mgmt"-Firewall-Richtlinie ermöglicht eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert haben oder wenn Sie eine eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff über den Connector-Host aktivieren. |
| Datensense <> ONTAP-Cluster | <ul style="list-style-type: none"> • Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS - 139 (TCP\UDP) und 445 (TCP\UDP) | <p>Für den Datensense ist eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP-Subnetz oder On-Prem ONTAP-System erforderlich. Firewalls oder Routingregeln für Cloud Volumes ONTAP müssen eingehende Verbindungen aus der Instanz Data Sense zulassen.</p> <p>Stellen Sie sicher, dass diese Ports für die Data Sense-Instanz offen sind:</p> <ul style="list-style-type: none"> • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 <p>NFS-Volume-Exportrichtlinien müssen den Zugriff aus der Data Sense Instanz zulassen.</p> |

| Verbindungstyp | Ports | Beschreibung |
|--------------------------------|---|---|
| Datensinn <=> Active Directory | 389 (TCP & UDP), 636 (TCP), 3268 (TCP) UND 3269 (TCP) | <p>Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben. Darüber hinaus benötigt Data Sense Active Directory-Anmeldeinformationen zum Scannen von CIFS-Volumes.</p> <p>Sie müssen über die folgenden Informationen für das Active Directory verfügen:</p> <ul style="list-style-type: none"> • DNS-Server-IP-Adresse oder mehrere IP-Adressen • Benutzername und Kennwort für den Server • Domain-Name (Active Directory-Name) • Ob Sie Secure LDAP (LDAPS) verwenden oder nicht • LDAP-Server-Port (normalerweise 389 für LDAP und 636 für sicheres LDAP) |

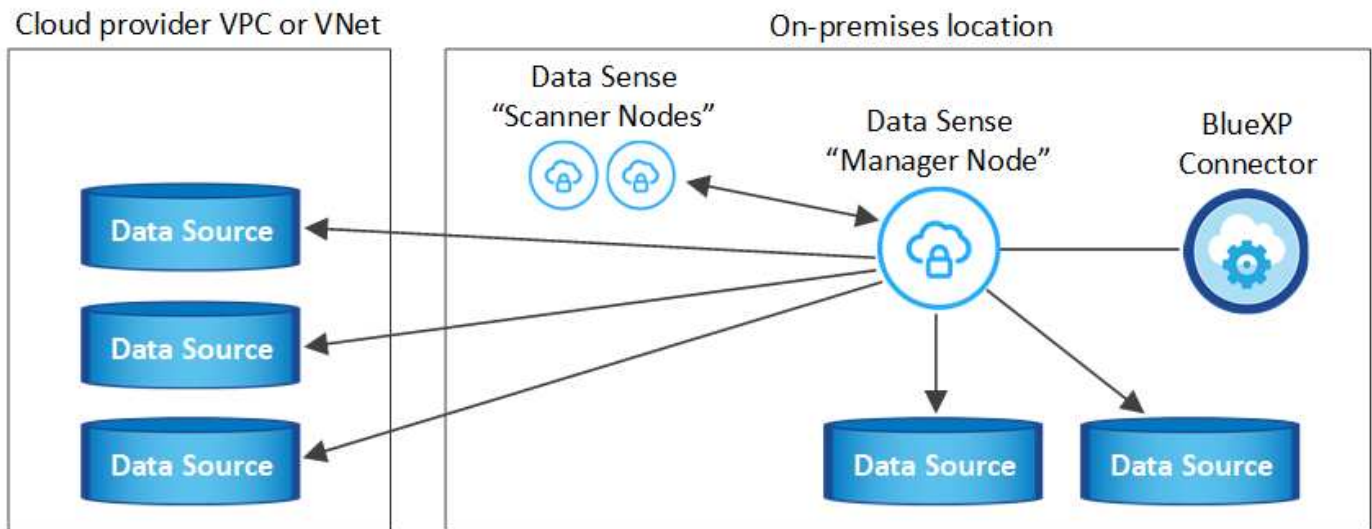
Wenn Sie mehrere Data Sense Hosts verwenden, um zusätzliche Verarbeitungsleistung für das Scannen Ihrer Datenquellen bereitzustellen, müssen Sie zusätzliche Ports/Protokolle aktivieren. ["Siehe zusätzliche Anschlussanforderungen"](#).

Implementieren Sie Data Sense vor Ort

Für typische Konfigurationen installieren Sie die Software auf einem einzigen Host-System. [Siehe diese Schritte hier](#).



Bei sehr großen Konfigurationen, bei denen Sie Petabyte an Daten scannen, können Sie mehrere Hosts einschließen, um zusätzliche Verarbeitungsleistung zu schaffen. [Siehe diese Schritte hier](#).



Siehe [Vorbereiten des Linux-Hostsystems](#) Und [Voraussetzungen prüfen](#) Eine vollständige Liste der Anforderungen vor der Implementierung von Cloud Data Sense erhalten.

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



Cloud Data Sense kann derzeit S3-Buckets, Azure NetApp Files oder FSX für ONTAP nicht scannen, wenn die Software vor Ort installiert ist. In diesen Fällen müssen Sie in der Cloud und darüber hinaus einen separaten Connector und Instanz der Daten implementieren ["Zwischen den Anschlüssen wechseln"](#) Für Ihre unterschiedlichen Datenquellen.

Installation mit einem Host für typische Konfigurationen

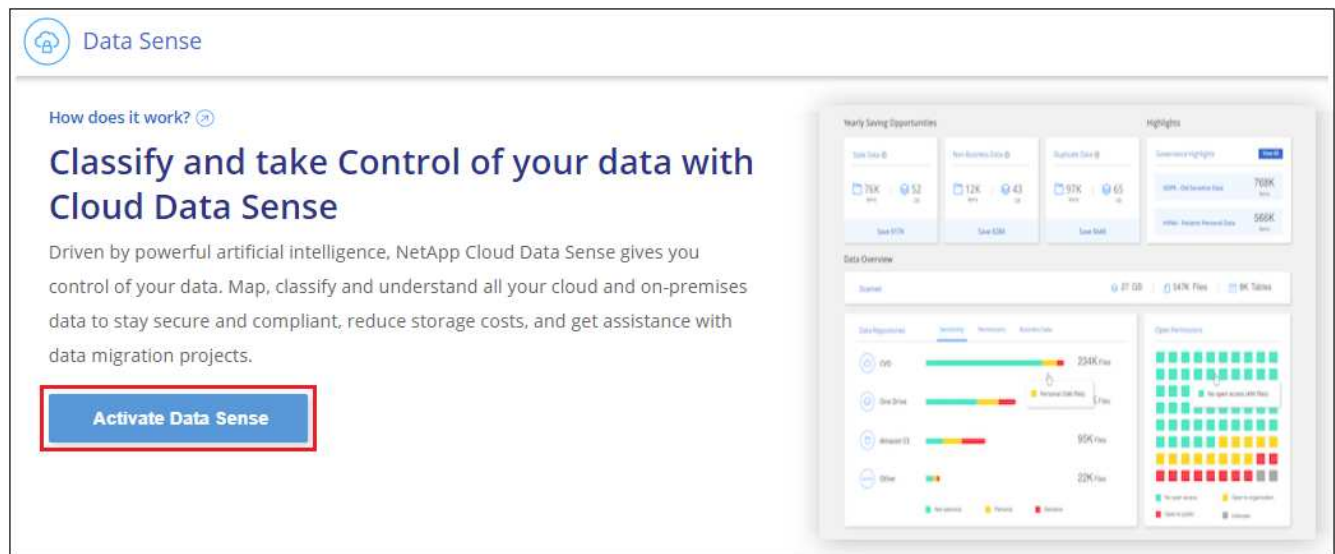
Führen Sie diese Schritte aus, wenn Sie Data Sense Software auf einem einzelnen lokalen Host installieren.

Was Sie benötigen

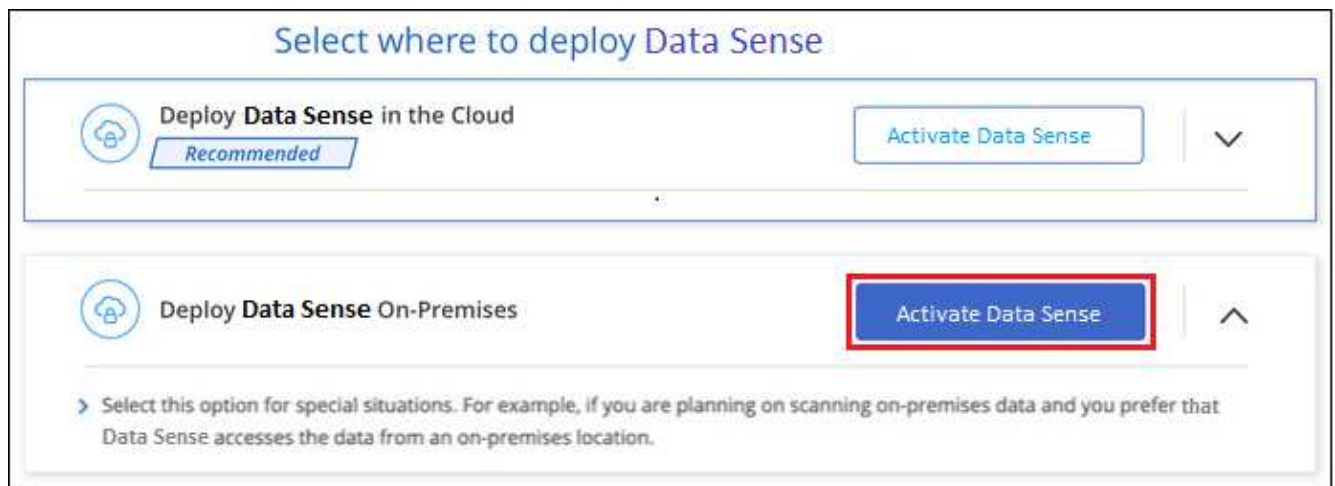
- Vergewissern Sie sich, dass Ihr Linux-System die erfüllt [Host-Anforderungen erfüllt](#).
- Vergewissern Sie sich, dass auf dem System die beiden erforderlichen Softwarepakete installiert sind (Docker Engine und Python 3).
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.
- Wenn Sie einen Proxy verwenden und TLS abfangen, müssen Sie den Pfad auf dem Data Sense Linux-System kennen, auf dem die TLS CA-Zertifikate gespeichert werden.
- Vergewissern Sie sich, dass die erforderliche Offline-Umgebung erfüllt ist [Berechtigungen und Konnektivität](#).

Schritte

1. Laden Sie die Software Cloud Data Sense von herunter ["NetApp Support Website"](#). Die ausgewählte Datei heißt **DATASENSE-INSTALLER-<Version>.tar.gz**.
2. Kopieren Sie die Installationsdatei auf den Linux-Host, den Sie verwenden möchten (mit `scp` Oder eine andere Methode).
3. Wählen Sie in BlueXP die Option **Governance > Klassifizierung** aus.
4. Klicken Sie Auf **Datensense Aktivieren**.



5. Klicken Sie auf **Activate Data Sense**, um den On-Prem Deployment Wizard zu starten.



6. Kopieren Sie im Dialogfeld *Deploy Data Sense on premise* den angegebenen Befehl und fügen Sie ihn in eine Textdatei ein, damit Sie ihn später verwenden können, und klicken Sie auf **Schließen**. Beispiel:

```
sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq
```

7. Entpacken Sie die Installationsdatei auf dem Hostcomputer, z. B.:

```
tar -xzf DATASENSE-INSTALLER-V1.16.1.tar.gz
```

8. Wenn Sie vom Installationsprogramm dazu aufgefordert werden, können Sie die erforderlichen Werte in eine Reihe von Eingabeaufforderungen eingeben oder Sie können die erforderlichen Parameter als Befehlszeilenargumente dem Installer angeben.

Beachten Sie, dass das Installationsprogramm eine Vorprüfung durchführt, um sicherzustellen, dass Ihre System- und Netzwerkanforderungen für eine erfolgreiche Installation erfüllt werden.

| Geben Sie die Parameter wie aufgefordert ein: | Geben Sie den vollständigen Befehl ein: |
|--|--|
| <p>a. Fügen Sie die Informationen ein, die Sie aus Schritt 6 kopiert haben:</p> <pre>sudo ./install.sh -a <account_id> -c <agent_id> -t <token></pre> <p>b. Geben Sie die IP-Adresse oder den Hostnamen des Data Sense Host-Rechners ein, damit auf diese durch die Connector-Instanz zugegriffen werden kann.</p> <p>c. Geben Sie die IP-Adresse oder den Hostnamen des BlueXP Connector-Hostcomputers ein, damit die Instanz Data Sense darauf zugreifen kann.</p> <p>d. Geben Sie die Proxy-Details wie aufgefordert ein. Wenn Ihr BlueXP Connector bereits einen Proxy verwendet, müssen diese Informationen hier nicht erneut eingegeben werden, da Data Sense den vom Connector verwendeten Proxy automatisch verwendet.</p> | <p>Alternativ können Sie den gesamten Befehl vorab erstellen und die erforderlichen Host- und Proxy-Parameter bereitstellen:</p> <pre>sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host> --manager-host <cm_host> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir></pre> |

Variablenwerte:

- *Account_id* = NetApp Konto-ID
- *Agent_id* = Konnektor-ID
- *Token* = jwt-Benutzer-Token
- *ds_Host* = IP-Adresse oder Hostname des Data Sense Linux-Systems.
- *Cm_Host* = IP-Adresse oder Hostname des BlueXP Connector-Systems.
- *Proxy_Host* = IP oder Hostname des Proxy-Servers, wenn sich der Host hinter einem Proxy-Server befindet.
- *Proxy_Port* = Port zur Verbindung mit dem Proxy-Server (Standard 80).
- *Proxy_Schema* = Verbindungsschema: https oder http (Standard http).
- *Proxy_User* = authentifizierter Benutzer zur Verbindung mit dem Proxy-Server, falls eine grundlegende Authentifizierung erforderlich ist.
- *Proxy_Password* = Passwort für den von Ihnen angegebenen Benutzernamen.
- *Ca_cert_dir* = Pfad auf dem Data Sense Linux System mit zusätzlichen TLS CA-Zertifikatpaketen. Nur erforderlich, wenn der Proxy TLS Abfangen durchführt.

Ergebnis

Das Cloud Data Sense Installationsprogramm installiert Pakete, installiert den Docker, registriert die Installation und installiert Data Sense. Die Installation dauert 10 bis 20 Minuten.

Wenn zwischen dem Host-Rechner und der Connector-Instanz eine Verbindung über Port 8080 besteht, sehen Sie den Installationsfortschritt auf der Registerkarte Data Sense in BlueXP.

Nächste Schritte

Auf der Seite Konfiguration können Sie die Datenquellen auswählen, die Sie scannen möchten.

Das können Sie auch "[Lizenzierung für Cloud Data Sense einrichten](#)" Derzeit. Sie werden erst berechnet, wenn die Datenmenge mehr als 1 TB beträgt.

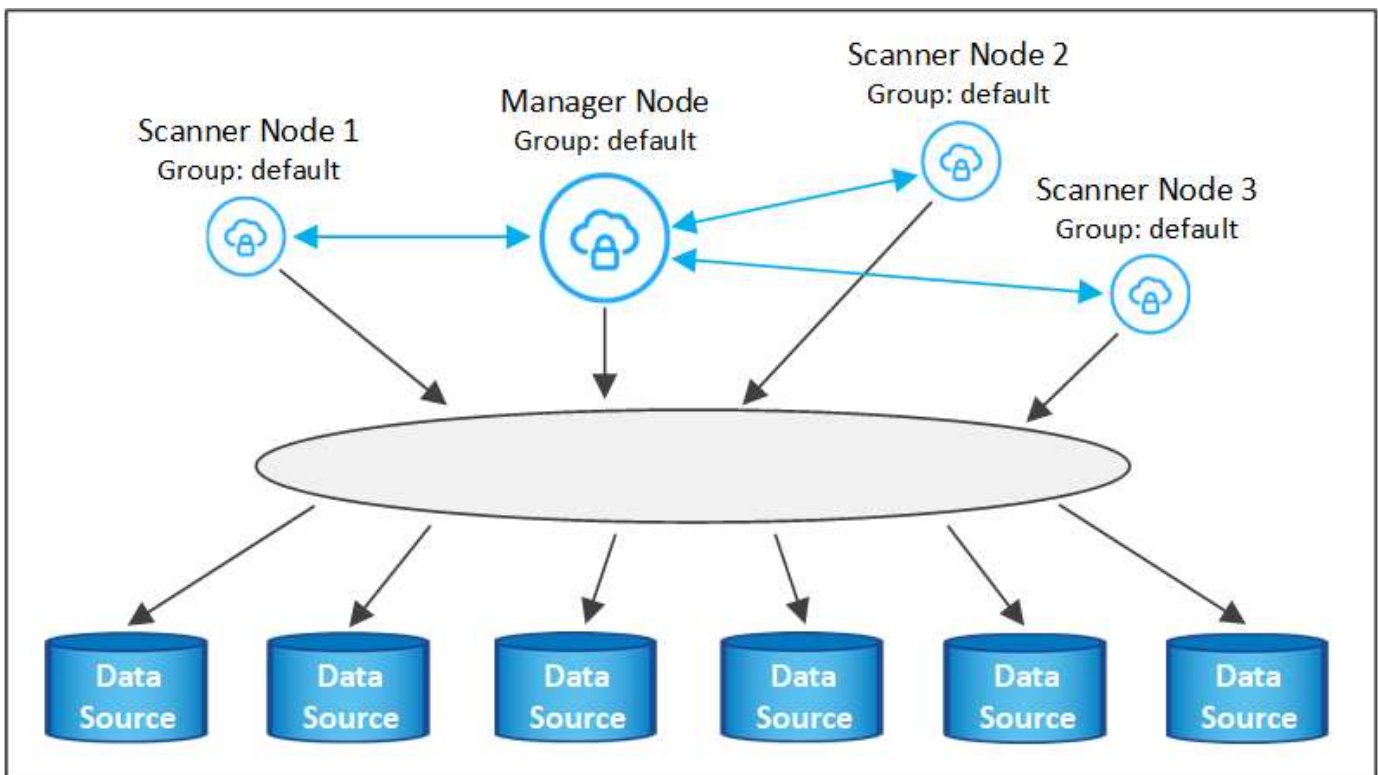
Fügen Sie Scannerknoten zu einer vorhandenen Implementierung hinzu

Sie können weitere Scanner-Knoten hinzufügen, wenn Sie feststellen, dass Sie mehr Scanleistung benötigen, um Ihre Datenquellen zu scannen. Sie können die Scanner-Knoten unmittelbar nach der Installation des Manager-Knotens hinzufügen oder später einen Scanner-Knoten hinzufügen. Wenn Sie beispielsweise feststellen, dass sich die Datenmenge in einer Ihrer Datenquellen nach 6 Monaten verdoppelt oder verdreifacht hat, können Sie einen neuen Scannerknoten hinzufügen, um die Datenüberprüfung zu unterstützen.

Es gibt zwei Möglichkeiten, weitere Scanner-Knoten hinzuzufügen:

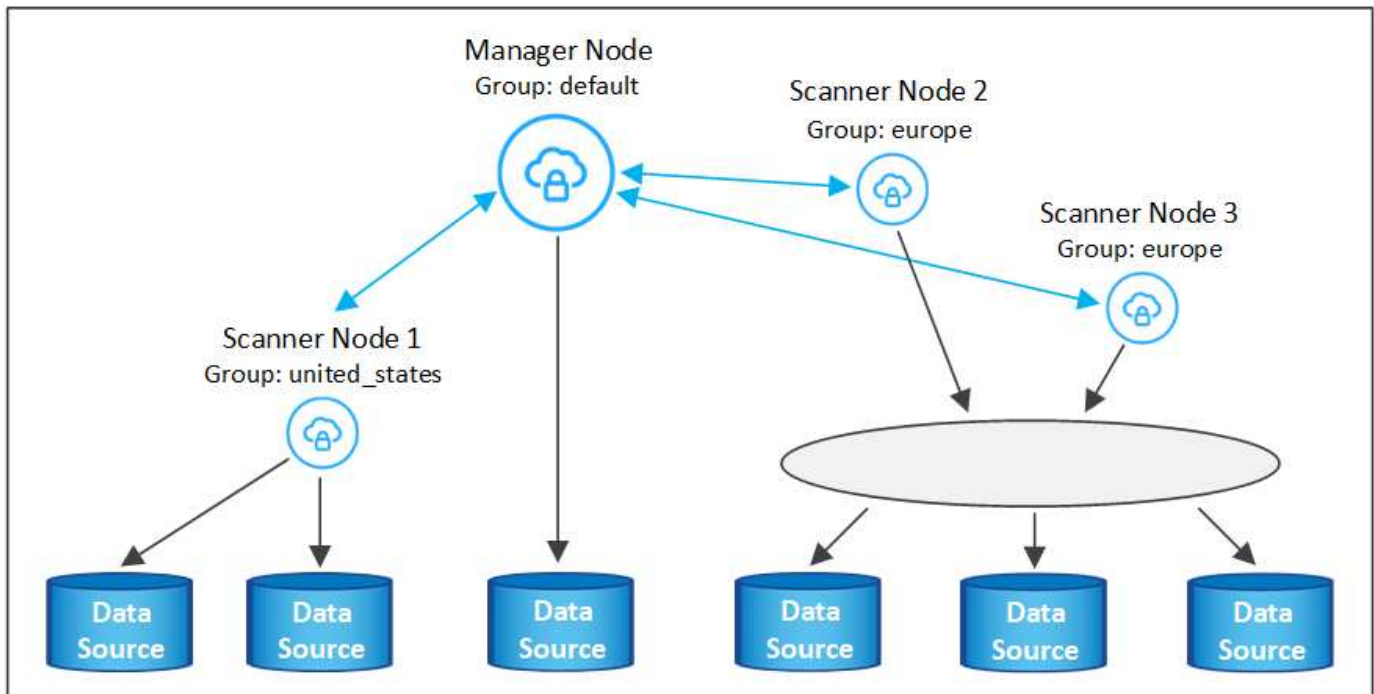
- Fügen Sie einen Knoten hinzu, um das Scannen aller Datenquellen zu unterstützen
- Fügen Sie einen Knoten hinzu, um das Scannen einer bestimmten Datenquelle oder einer bestimmten Gruppe von Datenquellen zu unterstützen

Standardmäßig werden alle neuen Scanner-Knoten, die Sie hinzufügen, dem allgemeinen Pool der Scanning-Ressourcen hinzugefügt. Dies wird als „Standard-Scannergruppe“ bezeichnet. In der Abbildung unten befinden sich 1 Manager-Knoten und 3 Scanner-Knoten in der „Standard“-Gruppe, die alle Scan-Daten aus allen 6 Datenquellen sind.



Wenn Sie bestimmte Datenquellen haben, die von Scannerknoten gescannt werden sollen, die sich physisch näher an den Datenquellen befinden, können Sie einen Scannerknoten oder eine Gruppe von Scannerknoten definieren, um eine bestimmte Datenquelle oder eine Gruppe von Datenquellen zu scannen. In der Abbildung unten befinden sich 1 Manager-Knoten und 3 Scanner-Knoten.

