Los geht's

BlueXP classification

NetApp
July 25, 2024

Inhalt

Los geht’s

Mehr zur BlueXP Klassifizierung

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

WICHTIG

Ab Mai 2024 mit Version 1.31 ist die BlueXP Klassifizierung als zentrale Funktion in BlueXP ohne Aufpreis verfügbar. Es ist keine Lizenz zur Klassifizierung oder kein Abonnement erforderlich. Wir haben die BlueXP Klassifizierungsfunktionen auch auf NetApp Storage-Systeme fokussiert, sodass einige nicht genutzte oder nicht ausgelastete Funktionen veraltet sind.

"Siehe eine Liste der veralteten Features".

Benutzer, die ältere Versionen 1.30 oder früher verwenden, können diese Version bis zum Ablauf ihres Abonnements weiterhin verwenden.

Funktionen

Die BlueXP Klassifizierung verwendet künstliche Intelligenz (KI), Natural Language Processing (NLP) und Machine Learning (ML), um den gescannten Inhalt zu verstehen. Anhand dessen werden Entitäten extrahiert und die Inhalte entsprechend kategorisiert. Dadurch kann die BlueXP Klassifizierung folgende Funktionsbereiche bieten.

"Weitere Informationen zu Anwendungsfällen für die BlueXP Klassifizierung".

Einhaltung von Compliance-Vorschriften

Die BlueXP Klassifizierung bietet verschiedene Tools, die Sie bei Ihren Compliance-Bemühungen unterstützen können. Die BlueXP Klassifizierung ermöglicht Ihnen:

- 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.

Erhöhte Sicherheit

Mit der BlueXP Klassifizierung können Daten identifiziert werden, die potenziell gefährdet sind, aus strafrechtlichen Gründen auf sie zugegriffen zu werden. Die BlueXP Klassifizierung ermöglicht Ihnen:

- 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 automatisch neue Sicherheitsprobleme zu erkennen, damit Sicherheitspersonal sofort Maßnahmen ergreifen kann.

Optimieren Sie die Storage-Auslastung

Die BlueXP Klassifizierung bietet Tools, die Sie bei Ihren Storage-Gesamtbetriebskosten (TCO) unterstützen. Die BlueXP Klassifizierung ermöglicht Ihnen:

- Erhöhte Storage-Effizienz durch Identifizierung doppelter oder nicht geschäftlicher Daten
- 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".

Unterstützte Arbeitsumgebungen und Datenquellen

Die BlueXP Klassifizierung kann strukturierte und unstrukturierte Daten aus den folgenden Arten von Arbeitsumgebungen und Datenquellen scannen und analysieren:

Arbeitsumgebungen

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

Datenquellen

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

Die BlueXP Klassifizierung unterstützt NFS-Versionen 3.x und CIFS-Versionen 1.x, 2.0, 2.1 und 3.0.

Kosten

Die BlueXP Klassifizierung ist jetzt kostenlos. Es ist keine Klassifizierungslizenz oder kostenpflichtiges Abonnement erforderlich.

Infrastrukturkosten

- Für die Installation der BlueXP Klassifizierung in der Cloud ist die Implementierung einer Cloud-Instanz erforderlich. Dies führt zu Gebühren beim Cloud-Provider, wo die Klassifizierung implementiert wird. Siehe Der für jeden Cloud-Provider implementierte Instanztyp. Die Installation der BlueXP Klassifizierung auf einem lokalen System kostet Sie nichts.
- Für die Klassifizierung von BlueXP müssen Sie einen BlueXP Connector implementiert haben. 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.

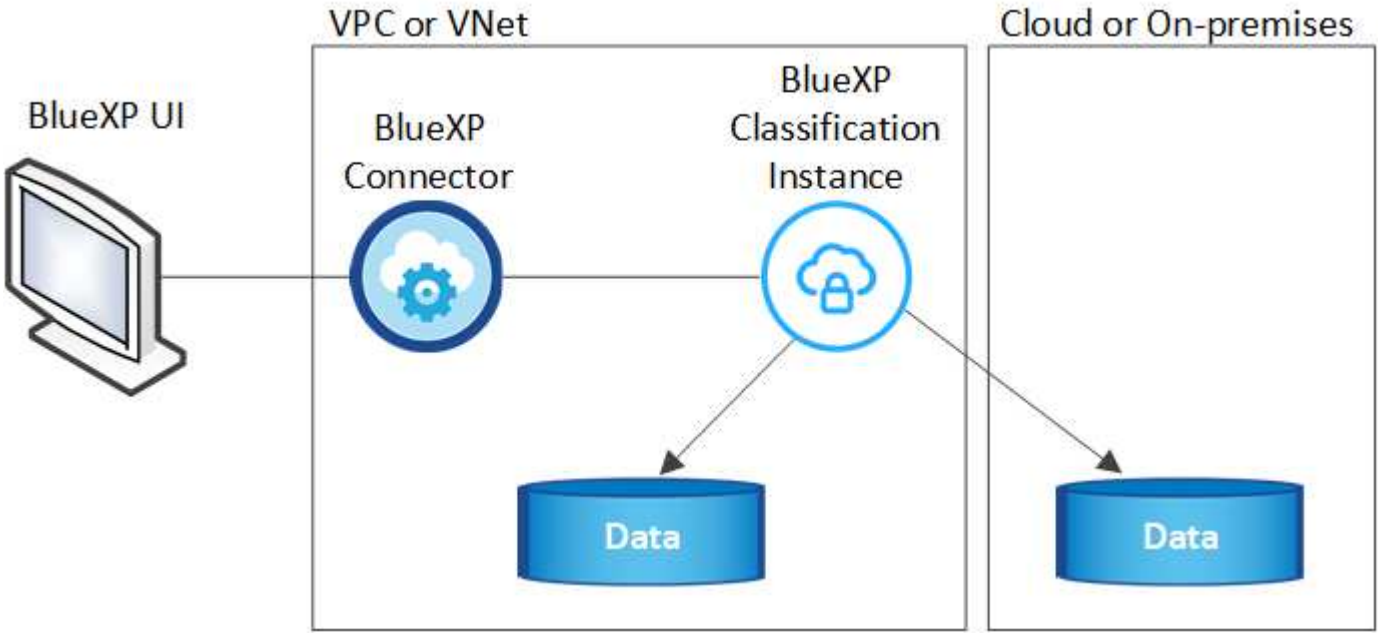
Datentransferkosten

Die Datentransferkosten hängen von Ihrer Einrichtung ab. Wenn sich die BlueXP Klassifizierungs-Instanz und Datenquelle in derselben Verfügbarkeitszone und -Region befinden, entstehen keine Kosten für Datentransfers. Wenn sich die Datenquelle, z. B. ein Cloud Volumes ONTAP-System, jedoch in einer „*different* Verfügbarkeitszone“ oder -Region befindet, werden Ihnen die Kosten für den Datentransfer von Ihrem Cloud-Provider in Rechnung gestellt. Weitere Informationen finden Sie unter diesen Links:

- "AWS – Amazon Elastic Compute Cloud (Amazon EC2) Preisstruktur"
- "Microsoft Azure: Preisangaben Für Die Bandbreite"
- "Google Cloud: Preis für Storage Transfer Service"

Die BlueXP Klassifizierungsinstanz

Wenn Sie die BlueXP Klassifizierung in der Cloud implementieren, stellt BlueXP die Instanz im selben Subnetz bereit, in dem sich der Connector befindet. "Erfahren Sie mehr über Steckverbinder."



Beachten Sie Folgendes über die Standardinstanz:

- In AWS wird die BlueXP Klassifizierung auf einer ausgeführt "M6i.4xlarge-Instanz" Mit einer GP2-Festplatte mit 500 gib. Das Betriebssystem-Image ist Amazon Linux 2. Bei der Implementierung in AWS können Sie

eine kleinere Instanzgröße wählen, wenn Sie eine kleine Datenmenge scannen.

- In Azure wird die BlueXP Klassifizierung auf einer ausgeführt "Standard_D16s_v3 VM" Auf einer Festplatte mit 500 gib. Das Betriebssystem-Image ist CentOS 7.9.
- In GCP wird die BlueXP Klassifizierung auf einer ausgeführt "n2-Standard-16-VM" Mit einer persistenten Festplatte mit 500 gib Standard. Das Betriebssystem-Image ist CentOS 7.9.
- In Regionen, in denen die Standardinstanz nicht verfügbar ist, wird die BlueXP Klassifizierung auf einer alternativen Instanz ausgeführt. "Sehen Sie sich die alternativen Instanztypen an".
- 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 BlueXP Klassifizierungsinstanz implementiert.

Sie können die BlueXP Klassifizierung auch auf einem Linux-Host vor Ort oder auf einem Host in Ihrem bevorzugten Cloud-Provider implementieren. Die Software funktioniert unabhängig von der gewählten Installationsmethode genau auf die gleiche Weise. Upgrades der BlueXP Klassifizierungs-Software werden automatisiert, solange die Instanz einen Internetzugang hat.

Die Instanz sollte immer ausgeführt werden, da die BlueXP Klassifizierung die Daten kontinuierlich scannt.

Implementierung auf verschiedenen Instanztypen

Sie können die BlueXP Klassifizierung auf einem System mit weniger CPUs und weniger RAM implementieren.

Systemgröße	Spezifikationen	Einschränkungen
Extra Groß	32 CPUs, 128 GB RAM, 1 tib SSD	Kann bis zu 500 Millionen Dateien scannen.
Groß (Standard)	16 CPUs, 64 GB RAM, 500 gib SSD	Kann bis zu 250 Millionen Dateien scannen.

Bei der Implementierung der BlueXP Klassifizierung in Azure oder GCP können Sie eine E-Mail an ng-contact-data-sense@netapp.com senden, um Unterstützung zu erhalten, wenn Sie einen kleineren Instanztyp verwenden möchten.

Funktionsweise der BlueXP Klassifizierung

Die allgemeine BlueXP Klassifizierung funktioniert wie folgt:

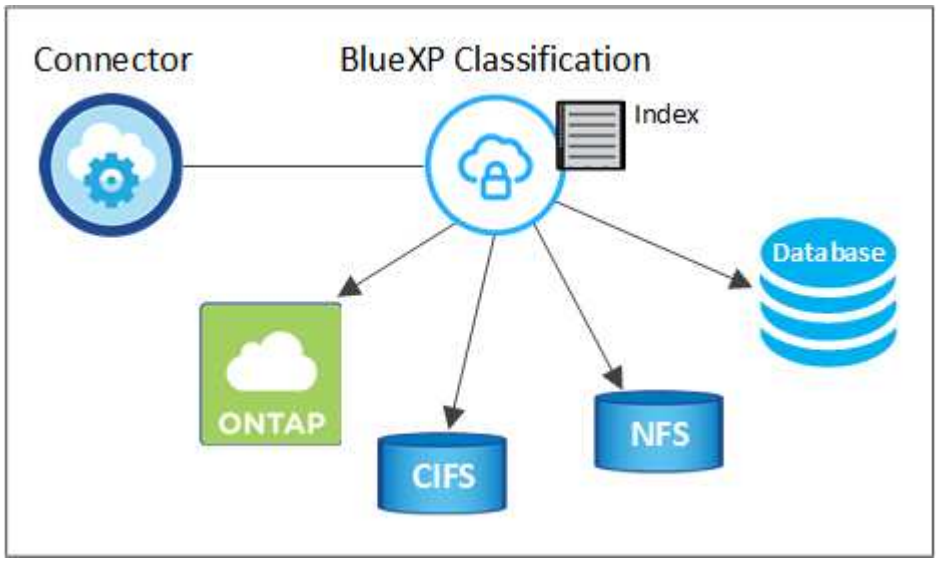
1. Sie implementieren eine Instanz der BlueXP Klassifizierung in BlueXP.
2. Sie ermöglichen ein hohes Mapping oder tiefes Scannen auf einer oder mehreren Datenquellen.
3. Bei der BlueXP Klassifizierung werden die Daten mithilfe eines KI-Lernprozesses gescannt.
4. Sie nutzen die bereitgestellten Dashboards und Berichterstellungs-Tools, um Ihre Compliance- und Governance-Bemühungen zu unterstützen.

Funktionsweise von Scans

Nachdem die BlueXP Klassifizierung aktiviert und die Repositorys ausgewählt wurden, die gescannt werden sollen (dies sind die Volumes, Datenbankschemas oder andere Benutzerdaten), beginnt der Service sofort mit

dem Scannen der Daten, um persönliche und sensible Daten zu identifizieren. Sie sollten sich in den meisten Fällen auf die Scans von Live-Produktionsdaten konzentrieren und nicht auf Backups, Spiegelungen oder DR-Standorte. Die BlueXP Klassifizierung ordnet anschließend Ihre Unternehmensdaten 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.

Wie bei jedem anderen Client lässt sich die BlueXP Klassifizierung mit den Daten verbinden, indem NFS- und CIFS-Volumes gemountet werden. NFS Volumes werden automatisch als schreibgeschützt abgerufen und müssen zur Überprüfung von CIFS Volumes Active Directory Anmeldeinformationen bereitstellen.



Nach dem ersten Scan scannt die BlueXP Klassifizierung Ihre Daten fortlaufend und nach Round Robin-Verfahren, um inkrementelle Änderungen zu erkennen (aus diesem Grund ist es wichtig, die Instanz weiterhin auszuführen).

Sie können Scans auf Volume-Ebene oder auf Datenbankschemaebene aktivieren und deaktivieren.

Was ist der Unterschied zwischen Mapping und Classification Scans

Die BlueXP Klassifizierung ermöglicht Ihnen die Durchführung eines allgemeinen „Mapping“-Scans für ausgewählte 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.

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
Scangeschgeschwindigkeit	Langsam	Schnell
Preisgestaltung	Kostenlos	Kostenlos
Kapazität	Begrenzt auf 500 TB	Begrenzt auf 500 TB
Liste der Dateitypen und der genutzten Kapazität	Ja.	Ja.

Merkmal	Klassifizierung	Zuordnung
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
Möglichkeit zur Ausführung anderer Berichte	Ja.	Nein
Fähigkeit, Metadaten aus Dateien zu sehen*	Nein	Ja.

*Die folgenden Metadaten werden während der Mapping-Scans aus Dateien extrahiert:

- Arbeitsumgebung
- Art der Arbeitsumgebung
- Storage Repository
- Dateityp
- Genutzte Kapazität
- Anzahl der Dateien
- Dateigröße
- Dateierstellung
- Letzter Zugriff auf die Datei
- Datei zuletzt geändert
- Erkannte Zeit der Datei
- Extraktion von Berechtigungen

Unterschiede in der Governance-Konsole:

Merkmal	Zuordnen Und Klassifizieren	Karte
Veraltete Daten	Ja.	Ja.
Nichtgeschäftliche Daten	Ja.	Ja.
Duplizierte Dateien	Ja.	Ja.
Vordefinierte Richtlinien	Ja.	Nein
Benutzerdefinierte Richtlinien	Ja.	Ja.
DDA-Bericht	Ja.	Ja.
Zuordnungsbericht	Ja.	Ja.
Erkennung des Empfindlichkeitsniveaus	Ja.	Nein

Merkmal	Zuordnen Und Klassifizieren	Karte
Sensible Daten mit großen Berechtigungen	Ja.	Nein
Berechtigungen öffnen	Ja.	Ja.
Alter der Daten	Ja.	Ja.
Datengröße	Ja.	Ja.
Kategorien	Ja.	Nein
Dateitypen	Ja.	Ja.

Unterschiede im Compliance-Dashboard:

Merkmal	Zuordnen Und Klassifizieren	Karte
Persönliche Angaben	Ja.	Nein
Sensible persönliche Daten	Ja.	Nein
Bericht zur Risikoanalyse personenbezogener Daten	Ja.	Nein
HIPAA-Bericht	Ja.	Nein
PCI DSS-Bericht	Ja.	Nein

Untersuchungsfilter Unterschiede:

Merkmal	Zuordnen Und Klassifizieren	Karte
Richtlinien	Ja.	Ja.
Art der Arbeitsumgebung	Ja.	Ja.
Arbeitsumgebung	Ja.	Ja.
Storage Repository	Ja.	Ja.
Dateityp	Ja.	Ja.
Dateigröße	Ja.	Ja.
Erstellungszeit	Ja.	Ja.
Entdeckte Zeit	Ja.	Ja.
Zuletzt geändert	Ja.	Ja.
Letzter Zugriff	Ja.	Ja.
Berechtigungen öffnen	Ja.	Ja.
Dateiverzeichnispfad	Ja.	Ja.
Kategorie	Ja.	Nein
Empfindlichkeitsstufe	Ja.	Nein
Anzahl der Kennungen	Ja.	Nein

Merkmal	Zuordnen Und Klassifizieren	Karte
Persönliche Daten	Ja.	Nein
Sensible persönliche Daten	Ja.	Nein
Betroffene Person	Ja.	Nein
Duplikate	Ja.	Ja.
Klassifizierungsstatus	Ja.	Status ist immer „Eingeschränkte Einblicke“
Analyseereignis scannen	Ja.	Ja.
Datei-Hash	Ja.	Ja.
Anzahl der Benutzer mit Zugriff	Ja.	Ja.
Benutzer-/Gruppenberechtigungen	Ja.	Ja.
Dateibesitzer	Ja.	Ja.
Verzeichnistyp	Ja.	Ja.