- Der Manager-Knoten befindet sich in der „Standard“-Gruppe, und er scannt 1 Datenquelle
- Der Scannerknoten 1 befindet sich in der Gruppe „united_States“ und scannt 2 Datenquellen
- Die Scannerknoten 2 und 3 befinden sich in der Gruppe „europa“, und sie teilen die Scanaufgaben für 3



Data Sense-Scannergruppen können als separate geografische Bereiche definiert werden, in denen Ihre Daten gespeichert sind. Sie können weltweit mehrere Data Sense Scanner-Knoten bereitstellen und für jeden Knoten eine Scannergruppe auswählen. Auf diese Weise scannt jeder Scanner-Knoten die Daten, die ihm am nächsten sind. Je näher der Scanner-Knoten an den Daten liegt, desto besser, da er die Netzwerklatenz so weit wie möglich beim Scannen der Daten reduziert.

Sie können festlegen, welche Scannergruppen zu Data Sense hinzugefügt werden sollen, und Sie können deren Namen auswählen. Data Sense setzt nicht fest, dass ein Knoten, der einer Scannergruppe namens „europa“ zugeordnet ist, in Europa eingesetzt wird.

So installieren Sie zusätzliche Data Sense Scanner-Knoten:

1. Bereiten Sie die Linux-Hostsysteme vor, die als Scanner-Knoten fungieren sollen
2. Laden Sie die Software Data Sense auf diese Linux-Systeme herunter
3. Führen Sie einen Befehl auf dem Knoten Manager aus, um die Scanner-Knoten zu identifizieren
4. Befolgen Sie die Schritte, um die Software auf den Scanner-Knoten bereitzustellen (und optional eine „Scannergruppe“ für bestimmte Scanner-Knoten zu definieren).
5. Wenn Sie eine Scannergruppe definiert haben, befinden Sie sich auf dem Knoten Manager:
 - a. Öffnen Sie die Datei „Working_Environment_to_Scanner_Group_config.yml“ und definieren Sie die Arbeitsumgebungen, die von jeder Scannergruppe gescannt werden sollen
 - b. Führen Sie das folgende Skript aus, um diese Zuordnungsinformationen bei allen Scanner-Knoten zu registrieren: `update_we_scanner_group_from_config_file.sh`

Was Sie benötigen

- Stellen Sie sicher, dass alle Linux-Systeme für Scanner-Knoten den erfüllen [Host-Anforderungen erfüllt](#).
- Überprüfen Sie, ob die Systeme über die beiden erforderlichen Softwarepakete installiert sind (Docker Engine und Python 3).

- Stellen Sie sicher, dass Sie auf den Linux-Systemen über Root-Rechte verfügen.
- Vergewissern Sie sich, dass Ihre Umgebung den erforderlichen Anforderungen entspricht [Berechtigungen und Konnektivität](#).
- Sie müssen über die IP-Adressen der Scanner-Knoten-Hosts verfügen, die Sie hinzufügen.
- Sie müssen über die IP-Adresse des Data Sense Manager-Node-Hostsystems verfügen
- Sie müssen über die IP-Adresse oder den Hostnamen des Connector-Systems, Ihre NetApp Account-ID, Connector Client-ID und Benutzer-Zugriffstoken verfügen. Wenn Sie planen, Scannergruppen zu verwenden, müssen Sie die ID der Arbeitsumgebung für jede Datenquelle in Ihrem Konto kennen. Weitere Informationen finden Sie unter „*Voraussetzungen Steps* weiter unten“.
- Die folgenden Ports und Protokolle müssen auf allen Hosts aktiviert sein:

| Port | Protokolle | Beschreibung |
|------|------------|--|
| 2377 | TCP | Cluster-Management-Kommunikation |
| 7946 | TCP, UDP | Kommunikation zwischen den Knoten |
| 4789 | UDP | Overlay-Netzwerk-Traffic |
| 50 | ESP | Verschlüsselter ESP-Datenverkehr (IPsec Overlay Network) |
| 111 | TCP, UDP | NFS-Server für die gemeinsame Nutzung von Dateien zwischen den Hosts (benötigt von jedem Scanner-Knoten zu Manager-Knoten) |
| 2049 | TCP, UDP | NFS-Server für die gemeinsame Nutzung von Dateien zwischen den Hosts (benötigt von jedem Scanner-Knoten zu Manager-Knoten) |

- Wenn Sie verwenden `firewalld` Auf Ihren Data Sense-Maschinen empfehlen wir Ihnen, diese vor der Installation von Data Sense zu aktivieren. Führen Sie die folgenden Befehle zum Konfigurieren aus `firewalld` Damit es mit Data Sense kompatibel ist:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

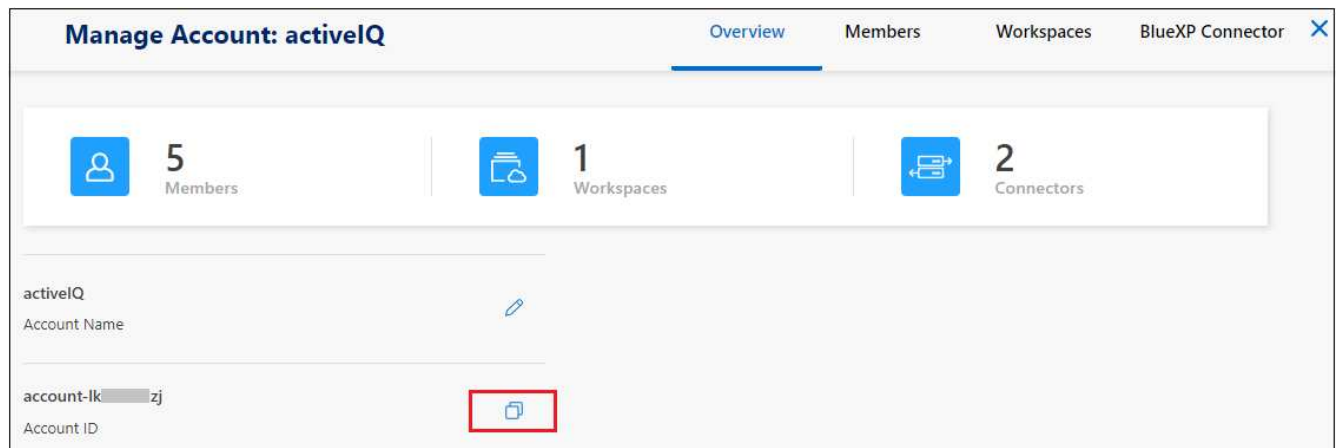
Wenn Sie aktivieren `firewalld` Nach der Installation von Data Sense müssen Sie den Docker neu starten.

Erforderliche Schritte

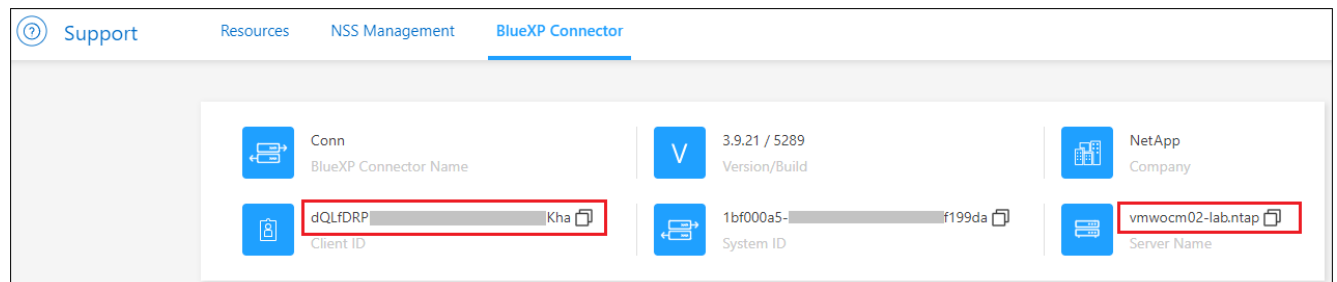
Führen Sie diese Schritte aus, um die NetApp Account ID, die Connector Client ID, den Connector Server-Namen und das Token für den Benutzerzugriff zu erhalten, die erforderlich sind, um Scanner-Nodes

hinzuzufügen.

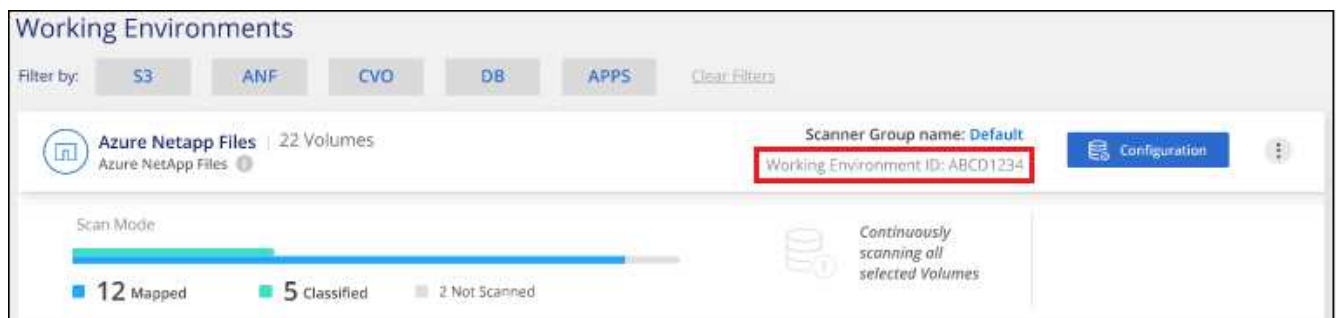
1. Klicken Sie in der Menüleiste von BlueXP auf **Konto > Konten verwalten**.



2. Kopieren Sie die *Konto-ID*.
3. Klicken Sie in der Menüleiste von BlueXP auf **Hilfe > Support > BlueXP Connector**.



4. Kopieren Sie die *Konnektor_Client-ID_* und die *Servername*.
5. Wenn Sie Scannergruppen verwenden möchten, kopieren Sie auf der Registerkarte „Data Sense Configuration“ die ID der Arbeitsumgebung für jede Arbeitsumgebung, die Sie einer Scannergruppe hinzufügen möchten.



6. Wechseln Sie zum "[API Documentation Developer Hub](#)" Und klicken Sie auf **Erfahren Sie, wie Sie sich authentifizieren**.

API Documentation

[Learn how to authenticate](#)

7. Befolgen Sie die Authentifizierungsanweisungen, und kopieren Sie das Token Access aus der Antwort.

Schritte

1. Führen Sie auf dem Knoten Data Sense Manager das Skript „add_Scanner_Node.sh“ aus. Mit diesem Befehl werden beispielsweise 2 Scannerknoten hinzugefügt:

```
sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h  
<ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
```

Variablenwerte:

- *Account_id* = NetApp Konto-ID
 - *Client_id* = Connector-Client-ID
 - *Cm_Host* = IP-Adresse oder Hostname des Steckverbindersystems
 - *ds_Manager_ip* = Private IP-Adresse des Datensense Manager-Knotensystems
 - *Node_private_ip* = IP-Adressen der Datensense-Scanner-Knotensysteme (mehrere Scanner-Knoten-IPs werden durch Komma getrennt)
 - *User_Token* = JWT-Benutzer-Zugriffstoken
2. Bevor das Skript add_Scanner_Node abgeschlossen wird, wird in einem Dialogfeld der Installationsbefehl angezeigt, der für die Scanner-Knoten benötigt wird. Kopieren Sie den Befehl und speichern Sie ihn in einer Textdatei. Beispiel:

```
sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j
```

3. Auf * jedem Scanner-Knoten-Host:
 - a. Kopieren Sie die Data Sense Installer-Datei (**DATASENSE-INSTALLER-<Version>.tar.gz**) auf den Host-Rechner (mit `scp` Oder eine andere Methode).
 - b. Entpacken Sie die Installationsdatei.
 - c. Fügen Sie den Befehl ein, den Sie in Schritt 2 kopiert haben, und führen Sie ihn aus.
 - d. Wenn Sie einen Scannerknoten zu einer "Scannergruppe" hinzufügen möchten, fügen Sie dem Befehl den Parameter **-r <Scanner_Group_Name>** hinzu. Andernfalls wird der Scannerknoten zur Gruppe „Standard“ hinzugefügt.

Wenn die Installation auf allen Scanner-Knoten abgeschlossen ist und sie mit dem Manager-Knoten verbunden wurden, wird das Skript „add_Scanner_Node.sh“ ebenfalls beendet. Die Installation dauert 10 bis 20 Minuten.

4. Wenn Sie Scannerknoten zu einer Scannergruppe hinzugefügt haben, kehren Sie zum Manager-Knoten zurück und führen Sie die folgenden beiden Aufgaben aus:
 - a. Öffnen Sie die Datei „/opt/netapp/Datacense/Working_Environment_to_Scanner_Group_config.yml“, und geben Sie die Zuordnung ein, für die Scannergruppen bestimmte Arbeitsumgebungen scannen. Sie benötigen die *Working Environment ID* für jede Datenquelle. Die folgenden Einträge fügen beispielsweise 2 Arbeitsumgebungen zur Scanner-Gruppe „europa“ und 2 zur Scannergruppe

„united_States“ hinzu:

```
scanner_groups:
  europe:
    working_environments:
      - "working_environment_id1"
      - "working_environment_id2"
  united_states:
    working_environments:
      - "working_environment_id3"
      - "working_environment_id4"
```

Jede Arbeitsumgebung, die nicht zur Liste hinzugefügt wird, wird von der Gruppe „Standard“ gescannt. Sie müssen mindestens einen Manager- oder Scannerknoten in der Gruppe „Standard“ haben.

- b. Führen Sie das folgende Skript aus, um diese Zuordnungsinformationen bei allen Scanner-Knoten zu registrieren:

```
/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh
```

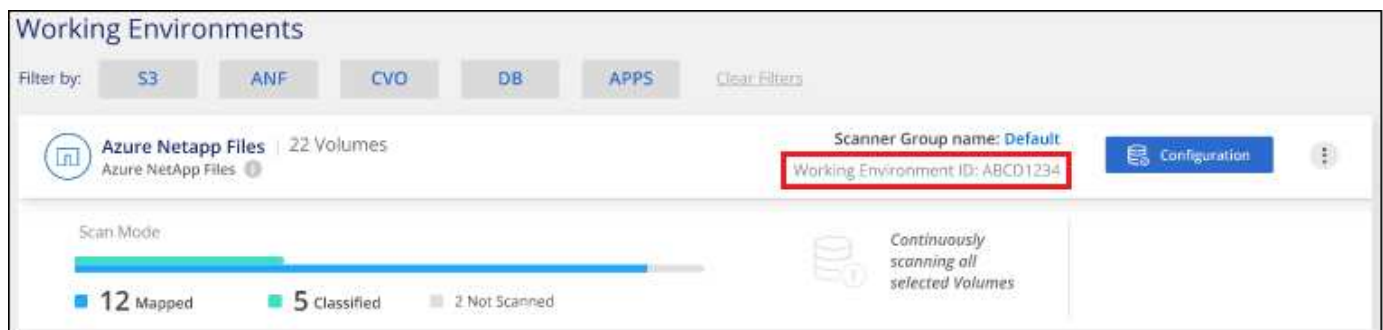
Ergebnis

Data Sense ist mit den Manager- und Scanner-Knoten eingerichtet, um alle Datenquellen zu scannen.

Nächste Schritte

Auf der Konfigurationsseite können Sie die Datenquellen auswählen, die Sie scannen möchten - wenn Sie das noch nicht getan haben. Wenn Sie Scannergruppen erstellt haben, wird jede Datenquelle von den Scanner-Knoten in der jeweiligen Gruppe gescannt.

Der Name der Scannergruppe für jede Arbeitsumgebung wird auf der Konfigurationsseite angezeigt.



Sie können auch die Liste aller Scannergruppen sowie die IP-Adresse und den Status für jeden Scannerknoten in der Gruppe unten auf der Konfigurationsseite anzeigen.

Scanner Groups

Search

Scanner Group: Default

Scanner nodes

2 Scanner nodes

| Scanner node host name | IP | Last active time | Status | Error |
|-----------------------------|---------|------------------|--------|-------|
| ip-172-...us-west-2.compute | 172-... | 23/09/2022 14:32 | Active | |
| ip-172-...us-west-2.compute | 172-... | 23/09/2022 14:32 | Active | |

Scanner Group: United_States

Scanner nodes

2 Scanner nodes

| Scanner node host name | IP | Last active time | Status | Error |
|-----------------------------|---------|------------------|--------|-------|
| ip-172-...us-west-2.compute | 172-... | 23/09/2022 14:32 | Active | |
| ip-172-...us-west-2.compute | 172-... | 23/09/2022 14:32 | Active | |

Scanner Group: Europe

Scanner nodes

Das können Sie "[Lizenzierung für Cloud Data Sense einrichten](#)" Derzeit. Sie werden erst berechnet, wenn die Datenmenge mehr als 1 TB beträgt.

Installation mit mehreren Hosts für große Konfigurationen

Bei sehr großen Konfigurationen, bei denen Sie Petabyte an Daten scannen, können Sie mehrere Hosts einschließen, um zusätzliche Verarbeitungsleistung zu schaffen. Bei der Verwendung mehrerer Hostsysteme wird das primäre System als *Manager-Node* bezeichnet, und die zusätzlichen Systeme, die zusätzliche Rechenleistung bieten, heißen *Scanner-Nodes*.

Führen Sie diese Schritte aus, wenn Sie Data Sense Software auf mehreren lokalen Hosts installieren.

Was Sie benötigen

- Stellen Sie sicher, dass alle Linux-Systeme für den Manager- und Scanner-Knoten den entsprechen [Host-Anforderungen erfüllt](#).
- Überprüfen Sie, ob die Systeme über die beiden erforderlichen Softwarepakete installiert sind (Docker Engine und Python 3).
- Stellen Sie sicher, dass Sie auf den Linux-Systemen über Root-Rechte verfügen.
- Vergewissern Sie sich, dass Ihre Umgebung den erforderlichen Anforderungen entspricht [Berechtigungen und Konnektivität](#).
- Sie müssen über die IP-Adressen der zu verwendenden Scanner-Knoten-Hosts verfügen.
- Die folgenden Ports und Protokolle müssen auf allen Hosts aktiviert sein:

| Port | Protokolle | Beschreibung |
|------|------------|----------------------------------|
| 2377 | TCP | Cluster-Management-Kommunikation |

| Port | Protokolle | Beschreibung |
|------|------------|--|
| 7946 | TCP, UDP | Kommunikation zwischen den Knoten |
| 4789 | UDP | Overlay-Netzwerk-Traffic |
| 50 | ESP | Verschlüsselter ESP-Datenverkehr (IPsec Overlay Network) |
| 111 | TCP, UDP | NFS-Server für die gemeinsame Nutzung von Dateien zwischen den Hosts (benötigt von jedem Scanner-Knoten zu Manager-Knoten) |
| 2049 | TCP, UDP | NFS-Server für die gemeinsame Nutzung von Dateien zwischen den Hosts (benötigt von jedem Scanner-Knoten zu Manager-Knoten) |

Schritte

1. Befolgen Sie die Schritte 1 bis 7 vom [Installation über einen Host](#) Auf dem Knoten Manager.
2. Wie in Schritt 8 gezeigt, können Sie bei Aufforderung durch das Installationsprogramm die erforderlichen Werte in eine Reihe von Eingabeaufforderungen eingeben oder die erforderlichen Parameter als Befehlszeilenargumente für das Installationsprogramm bereitstellen.

Zusätzlich zu den Variablen, die für eine Installation mit einem Host verfügbar sind, wird eine neue Option **-n <Node_ip>** verwendet, um die IP-Adressen der Scannerknoten anzugeben. Mehrere Scanner-Knoten-IPs werden durch Komma getrennt.

Mit diesem Befehl werden beispielsweise 3 Scannerknoten hinzugefügt:

```
sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host>
--manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy-host
<proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy
-user <proxy_user> --proxy-password <proxy_password>
```

3. Bevor die Installation des Manager-Node abgeschlossen ist, wird in einem Dialogfeld der für die Scanner-Knoten erforderliche Installationsbefehl angezeigt. Kopieren Sie den Befehl und speichern Sie ihn in einer Textdatei. Beispiel:

```
sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212
```

4. Auf * jedem Scanner-Knoten-Host:
 - a. Kopieren Sie die Data Sense Installer-Datei (**DATASENSE-INSTALLER-<Version>.tar.gz**) auf den Host-Rechner (mit `scp` Oder eine andere Methode).
 - b. Entpacken Sie die Installationsdatei.
 - c. Fügen Sie den Befehl ein, den Sie in Schritt 3 kopiert haben, und führen Sie ihn aus.

Wenn die Installation auf allen Scanner-Knoten abgeschlossen ist und sie mit dem Manager-Knoten verbunden wurden, wird auch die Installation des Manager-Knotens abgeschlossen.

Ergebnis

Das Installationsprogramm von Cloud Data Sense beendet die Installation von Paketen, Docker und registriert die Installation. Die Installation dauert 10 bis 20 Minuten.

Nächste Schritte

Auf der Seite Konfiguration können Sie die Datenquellen auswählen, die Sie scannen möchten.

Das können Sie auch ["Lizenzierung für Cloud Data Sense einrichten"](#) Derzeit. Sie werden erst berechnet, wenn die Datenmenge mehr als 1 TB beträgt.

Cloud-Daten lokal sinnvoll nutzen ohne Internetzugang

Führen Sie ein paar Schritte zu implementieren Cloud Data Sense auf einem Host in einer On-Premises-Website, die keinen Internetzugang hat. Diese Art der Installation ist perfekt für Ihre sicheren Standorte.

Beachten Sie, dass Sie auch können ["Implementieren Sie Data Sense in einer lokalen Website mit Internetzugang"](#).

Unterstützte Datenquellen

Bei Installation auf diese Weise (manchmal auch als „offline“ oder „Dark“-Website bezeichnet) kann Data Sense Daten nur aus Datenquellen scannen, die auch lokal auf dem lokalen Standort vorhanden sind. Zu diesem Zeitpunkt kann Data Sense die folgenden **lokalen** Datenquellen scannen:

- On-Premises ONTAP Systeme
- Datenbankschemas
- SharePoint On-Premises-Accounts (SharePoint Server)
- NFS- oder CIFS-Dateifreigaben anderer Anbieter
- Objekt-Storage, der das Simple Storage Service (S3)-Protokoll verwendet

Für besondere Situationen, in denen Sie eine sehr sichere BlueXP-Installation benötigen, aber auch lokale Daten von OneDrive-Konten oder SharePoint Online-Konten scannen möchten, können Sie das Data Sense Offline-Installationsprogramm verwenden und einigen ausgewählten Endpunkten den Internet-Zugriff gewähren. Siehe [Spezielle Anforderungen für SharePoint und OneDrive](#) Entsprechende Details.

Derzeit werden die Konten von Cloud Volumes ONTAP, Azure NetApp Files, FSX für ONTAP, AWS S3 oder Google Drive nicht unterstützt, wenn Daten Sense in einer dunklen Site eingesetzt wird.

Einschränkungen

Die meisten Funktionen von Data Sense funktionieren, wenn sie in einer Site ohne Internetzugang bereitgestellt werden. Bestimmte Funktionen, für die ein Internetzugang erforderlich ist, werden jedoch nicht unterstützt, z. B.:

- Verwalten von Etiketten in Microsoft Azure Information Protection (AIP)
- Senden von E-Mail-Warnungen an BlueXP-Benutzer, wenn bestimmte kritische Richtlinien Ergebnisse liefern
- Festlegen von BlueXP-Rollen für unterschiedliche Benutzer (z. B. Account Admin oder Compliance Viewer)
- Kopieren und Synchronisieren von Quelldateien mit Cloud Sync
- Benutzerfeedback wird empfangen
- Automatisierte Software-Upgrades von BlueXP

Sowohl BlueXP Connector als auch Data Sense erfordern regelmäßige manuelle Upgrades, um neue Funktionen zu ermöglichen. Die Data Sense-Version finden Sie unten auf den Data Sense-UI-Seiten.