Wie schnell scannt die BlueXP Klassifizierung Daten

Die Scan-Geschwindigkeit wird durch Netzwerklatenz, Festplattenlatenz, Netzwerkbandbreite, Umgebungsgröße und Dateiverteilungsgrößen beeinflusst.

- Bei der Durchführung von Mapping-Scans kann die BlueXP Klassifizierung zwischen 100-150 TIBS Daten pro Tag scannen.
- Bei der Durchführung von Classification Scans können mit der BlueXP Klassifizierung Daten zwischen 15-40 TIBS pro Tag gescannt werden.

Informationen, die die BlueXP Klassifizierung indexiert

Die BlueXP Klassifizierung erfasst, indiziert und weist Ihren Daten (Dateien) Kategorien zu. Die Daten, die die BlueXP Klassifizierung indiziert, umfassen die folgenden:

- **Standard-Metadaten** die BlueXP-Klassifizierung sammelt Standardmetadaten über Dateien: Dateityp, Größe, Erstellungsdatum und Änderungsdatum usw.
- **Personenbezogene Daten**: Personenbezogene Daten (PII) wie E-Mail-Adressen, Identifikationsnummern oder Kreditkartennummern. "Weitere Informationen zu personenbezogenen Daten".
- **Sensible personenbezogene Daten**: Besondere Arten von sensiblen personenbezogenen Daten (SPii), wie Gesundheitsdaten, ethnische Herkunft oder politische Meinungen, wie sie durch die DSGVO und andere Datenschutzvorschriften definiert sind. "Erfahren Sie mehr über sensible persönliche Daten".
- **Categories**: Die BlueXP-Klassifizierung nimmt die gescannten Daten auf und teilt sie in verschiedene Kategorien auf. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Weitere Informationen zu Kategorien".
- **Types**: Die BlueXP Klassifizierung erfasst die gescannten Daten und unterteilt sie nach Dateityp. "Erfahren Sie mehr über Types".
- **Name Entity Recognition**: BlueXP Klassifikation verwendet KI, um natürliche Namen von Personen aus

Dokumenten zu extrahieren. "Informieren Sie sich über die Reaktion auf Zugriffsanfragen von Betroffenen".

Netzwerkübersicht

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

Wenn Sie BlueXP im SaaS-Modus verwenden, wird die Verbindung zu BlueXP über HTTPS hergestellt. Die privaten Daten, die zwischen Ihrem Browser und der BlueXP Klassifizierungsinstanz gesendet werden, sind durch End-to-End-Verschlüsselung mit TLS 1.2 geschützt. Dies bedeutet, dass NetApp und Drittanbieter die Daten nicht lesen können.

Ausgehende Regeln sind vollständig geöffnet. Zum Installieren und Aktualisieren der BlueXP Klassifizierungssoftware und zum Senden von Nutzungsmetriken ist ein Internetzugriff erforderlich.

Wenn Sie strenge Netzwerkanforderungen erfüllen, "Erfahren Sie mehr über die Endpunkte, auf die BlueXP Klassifizierungen setzt".

Zugriff des Benutzers auf Compliance-Informationen

Die Rolle, die jedem Benutzer zugewiesen wurde, bietet unterschiedliche Funktionen in BlueXP und innerhalb der BlueXP Klassifizierung:

- 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 keine Compliance-Informationen für die Arbeitsumgebung auf der Registerkarte BlueXP Klassifizierung 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.

"Erfahren Sie mehr über BlueXP-Rollen" Und wie "Benutzer mit bestimmten Rollen hinzufügen".

Implementieren Sie die BlueXP Klassifizierung

Welche BlueXP Klassifizierungs-Implementierung sollten Sie verwenden?

Die BlueXP Klassifizierung kann auf unterschiedliche Weise implementiert werden. Erfahren Sie, welche Methode Ihren Anforderungen entspricht.

Die BlueXP Klassifizierung kann wie folgt implementiert werden:

- "Implementieren Sie mit BlueXP in der Cloud". BlueXP implementiert die BlueXP Klassifizierungsinstanz im selben Cloud-Provider-Netzwerk wie der BlueXP Connector.
- "Installation auf einem Linux-Host mit Internetzugang". Installieren Sie die BlueXP Klassifizierung auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud mit Internetzugang. Diese Art der Installation ist möglicherweise eine gute Option, wenn Sie lokale ONTAP Systeme mit einer BlueXP Klassifizierungsinstanz scannen möchten, die sich auch vor Ort befindet. Das ist jedoch keine Anforderung.

- "Installation auf einem Linux-Host an einem Standort ohne Internetzugang", Auch bekannt als *privater Modus.* Diese Art der Installation, die ein Installationsskript verwendet, ist gut für Ihre sicheren Seiten.

Sowohl die Installation auf einem Linux-Host mit Internetzugang als auch die Installation vor Ort auf einem Linux-Host ohne Internetzugang verwenden ein Installationsskript. Das Skript beginnt mit der Überprüfung, ob das System und die Umgebung die Voraussetzungen erfüllen. Wenn die Voraussetzungen erfüllt sind, wird die Installation gestartet. Wenn Sie die Voraussetzungen unabhängig vom Ausführen der BlueXP Klassifizierungssysteminstallation überprüfen möchten, steht Ihnen ein separates Softwarepaket zur Verfügung, das nur auf die Voraussetzungen testet.

Siehe "Stellen Sie sicher, dass Ihr Linux Host bereit ist, die BlueXP Klassifizierung zu installieren".

Implementieren Sie die BlueXP Klassifizierung in der Cloud mit BlueXP

Führen Sie einige Schritte durch, um die BlueXP Klassifizierung in der Cloud zu implementieren. BlueXP implementiert die BlueXP Klassifizierungsinstanz im selben Cloud-Provider-Netzwerk wie der BlueXP Connector.

Beachten Sie, dass Sie auch können "Installieren Sie die BlueXP Klassifizierung auf einem Linux-Host mit Internetzugang". Diese Art der Installation ist möglicherweise eine gute Option, wenn Sie lokale ONTAP Systeme mit einer BlueXP Klassifizierungsinstanz scannen möchten, die sich auch vor Ort befindet. Das ist jedoch keine Anforderung. 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 "Installieren Sie den Steckverbinder vor Ort" Auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud.

2 Voraussetzungen prüfen

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllen kann. Dazu gehören abgehender Internetzugang für die Instanz, Konnektivität zwischen dem Connector und BlueXP Klassifizierung über Port 443 und mehr. Eine vollständige Liste finden Sie hier.

3 Implementieren Sie die BlueXP Klassifizierung

Starten Sie den Installationsassistenten, um die BlueXP Klassifizierungsinstanz in der Cloud zu implementieren.

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 ist wahrscheinlich vor der Aktivierung der BlueXP Klassifizierung ein Connector eingerichtet "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 oder Amazon FSX für ONTAP-Buckets verwenden Sie einen Connector in AWS.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Connector 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.

Lokale ONTAP-Systeme, NetApp-Dateifreigaben und Datenbanken können mit einem dieser Cloud Connectors gescannt werden.

Beachten Sie, dass Sie auch können "Installieren Sie den Steckverbinder vor Ort" Auf einem Linux-Host in Ihrem Netzwerk oder in der Cloud. Einige Benutzer, die die BlueXP Klassifizierung lokal installieren möchten, können den Connector möglicherweise auch On-Premises installieren.

Wie Sie sehen können, gibt es einige Situationen, in denen Sie verwenden müssen "Mehrere Anschlüsse".

Unterstützung für Regierungsregionen

Die BlueXP Klassifizierung wird unterstützt, wenn der Connector in einer Regierungsregion (AWS GovCloud, Azure Gov oder Azure DoD) implementiert wird. Bei einer solchen Implementierung unterliegt die BlueXP Klassifizierung folgenden Einschränkungen:

"Weitere Informationen zur Bereitstellung des Connectors in einer Regierungsregion finden Sie unter".

Voraussetzungen prüfen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass eine unterstützte Konfiguration vorhanden ist, bevor Sie die BlueXP Klassifizierung in der Cloud implementieren. Wenn Sie die BlueXP Klassifizierung in der Cloud implementieren, befindet sich diese im selben Subnetz wie der Connector.

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

Für die BlueXP Klassifizierung ist Outbound-Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxy-Server für den Internetzugang verwendet, stellen Sie sicher, dass die BlueXP Klassifizierungsinstanz über Outbound-Internetzugang verfügt, um die folgenden Endpunkte zu kontaktieren. Der Proxy muss nicht transparent sein - wir unterstützen derzeit keine transparenten Proxys.

Je nachdem, ob Sie die BlueXP Klassifizierung in AWS, Azure oder GCP implementieren, können Sie die entsprechende Tabelle unten durchsehen.

Erforderliche Endpunkte für AWS

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://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://dseasb33srnrn.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	Die BlueXP Klassifizierung ermöglicht den Zugriff auf Manifeste und Vorlagen sowie das Senden von Protokollen und Kennzahlen.

Erforderliche Endpunkte für Azure

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://dseasb33srnrn.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.

Erforderliche Endpunkte für GCP

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.

Endpunkte	Zweck
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://dseasb33srnrn.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.

Stellen Sie sicher, dass BlueXP über die erforderlichen Berechtigungen verfügt

Stellen Sie sicher, dass BlueXP über Berechtigungen zum Implementieren von Ressourcen und zum Erstellen von Sicherheitsgruppen für die BlueXP Klassifizierungsinstanz verfügt. Die neuesten BlueXP-Berechtigungen finden Sie in "Die von NetApp bereitgestellten Richtlinien".

Sicherstellen, dass der BlueXP Connector auf die BlueXP Klassifizierung zugreifen kann

Stellen Sie die Konnektivität zwischen dem Connector und der BlueXP Klassifizierungsinstanz sicher. Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über Port 443 zur und von der BlueXP Klassifizierungsinstanz zulassen. Über diese Verbindung wird die Bereitstellung der BlueXP Klassifizierungsinstanz ermöglicht und Sie können Informationen auf der Registerkarte für Compliance und Governance einsehen. Die BlueXP Klassifizierung 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 die BlueXP Klassifizierung weiter ausgeführt werden kann

Die BlueXP Klassifizierungs-Instanz muss aktiviert bleiben, um Ihre Daten kontinuierlich zu scannen.

Webbrowser-Konnektivität zur BlueXP Klassifizierung sicherstellen

Nachdem die Klassifizierung von BlueXP aktiviert ist, stellen Sie sicher, dass Benutzer von einem Host, der über eine Verbindung zur BlueXP Klassifizierungsinstanz verfügt, auf die BlueXP Schnittstelle zugreifen.

Die BlueXP Klassifizierungs-Instanz verwendet eine private IP-Adresse, um sicherzustellen, dass die indizierten Daten nicht für das Internet 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 aus einer direkten Verbindung zu Ihrem Cloud-Provider (z. B. einem VPN) oder von einem Host im selben Netzwerk wie die BlueXP Klassifizierungsinstanz stammen.

Überprüfen Sie Ihre vCPU-Limits

Stellen Sie sicher, dass die vCPU-Begrenzung Ihres Cloud-Providers die Bereitstellung einer Instanz mit der erforderlichen Anzahl an Kernen 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"

Hinweis: Sie können die BlueXP Klassifizierung auf einer Instanz in AWS-Cloud-Umgebungen mit weniger CPUs und weniger RAM implementieren. Bei der Verwendung dieser Systeme bestehen jedoch Einschränkungen. Siehe "Verwenden eines kleineren Instanztyps" Entsprechende Details.

Implementieren Sie die BlueXP Klassifizierung in der Cloud

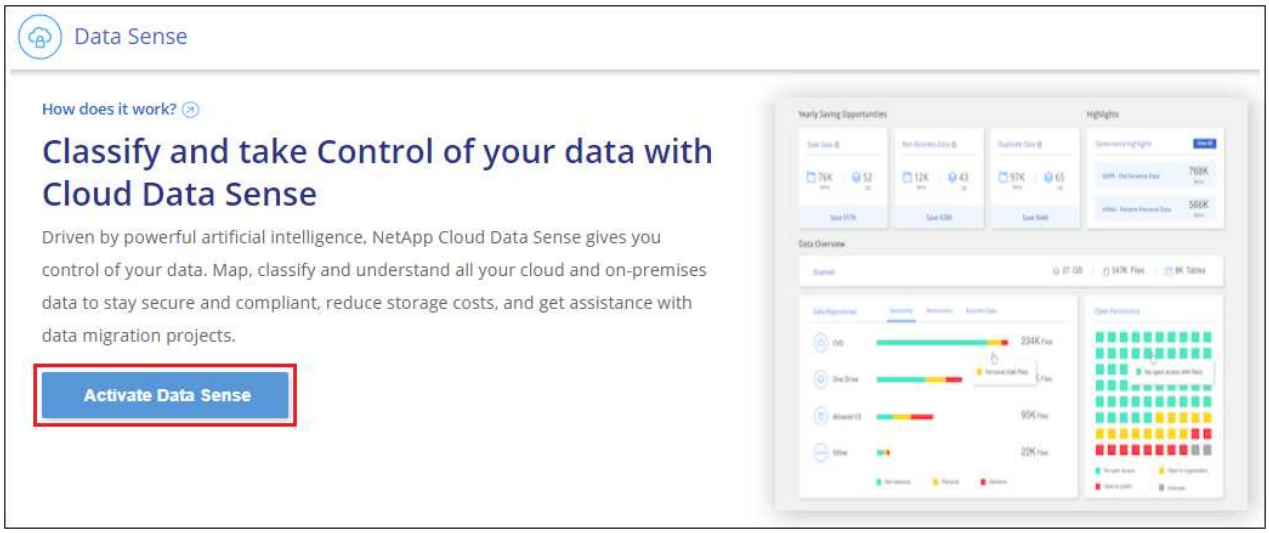
Führen Sie diese Schritte aus, um eine Instanz der BlueXP Klassifizierung in der Cloud zu implementieren. Der Connector implementiert die Instanz in der Cloud und installiert dann die BlueXP Klassifizierungssoftware auf dieser Instanz.

Hinweis: Wenn Sie die BlueXP Klassifizierung aus einem BlueXP Connector in einer AWS-Umgebung implementieren, können Sie die Standardgröße der Instanzen auswählen oder zwischen zwei kleineren Instanztypen wählen. "Anzeigen der verfügbaren Instanztypen und Einschränkungen". In Regionen, in denen der Standardinstanztyp nicht verfügbar ist, wird die BlueXP Klassifizierung auf einem ausgeführt "Alternativer Instanztyp".

Implementieren in AWS

Schritte

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



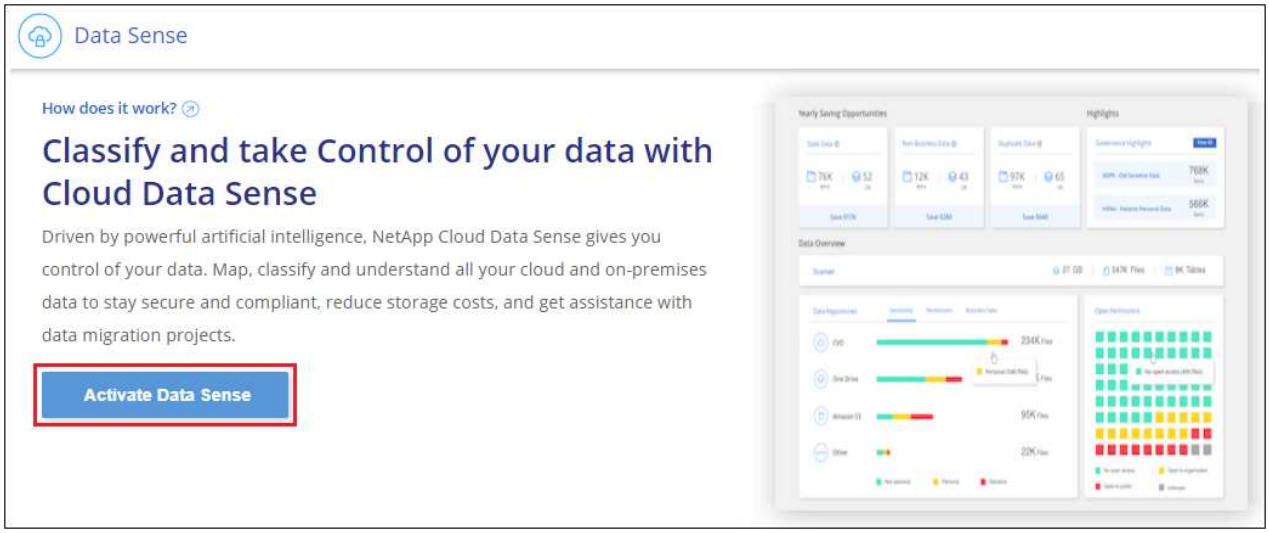
2. Klicken Sie Auf **Datensense Aktivieren**.
3. Klicken Sie auf der Seite *Installation* auf **Deploy > Deploy**, um die „große“ Instanzgröße zu verwenden und den Cloud-Bereitstellungsassistenten zu starten.
4. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Es wird angehalten und zur Eingabe aufgefordert, wenn Probleme auftreten.