Prüfen Sie die ["Cloud Data Sense – Versionsinformationen"](#) Um sich die neuen Funktionen in jeder Version und deren Wunsch nach jenen Funktionen ansehen zu können. Anschließend können Sie die Schritte befolgen [Aktualisieren Sie Ihre Data Sense Software](#).

Schnellstart

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

1

Installieren Sie den BlueXP-Anschluss

Wenn Sie noch keinen Connector an Ihrem Offline-Standort installiert haben, ["Den Stecker einsetzen"](#) Jetzt auf einem Linux-Host.

2

Prüfen Sie die Voraussetzungen für den Data Sense

Stellen Sie sicher, dass Ihr Linux-System die erfüllt [Host-Anforderungen erfüllt](#), Dass es alle erforderliche Software installiert hat, und dass Ihre Offline-Umgebung die erforderlichen erfüllt [Berechtigungen und Konnektivität](#).

3

Laden Sie Data Sense herunter und implementieren Sie es

Laden Sie die Cloud Data Sense Software von der NetApp Support Site herunter, und kopieren Sie die Installer-Datei auf den Linux-Host, den Sie verwenden möchten. Starten Sie dann den Installationsassistenten, und befolgen Sie die Anweisungen zur Bereitstellung der Cloud Data Sense Instanz.

4

Abonnieren Sie den Cloud Data Sense Service

Die ersten 1 TB an Daten, die Cloud Data Sense in BlueXP scannt, sind kostenlos. Nach diesem Zeitpunkt ist eine BYOL-Lizenz von NetApp erforderlich, um das Scannen von Daten fortzusetzen.

Installieren Sie den BlueXP-Anschluss

Wenn Sie noch keinen BlueXP Connector an Ihrem lokalen Offline-Standort installiert haben, ["Den Stecker einsetzen"](#) Auf einem Linux-Host in Ihrer Offline-Site.

Bereiten Sie das Linux-Hostsystem vor

Data Sense Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Softwareanforderungen usw. erfüllt. Data Sense wird auf einem Host, der für andere Anwendungen freigegeben ist, nicht unterstützt - der Host muss ein dedizierter Host sein.

- **Betriebssystem:** Red hat Enterprise Linux oder CentOS Versionen 8.0 bis 8.7
 - Version 7.8 oder 7.9 kann verwendet werden, aber die Linux-Kernel-Version muss 4.0 oder höher sein
 - Das Betriebssystem muss in der Lage sein, die Docker Engine zu installieren
- **Disk:** SSD mit 500 gib erhältlich auf /, oder
 - 100 gib verfügbar auf /opt
 - 400 gib verfügbar auf /var

- 5 gib auf /tmp
- **RAM:** 64 GB (Swap-Speicher muss auf dem Host deaktiviert sein)
- **CPU:** 16 Kerne

Beachten Sie, dass Sie Daten Sense auf einem System mit weniger CPUs und weniger RAM implementieren können, es gibt jedoch Einschränkungen bei der Verwendung dieser Systeme. Siehe ["Verwenden eines kleineren Instanztyps"](#) Entsprechende Details.

- **Zusätzliche Software:** Sie müssen die folgende Software auf dem Host installieren, bevor Sie Data Sense installieren:
 - Docker Engine Version 19 oder höher. ["Installationsanweisungen anzeigen"](#).
 - Python 3 Version 3.6 oder höher. ["Installationsanweisungen anzeigen"](#).
- **Firewalld Überlegungen:** Wenn Sie planen zu verwenden firewalld, Wir empfehlen, dass Sie es aktivieren, bevor Sie Data Sense installieren. Führen Sie die folgenden Befehle zum Konfigurieren aus firewalld Damit es mit Data Sense kompatibel ist:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-service=mysql
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=555/tcp
firewall-cmd --permanent --add-port=3306/tcp
firewall-cmd --reload
```

Wenn Sie aktivieren firewalld Nach der Installation von Data Sense müssen Sie den Docker neu starten.



Die IP-Adresse des Data Sense Hostsystems kann nach der Installation nicht geändert werden.

Überprüfen Sie die Voraussetzungen für BlueXP und Data Sense

Prüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie Cloud Data Sense implementieren.

- Stellen Sie sicher, dass der Connector über die Berechtigungen zum Bereitstellen von Ressourcen verfügt und Sicherheitsgruppen für die Cloud Data Sense Instanz erstellt. Die neuesten BlueXP-Berechtigungen finden Sie in ["Die von NetApp bereitgestellten Richtlinien"](#).
- Sorgen Sie dafür, dass Cloud Data Sense ausgeführt wird. Die Cloud Data Sense Instanz muss kontinuierlich ausgeführt werden, um Ihre Daten kontinuierlich zu scannen.
- Stellen Sie sicher, dass Webbrowser mit Cloud Data Sense verbunden ist. Wenn Cloud Data Sense aktiviert ist, stellen Sie sicher, dass Benutzer von einem Host, der über eine Verbindung zur Data Sense Instanz verfügt, auf die BlueXP-Schnittstelle zugreifen.

Die Instanz Data Sense verwendet eine private IP-Adresse, um sicherzustellen, dass die indizierten Daten für andere nicht zugänglich sind. Daher muss der Webbrowser, den Sie für den Zugriff auf BlueXP

verwenden, über eine Verbindung mit dieser privaten IP-Adresse verfügen. Diese Verbindung kann von einem Host stammen, der sich im gleichen Netzwerk wie die Data Sense Instanz befindet.

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

Sie müssen sicherstellen, dass alle erforderlichen Ports für die Kommunikation zwischen Connector, Data Sense, Active Directory und Ihren Datenquellen offen sind.

| Verbindungstyp | Ports | Beschreibung |
|----------------------------------|--|--|
| Connector <> Data Sense | 8080 (TCP), 443 (TCP) und 80 | Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über Port 443 zu und aus der Instanz Data Sense zulassen. Stellen Sie sicher, dass Port 8080 geöffnet ist, damit Sie den Installationsfortschritt in BlueXP sehen können. |
| Connector <> ONTAP-Cluster (NAS) | 443 (TCP) | <p>BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen:</p> <ul style="list-style-type: none"> • Der Connector-Host muss ausgehenden HTTPS-Zugriff über Port 443 ermöglichen. Wenn sich der Connector in der Cloud befindet, ist die gesamte ausgehende Kommunikation durch die vordefinierte Sicherheitsgruppe zulässig. • Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen. Die standardmäßige "mgmt"-Firewall-Richtlinie ermöglicht eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert haben oder wenn Sie eine eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff über den Connector-Host aktivieren. |
| Datensense <> ONTAP-Cluster | <ul style="list-style-type: none"> • Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS - 139 (TCP\UDP) und 445 (TCP\UDP) | <p>Für den Datensense ist eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP-Subnetz oder On-Prem ONTAP-System erforderlich. Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen aus der Datensense-Instanz zulassen.</p> <p>Stellen Sie sicher, dass diese Ports für die Data Sense-Instanz offen sind:</p> <ul style="list-style-type: none"> • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 <p>NFS-Volume-Exportrichtlinien müssen den Zugriff aus der Data Sense Instanz zulassen.</p> |

| Verbindungstyp | Ports | Beschreibung |
|-------------------------------|---|---|
| Datensinn <> Active Directory | 389 (TCP & UDP), 636 (TCP), 3268 (TCP) UND 3269 (TCP) | <p>Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben. Darüber hinaus benötigt Data Sense Active Directory-Anmeldeinformationen zum Scannen von CIFS-Volumes.</p> <p>Sie müssen über die folgenden Informationen für das Active Directory verfügen:</p> <ul style="list-style-type: none"> • DNS-Server-IP-Adresse oder mehrere IP-Adressen • Benutzername und Kennwort für den Server • Domain-Name (Active Directory-Name) • Ob Sie Secure LDAP (LDAPS) verwenden oder nicht • LDAP-Server-Port (normalerweise 389 für LDAP und 636 für sicheres LDAP) |

Wenn Sie mehrere Data Sense Hosts verwenden, um zusätzliche Verarbeitungsleistung für das Scannen Ihrer Datenquellen bereitzustellen, müssen Sie zusätzliche Ports/Protokolle aktivieren. "[Siehe zusätzliche Anschlussanforderungen](#)".

Spezielle Anforderungen für SharePoint und OneDrive

Wenn BlueXP und Data Sense in einer Site ohne Internetzugang bereitgestellt werden, können Sie Dateien in SharePoint Online- und OneDrive-Konten scannen, indem Sie für einige ausgewählte Endpunkte den Internetzugriff gewähren.

Lokal installierte SharePoint-Konten vor Ort können ohne Internetzugang gescannt werden.

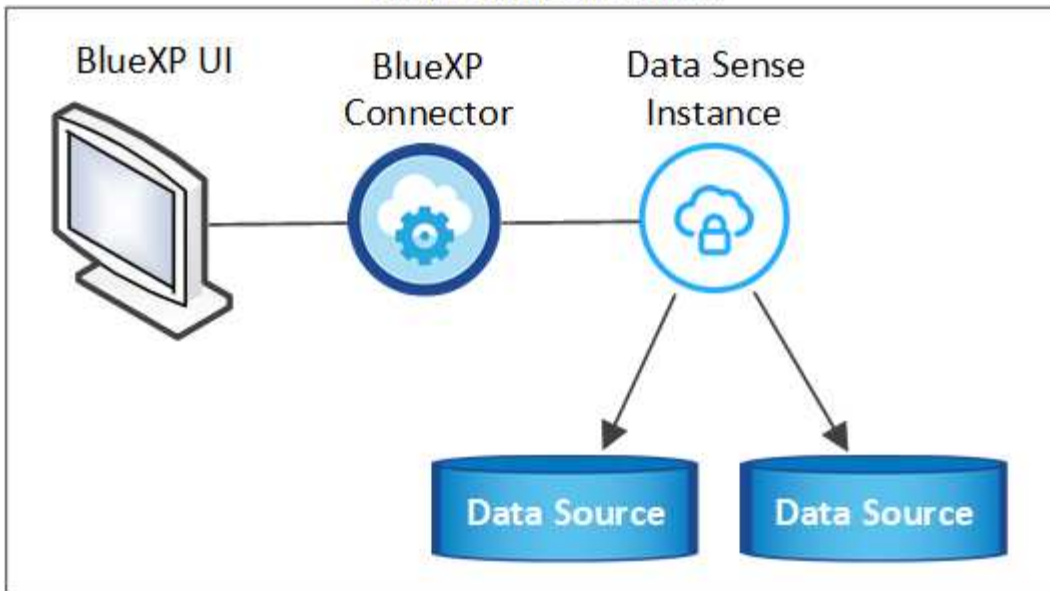
| Endpunkte | Zweck |
|---|--|
| \login.microsoft.com \graph.microsoft.com | Kommunikation mit Microsoft-Servern zur Anmeldung beim ausgewählten Online-Dienst. |
| https://api.bluexp.netapp.com | Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts |

Der Zugriff auf *api.bluexp.netapp.com* ist nur während der ersten Verbindung zu diesen externen Diensten erforderlich.

Sinnvolle Implementierung Von Daten

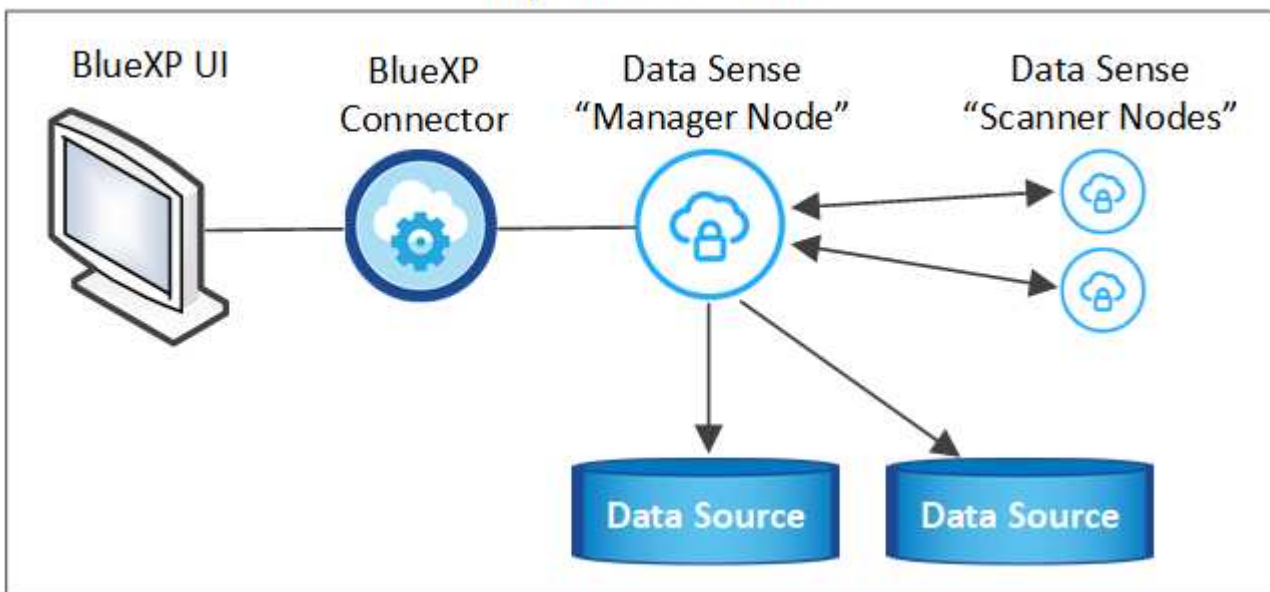
Für typische Konfigurationen installieren Sie die Software auf einem einzigen Host-System. "[Siehe diese Schritte hier](#)".

On-premises location



Bei sehr großen Konfigurationen, bei denen Sie Petabyte an Daten scannen, können Sie mehrere Hosts einschließen, um zusätzliche Verarbeitungsleistung zu schaffen. ["Siehe diese Schritte hier"](#).

On-premises location



Installation mit einem Host für typische Konfigurationen

Führen Sie diese Schritte aus, wenn Sie die Data Sense Software auf einem einzelnen lokalen Host in einer Offline-Umgebung installieren.

Was Sie benötigen

- Vergewissern Sie sich, dass Ihr Linux-System die erfüllt [Host-Anforderungen erfüllt](#).
- Vergewissern Sie sich, dass Sie die beiden erforderlichen Softwarepakete (Docker Engine und Python 3) installiert haben.
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.

- Vergewissern Sie sich, dass die erforderliche Offline-Umgebung erfüllt ist [Berechtigungen und Konnektivität](#).

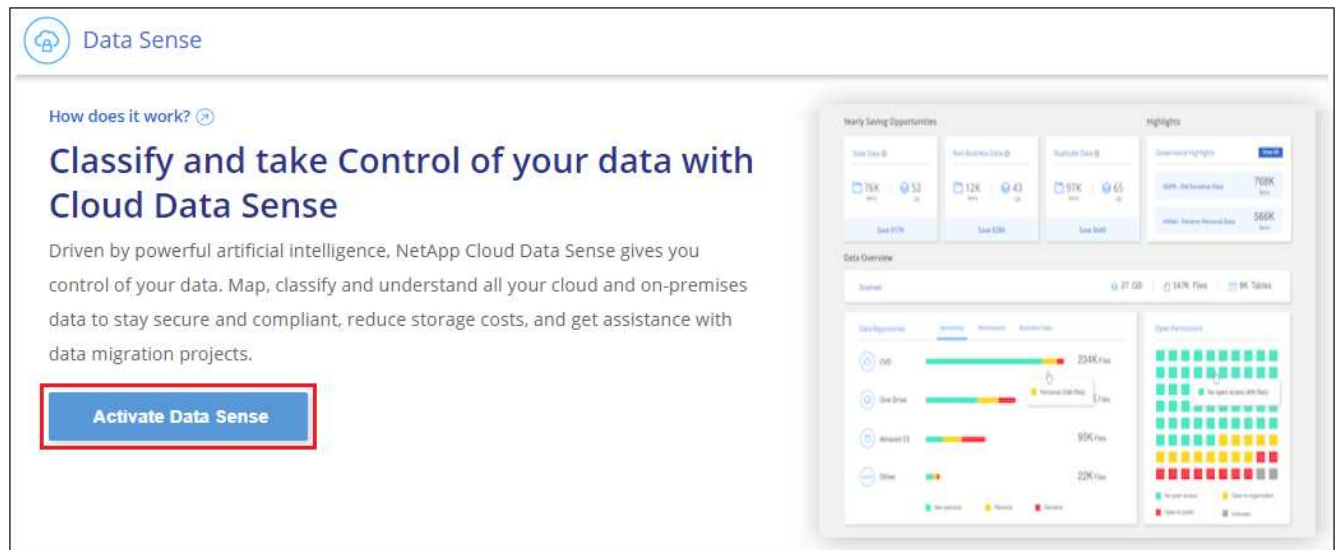
Schritte

1. Laden Sie auf einem internetkonfigurierten System die Cloud Data Sense-Software aus dem herunter ["NetApp Support Website"](#). Die ausgewählte Datei heißt **DataSense-offline-Bundle-<Version>.tar.gz**.
2. Kopieren Sie das Installationspaket auf den Linux-Host, den Sie für die dunkle Seite verwenden möchten.
3. Entpacken Sie das Installationspaket auf dem Hostcomputer, z. B.:

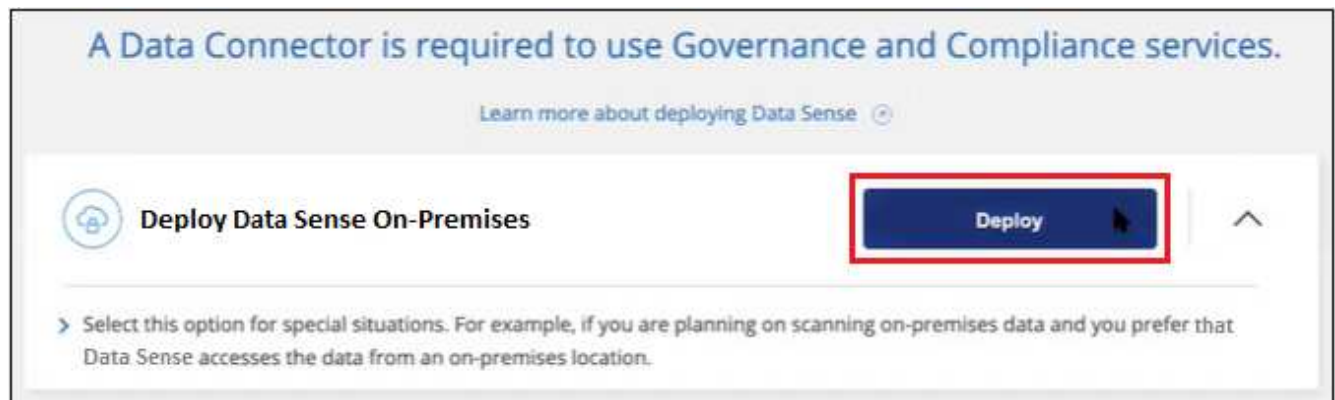
```
tar -xzf DataSense-offline-bundle-v1.16.1.tar.gz
```

Diese extrahiert erforderliche Software und die eigentliche Installationsdatei **DATASENSE-INSTALLER-V1.16.1.tar.gz**.

4. Starten Sie BlueXP, und wählen Sie **Governance > Klassifizierung**.
5. Klicken Sie Auf **Datensense Aktivieren**.



6. Klicken Sie auf **Bereitstellen**, um den Assistenten für die lokale Bereitstellung zu starten.



7. Kopieren Sie im Dialogfeld *Deploy Data Sense on premise* den angegebenen Befehl und fügen Sie ihn in eine Textdatei ein, damit Sie ihn später verwenden können, und klicken Sie auf **Schließen**. Beispiel:


```
sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite
```

8. Entpacken Sie die Installationsdatei auf dem Host-Rechner, z. B.:

```
tar -xzf DATASENSE-INSTALLER-V1.16.1.tar.gz
```

9. Wenn Sie vom Installationsprogramm dazu aufgefordert werden, können Sie die erforderlichen Werte in eine Reihe von Eingabeaufforderungen eingeben oder Sie können die erforderlichen Parameter als Befehlszeilenargumente dem Installer angeben:

Beachten Sie, dass das Installationsprogramm eine Vorprüfung durchführt, um sicherzustellen, dass Ihre System- und Netzwerkanforderungen für eine erfolgreiche Installation erfüllt werden.

| Geben Sie die Parameter wie aufgefordert ein: | Geben Sie den vollständigen Befehl ein: |
|---|---|
| <p>a. Fügen Sie die Informationen ein, die Sie aus Schritt 7 kopiert haben:</p> <pre>sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --darksite</pre> <p>b. Geben Sie die IP-Adresse oder den Hostnamen des Data Sense Host-Rechners ein, damit auf diese durch die Connector-Instanz zugegriffen werden kann.</p> <p>c. Geben Sie die IP-Adresse oder den Hostnamen des BlueXP Connector-Hostcomputers ein, damit die Instanz Data Sense darauf zugreifen kann.</p> | <p>Alternativ können Sie den gesamten Befehl vorab erstellen und die erforderlichen Host-Parameter bereitstellen:</p> <pre>sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite</pre> |

Variablenwerte:

- *Account_id* = NetApp Konto-ID
- *Agent_id* = Konnektor-ID
- *Token* = jwt-Benutzer-Token
- *ds_Host* = IP-Adresse oder Hostname des Data Sense Linux-Systems.
- *Cm_Host* = IP-Adresse oder Hostname des BlueXP Connector-Systems.

Ergebnis

Das Data Sense Installationsprogramm installiert Pakete, registriert die Installation und installiert Data Sense. Die Installation dauert 10 bis 20 Minuten.

Wenn zwischen dem Host-Rechner und der Connector-Instanz eine Verbindung über Port 8080 besteht, sehen Sie den Installationsfortschritt auf der Registerkarte Data Sense in BlueXP.

Nächste Schritte

Auf der Konfigurationsseite können Sie das lokale auswählen ["ONTAP-Cluster vor Ort"](#) Und ["Datenbanken"](#) Die Sie scannen möchten.

Das können Sie auch ["Byol-Lizenzierung für Cloud-Data Sense einrichten"](#) Derzeit auf der Seite „Digital Wallet“. Sie werden erst berechnet, wenn die Datenmenge mehr als 1 TB beträgt.

Installation mit mehreren Hosts für große Konfigurationen

Bei sehr großen Konfigurationen, bei denen Sie Petabyte an Daten scannen, können Sie mehrere Hosts einschließen, um zusätzliche Verarbeitungsleistung zu schaffen. Bei der Verwendung mehrerer Hostsysteme wird das primäre System als *Manager-Node* bezeichnet, und die zusätzlichen Systeme, die zusätzliche Rechenleistung bieten, heißen *Scanner-Nodes*.

Führen Sie die folgenden Schritte aus, wenn Sie Data Sense Software auf mehreren lokalen Hosts in einer Offline-Umgebung installieren.

Was Sie benötigen

- Stellen Sie sicher, dass alle Linux-Systeme für den Manager- und Scanner-Knoten den entsprechen [Host-Anforderungen erfüllt](#).
- Vergewissern Sie sich, dass Sie die beiden erforderlichen Softwarepakete (Docker Engine und Python 3) installiert haben.
- Stellen Sie sicher, dass Sie auf den Linux-Systemen über Root-Rechte verfügen.
- Vergewissern Sie sich, dass die erforderliche Offline-Umgebung erfüllt ist [Berechtigungen und Konnektivität](#).
- Sie müssen über die IP-Adressen der zu verwendenden Scanner-Knoten-Hosts verfügen.
- Die folgenden Ports und Protokolle müssen auf allen Hosts aktiviert sein:

| Port | Protokolle | Beschreibung |
|------|------------|--|
| 2377 | TCP | Cluster-Management-Kommunikation |
| 7946 | TCP, UDP | Kommunikation zwischen den Knoten |
| 4789 | UDP | Overlay-Netzwerk-Traffic |
| 50 | ESP | Verschlüsselter ESP-Datenverkehr (IPsec Overlay Network) |
| 111 | TCP, UDP | NFS-Server für die gemeinsame Nutzung von Dateien zwischen den Hosts (benötigt von jedem Scanner-Knoten zu Manager-Knoten) |
| 2049 | TCP, UDP | NFS-Server für die gemeinsame Nutzung von Dateien zwischen den Hosts (benötigt von jedem Scanner-Knoten zu Manager-Knoten) |

Schritte

1. Befolgen Sie die Schritte 1 bis 8 vom "[Installation über einen Host](#)" Auf dem Knoten Manager.
2. Wie in Schritt 9 gezeigt, können Sie bei Aufforderung durch das Installationsprogramm die erforderlichen Werte in eine Reihe von Eingabeaufforderungen eingeben oder die erforderlichen Parameter als Befehlszeilenargumente für das Installationsprogramm bereitstellen.

Zusätzlich zu den Variablen, die für eine Installation mit einem Host verfügbar sind, wird eine neue Option **-n <Node_ip>** verwendet, um die IP-Adressen der Scannerknoten anzugeben. Mehrere Knoten-IPs werden durch Komma getrennt.

Mit diesem Befehl werden beispielsweise 3 Scannerknoten hinzugefügt:

```
sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host>
--manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no-proxy
--darksite
```

3. Bevor die Installation des Manager-Node abgeschlossen ist, wird in einem Dialogfeld der für die Scanner-Knoten erforderliche Installationsbefehl angezeigt. Kopieren Sie den Befehl und speichern Sie ihn in einer Textdatei. Beispiel:

```
sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212
```

4. Auf * jedem Scanner-Knoten-Host:
 - a. Kopieren Sie die Data Sense Installer-Datei (**DATASENSE-INSTALLER-<Version>.tar.gz**) auf den Host-Rechner.
 - b. Entpacken Sie die Installationsdatei.
 - c. Fügen Sie den Befehl ein, den Sie in Schritt 3 kopiert haben, und führen Sie ihn aus.

Wenn die Installation auf allen Scanner-Knoten abgeschlossen ist und sie mit dem Manager-Knoten verbunden wurden, wird auch die Installation des Manager-Knotens abgeschlossen.

Ergebnis

Das Installationsprogramm von Cloud Data Sense beendet die Installation von Paketen und registriert die Installation. Die Installation dauert 15 bis 25 Minuten.

Nächste Schritte

Auf der Konfigurationsseite können Sie das lokale auswählen ["ONTAP-Cluster vor Ort"](#) Und lokal ["Datenbanken"](#) Die Sie scannen möchten.

Das können Sie auch ["Byol-Lizenzierung für Cloud-Data Sense einrichten"](#) Derzeit auf der Seite „Digital Wallet“. Sie werden erst berechnet, wenn die Datenmenge mehr als 1 TB beträgt.

Upgrade von Data Sense Software

Da die Software Data Sense regelmäßig mit neuen Funktionen aktualisiert wird, sollten Sie sich regelmäßig auf eine neue Version verlassen, um sicherzustellen, dass Sie die neueste Software und Funktionen verwenden. Sie müssen die Software Data Sense manuell aktualisieren, da keine Internetverbindung vorhanden ist, um das Upgrade automatisch durchzuführen.

Bevor Sie beginnen

- Die Software Data Sense kann jeweils eine Hauptversion aktualisiert werden. Wenn beispielsweise Version 1.15.x installiert ist, können Sie nur auf 1.16.x aktualisieren Wenn Sie einige Hauptversionen hinter sich haben, müssen Sie die Software mehrmals aktualisieren.
- Stellen Sie sicher, dass Ihre On-Prem Connector-Software auf die neueste verfügbare Version aktualisiert wurde. ["Siehe die Schritte zur Aktualisierung des Connectors"](#).

Schritte

1. Laden Sie auf einem internetkonfigurierten System die Cloud Data Sense-Software aus dem herunter ["NetApp Support Website"](#). Die ausgewählte Datei heißt **DataSense-offline-Bundle-<Version>.tar.gz**.
2. Kopieren Sie das Software-Bundle auf den Linux-Host, auf dem Data Sense im dunklen Ort installiert ist.
3. Entpacken Sie das Software-Bundle auf dem Host-Rechner, zum Beispiel:

```
tar -xvf DataSense-offline-bundle-v1.16.1.tar.gz
```

Diese extrahiert die Installationsdatei **DATASENSE-INSTALLER-V1.16.1.tar.gz**.

4. Entpacken Sie die Installationsdatei auf dem Host-Rechner, z. B.:

```
tar -xzf DATASENSE-INSTALLER-V1.16.1.tar.gz
```

Dadurch wird das Upgrade-Skript **Start_darksite_Upgrade.sh** und jede erforderliche Software von Drittanbietern extrahiert.

5. Führen Sie das Upgrade-Skript auf dem Hostcomputer aus, z. B.:

```
start_darksite_upgrade.sh
```

Ergebnis

Die Software Data Sense wird auf Ihrem Host aktualisiert. Die Aktualisierung kann 5 bis 10 Minuten dauern.

Beachten Sie, dass auf den Scanner-Knoten kein Upgrade erforderlich ist, wenn Sie Data Sense auf mehreren Hostsystemen zum Scannen sehr großer Konfigurationen implementiert haben.

Sie können überprüfen, ob die Software aktualisiert wurde, indem Sie die Version unten auf den Seiten der Data Sense-Benutzeroberfläche prüfen.

Aktivieren Sie das Scannen Ihrer Datenquellen

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

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

Schnellstart

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

1

Ermitteln Sie die Datenquellen, die Sie scannen möchten

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

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

2

Implementieren Sie die Cloud Data Sense Instanz

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

3

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

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

4

Zugriff auf Volumes sicherstellen

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

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

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

5

Verwalten Sie die Volumes, die Sie scannen möchten

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

Ermitteln der Datenquellen, die gescannt werden sollen

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

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

Bereitstellen der Cloud Data Sense Instanz

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

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

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

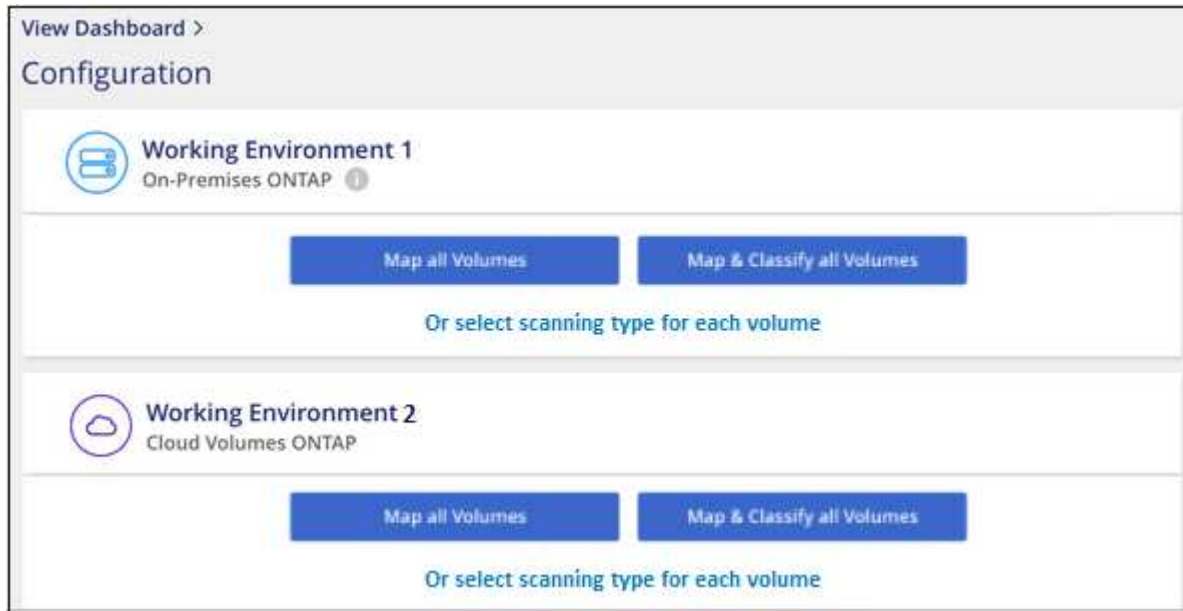
Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine

Internetverbindung verfügt.

Cloud-Daten sinnvoll in Ihren Arbeitsumgebungen einsetzen

Sie können Cloud Data Sense auf Cloud Volumes ONTAP Systemen in jedem unterstützten Cloud-Provider und On-Premises ONTAP Clustern aktivieren.

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



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

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

3. Klicken Sie im Bestätigungsdialogfeld auf **Genehmigen**, damit Data Sense Ihre Volumes scannen kann.

Ergebnis

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

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

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

Schritte

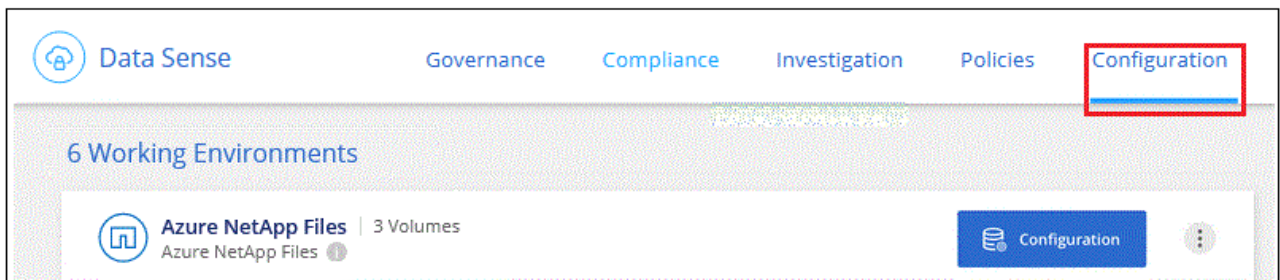
1. Vergewissern Sie sich, dass es eine Netzwerkverbindung zwischen der Cloud Data Sense Instanz und

jedem Netzwerk gibt, das Volumes für Cloud Volumes ONTAP oder lokale ONTAP Cluster enthält.

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

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

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

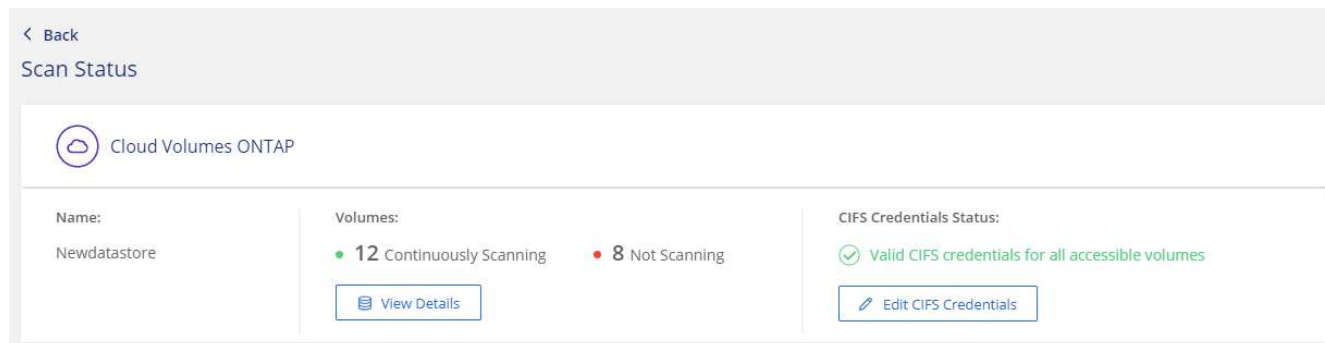


- b. Klicken Sie für jede Arbeitsumgebung auf **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Data Sense für den Zugriff auf CIFS-Volumes auf dem System benötigt.

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

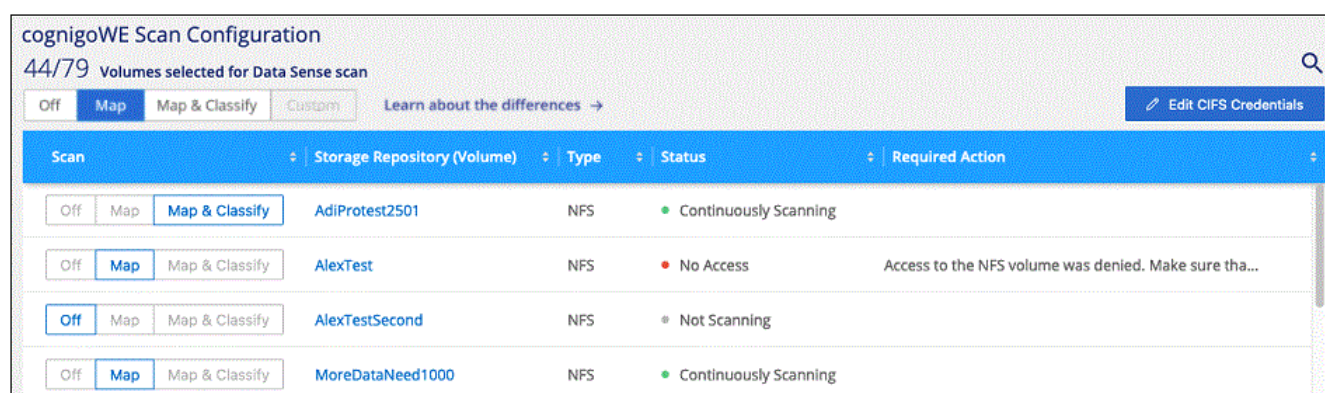
Wenn Sie sicherstellen möchten, dass Ihre Dateien „letzte Zugriffszeiten“ durch Data Sense Klassifizierungsscans unverändert bleiben, empfehlen wir dem Benutzer die Berechtigung Schreibattribute zu besitzen. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete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

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



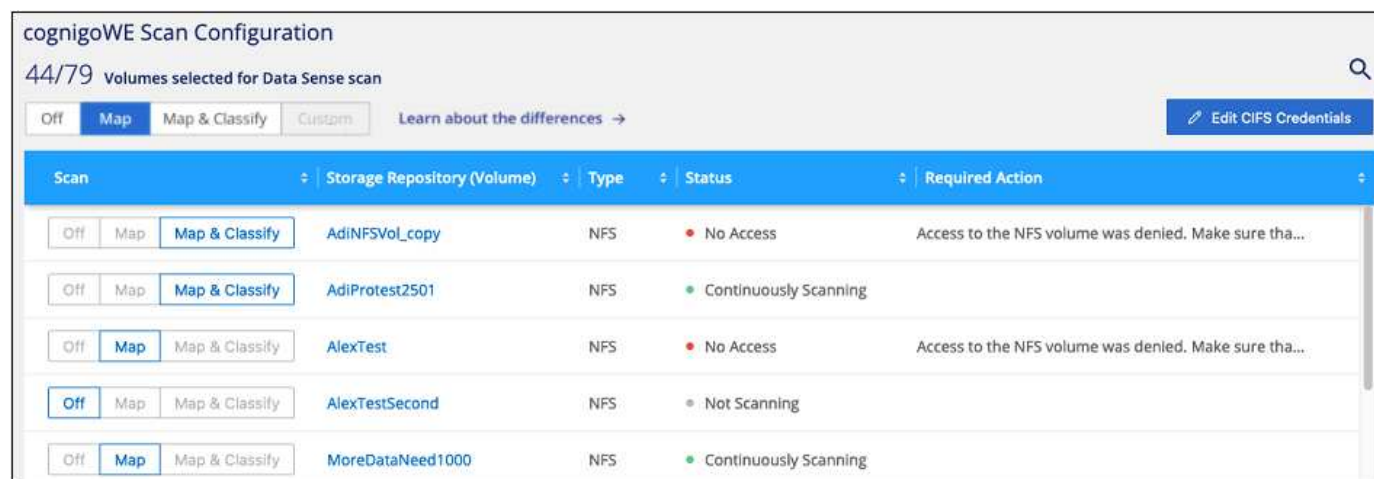
- Klicken Sie auf der Seite *Configuration* auf **Details anzeigen**, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und eventuelle Fehler zu beheben.

Das folgende Bild zeigt beispielsweise vier Volumes, von denen Cloud Data Sense aufgrund von Netzwerkverbindungsproblemen zwischen der Data Sense Instanz und dem Volume nicht scannen kann.



Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

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



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



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

Scannen von Datensicherungs-Volumes

Standardmäßig werden Datensicherungs-Volumes nicht gescannt, weil sie nicht extern zugänglich sind und Cloud Data Sense nicht auf sie zugreifen kann. Es handelt sich dabei um Ziel-Volumes für SnapMirror Vorgänge von einem ONTAP System vor Ort oder von einem Cloud Volumes ONTAP System aus.

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

The screenshot shows the 'Working Environment Name' Configuration page. At the top, it says '22/28 Volumes selected for compliance scan'. There are buttons for 'Off', 'Map', 'Map & Classify', and 'Custom'. A red box highlights the 'Enable Access to DP Volumes' button. Below the buttons is a table with columns: Scan, Storage Repository (Volume), Type, Status, and Required Action.

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

Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

1. Klicken Sie oben auf der Seite auf **Zugriff auf DP-Volumes aktivieren**.
2. Überprüfen Sie die Bestätigungsmeldung und klicken Sie erneut auf **Zugriff auf DP-Volumes**.
 - Volumes, die anfangs als NFS Volumes im ONTAP Quellsystem erstellt wurden, sind aktiviert.
 - Für Volumes, die ursprünglich als CIFS Volumes im Quell-ONTAP System erstellt wurden, müssen Sie die CIFS-Anmeldeinformationen eingeben, um diese DP-Volumes zu scannen. Wenn Sie bereits Active Directory-Anmeldeinformationen eingegeben haben, damit Cloud Data Sense CIFS-Volumes scannen

kann, können Sie diese Anmeldedaten verwenden oder einen anderen Satz von Admin-Anmeldeinformationen angeben.

The image shows two versions of the 'Provide Active Directory Credentials' dialog box. In the left version, the radio button for 'Use existing CIFS Scanning Credentials (user1@domain2)' is selected and highlighted with a red rectangle. In the right version, the radio button for 'Use Custom Credentials' is selected and highlighted with a red rectangle. Both versions include input fields for Username, Password, Active Directory Domain, and DNS IP Address. Below these fields is a text block explaining that DP Volumes created from a SnapMirror relationship do not allow external access by default, and that continuing will create NFS shares from DP Volumes which have been activated for Data Sense. At the bottom of each dialog are two buttons: 'Enable Access to DP Volumes' and 'Cancel'.

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

Ergebnis

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

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



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

Erste Schritte mit Cloud Data Sense für Azure NetApp Files

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

Schnellstart

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

1

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

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

2

Implementieren Sie die Cloud Data Sense Instanz

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

3

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

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

4

Zugriff auf Volumes sicherstellen

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

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

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

5

Verwalten Sie die Volumes, die Sie scannen möchten

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

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

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

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

Bereitstellen der Cloud Data Sense Instanz

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

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

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

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

Cloud-Daten sinnvoll in Ihren Arbeitsumgebungen einsetzen

Sie können den Einsatz von Cloud-Daten in Ihren Azure NetApp Files Volumes sinnvoll aktivieren.

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



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

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

3. Klicken Sie im Bestätigungsdialogfeld auf **Genehmigen**, damit Data Sense Ihre Volumes scannen kann.

Ergebnis

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

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

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

Schritte

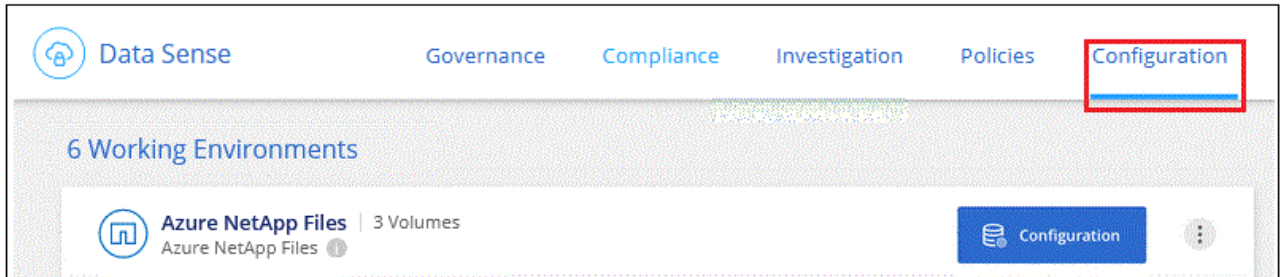
1. Stellen Sie sicher, dass es eine Netzwerkverbindung zwischen Cloud Data Sense Instanz und jedem Netzwerk gibt, das Volumes für Azure NetApp Files enthält.



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

2. Stellen Sie sicher, dass die folgenden Ports für die Data Sense-Instanz offen sind:
 - Für NFS – die Ports 111 und 2049.
 - Für CIFS – die Ports 139 und 445.
3. Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Sense Instanz enthalten, damit sie auf die Daten auf jedem Volume zugreifen können.
4. Wenn Sie CIFS verwenden, geben Sie Data Sense mit Active Directory Anmeldeinformationen ein, damit CIFS Volumes gescannt werden können.

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

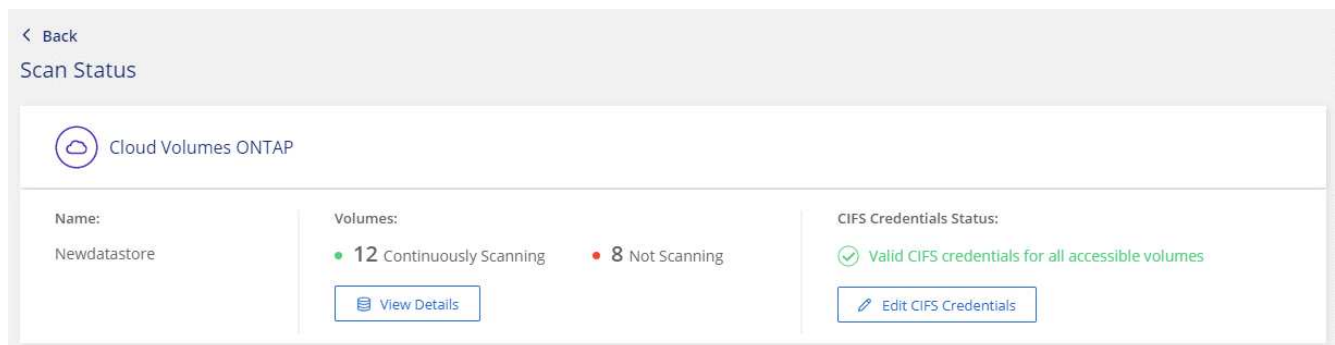


- b. Klicken Sie für jede Arbeitsumgebung auf **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Data Sense für den Zugriff auf CIFS-Volumes auf dem System benötigt.

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

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

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



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

Das folgende Bild zeigt beispielsweise vier Volumes, von denen Cloud Data Sense aufgrund von Netzwerkverbindungsproblemen zwischen der Data Sense Instanz und dem Volume nicht scannen kann.

| cognitoWE Scan Configuration | | | | |
|--|-----------------------------|------|-----------------------|---|
| 44/79 Volumes selected for Data Sense scan | | | | |
| <div> Off Map Map & Classify Custom </div> <div>Learn about the differences →</div> <div>Edit CIFS Credentials</div> | | | | |
| Scan | Storage Repository (Volume) | Type | Status | Required Action |
| Off Map Map & Classify | AdiProtest2501 | NFS | Continuously Scanning | |
| Off Map Map & Classify | AlexTest | NFS | No Access | Access to the NFS volume was denied. Make sure tha... |
| Off Map Map & Classify | AlexTestSecond | NFS | Not Scanning | |
| Off Map Map & Classify | MoreDataNeed1000 | NFS | Continuously Scanning | |

Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

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

| cognitoWE Scan Configuration | | | | |
|--|-----------------------------|------|-----------------------|---|
| 44/79 Volumes selected for Data Sense scan | | | | |
| <div> Off Map Map & Classify Custom </div> <div>Learn about the differences →</div> <div>Edit CIFS Credentials</div> | | | | |
| Scan | Storage Repository (Volume) | Type | Status | Required Action |
| Off Map Map & Classify | AdiNFSVol_copy | NFS | No Access | Access to the NFS volume was denied. Make sure tha... |
| Off Map Map & Classify | AdiProtest2501 | NFS | Continuously Scanning | |
| Off Map Map & Classify | AlexTest | NFS | No Access | Access to the NFS volume was denied. Make sure tha... |
| Off Map Map & Classify | AlexTestSecond | NFS | Not Scanning | |
| Off Map Map & Classify | MoreDataNeed1000 | NFS | Continuously Scanning | |

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



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

Erste Schritte mit Cloud Data Sense für Amazon FSX für ONTAP

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

Bevor Sie beginnen

- Für die Implementierung und das Management von Data Sense benötigen Sie einen aktiven Connector in AWS.
- Die Sicherheitsgruppe, die Sie beim Erstellen der Arbeitsumgebung ausgewählt haben, muss Datenverkehr aus der Instanz Cloud Data Sense zulassen. Sie können die zugehörige Sicherheitsgruppe mithilfe der ENI finden, die mit dem FSX für ONTAP-Dateisystem verbunden ist, und es mit der AWS-Verwaltungskonsolle bearbeiten.

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

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

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

Schnellstart

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

1

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

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

2

Implementieren Sie die Cloud Data Sense Instanz

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

3

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

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

4

Zugriff auf Volumes sicherstellen

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

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

5

Verwalten Sie die Volumes, die Sie scannen möchten

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

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

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

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

Bereitstellen der Cloud Data Sense Instanz

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

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

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

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

Cloud-Daten sinnvoll in Ihren Arbeitsumgebungen einsetzen

Sie können Cloud Data Sense für FSX für ONTAP Volumes aktivieren.


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

Filter by:

S3

FSx

[Clear filters](#)


mjulia
Amazon FSx for ONTAP

Map all Volumes

Map & Classify all Volumes

Or select scanning type per each volume

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

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

- Klicken Sie im Bestätigungsdialogfeld auf **Genehmigen**, damit Data Sense Ihre Volumes scannen kann.

Ergebnis

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

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

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

Sie müssen Data Sense mit CIFS Credentials bereitstellen, um auf CIFS Volumes zugreifen zu können.

Schritte

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

Das folgende Bild zeigt beispielsweise, dass ein Volume Cloud Data Sense aufgrund von Netzwerkverbindungsproblemen zwischen der Data Sense Instanz und dem Volume nicht scannen kann.

| Scan | Storage Repository (Volume) | Type | Status | Required Action |
|---|-----------------------------|------|--|---|
| <div>Off</div> <div>Map</div> <div>Map & Classify</div> | jrmclone | NFS | ● No Access | Check network connectivity between the Data Sense ... |

- Stellen Sie eine Netzwerkverbindung zwischen Cloud Data Sense Instanz und jedem Netzwerk, das Volumes für FSX für ONTAP enthält, sicher.



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

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

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

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

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

Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

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

cognitoWE Scan Configuration

44/79 Volumes selected for Data Sense scan

Off

Map

Map & Classify

Custom

Learn about the differences →

Edit CIFS Credentials

| Scan | Storage Repository (Volume) | Type | Status | Required Action |
|---|-----------------------------|------|-----------------------|---|
| <div>Off</div> <div>Map</div> <div>Map & Classify</div> | AdiNFSVol_copy | NFS | No Access | Access to the NFS volume was denied. Make sure tha... |
| <div>Off</div> <div>Map</div> <div>Map & Classify</div> | AdiProtest2501 | NFS | Continuously Scanning | |
| <div>Off</div> <div>Map</div> <div>Map & Classify</div> | AlexTest | NFS | No Access | Access to the NFS volume was denied. Make sure tha... |
| <div>Off</div> <div>Map</div> <div>Map & Classify</div> | AlexTestSecond | NFS | Not Scanning | |
| <div>Off</div> <div>Map</div> <div>Map & Classify</div> | MoreDataNeed1000 | NFS | Continuously Scanning | |

| | |
|--|--|
| An: | Tun Sie dies: |
| Aktivieren von mappinggeschützten Scans auf einem Volume | Klicken Sie im Volumenbereich auf Karte |

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



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

Scannen von Datensicherungs-Volumes

Standardmäßig werden Datensicherungs-Volumes nicht gescannt, weil sie nicht extern zugänglich sind und Cloud Data Sense nicht auf sie zugreifen kann. Dies sind die Ziel-Volumes für SnapMirror Vorgänge von einem FSX für ONTAP Filesystem.

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

The screenshot shows the 'Working Environment Name' Configuration page. At the top, it says '22/28 Volumes selected for compliance scan'. There are buttons for 'Off', 'Map', 'Map & Classify', and 'Custom'. A red box highlights the 'Enable Access to DP Volumes' button. Below the buttons is a table with the following data:

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

Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

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

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

Ergebnis

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

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



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

Erste Schritte mit Cloud Data Sense für Amazon S3

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

Schnellstart

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

1

S3-Anforderungen in Ihrer Cloud-Umgebung einrichten

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

2

Implementieren Sie die Cloud Data Sense Instanz

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

3

Aktivieren Sie Data Sense in Ihrer S3-Arbeitsumgebung

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

4

Wählen Sie die zu scannenden Buckets aus

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

Überprüfen der S3-Voraussetzungen

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

Einrichten einer IAM-Rolle für die Cloud Data Sense Instanz

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