5. Wenn die Instanz bereitgestellt und die BlueXP-Klassifizierung installiert ist, klicken Sie auf **Weiter zur Konfiguration**, um zur Seite *Configuration* zu gelangen.

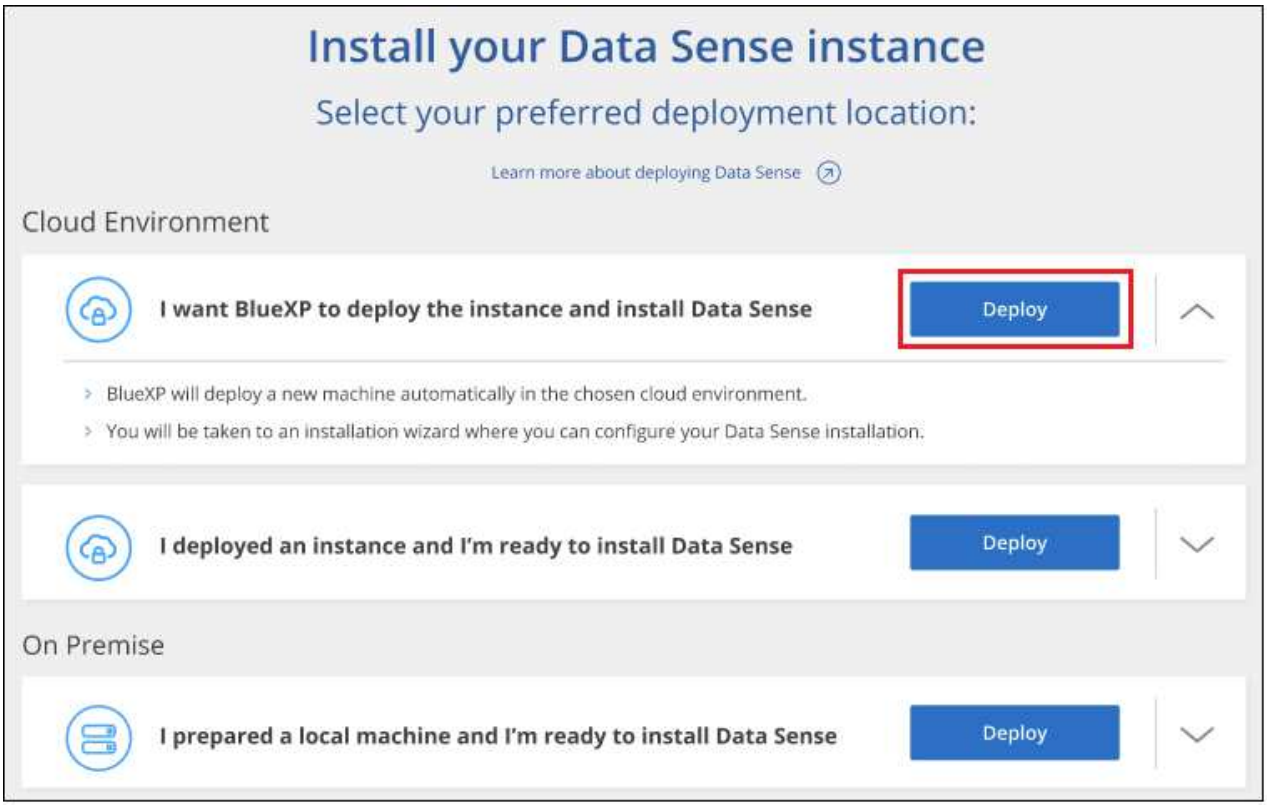
Implementieren in Azure

Schritte

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



3. Klicken Sie auf **Bereitstellen**, um den Cloud-Bereitstellungsassistenten zu starten.



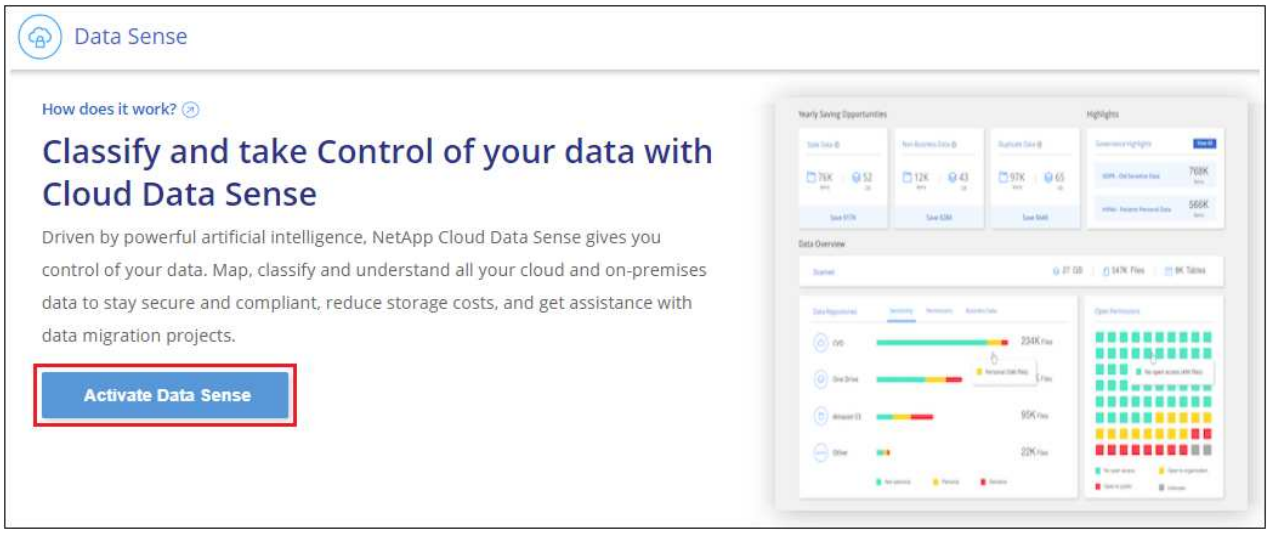
4. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Es wird angehalten und zur Eingabe aufgefordert, wenn Probleme auftreten.

5. Wenn die Instanz bereitgestellt und die BlueXP-Klassifizierung installiert ist, klicken Sie auf **Weiter zur Konfiguration**, um zur Seite *Configuration* zu gelangen.

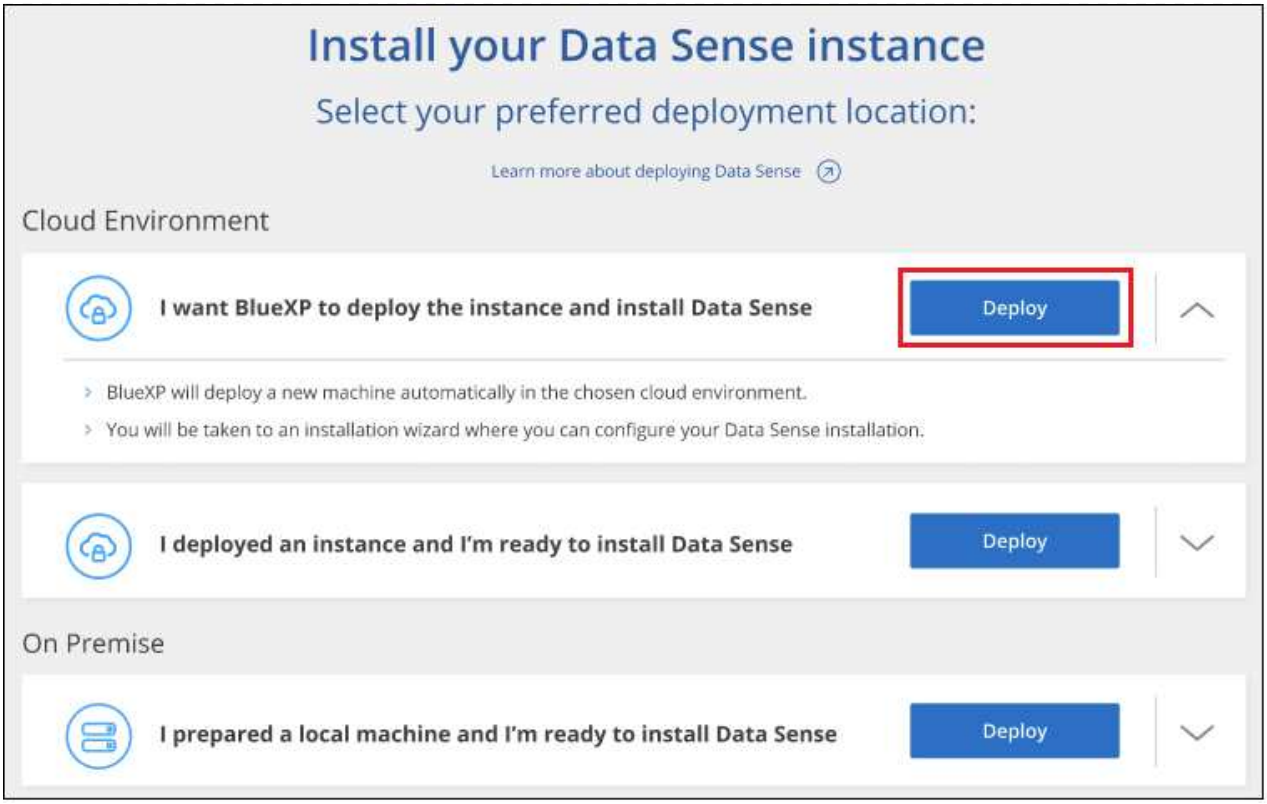
Implementieren in Google Cloud

Schritte

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



3. Klicken Sie auf **Bereitstellen**, um den Cloud-Bereitstellungsassistenten zu starten.



4. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Es wird angehalten und zur Eingabe aufgefordert, wenn Probleme auftreten.

5. Wenn die Instanz bereitgestellt und die BlueXP-Klassifizierung installiert ist, klicken Sie auf **Weiter zur Konfiguration**, um zur Seite *Configuration* zu gelangen.

Ergebnis

BlueXP implementiert die BlueXP Klassifizierungsinstanz in Ihrem Cloud-Provider.

Ein Upgrade der Klassifizierungs-Software BlueXP Connector und BlueXP wird automatisiert, solange die Instanzen über eine Internet-Konnektivität verfügen.

Nächste Schritte

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

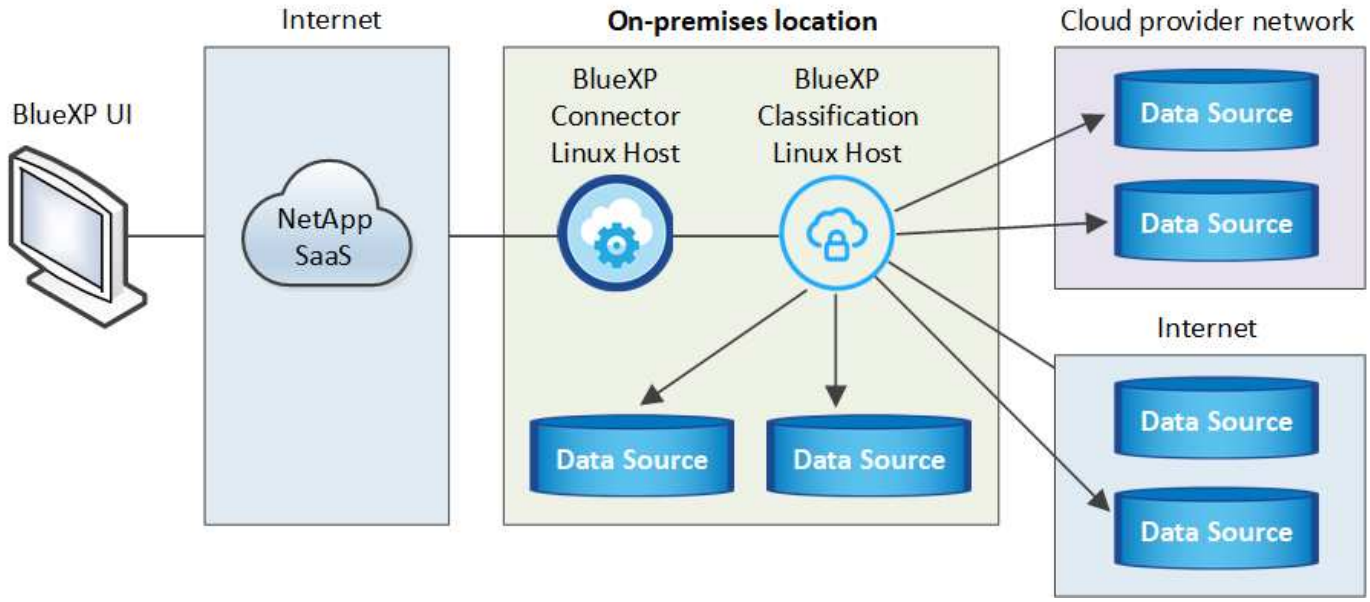
Installieren Sie die BlueXP Klassifizierung auf einem Host mit Internetzugang

Führen Sie einige Schritte durch, um die BlueXP Klassifizierung auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud mit Internetzugang zu installieren. Im Rahmen dieser Installation müssen Sie den Linux-Host manuell in Ihrem Netzwerk oder in der Cloud bereitstellen.

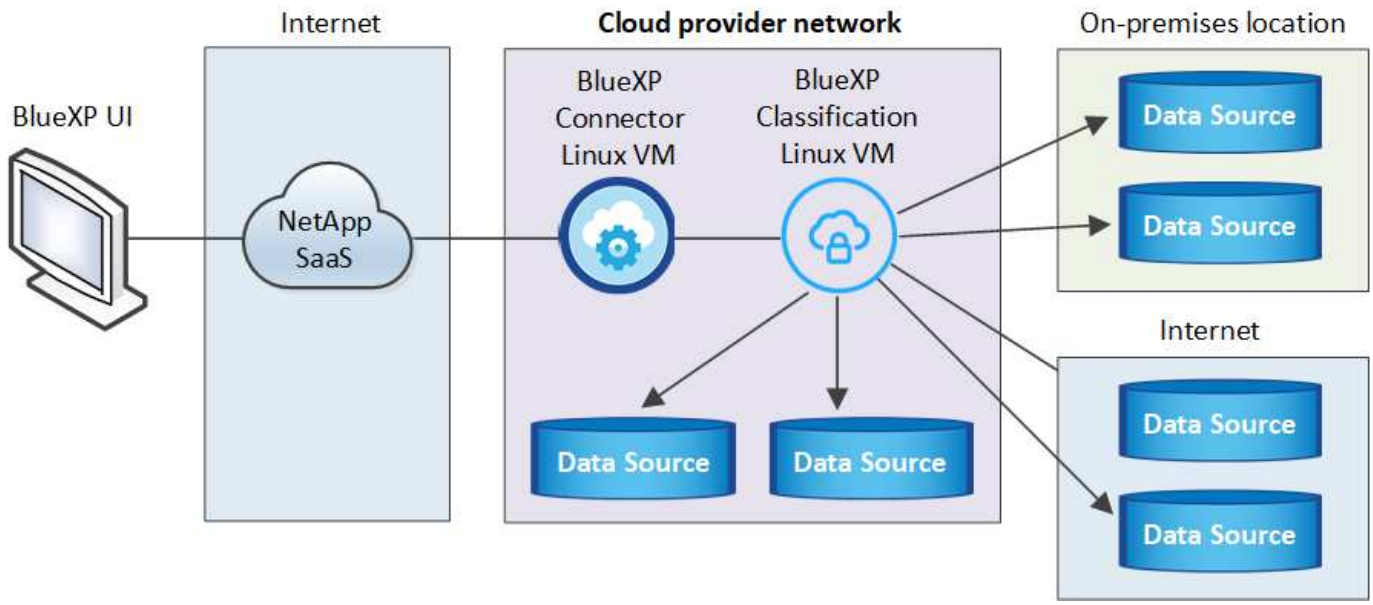
Die On-Premises-Installation ist möglicherweise eine gute Option, wenn Sie On-Premises-ONTAP Systeme mit einer BlueXP Klassifizierungsinstanz scannen möchten, die sich auch vor Ort befindet – dies ist jedoch keine Anforderung. Die Software funktioniert unabhängig von der gewählten Installationsmethode genau auf die gleiche Weise.