```

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

```

Konnektivität von Cloud Data Sense zu Amazon S3

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

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

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

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



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

Bereitstellen der Cloud Data Sense Instanz

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

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

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

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

Aktivieren von Data Sense in Ihrer S3-Arbeitsumgebung

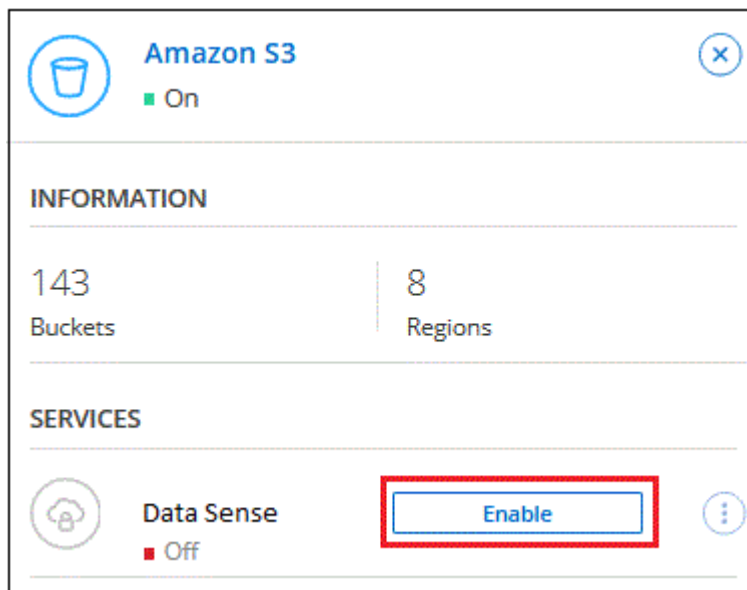
Aktivieren Sie Cloud Data Sense auf Amazon S3, nachdem Sie die Voraussetzungen überprüft haben.

Schritte

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



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



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

Assign an AWS IAM Role for Cloud Data Sense

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

Select IAM Role

occm

VPC Endpoint for Amazon S3 Required

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

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

Free for the 1st TB

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

Enable

Cancel

5. Klicken Sie Auf **Aktivieren**.



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

Ergebnis

BlueXP weist der Instanz die IAM-Rolle zu.

Aktivieren und Deaktivieren von Compliance-Scans auf S3-Buckets

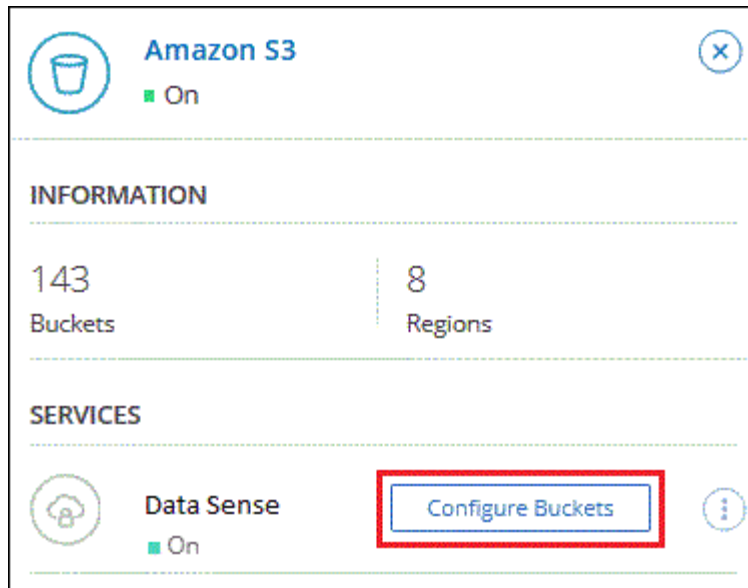
Nachdem BlueXP Cloud Data Sense in Amazon S3 aktiviert hat, müssen im nächsten Schritt die Buckets konfiguriert werden, die gescannt werden sollen.

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

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

Schritte

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



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

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

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

Ergebnis

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

Scannen von Buckets für weitere AWS Konten

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

Schritte

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

Create role




Select type of trusted entity

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

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

Specify accounts that can use this role

Account ID*

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

Gehen Sie wie folgt vor:

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

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

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

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

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

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



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

Ergebnis

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

Datenbankschemas werden gescannt

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

Sense zu beginnen.

Schnellstart

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

1

Datenbankvoraussetzungen prüfen

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

2

Implementieren Sie die Cloud Data Sense Instanz

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

3

Fügen Sie den Datenbankserver hinzu

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

4

Wählen Sie die Schemas aus

Wählen Sie die Schemata aus, die Sie scannen möchten.

Voraussetzungen prüfen

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

Unterstützte Datenbanken

Cloud Data Sense kann Schemen aus den folgenden Datenbanken scannen:

- Amazon Relational Database Service (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)



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

Datenbankanforderungen erfüllt

Jede Datenbank mit Anbindung an die Cloud Data Sense Instanz kann unabhängig vom gehosteten Speicherort gescannt werden. Sie benötigen lediglich die folgenden Informationen, um eine Verbindung zur Datenbank herzustellen:

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

Bei der Auswahl eines Benutzernamens und Kennworts ist es wichtig, einen zu wählen, der volle Lese-Berechtigungen für alle Schemas und Tabellen, die Sie scannen möchten. Es wird empfohlen, einen dedizierten Benutzer für das Cloud Data Sense System mit allen erforderlichen Berechtigungen zu erstellen.

Hinweis: für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

Bereitstellen der Cloud Data Sense Instanz

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

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

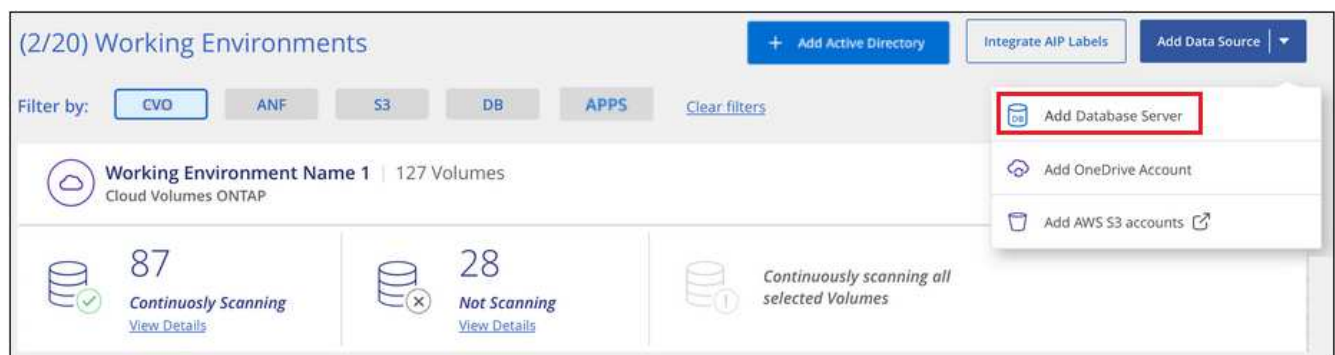
Wenn Sie Datenbankschemas scannen, die in einer dunklen Site installiert wurden, die keinen Internetzugang hat, müssen Sie dies tun ["Cloud Data Sense implementieren – auf demselben lokalen Standort ohne Internetzugang"](#). Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

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

Hinzufügen des Datenbankservers

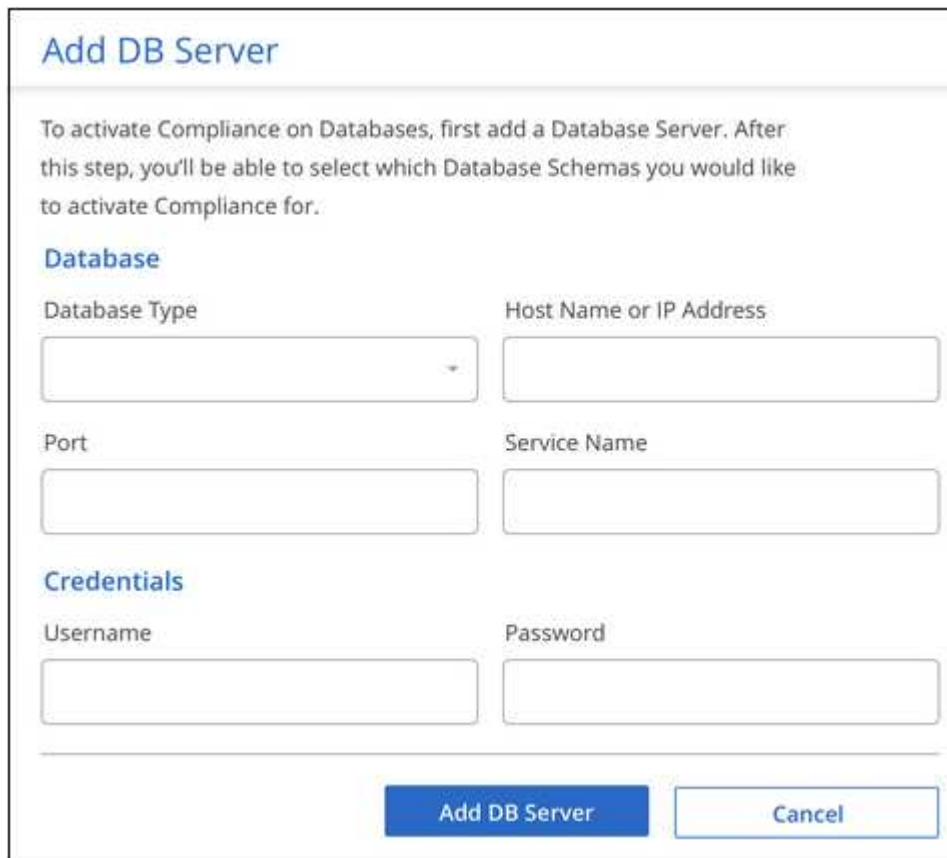
Fügen Sie den Datenbankserver dort hinzu, wo sich die Schemas befinden.

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



2. Geben Sie die erforderlichen Informationen ein, um den Datenbankserver zu identifizieren.
 - 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 Data Sense auf den Server zugreifen kann.
- e. Klicken Sie auf **DB-Server hinzufügen**.



Add DB Server

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

Database

Database Type: Host Name or IP Address:

Port: Service Name:

Credentials

Username: Password:

Add DB Server **Cancel**

Die Datenbank wird zur Liste der Arbeitsumgebungen hinzugefügt.

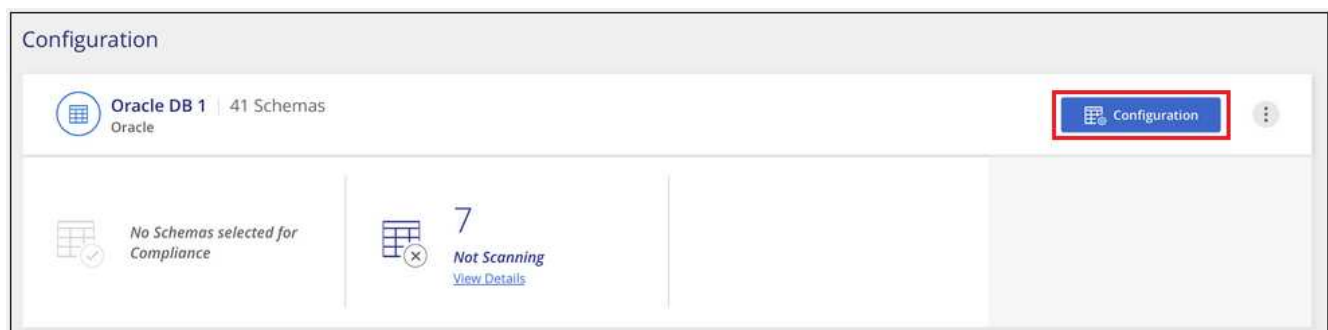
Aktivieren und Deaktivieren von Compliance-Scans auf Datenbankschemas

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



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

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



Configuration

Oracle DB 1 | 41 Schemas
Oracle

Configuration

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' Configuration | | | |
|--|-------------------|---|-------------------|
| 28/28 Schemas selected for compliance scan | | <input type="text"/> Edit Credentials | |
| Scan | Schema Name | Status | Required Action |
| <input type="checkbox"/> | DB1 - SchemaName1 | Not Scanning | Add Credentials ⓘ |
| <input type="checkbox"/> | DB1 - SchemaName2 | Continuously Scanning | |
| <input type="checkbox"/> | DB1 - SchemaName3 | Continuously Scanning | |
| <input type="checkbox"/> | DB1 - SchemaName4 | Continuously Scanning | |

Ergebnis

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

OneDrive-Konten werden gescannt

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

Schnellstart

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

1

Alle Voraussetzungen für OneDrive prüfen

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

2

Implementieren Sie die Cloud Data Sense Instanz

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

3

Fügen Sie das OneDrive Konto hinzu

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

4

Fügen Sie die Benutzer hinzu und wählen Sie den Scantyp aus

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

OneDrive Anforderungen können Sie überprüfen

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

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

Bereitstellen der Cloud Data Sense Instanz

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

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

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

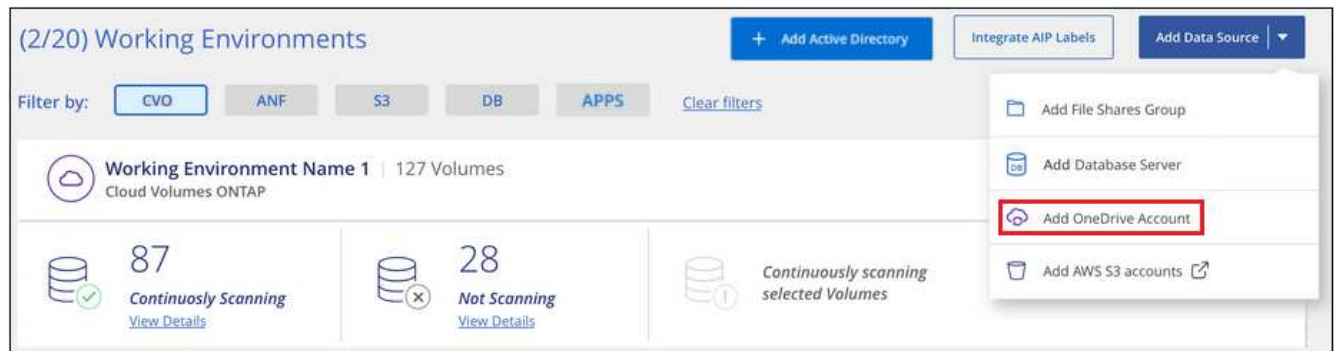
Auch der Datensinn kann sein ["Die Implementierung erfolgt an einem lokalen Standort ohne Internetzugang"](#). Allerdings müssen Sie einen Internetzugang für einige ausgewählte Endpunkte zur Verfügung stellen, um Ihre lokalen OneDrive-Dateien zu scannen. ["Hier finden Sie die Liste der erforderlichen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

Hinzufügen des OneDrive Kontos

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

Schritte

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



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

Das OneDrive-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

Hinzufügen von OneDrive Benutzern zu Compliance-Scans

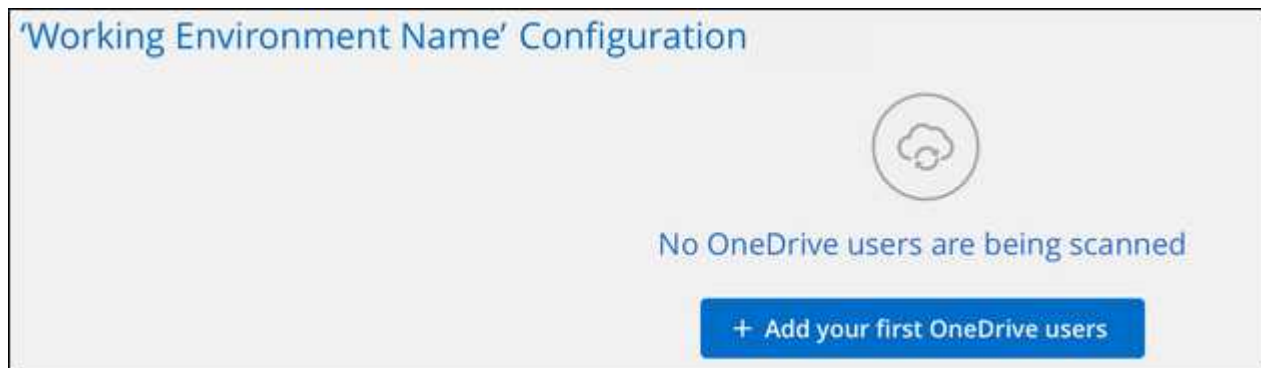
Sie können einzelne OneDrive-Benutzer oder alle OneDrive-Benutzer hinzufügen, damit ihre Dateien nach Cloud Data Sense gescannt werden.

Schritte

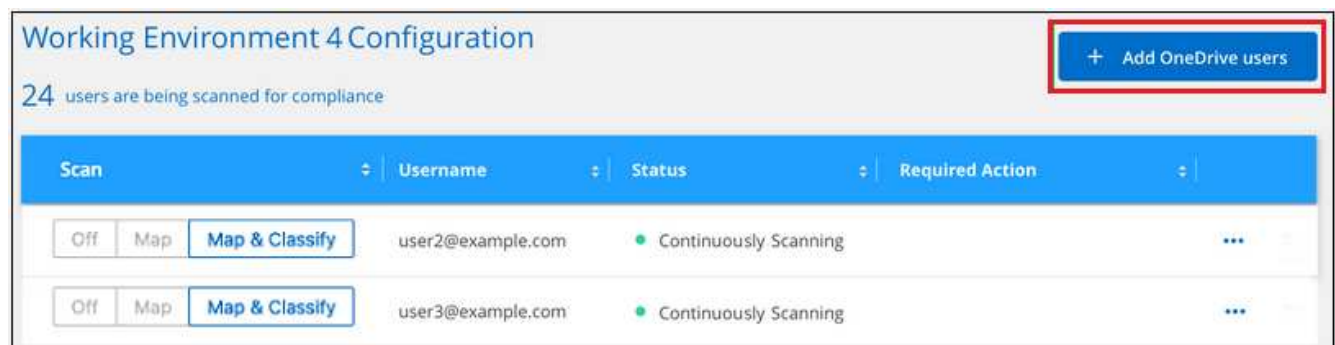
1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Configuration** für das OneDrive-Konto.



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



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



3. Fügen Sie die E-Mail-Adressen für die Benutzer hinzu, deren Dateien Sie scannen möchten - eine E-Mail-Adresse pro Zeile (bis zu 100 maximal pro Sitzung) - und klicken Sie auf **Benutzer hinzufügen**.

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

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

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

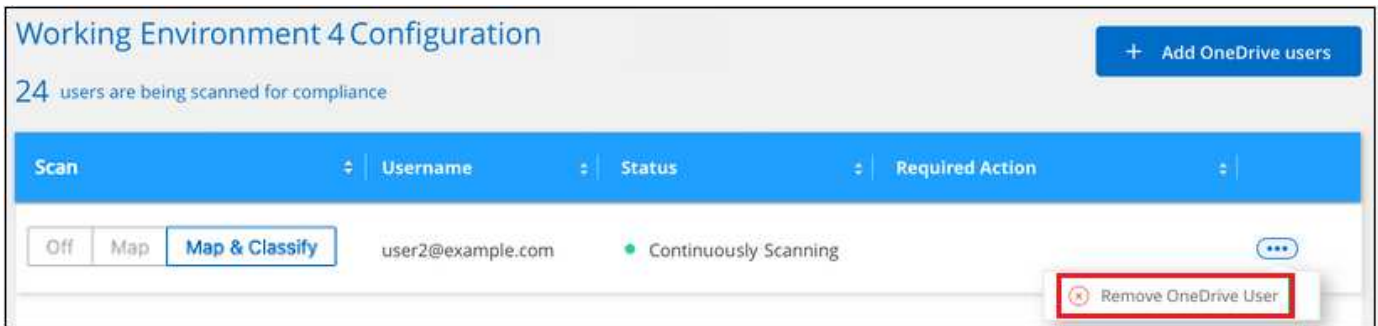
| An: | Tun Sie dies: |
|---|---|
| Aktivieren Sie mappingonly Scans von Benutzerdateien | Klicken Sie Auf Karte |
| Aktivieren Sie vollständige Scans von Benutzerdateien | Klicken Sie Auf Karte & Klassieren |
| Deaktivieren Sie das Scannen von Benutzerdateien | Klicken Sie Auf Aus |

Ergebnis

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

Entfernen eines OneDrive-Benutzers aus Compliance-Scans

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



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

Scannen von SharePoint-Konten

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

Schnellstart

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

1

SharePoint-Voraussetzungen prüfen

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

2

Implementieren Sie die Cloud Data Sense Instanz

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

3

Melden Sie sich beim SharePoint-Konto an

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

4

Fügen Sie die URLs der SharePoint-Website zum Scannen hinzu

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

Überprüfung der SharePoint Anforderungen

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

- Sie müssen über die Admin-Anmeldeinformationen für das SharePoint-Konto verfügen, das Lesezugriff auf alle SharePoint-Sites bietet.

- Für SharePoint vor Ort benötigen Sie auch die URL des SharePoint Servers.
- Für alle zu scannenden Daten benötigen Sie eine Liste der URLs der SharePoint-Website.

Bereitstellen der Cloud Data Sense Instanz

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

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

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

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

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

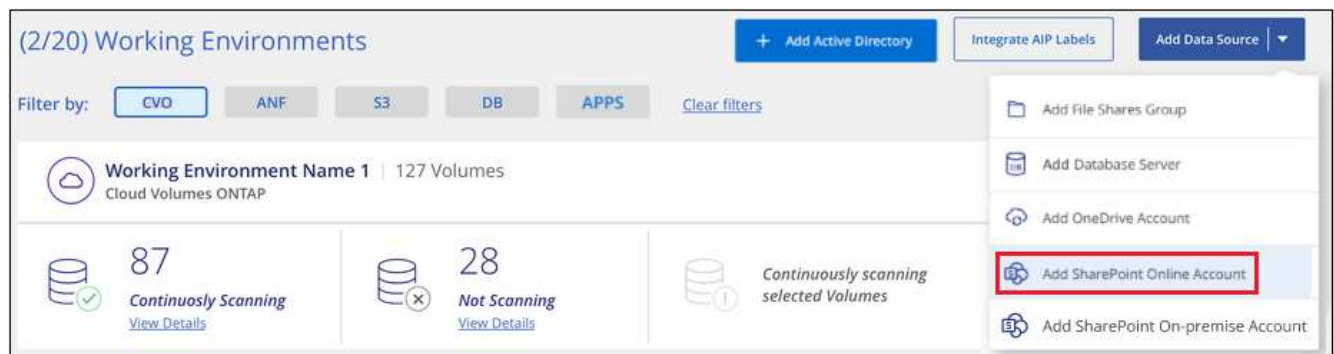
Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen eines SharePoint Online-Kontos

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

Schritte

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



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

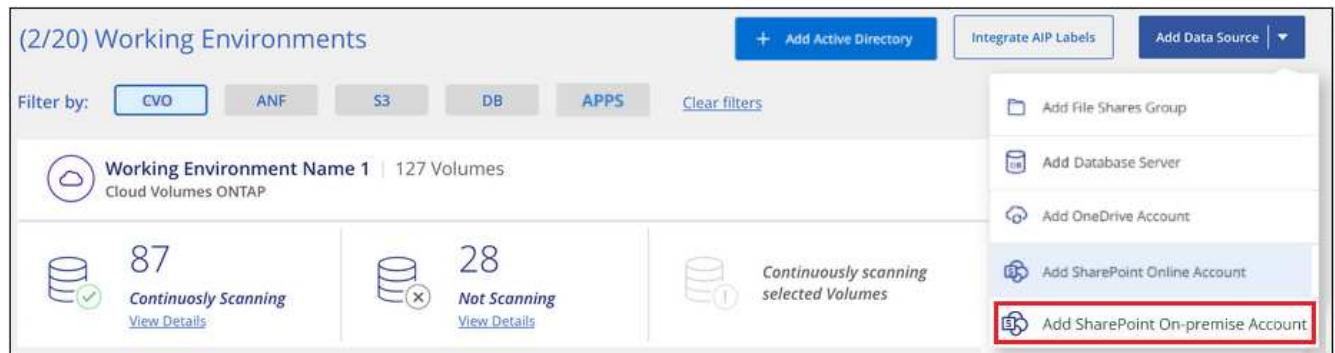
Das SharePoint Online-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

Hinzufügen eines SharePoint-Kontos vor Ort

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

Schritte

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



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

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

3. Klicken Sie Auf **Verbinden**.

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

Hinzufügen von SharePoint Sites zu Compliance-Scans

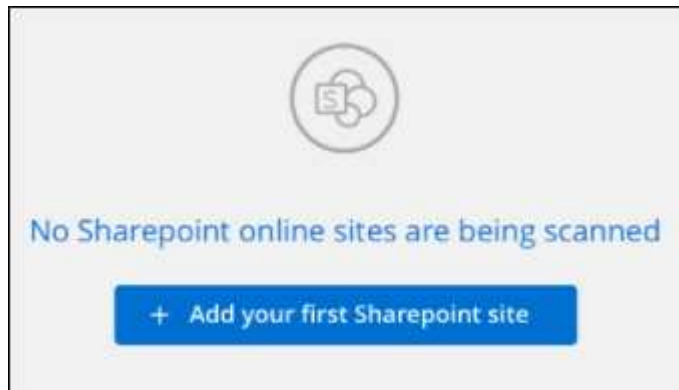
Sie können einzelne SharePoint-Sites oder alle SharePoint-Sites im Konto hinzufügen, damit die zugehörigen Dateien nach Cloud Data Sense gescannt werden. Die Schritte sind die gleichen, wenn SharePoint Online oder SharePoint On-Premise-Websites hinzugefügt werden.

Schritte

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



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



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



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

In einem Bestätigungsdiaologfeld wird die Anzahl der hinzugefügten Standorte angezeigt.

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

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

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

Ergebnis

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

Entfernen einer SharePoint-Website aus Compliance-Scans

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

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

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

Google Drive-Konten werden durchsucht

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

Schnellstart

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

1

Prüfen Sie die Voraussetzungen für Google Drive

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

2

Sinnvolle Implementierung Von Cloud-Daten

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

3

Melden Sie sich beim Google Drive-Konto an

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

4

Wählen Sie den Scantyp für die Benutzerdateien aus

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

Überprüfen der Google-Laufwerksanforderungen

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

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

Aktuelle Einschränkungen

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

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

Cloud Data Sense Implementieren

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

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

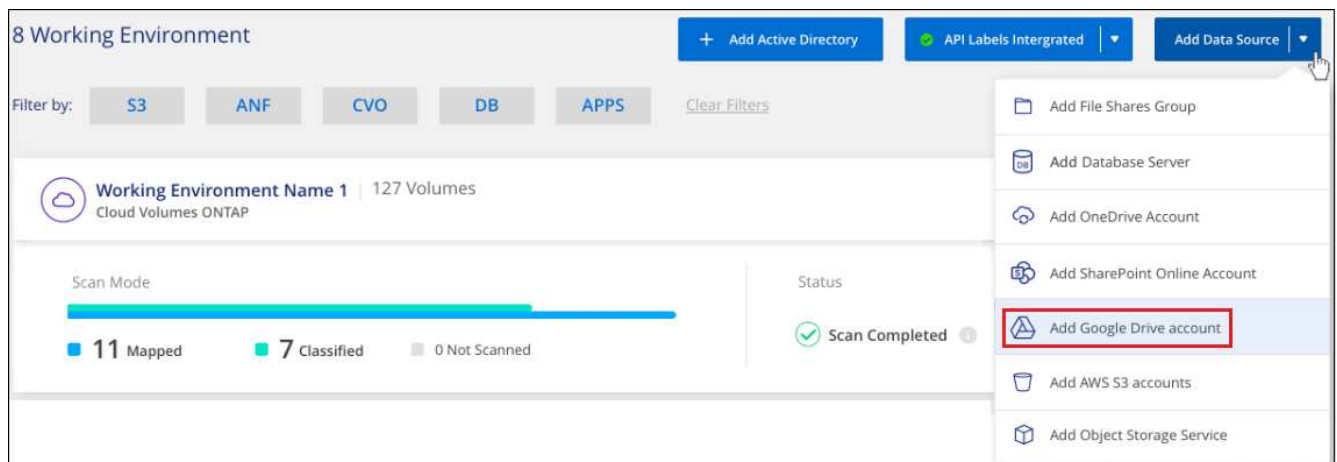
Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des Google Drive-Kontos

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

Schritte

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



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

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

Auswählen des Scantyps für Benutzerdaten

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

Schritte

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



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



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

Ergebnis

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

Entfernen eines Google Drive-Kontos aus Compliance-Scans

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

Scannen von Dateifreigaben

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

Schnellstart

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



Prüfen Sie die Voraussetzungen für die Dateifreigabe

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

2**Implementieren Sie die Cloud Data Sense Instanz**

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

3**Erstellen Sie eine Gruppe, um die Dateifreigaben zu halten**

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

4**Fügen Sie die Dateifreigaben hinzu und wählen Sie die zu scannenden Freigaben aus**

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

Prüfen der Anforderungen für die Dateifreigabe

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

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

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

Bereitstellen der Cloud Data Sense Instanz

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

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

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

am selben Standort erforderlich.

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

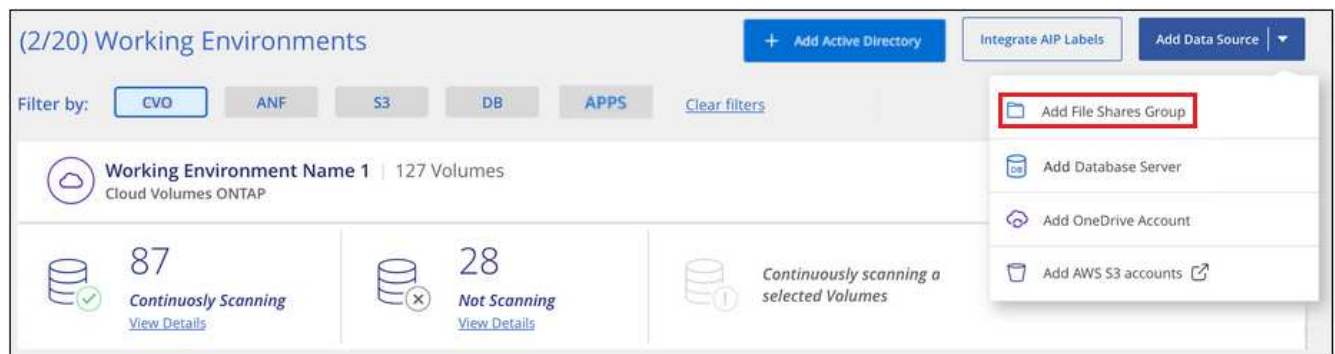
Erstellen der Gruppe für die Dateifreigaben

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

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

Schritte

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



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

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

Hinzufügen von Dateifreigaben zu einer Gruppe

Sie fügen der File Shares-Gruppe Dateifreigaben hinzu, damit die Dateien in diesen Freigaben nach Cloud Data Sense gescannt werden. Sie fügen die Freigaben im Format hinzu `<host_name>:/<share_path>`.

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

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

Schritte

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



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



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



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

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

Ein Bestätigungsdialogfeld zeigt die Anzahl der hinzugefügten Freigaben an.

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

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

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

Ergebnis

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

Entfernen einer Dateifreigabe aus Compliance-Scans

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



Objekt-Storage wird mit S3-Protokoll gescannt

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

Schnellstart

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

1

Prüfen Sie die Voraussetzungen für den Objekt-Storage

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

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

2

Implementieren Sie die Cloud Data Sense Instanz

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

3

Fügen Sie den Objekt-Storage-Service hinzu

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

4

Wählen Sie die zu scannenden Buckets aus

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

Überprüfung der Objekt-Storage-Anforderungen

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

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

Bereitstellen der Cloud Data Sense Instanz

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

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

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

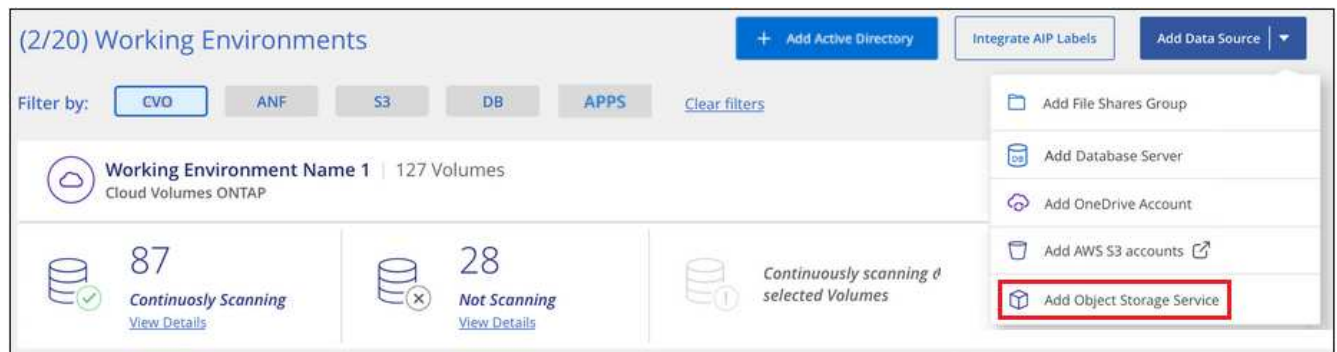
Upgrades auf die Software Data Sense werden automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des Objekt-Storage-Service zu Cloud Data Sense

Fügen Sie den Objekt-Storage-Service hinzu.

Schritte

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



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

Add Object Storage Service

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

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

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

Ergebnis

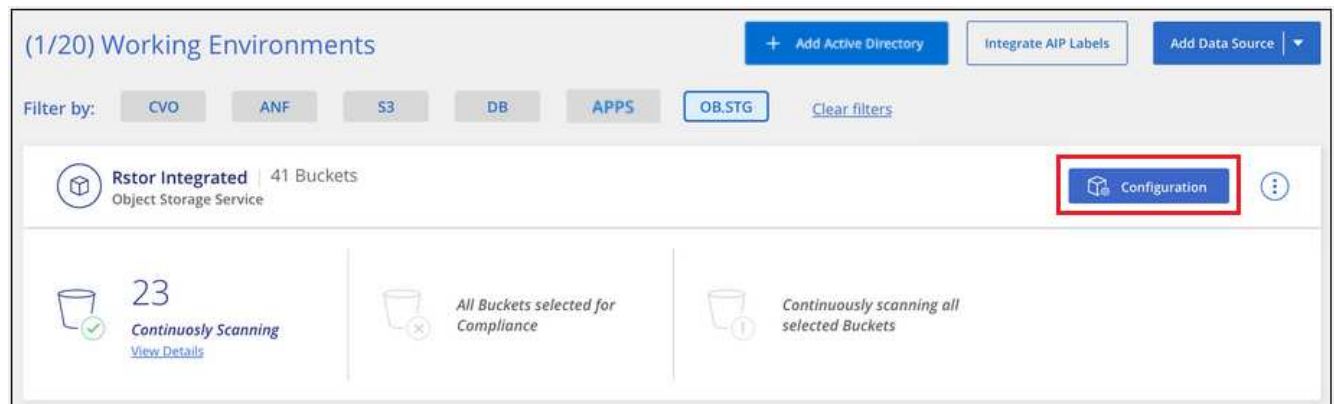
Der neue Objekt-Speicherdienst wird der Liste der Arbeitsumgebungen hinzugefügt.

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

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

Schritte

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



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

| Rstor Integrated Configuration | | | |
|---|--------------------------------|-------------------------|--------------------|
| 3/55 Buckets selected for Compliance scan | | | |
| Scan | Storage Repository (Bucket) ↓↑ | Status ↓↑ | Required Action ↓↑ |
| Off Map Map & Classify | logs-759995470648-us-east-1 | ● Not Scanning | |
| Off Map Map & Classify | logs-759995470648-us-west-2 | ● Not Scanning | |
| Off Map Map & Classify | carstock | ● Continuously Scanning | |

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

Ergebnis

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

Integrieren Sie Active Directory in Cloud Data Sense

Sie können ein globales Active Directory in Cloud Data Sense integrieren, um die Ergebnisse zu verbessern, die Data Sense-Berichte über Dateibesitzer und welche Benutzer und Gruppen Zugriff auf Ihre Dateien haben.

Wenn Sie bestimmte Datenquellen einrichten (siehe unten), müssen Sie Active Directory-Anmeldeinformationen eingeben, damit Data Sense CIFS-Volumes scannen kann. Diese Integration bietet Data Sense mit Details zu Dateieigentümerdaten und Berechtigungen für die Daten, die sich in diesen Datenquellen befinden. Das für diese Datenquellen eingegebene Active Directory kann sich von den hier eingegebenen globalen Active Directory-Anmeldeinformationen unterscheiden. Data Sense wird in allen integrierten Active-Verzeichnissen für Benutzer- und Berechtigungsdetails angezeigt.

Diese Integration bietet zusätzliche Informationen an den folgenden Orten in Data Sense:

- Sie können den „Dateieigentümer“ verwenden. **"Filtern"** Und siehe Ergebnisse in den Metadaten der Datei im Untersuchungsbereich. Anstelle des Dateieigentümers, der den SID (Security Identifier) enthält, wird er mit dem tatsächlichen Benutzernamen gefüllt.
- Sie sehen **"Volldateiberechtigungen"** Klicken Sie für jede Datei und jedes Verzeichnis auf die Schaltfläche „Alle Berechtigungen anzeigen“.
- Im **"Governance-Dashboard"**, Das Fenster „Offene Berechtigungen“ zeigt eine größere Detailebene über Ihre Daten an.



Die SIDs des lokalen Benutzers und SIDs unbekannter Domänen werden nicht in den tatsächlichen Benutzernamen übersetzt.

Unterstützte Datenquellen

Eine Active Directory-Integration mit Cloud Data Sense kann Daten aus den folgenden Datenquellen identifizieren:

- On-Premises ONTAP Systeme
- Cloud Volumes ONTAP
- Azure NetApp Dateien
- FSX für ONTAP
- CIFS-File-Shares von anderen Anbietern (keine NFS-File-Shares)

Die Identifizierung von Benutzer- und Berechtigungsinformationen aus Datenbankschemas, OneDrive-Konten, SharePoint-Konten, Google-Drive-Konten, Amazon S3-Konten, Oder Objekt-Storage, der das Simple Storage Service (S3)-Protokoll nutzt.

Verbindung zu Ihrem Active Directory-Server herstellen

Nachdem Sie Data Sense implementiert und das Scannen an Ihren Datenquellen aktiviert haben, können Sie Data Sense in Ihr Active Directory integrieren. Auf Active Directory kann über eine DNS-Server-IP-Adresse oder eine LDAP-Server-IP-Adresse zugegriffen werden.

Die Active Directory-Anmeldeinformationen können schreibgeschützt sein, jedoch stellt die Bereitstellung von Admin-Anmeldeinformationen sicher, dass Daten Sense alle Daten lesen kann, die erhöhte Berechtigungen erfordern. Die Anmeldedaten werden in der Cloud Data Sense Instanz gespeichert.

Wenn Sie für CIFS Volumes/File Shares sicherstellen möchten, dass Ihre Dateien „zuletzt zugegriffen Zeiten“ durch Data Sense Klassifizierungsscans unverändert bleiben, empfehlen wir, dass der Benutzer über die Berechtigung Schreibattribute verfügt. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

Anforderungen

- Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben.
- Sie müssen über die folgenden Informationen für das Active Directory verfügen:
 - DNS-Server-IP-Adresse oder mehrere IP-Adressen

Oder

LDAP-Server-IP-Adresse oder mehrere IP-Adressen

- Benutzername und Kennwort für den Zugriff auf den Server
- Domain-Name (Active Directory-Name)
- Ob Sie Secure LDAP (LDAPS) verwenden oder nicht
- LDAP-Server-Port (normalerweise 389 für LDAP und 636 für sicheres LDAP)
- Die folgenden Ports müssen für die ausgehende Kommunikation durch die Instanz Data Sense geöffnet sein:

| Protokoll | Port | Ziel | Zweck |
|-------------|------|------------------|-------|
| TCP UND UDP | 389 | Active Directory | LDAP |

| Protokoll | Port | Ziel | Zweck |
|-----------|------|------------------|---------------------------|
| TCP | 636 | Active Directory | LDAP über SSL |
| TCP | 3268 | Active Directory | Globaler Katalog |
| TCP | 3269 | Active Directory | Globaler Katalog über SSL |

Schritte

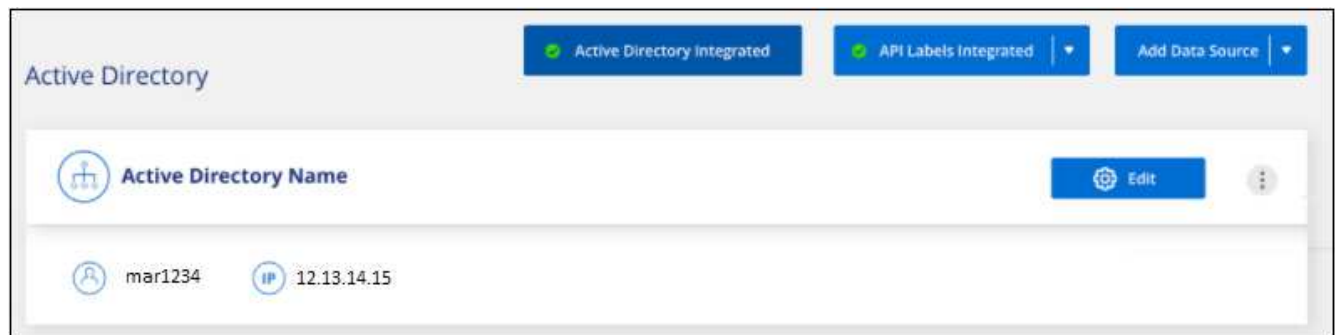
1. Klicken Sie auf der Seite Cloud Data Sense Configuration auf **Active Directory hinzufügen**.



2. Geben Sie im Dialogfeld mit Active Directory verbinden die Active Directory-Details ein, und klicken Sie auf **Verbinden**.


Sie können bei Bedarf mehrere IP-Adressen hinzufügen, indem Sie auf **IP hinzufügen** klicken.

Data Sense integriert sich in das Active Directory, und ein neuer Abschnitt wird zur Konfigurationsseite hinzugefügt.



Verwalten Ihrer Active Directory-Integration

Wenn Sie Werte in Ihrer Active Directory-Integration ändern müssen, klicken Sie auf die Schaltfläche **Bearbeiten** und nehmen Sie die Änderungen vor.

Sie können die Integration auch löschen, wenn Sie sie nicht mehr benötigen, indem Sie auf die klicken  Und dann **Active Directory entfernen**.

Lizenzierung für Cloud Data Sense einrichten

Die ersten 1 TB an Daten, die Cloud Data Sense in einem BlueXP-Arbeitsbereich scannt, sind kostenlos. Für den weiteren Scan der Daten ist eine BYOL-Lizenz von NetApp oder ein Abonnement vom Marketplace Ihres Cloud-Providers erforderlich.

Ein paar Notizen, bevor Sie weitere lesen:

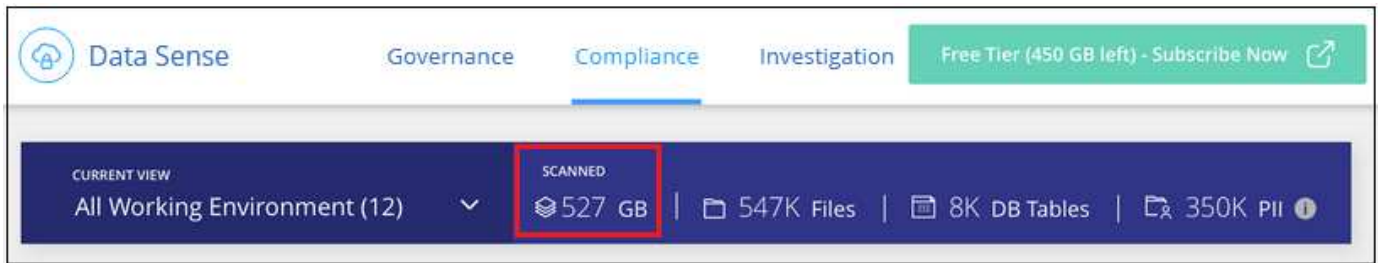
- Wenn Sie das BlueXP Pay-as-you-go-Abonnement (PAYGO) bereits auf dem Markt Ihres Cloud-Providers abonniert haben, haben Sie sich auch automatisch für Cloud Data Sense angemeldet. Sie müssen sich nicht erneut anmelden.
- Die Cloud Data Sense Bring-Your-Own-License (BYOL) ist eine „*Floating*“-Lizenz, die Sie für alle Arbeitsumgebungen und Datenquellen im zu scannenden Arbeitsbereich verwenden können. Im Digital Wallet wird ein aktives Abonnement angezeigt.

["Informieren Sie sich über die Lizenzierung und die Kosten im Zusammenhang mit Cloud Data Sense".](#)

Nutzen Sie ein Cloud Data Sense PAYGO-Abonnement

Mit Pay-as-you-go-Abonnements auf dem Markt Ihres Cloud-Providers können Sie die Nutzung von Cloud Volumes ONTAP Systemen und vielen Cloud-Datenservices wie Cloud Data Sense lizenzieren.

Sie können sich jederzeit für eine Anmeldung anmelden. Die Abrechnung erfolgt erst, wenn die Datenmenge mehr als 1 TB beträgt. Sie können immer die Gesamtmenge der Daten anzeigen, die über das Data Sense Dashboard gescannt werden. Und die Schaltfläche *Jetzt abonnieren* erleichtert die Anmeldung, wenn Sie bereit sind.



Schritte

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

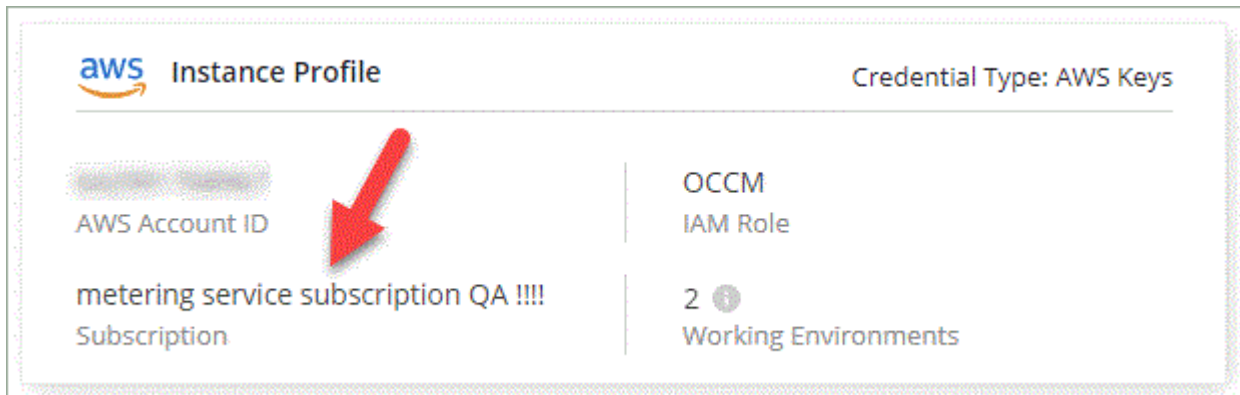
1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



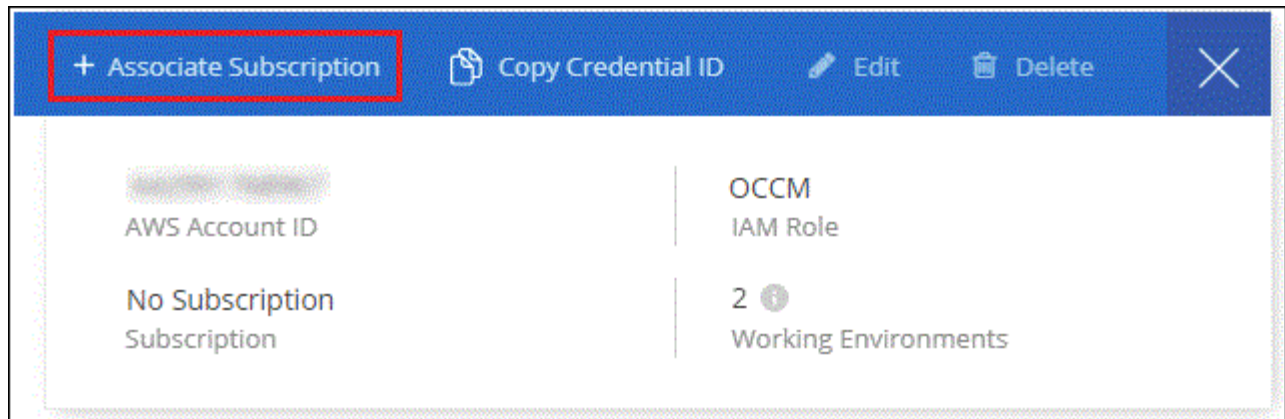
2. Anmeldedaten für AWS Instance Profile, Azure Managed Service Identity oder Google Project finden Sie hier.

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

Wenn Sie bereits über ein BlueXP-Abonnement (siehe unten für AWS) verfügen, sind Sie alle eingerichtet. Es gibt nichts anderes, das Sie tun müssen.



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



4. Wählen Sie ein vorhandenes Abonnement aus und klicken Sie auf **Associate**, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte.

Das folgende Video zeigt, wie ein zugeordnet werden soll "AWS Marketplace" Abonnement eines AWS Abonnements:

► https://docs.netapp.com/de-de/cloud-manager-data-sense//media/video_subscribing_aws.mp4 (video)

Das folgende Video zeigt, wie ein zugeordnet werden soll "Azure Marketplace" Abonnement eines Azure Abonnements:

► https://docs.netapp.com/de-de/cloud-manager-data-sense//media/video_subscribing_azure.mp4 (video)

Das folgende Video zeigt, wie ein zugeordnet werden soll "GCP Marketplace" Abonnement eines GCP-Abonnements:

► https://docs.netapp.com/de-de/cloud-manager-data-sense//media/video_subscribing_gcp.mp4 (video)

Verwenden einer Cloud Data Sense BYOL-Lizenz

Mit den Bring-Your-Own-License-Lizenzen von NetApp erhalten Sie Vertragsbedingungen mit 1, 2 oder 3 Jahren. Die BYOL **Cloud Data Sense**-Lizenz ist eine *Floating*-Lizenz, bei der die Gesamtkapazität unter **all** Ihrer Arbeitsumgebungen und Datenquellen aufgeteilt wird, was die Erstlizenzierung und Erneuerung vereinfacht.

Wenn Sie keine Cloud Data Sense Lizenz haben, nehmen Sie mit uns Kontakt auf, um eine Lizenz zu erwerben:

- [Mailto:ng-contact-data-sense@netapp.com?Subject=Lizenzierung](mailto:ng-contact-data-sense@netapp.com?Subject=Lizenzierung)[E-Mail senden, um eine Lizenz zu erwerben].
- Klicken Sie rechts unten auf das Chat-Symbol von BlueXP, um eine Lizenz anzufordern.

Wenn Sie optional eine nicht zugewiesene Node-basierte Lizenz für Cloud Volumes ONTAP haben, die Sie nicht verwenden werden, können Sie diese in eine Cloud Data Sense Lizenz mit derselben Dollaräquivalenz und demselben Ablaufdatum konvertieren. "[Weitere Informationen finden Sie hier](#)".