Das BlueXP Klassifizierungs-Installationsskript wird zunächst überprüft, ob das System und die Umgebung die erforderlichen Voraussetzungen erfüllen. Wenn alle Voraussetzungen erfüllt sind, wird die Installation gestartet. Wenn Sie die Voraussetzungen unabhängig vom Ausführen der BlueXP Klassifizierungssysteminstallation überprüfen möchten, steht Ihnen ein separates Softwarepaket zur Verfügung, das nur auf die Voraussetzungen testet. "Erfahren Sie, wie Sie überprüfen können, ob Ihr Linux-Host bereit ist, die BlueXP Klassifizierung zu installieren".

Die typische Installation auf einem Linux-Host *in your premises* hat folgende Komponenten und Verbindungen.



Die typische Installation auf einem Linux-Host *in der Cloud* hat die folgenden Komponenten und Verbindungen.



Bei sehr großen Konfigurationen, bei denen Sie mehrere Petabyte an Daten scannen werden, können Sie bei Versionen 1.30 und früher mehrere Hosts integrieren, um zusätzliche Verarbeitungsleistung bereitzustellen. Bei der Verwendung mehrerer Hostsysteme wird das primäre System als *Manager Node* bezeichnet, und die zusätzlichen Systeme, die zusätzliche Rechenleistung bieten, heißen *Scanner Nodes*.

> Informationen zu älteren Versionen 1.30 und älteren Versionen finden Sie unter, wenn Sie BlueXP Klassifizierung auf mehreren Hosts installieren müssen "Installieren Sie die BlueXP Klassifizierung auf mehreren Hosts ohne Internetzugang".

Das können Sie auch "Installieren Sie die BlueXP Klassifizierung auf einer lokalen Website ohne Internetzugang" Für vollständig sichere Standorte.

> Informationen zum Hinzufügen von Scannerknoten für ältere Versionen 1.30 und früher finden Sie unter "Fügen Sie Scannerknoten zu einer vorhandenen Implementierung hinzu".

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 auf einem Linux-Host 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 abgehender Internetzugang für die Instanz, Konnektivität zwischen dem Connector und BlueXP Klassifizierung über Port 443 und mehr. Eine vollständige Liste finden Sie hier.

Außerdem benötigen Sie ein Linux-System, das die erfüllt Erfüllt.

3 Laden Sie die BlueXP Klassifizierung herunter und implementieren Sie sie

Laden Sie die Cloud BlueXP Klassifizierungssoftware von der NetApp Support-Website herunter und kopieren Sie die Installer-Datei auf den geplanten Linux-Host. Starten Sie dann den Installationsassistenten und befolgen Sie die Anweisungen zur Implementierung der BlueXP Klassifizierungsinstanz.

Einen Konnektor erstellen

Ein BlueXP Connector ist erforderlich, bevor Sie die BlueXP Klassifizierung installieren und verwenden können. In den meisten Fällen ist wahrscheinlich vor der Aktivierung der BlueXP Klassifizierung ein Connector eingerichtet. Die meisten dieser Funktionen sind jedoch vorhanden "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 oder Amazon FSX für ONTAP verwenden Sie einen Connector in AWS.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Connector 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.

Lokale ONTAP-Systeme, NetApp-Dateifreigaben und Datenbankkonten können mit jedem 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 auf einem Linux-Host in der Cloud. Einige Benutzer, die die BlueXP Klassifizierung lokal installieren möchten, können den Connector möglicherweise auch On-Premises installieren.

Bei der Installation der BlueXP-Klassifizierung 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

Die BlueXP Klassifizierungssoftware muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Software-Anforderungen usw. erfüllt. Der Linux-Host kann sich in Ihrem Netzwerk oder in der Cloud befinden.

Sorgen Sie dafür, dass die BlueXP Klassifizierung weiter ausgeführt werden kann. Die BlueXP Klassifizierungs-Maschine muss aktiviert bleiben, um Ihre Daten kontinuierlich zu scannen.

- Die BlueXP Klassifizierung wird auf einem Host, der mit anderen Applikationen gemeinsam genutzt wird, nicht unterstützt – der Host muss ein dedizierter Host sein.

- Wenn Sie das Host-System an Ihrem Standort aufbauen, können Sie zwischen diesen Systemgrößen wählen, je nach Größe des Datensatzes, den Sie die BlueXP Klassifizierung scannen möchten.

Systemgröße	CPU	RAM (Swap-Speicher muss deaktiviert sein)	Festplatte
Extra Groß	32 CPUs	128 GB RAM	1 tib SSD auf /, oder - 100 gib verfügbar auf /opt - 895 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Groß	16 CPUs	64 GB RAM	500 gib SSD auf /, oder - 100 gib verfügbar auf /opt - 395 gib verfügbar auf /var/lib/docker oder für Podman /var/lib/Containers oder für Podman /var/lib/Containers - 5 gib auf /tmp

- Bei der Implementierung einer Computing-Instanz in der Cloud für Ihre BlueXP Klassifizierungsinstallation empfehlen wir ein System, das die oben genannten „großen“ Systemanforderungen erfüllt:
  - **Amazon Elastic Compute Cloud (Amazon EC2) Instanztyp**: Wir empfehlen "m6i.4xlarge". "Siehe zusätzliche AWS-Instanztypen".
  - **Größe der Azure VM**: Wir empfehlen „Standard_D16s_v3“. "Siehe zusätzliche Azure-Instanztypen".
  - **GCP-Maschinentyp**: Wir empfehlen "n2-Standard-16". "Weitere GCP-Instanztypen finden Sie unter".
- **UNIX-Ordnerberechtigungen**: Folgende UNIX-Mindestberechtigungen sind erforderlich:

Ordner	Mindestberechtigungen
/Tmp	`rwxrwxrwt`
/Opt	`rwxr-xr-x`
/Var/lib/Docker	`rwx------`
/Usr/lib/systemd/System	`rwxr-xr-x`

- **Betriebssystem**:
  - Für die folgenden Betriebssysteme ist die Verwendung der Docker Container-Engine erforderlich:
    - Red hat Enterprise Linux Version 7.8 und 7.9
    - CentOS Version 7.8 und 7.9
    - Ubuntu 22.04 (BlueXP Klassifikation ab Version 1.23 erforderlich)
  - Die folgenden Betriebssysteme erfordern die Verwendung der Podman Container-Engine. Sie erfordern eine BlueXP Klassifikation der Version 1.30 oder höher:
    - Red hat Enterprise Linux Version 8.8, 9.0, 9.1, 9.2 und 9.3

      Beachten Sie, dass die folgenden Funktionen derzeit nicht unterstützt werden, wenn RHEL 8.x und RHEL 9.x verwendet werden:

      - Installation an einem dunklen Ort

        - Verteiltes Scannen; Verwendung eines Master-Scanner-Knotens und Remote-Scanner-Knoten
- **Red hat Subscription Management**: Der Host muss bei Red hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.
- **Zusätzliche Software**: Sie müssen die folgende Software auf dem Host installieren, bevor Sie die BlueXP-Klassifizierung installieren:
    - Je nach verwendetem Betriebssystem müssen Sie eine der Container-Engines installieren:
        - Docker Engine ab Version 19.3.1. "Installationsanweisungen anzeigen".

          "Hier geht's zum Video" Eine kurze Demo zur Installation von Docker auf CentOS.

        - Podman Version 4 oder höher. Um Podman zu installieren, geben Sie) ein (`sudo yum install podman netavark -y`.
- Python Version 3.6 oder höher. "Installationsanweisungen anzeigen".