Sie verwenden die Seite „Digital Wallet“ in BlueXP, um Cloud Data Sense-Lizenzen zu verwalten. Sie können neue Lizenzen hinzufügen und vorhandene Lizenzen aktualisieren.

Holen Sie sich Ihre Cloud Data Sense Lizenzdatei

Nachdem Sie Ihre Cloud Data Sense Lizenz erworben haben, aktivieren Sie die Lizenz in BlueXP, indem Sie die Seriennummer und das NSS-Konto von Cloud Data Sense eingeben oder die Lizenzdatei NLF hochladen. Die folgenden Schritte zeigen, wie Sie die Lizenzdatei NLF abrufen können, wenn Sie diese Methode verwenden möchten.

Wenn Sie Cloud Data Sense auf einem Host in einer On-Premises-Website, die keinen Internetzugang hat, bereitgestellt haben, müssen Sie die Lizenzdatei von einem Internet-verbundenen System erhalten. Die Aktivierung der Lizenz unter Verwendung der Seriennummer und des NSS-Kontos ist für Installationen am dunklen Standort nicht verfügbar.

Schritte

1. Melden Sie sich beim an ["NetApp Support Website"](#) Klicken Sie anschließend auf **Systeme > Softwarelizenzen**.
2. Geben Sie die Seriennummer Ihrer Cloud Data Sense Lizenz ein.

| Serial # | Cluster SN | License Name | License Key | Host ID | Value | End Date |
|----------|------------|--------------------------|---|---------|-------|------------|
| 4810 | | SUBS-CLD-DAT-SENSE-TB-2Y | Get NetApp License File | | 100 | 12/31/9998 |

3. Klicken Sie unter **Lizenzschlüssel** auf **NetApp Lizenzdatei erhalten**.
4. Geben Sie Ihre BlueXP-Konto-ID ein (dies wird als Mandanten-ID auf der Support-Website bezeichnet) und klicken Sie auf **Absenden**, um die Lizenzdatei herunterzuladen.

Get License

SERIAL NUMBER: 4810

LICENSE: SUBS-CLD-DAT-SENSE-TB-2Y

SALES ORDER: 3005

TENANT ID:

Example: account-xxxxxxx

[Cancel](#)

Sie können Ihre BlueXP-Konto-ID finden, indem Sie oben in BlueXP das Dropdown-Menü **Konto** auswählen und dann neben Ihrem Konto auf **Konto verwalten** klicken. Ihre Account-ID wird auf der Registerkarte „Übersicht“ angezeigt.

Fügen Sie Ihrem Konto Cloud Data Sense BYOL-Lizenzen hinzu

Nachdem Sie eine Cloud Data Sense Lizenz für Ihr BlueXP-Konto erworben haben, müssen Sie BlueXP die Lizenz hinzufügen, um den Data Sense Service nutzen zu können.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Digital Wallet** und wählen Sie dann die Registerkarte **Data Services Licenses** aus.
2. Klicken Sie Auf **Lizenz Hinzufügen**.
3. Geben Sie im Dialogfeld „Lizenz hinzufügen“ die Lizenzinformationen ein, und klicken Sie auf **Lizenz hinzufügen**:
 - Wenn Sie über die Seriennummer der Data Sense-Lizenz verfügen und Ihr NSS-Konto kennen, wählen Sie die Option **Seriennummer eingeben** aus, und geben Sie diese Informationen ein.

Wenn Ihr NetApp Support Site Konto nicht in der Dropdown-Liste verfügbar ist, "[Fügen Sie das NSS-Konto zu BlueXP hinzu](#)".

- Wenn Sie über die Lizenzdatei für den Datensense verfügen (erforderlich, wenn sie auf einer dunklen Seite installiert wird), wählen Sie die Option **Lizenzdatei hochladen** aus, und befolgen Sie die Anweisungen, um die Datei anzuhängen.

The image displays two versions of the 'Add License' dialog box. The left version is for entering a serial number, featuring a text input for the serial number and a dropdown for the NetApp Support Site Account. The right version is for uploading a license file, providing step-by-step instructions and an 'Upload' button to select the file.

Ergebnis

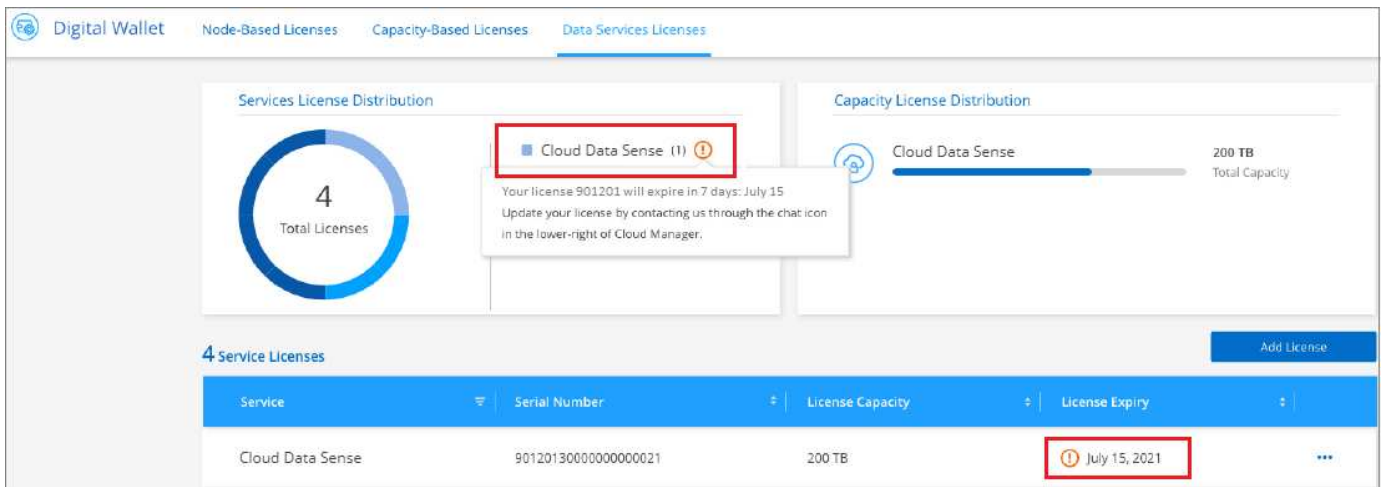
BlueXP fügt die Lizenz hinzu, damit Ihr Cloud Data Sense Service aktiv ist.

Aktualisieren einer Cloud Data Sense BYOL-Lizenz

Wenn sich Ihre Lizenzlaufzeit dem Ablaufdatum nähert oder Ihre lizenzierte Kapazität die Obergrenze erreicht, werden Sie in Cloud Data Sense benachrichtigt.



Dieser Status wird auch im Digital Wallet angezeigt.



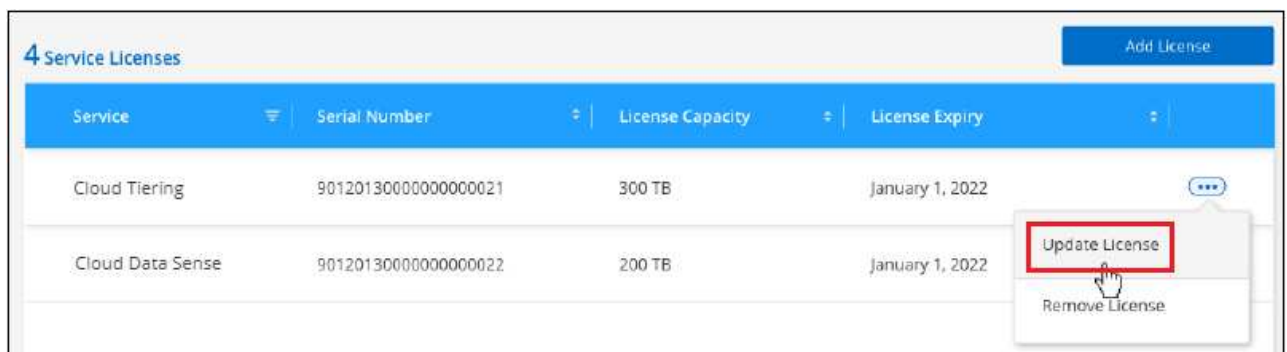
Sie können Ihre Cloud Data Sense Lizenz aktualisieren, bevor sie abläuft, damit Sie nicht auf Ihre gescannten Daten zugreifen können.

Schritte

1. Klicken Sie auf das Chat-Symbol rechts unten bei BlueXP, um eine Erweiterung Ihres Terms oder zusätzliche Kapazität für Ihre Cloud Data Sense Lizenz für die jeweilige Seriennummer anzufordern. Sie können auch [Senden Sie eine E-Mail](#).

Nach der Zahlung für die Lizenz und der Registrierung auf der NetApp Support-Website aktualisiert BlueXP automatisch die Lizenz im Digital Wallet. Auf der Seite „Data Services Licenses“ wird die Änderung in 5 bis 10 Minuten dargestellt.

2. Wenn BlueXP die Lizenz nicht automatisch aktualisieren kann (zum Beispiel, wenn sie auf einer dunklen Seite installiert wird), müssen Sie die Lizenzdatei manuell hochladen.
 - a. Das können Sie [Beziehen Sie die Lizenzdatei über die NetApp Support-Website](#).
 - b. Klicken Sie auf der Seite Digital Wallet auf der Registerkarte „Data Services Licenses“ auf **...** Klicken Sie für die Serviceseriennummer, die Sie aktualisieren, auf **Lizenz aktualisieren**.



- c. Laden Sie auf der Seite *Update License* die Lizenzdatei hoch und klicken Sie auf **Update License**.

Ergebnis

BlueXP aktualisiert die Lizenz, damit Ihr Cloud Data Sense Service weiterhin aktiv ist.

Überlegungen zu BYOL-Lizenzen

Bei Verwendung einer Cloud Data Sense BYOL-Lizenz zeigt BlueXP in der Data Sense UI und in der Digital Wallet UI eine Warnung an, wenn sich die Größe aller zu scannenden Daten dem Kapazitätslimit nähert oder

dem Ablaufdatum der Lizenz nähert. Sie erhalten folgende Warnungen:

- Wenn die Menge der Daten, die Sie scannen, erreicht hat 80% der lizenzierten Kapazität, und wieder, wenn Sie das Limit erreicht haben
- 30 Tage, bevor eine Lizenz abläuft, und wieder, wenn die Lizenz abläuft

Verwenden Sie das Chat-Symbol rechts unten in der BlueXP-Schnittstelle, um Ihre Lizenz zu verlängern, wenn diese Warnungen angezeigt werden.

Wenn Ihre Lizenz abgelaufen ist, wird Data Sense weiterhin ausgeführt, der Zugriff auf die Dashboards ist jedoch blockiert, sodass Sie keine Informationen zu Ihren gescannten Daten anzeigen können. Nur die Seite *Configuration* steht zur Verfügung, wenn Sie die Anzahl der eingescannten Volumes reduzieren möchten, um die Kapazitätsnutzung unter das Lizenzlimit zu bringen.

Sobald Sie Ihre Byol-Lizenz erneuern, aktualisiert BlueXP die Lizenz automatisch im Digital Wallet und bietet vollständigen Zugriff auf alle Dashboards. Wenn BlueXP nicht über die sichere Internetverbindung auf die Lizenzdatei zugreifen kann (z. B. bei Installation in einer dunklen Site), können Sie die Datei selbst beziehen und sie manuell auf BlueXP hochladen. Anweisungen hierzu finden Sie unter [So aktualisieren Sie eine Cloud Data Sense Lizenz](#).



Wenn das Konto, das Sie verwenden, sowohl eine BYOL-Lizenz als auch ein PAYGO-Abonnement hat, wird Data Sense *beim Ablauf der BYOL-Lizenz nicht* in das PAYGO-Abonnement verschoben. Sie müssen die BYOL-Lizenz verlängern.

Häufig gestellte Fragen zu Cloud Data Sense

Diese FAQ kann Ihnen helfen, wenn Sie nur nach einer schnellen Antwort auf eine Frage suchen.

Cloud Data Sense Service

Die folgenden Fragen vermitteln ein allgemeines Verständnis von Cloud Data Sense.

Was ist Cloud Data Sense?

Cloud Data Sense ist ein Cloud-Angebot, das auf KI-basierter Technologie (Artificial Intelligence, künstliche Intelligenz) setzt, um den Datenkontext zu verstehen und sensible Daten in Ihren Storage-Systemen zu identifizieren. Die Systeme können Arbeitsumgebungen sein, die Sie dem BlueXP Canvas hinzugefügt haben, und viele Arten von Datenquellen, auf die Data Sense über Ihre Netzwerke zugreifen kann. ["Die vollständige Liste finden Sie unten"](#).

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

Wie sinnvoll sind Cloud Data Lösungen?

Cloud Data Sense implementiert gemeinsam mit Ihrem BlueXP System und Ihren Storage-Systemen eine weitere Schicht künstlicher Intelligenz. Anschließend werden die Daten auf Volumes, Buckets, Datenbanken und anderen Storage-Konten überprüft und die gefundenen Dateneinblicke indiziert. Bei „Data Sense“ werden sowohl künstliche Intelligenz als auch natürliche Sprachverarbeitung verwendet. Im Gegensatz zu alternativen Lösungen, die sich häufig auf der Grundlage regelmäßiger Ausdrücke und Musterabgleich aufbauen.

Cloud Data Sense verwendet KI für kontextabhängiges Verständnis der Daten zur genauen Erkennung und

Klassifizierung. Der Fokus liegt auf KI, da sie für moderne Datentypen und Skalierungen konzipiert wurde. Er versteht auch den Datenkontext und sorgt so für starke, präzise, Erkennungs- und Klassifizierungsmöglichkeiten.

["Finden Sie heraus, wie Cloud Data Sense funktioniert".](#)

Welche Anwendungsfälle gibt es für Cloud-Daten Sense?

- Ermitteln von personenbezogenen Daten
- 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.
- Einhaltung neuer und anstehender Datenschutzvorschriften
- Einhaltung von Daten-Compliance- und Datenschutzvorschriften
- Migrieren von Daten von Legacy-Systemen zur Cloud
- Einhaltung von Richtlinien zur Datenaufbewahrung.

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

Welche Bedeutung hat die Architektur von Cloud-Daten?

Cloud Data Sense implementiert einen einzelnen Server oder Cluster – ganz gleich, ob in der Cloud oder vor Ort. Die Server verbinden sich über Standardprotokolle mit den Datenquellen und indizieren die Ergebnisse in einem Elasticsearch-Cluster, der ebenfalls auf denselben Servern implementiert wird. Dies ermöglicht die Unterstützung sowohl für Cloud-übergreifende Umgebungen als auch für Private-Cloud- und On-Premises-Umgebungen.

Welche Cloud-Provider werden unterstützt?

Cloud Data Sense funktioniert als Teil von BlueXP und unterstützt AWS, Azure und GCP. Dadurch erhält Ihr Unternehmen Transparenz im Hinblick auf den Datenschutz bei verschiedenen Cloud-Providern.

Hat Cloud Data Sense eine REST API und funktioniert es mit Tools von Drittanbietern?

BlueXP unterstützt REST-API-Funktionen für seine Services. Wenn BlueXP nicht der bevorzugte Managementpunkt ist, können Services wie Cloud Data Sense auch über EINE REST API verwendet werden. Jede Benutzeraktion hat eine REST-API, die in Systeme von Drittanbietern integriert werden kann.

Ist Cloud Data Sense über die Märkte verfügbar?

Ja, BlueXP und Cloud Data Sense sind über den AWS, Azure und GCP Marketplace erhältlich.

Cloud Data Sense-Scan und Analysen

Die folgenden Fragen beziehen sich auf die Leistung von Cloud Data Sense-Scans und die Analysen, die Benutzern zur Verfügung stehen.

Wie oft scannt Cloud Data Sense meine Daten?

Da sich die Daten häufig ändern, scannt Cloud Data Sense 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"](#).

Datenscans haben keine nennenswerten Auswirkungen auf Ihre Storage-Systeme und Ihre Daten. Wenn Sie jedoch auch nur geringe Auswirkungen haben, können Sie Data Sense so konfigurieren, dass Sie „langsame“ Scans durchführen. ["Erfahren Sie, wie Sie die Scangeschwindigkeit verringern"](#).

Kann ich meine Daten mit Cloud Data Sense durchsuchen?

Cloud Data Sense bietet umfangreiche Suchfunktionen, mit denen Sie ganz einfach nach einer bestimmten Datei oder einem bestimmten Datenelement aus allen verbundenen Quellen suchen können. Mit Data Sense können Benutzer tiefer suchen, als nur die Metadaten widerspiegeln. Es ist ein sprachunabhängiger Dienst, der auch die Dateien lesen und eine Vielzahl sensibler Datentypen, wie Namen und IDs, analysieren kann. So können Benutzer beispielsweise sowohl strukturierte als auch unstrukturierte Datenspeicher durchsuchen, um Daten zu finden, die von Datenbanken bis zu Benutzerdateien ausgetreten sind, und dies unter Verletzung von Unternehmensrichtlinien. Suchvorgänge können für einen späteren Zeitpunkt gespeichert werden. Richtlinien können erstellt werden, um die Ergebnisse zu einer festgelegten Häufigkeit zu suchen und entsprechend zu reagieren.

Sobald die entsprechenden Dateien gefunden wurden, können die Merkmale aufgelistet werden, einschließlich Tags, Konto der Arbeitsumgebung, Bucket, Dateipfad Kategorie (aus Klassifizierung), Dateigröße, letzte Änderung, Berechtigungsstatus, Duplikate, Empfindlichkeitsstufe, persönliche Daten, sensible Datentypen innerhalb der Datei, Eigentümer, Dateityp, Dateigröße, Erstellungszeit, Datei-Hash, unabhängig davon, ob die Daten einer Person zugewiesen wurden, die ihre Aufmerksamkeit sucht, und vieles mehr. Filter können auf Merkmale angewendet werden, die nicht relevant sind. Data Sense bietet auch RBAC-Steuerelemente zum Verschieben oder Löschen von Dateien, sofern die entsprechenden Berechtigungen vorhanden sind. Wenn die richtigen Berechtigungen nicht vorhanden sind, können die Aufgaben einer Person in der Organisation zugewiesen werden, die über die entsprechenden Berechtigungen verfügt.

Welche Art von Analysen bietet Cloud Data Sense?

Datenquellen können visuell dargestellt und Beziehungen definiert und grafisch dargestellt werden. Administratoren können beispielsweise alle veralteten, doppelten und nicht geschäftsbezogenen Daten aus allen Datenquellen im gesamten Unternehmen sehen (On-Premises-Systeme, Datenbanken, Dateifreigaben, S3-Speicher, OneDrive, Usw.). Anschließend können sie Daten kopieren, verschieben, löschen und managen, um so die Storage-Kosten zu optimieren und Risiken zu minimieren. Benutzer können Risiken minimieren, indem sie erkennen, welche sensiblen Daten offengelegt werden können. Sie können zudem Jobs zum Management der Berechtigungen für eine starke Datensicherung erstellen. Außerdem werden in Data Sense alle verschiedenen Datentypen klassifiziert, sodass Administratoren nach Datentypen untersuchen und sehen können, welche Aktionen für die Daten getroffen wurden und wann diese durchgeführt wurden.

Bietet Cloud Data Sense Berichte an?

Ja. Die von Cloud Data Sense bereitgestellten Informationen können für andere Beteiligte in Ihrem Unternehmen relevant sein, damit Sie Berichte erstellen und die Erkenntnisse weitergeben können. Die folgenden Berichte stehen für Data Sense 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 ."](#)

Datenzuordnungsbericht

Stellt Informationen zur Größe und Anzahl der Dateien in Ihren Arbeitsumgebungen bereit. Dazu zählen Nutzungskapazität, Alter der Daten, Größe der Daten und Dateitypen. ["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 ."](#)

Ist die Scanleistung unterschiedlich?

Die Scan-Performance kann je nach Netzwerkbandbreite und durchschnittlicher Dateigröße in der Umgebung variieren. Es kann auch von der Größe des Host-Systems abhängen (entweder in der Cloud oder lokal). Siehe ["Die Instanz Cloud Data Sense"](#) Und ["Cloud Data Sense Implementieren"](#) Finden Sie weitere Informationen.

Beim ersten Hinzufügen neuer Datenquellen können Sie auch nur einen „Mapping“-Scan anstelle eines vollständigen „Classification“-Scans durchführen. Das Mapping kann auf Ihren Datenquellen sehr schnell durchgeführt werden, da es nicht auf Dateien zugegriffen wird, um die darin enthaltenen Daten zu sehen.
["Sehen Sie den Unterschied zwischen einer Mapping- und Klassifizierungsscan"](#).

Cloud Data Sense Management und Datenschutz

Die folgenden Fragen enthalten Informationen zum Management von Cloud Data Sense- und Datenschutzeinstellungen.

Wie kann ich Cloud Data Sense aktivieren?

Zunächst müssen Sie eine Instanz von Cloud Data Sense in BlueXP oder auf einem On-Premises-System implementieren. Sobald die Instanz ausgeführt wurde, können Sie den Dienst auf bestehenden Arbeitsumgebungen, Datenbanken und anderen Datenquellen über die Registerkarte **Data Sense** oder durch Auswahl einer bestimmten Arbeitsumgebung aktivieren.

["Erste Schritte"](#).



Die Aktivierung von Cloud Data Sense auf einer Datenquelle führt zu einem sofortigen ersten Scan. Ergebnisse des Scans werden kurz danach angezeigt.

Wie deaktiviere ich Cloud Data Sense?

Sie können Cloud Data Sense deaktivieren, indem Sie eine individuelle Arbeitsumgebung, Datenbank, Dateifreigabegruppe, OneDrive-Konto oder SharePoint-Konto auf der Seite Data Sense Configuration scannen.

["Weitere Informationen ."](#)



Wenn Sie die Cloud Data Sense Instanz vollständig entfernen möchten, können Sie die Data Sense Instanz manuell aus dem Portal Ihres Cloud-Providers oder vor-Ort-Standorts entfernen.

Kann ich den Service an die Anforderungen meines Unternehmens anpassen?

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

Darüber hinaus bietet Data Sense Ihnen zahlreiche Möglichkeiten, eine benutzerdefinierte Liste von „personenbezogenen Daten“ hinzuzufügen, die Data Sense in Scans identifizieren kann, und Sie erhalten das vollständige Bild darüber, wo sich möglicherweise vertrauliche Daten in Dateien all Ihrer Unternehmen befinden.

- Sie können eindeutige Kennungen hinzufügen, die auf bestimmten Spalten in Datenbanken basieren, die Sie scannen - wir nennen dies **Data Fusion**.
- Sie können benutzerdefinierte Schlüsselwörter aus einer Textdatei hinzufügen.
- Sie können benutzerdefinierte Muster mit einem regulären Ausdruck (regex) hinzufügen.

["Weitere Informationen ."](#)

Kann ich die Informationen zur Nutzung von Cloud-Daten auf bestimmte Benutzer begrenzen?

Ja, Cloud Data Sense ist vollständig in BlueXP integriert. BlueXP-Benutzer können nur Informationen für die Arbeitsumgebungen sehen, für die sie gemäß ihren Arbeitsbereichsberechtigungen angezeigt werden können.

Wenn Sie bestimmten Benutzern die Möglichkeit geben möchten, nur die Ergebnisse des Data Sense-Scans anzuzeigen, ohne die Möglichkeit zu haben, Einstellungen für den Datensense zu verwalten, können Sie diesen Benutzern die Rolle Cloud Compliance Viewer zuweisen.

["Weitere Informationen ."](#)

Kann jeder auf die privaten Daten zugreifen, die zwischen meinem Browser und Data Sense gesendet werden?

Nein Die zwischen Ihrem Browser und der Data Sense Instanz gesendeten privaten Daten sind durch eine lückenlose Verschlüsselung gesichert, sodass NetApp und Dritte sie nicht lesen können. Der „Data Sense“ gibt keine Daten oder Ergebnisse an NetApp weiter, es sei denn, Sie fordern und genehmigen den Zugriff.

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

Vielleicht möchten Sie Cloud Data Sense auf ONTAP Systemen aktivieren, die selten genutzte Daten auf Objekt-Storage verschieben. Wenn das Daten-Tiering aktiviert ist, scannt Data Sense alle Daten - Daten, die sich auf Festplatten befinden, und kalte Daten werden auf Objekt-Storage verschoben.

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

Kann Cloud Data Sense Benachrichtigungen an mein Unternehmen senden?

Ja. In Verbindung mit der Funktion Richtlinien können Sie E-Mail-Benachrichtigungen an BlueXP-Benutzer (täglich, wöchentlich oder monatlich) oder andere E-Mail-Adressen senden, wenn eine Richtlinie Ergebnisse liefert, damit Sie Benachrichtigungen zum Schutz Ihrer Daten erhalten können. Weitere Informationen zu ["Richtlinien"](#).

Sie können auch Statusberichte von der Seite Governance und Untersuchung herunterladen, die Sie intern in Ihrem Unternehmen teilen können.

Kann Cloud Data Sense mit den in meinen Dateien eingebetteten AIP-Etiketten arbeiten?

Ja. Sie können AIP-Etiketten in den Dateien verwalten, die Cloud Data Sense scannt, wenn Sie abonniert haben "[Azure Information Protection \(AIP\)](#)". Sie können die bereits zugewiesenen Beschriftungen anzeigen, Dateien Beschriftungen hinzufügen und vorhandene Beschriftungen ändern.

["Weitere Informationen ."](#)

Arten von Quellsystemen und Datentypen

Die folgenden Fragen beziehen sich auf die Art des zu scannenden Speichers und die Arten der gescannten Daten.

Welche Datenquellen können mit Data Sense gescannt werden?

Cloud Data Sense kann Daten aus Arbeitsumgebungen, die Sie dem BlueXP Canvas hinzugefügt haben, und aus vielen Arten von strukturierten und unstrukturierten Datenquellen scannen, auf die Data Sense über Ihre Netzwerke zugreifen kann.

- Arbeitsumgebungen:*
- Cloud Volumes ONTAP (implementiert in AWS, Azure oder GCP)
- On-Premises ONTAP Cluster
- Azure NetApp Dateien
- Amazon FSX für ONTAP
- Amazon S3

Datenquellen:

- File Shares von anderen Anbietern
- Objekt-Storage (nutzt S3-Protokoll)
- Datenbanken (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA, SQL SERVER)
- OneDrive Accounts
- SharePoint Online- und On-Premises-Accounts
- Google Drive-Konten

Data Sense unterstützt NFS-Versionen 3.x, 4.0 und 4.1 sowie CIFS Versionen 1.x, 2.0, 2.1 und 3.0.

Gibt es Einschränkungen bei der Bereitstellung in einer Regierungsregion?

Cloud Data Sense wird unterstützt, wenn der Connector in einer Regierungsregion bereitgestellt wird (AWS GovCloud, Azure Gov oder Azure DoD). Wenn Daten Sense auf diese Weise eingesetzt wird, gelten folgende Einschränkungen:

- OneDrive-Konten, SharePoint-Konten und Google-Laufwerk Konten können nicht gescannt werden.
- Die Funktionalität der Microsoft Azure Information Protection (AIP)-Etiketten kann nicht integriert werden.

Welche Datenquellen kann ich scannen, wenn ich Daten Sense auf einer Website ohne Internetzugang installiere?

Data Sense kann Daten nur von lokalen Datenquellen scannen, die sich am lokalen Standort befinden. Derzeit scannt Data Sense die folgenden lokalen Datenquellen an einem „dunklen“ Standort:

- On-Premises ONTAP Systeme
- Datenbankschemas
- SharePoint On-Premises-Accounts (SharePoint Server)
- NFS- oder CIFS-Dateifreigaben anderer Anbieter
- Objekt-Storage, der das Simple Storage Service (S3)-Protokoll verwendet

Welche Dateitypen werden unterstützt?

Cloud Data Sense scannt alle Dateien nach Informationen zu Kategorie und Metadaten und zeigt alle Dateitypen im Abschnitt Dateitypen im Dashboard an.

Wenn Data Sense personenbezogene Daten (PII) erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt:

.CSV, .DCM, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs, Sheets, and Slides

Welche Arten von Daten und Metadaten ist für Cloud Data sinnvoll?

Cloud Data Sense ermöglicht Ihnen einen allgemeinen Scan mit den Zuordnungen oder einen vollständigen Scan nach Ihren Datenquellen. Das Mapping bietet nur einen Überblick über Ihre Daten auf hoher Ebene, während die Klassifizierung ein tiefes Scannen Ihrer Daten ermöglicht. Das Mapping kann auf Ihren Datenquellen sehr schnell durchgeführt werden, da es nicht auf Dateien zugegriffen wird, um die darin enthaltenen Daten zu sehen.

- Scan der Datenzuordnung

Data Sense scannt nur die Metadaten. Dies ist nützlich für das allgemeine Datenmanagement und die Datenverwaltung, für eine schnelle Projektabwicklung, für sehr große Bestände und für die Priorisierung. Die Datenzuordnung basiert auf Metadaten und gilt als **fast** Scan.

Nach einem schnellen Scan können Sie einen Daten-Mapping-Bericht erstellen. Dieser Bericht bietet einen Überblick über die in Ihren Datenquellen gespeicherten Daten, um Sie bei Entscheidungen zu Ressourcenauslastung, Migration, Backup-, Sicherheits- und Compliance-Prozessen zu unterstützen.

- Scan der Datenklassifizierung (Deep):

Sinngemäß scannt Daten mithilfe von Standardprotokollen und schreibgeschützten Zugriffsrechten in allen Umgebungen. Ausgewählte Dateien werden nach sensiblen Daten, privaten Informationen und Ransomware-Problemen geöffnet und gescannt, die damit verbunden sind.

Nach einem vollständigen Scan gibt es viele zusätzliche Data Sense-Funktionen, die Sie auf Ihre Daten anwenden können, wie zum Beispiel Daten auf der Seite Data Investigation anzeigen und verfeinern, nach Namen innerhalb von Dateien suchen, Quelldateien kopieren, verschieben und löschen und vieles mehr.

Lizenzen und Kosten

Die folgenden Fragen beziehen sich auf Lizenzierung und Kosten für die Verwendung von Cloud Data Sense.

Wie viel kostet Cloud-Daten?

Die Kosten für die Verwendung von Cloud Data Sense hängen von der Datenmenge ab, die Sie scannen. Die ersten 1 TB an Daten, die Data Sense in einem BlueXP-Arbeitsbereich scannt, sind kostenlos. Nach Erreichen dieser Obergrenze benötigen Sie einen der folgenden Methoden, um mit dem Scannen von Daten über 1 TB fortzufahren:

- Ein Abonnement des BlueXP Marketplace-Abonnements von Ihrem Cloud-Provider oder
- Byol-Modell (Bring-Your-Own-License) von NetApp

Siehe "[Preisgestaltung](#)" Entsprechende Details.

Was geschieht, wenn ich das BYOL-Kapazitätslimit erreicht habe?

Wenn Sie eine Byol-Kapazitätsgrenze erreichen, läuft Data Sense weiter, der Zugriff auf die Dashboards ist jedoch blockiert, sodass Sie keine Informationen zu Ihren gescannten Daten anzeigen können. Nur die Konfigurationsseite ist verfügbar, wenn Sie die Anzahl der eingescannten Volumes reduzieren möchten, um die Kapazitätsnutzung unter das Lizenzlimit zu bringen. Um den vollen Zugriff auf Data Sense zu erhalten, müssen Sie Ihre Byol-Lizenz verlängern.

Connector-Bereitstellung

Die folgenden Fragen beziehen sich auf den BlueXP Connector.

Was ist der Steckverbinder?

Der Connector ist eine Software, die auf einer Computing-Instanz entweder in Ihrem Cloud-Konto oder vor Ort ausgeführt wird und es BlueXP ermöglicht, Cloud-Ressourcen sicher zu managen. Sie müssen einen Connector bereitstellen, um Cloud Data Sense zu verwenden.

Wo muss der Connector installiert werden?

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS, Amazon FSX für ONTAP oder in AWS S3 Buckets wird in AWS ein Connector verwendet.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konnektor in Azure.
- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP wird ein Connector in GCP verwendet.
- Beim Scannen von Daten in lokalen ONTAP Systemen, File Shares anderer Anbieter, generischer S3 Objekt-Storage, Datenbanken, OneDrive Ordner, SharePoint Konten und Google Drive Konten können Sie einen Konnektor in jedem dieser Cloud-Standorte verwenden.

Wenn die Daten an vielen dieser Standorte gespeichert sind, müssen Sie eventuell verwenden "[Mehrere Anschlüsse](#)".

Kann ich den Connector auf meinem eigenen Host bereitstellen?

Ja. Das können Sie "[Stellen Sie den Connector vor Ort bereit](#)" Auf einem Linux-Host in Ihrem Netzwerk oder in der Cloud. Wenn Sie planen, Data Sense vor Ort zu implementieren, sollten Sie möglicherweise auch den

Connector vor Ort installieren, dieser ist jedoch nicht erforderlich.

Wie sieht es mit sicheren Websites ohne Internetzugang aus?

Ja, das wird auch unterstützt. Das können Sie ["Stellen Sie den Connector auf einem lokalen Linux-Host, der keinen Internetzugang hat"](#). Anschließend können Sie ONTAP Cluster vor Ort und andere lokale Datenquellen erkennen und die Daten mit Data Sense durchsuchen.

Sinnvolle Implementierung von Daten

Die folgenden Fragen beziehen sich auf die separate Instanz Data Sense.

Welche Implementierungsmodelle unterstützt Cloud Data Sense?

Mit BlueXP können Benutzer Systeme praktisch überall scannen und protokollieren, einschließlich On-Premises-, Cloud- und Hybridumgebungen. Cloud Data Sense wird normalerweise mit einem SaaS-Modell implementiert, bei dem der Service über die BlueXP-Schnittstelle aktiviert ist und keine Hardware- oder Softwareinstallation erfordert. Selbst im Implementierungs-Modus mit einem Klick und einem Klick ist das Datenmanagement möglich, unabhängig davon, ob die Datenspeicher sich vor Ort oder in der Public Cloud befinden.

Welche Instanz oder VM ist für Cloud Data Sense erforderlich?

Wenn ["In der Cloud implementiert"](#):

- In AWS läuft Cloud Data Sense auf einer m5.4xlarge-Instanz mit einer 500-GB-GP2-Festplatte.
- In Azure wird Cloud Data Sense auf einer Standard_D16s_v3 VM mit einer 512-GB-Festplatte ausgeführt.
- In GCP läuft Cloud Data Sense auf einer n2-Standard-16-VM mit einem persistenten 512-GB-Standard-Laufwerk.

Beachten Sie, dass Sie Daten Sense auf einem System mit weniger CPUs und weniger RAM implementieren können, es gibt jedoch Einschränkungen bei der Verwendung dieser Systeme. Siehe ["Verwenden eines kleineren Instanztyps"](#) Entsprechende Details.

["Finden Sie heraus, wie Cloud Data Sense funktioniert"](#).

Kann ich den Data Sense auf meinem eigenen Host bereitstellen?

Ja. Sie können die Software Data Sense auf einem Linux-Host installieren, der Internetzugang in Ihrem Netzwerk oder in der Cloud hat. Alles funktioniert gleich, und Sie verwalten Ihre Scankonfiguration und -Ergebnisse weiterhin mit BlueXP. Siehe ["Cloud-Daten sinnvoll vor Ort"](#) Für die Systemanforderungen und Installationsdetails.

Wie sieht es mit sicheren Websites ohne Internetzugang aus?

Ja, das wird auch unterstützt. Das können Sie ["Implementieren Sie Data Sense auf einem lokalen Standort, der keinen Internetzugang hat"](#) Für vollständig sichere Standorte.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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