    - **NTP-Überlegungen**: NetApp empfiehlt die Konfiguration des BlueXP Klassifizierungssystems für die Verwendung eines NTP-Dienstes (Network Time Protocol). Die Zeit muss zwischen dem BlueXP Klassifizierungssystem und dem BlueXP Connector System synchronisiert werden.
    - **Firewalld Überlegungen**: Wenn Sie planen zu verwenden `firewalld`, Wir empfehlen, dass Sie es aktivieren, bevor Sie BlueXP Klassifizierung installieren. Führen Sie die folgenden Befehle zum Konfigurieren aus `firewalld` Damit es mit der BlueXP Klassifizierung 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 BlueXP Klassifizierungs-Hosts als Scanner-Nodes zu verwenden, fügen Sie diese Regeln derzeit Ihrem Primärsystem 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
```

+
Beachten Sie, dass Sie Docker oder Podman neu starten müssen, wenn Sie aktivieren oder aktualisieren `firewalld` Einstellungen.

> Die IP-Adresse des Host-Systems für die BlueXP Klassifizierung kann nach der Installation nicht mehr geändert werden.

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

Für die BlueXP Klassifizierung ist Outbound-Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxy-Server für den Internetzugang verwendet, stellen Sie sicher, dass die BlueXP Klassifizierungsinstanz 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://dseasb33srnrn.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	Enthält die erforderlichen Pakete für die Installation von Dockern.
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 erforderlichen Pakete für die CentOS-Installation.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Enthält die erforderlichen Pakete für die Ubuntu-Installation.

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

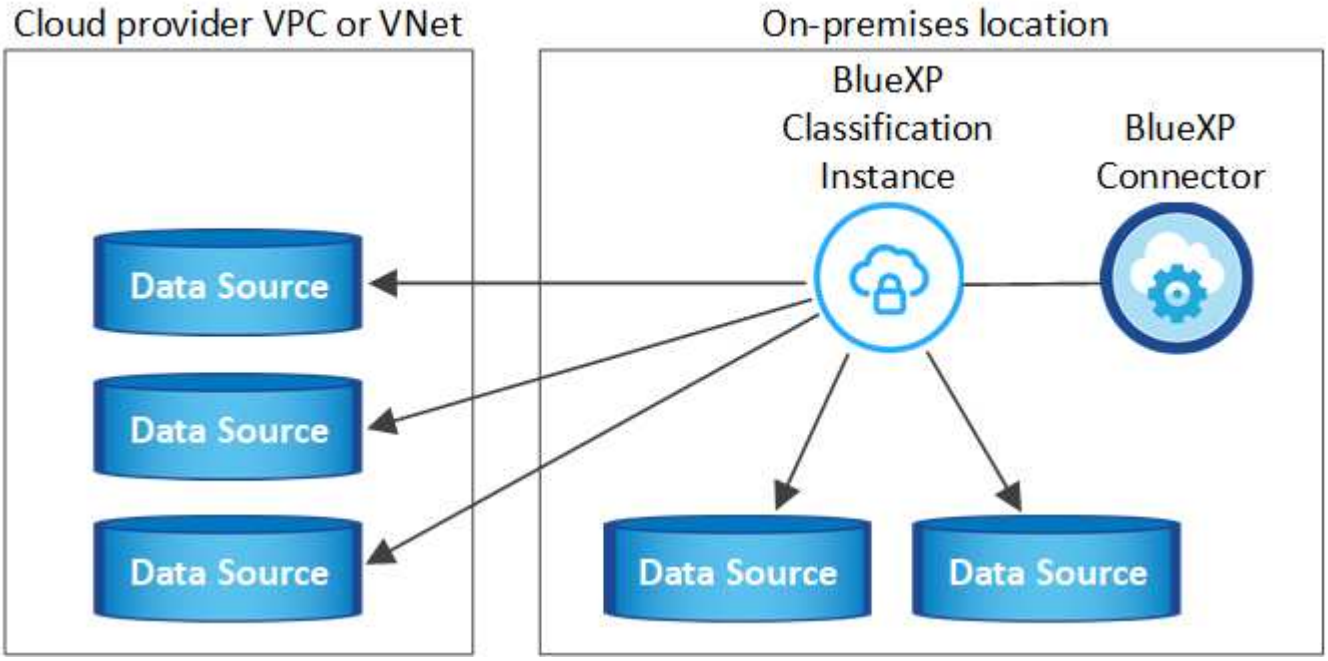
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 443 (TCP) und 80	Die Firewall- oder Routing-Regeln für den Connector müssen ein- und ausgehenden Datenverkehr über Port 443 zur und von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass Port 8080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

Verbindungstyp	Ports	Beschreibung
Connector <> ONTAP-Cluster (NAS)	443 (TCP)	BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen: • 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.
BlueXP Klassifizierung <> ONTAP Cluster	• Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS - 139 (TCP\UDP) und 445 (TCP\UDP)	Für die BlueXP Klassifizierung benötigen Sie eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder Ihrem lokalen ONTAP System. Firewalls oder Routingregeln für Cloud Volumes ONTAP müssen eingehende Verbindungen von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind: • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.

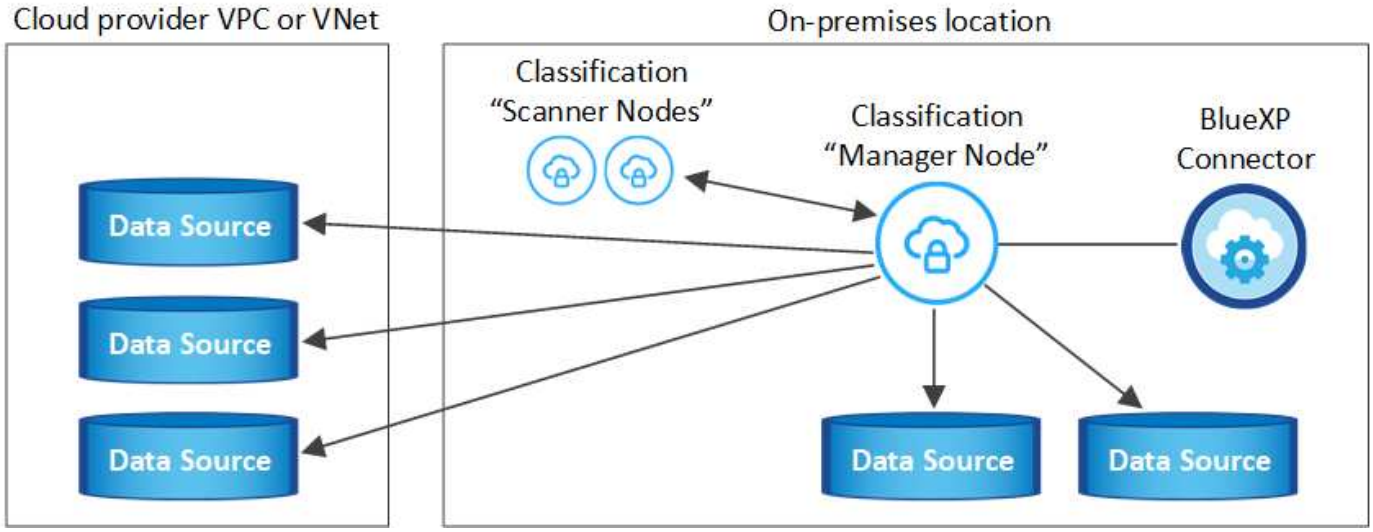
Verbindungstyp	Ports	Beschreibung
BlueXP Klassifizierung <> Active Directory	389 (TCP & UDP), 636 (TCP), 3268 (TCP) UND 3269 (TCP)	Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben. Darüber hinaus sind für die BlueXP Klassifizierung Active Directory Anmeldeinformationen erforderlich, um CIFS-Volumes zu scannen. Sie müssen über die folgenden Informationen für das Active Directory verfügen: • 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)

BlueXP Klassifizierung auf dem Linux-Host installieren

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. Weitere Informationen Link:Task-deploy-multi-Host-install-dark-site.HTML> über die Installation auf mehreren Hosts für große Konfigurationen.



Siehe Vorbereiten des Linux-Hostsystems Und Voraussetzungen prüfen Sie erhalten eine vollständige Liste der Anforderungen vor der Implementierung der BlueXP Klassifizierung.

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

> Die BlueXP Klassifizierung kann derzeit nicht S3 Buckets, Azure NetApp Files oder FSX for ONTAP scannen, wenn die Software vor Ort installiert ist. In diesen Fällen müssen Sie eine separate Connector- und Instanz der BlueXP Klassifizierung in der Cloud und implementieren "Zwischen den Anschlüssen wechseln" Für Ihre unterschiedlichen Datenquellen.

Installation mit einem Host für typische Konfigurationen

Anforderungen prüfen und bei der Installation der BlueXP Klassifizierungssoftware auf einem einzelnen lokalen Host befolgen.

"Hier geht's zum Video" Informationen zur Installation der BlueXP Klassifizierung.

Beachten Sie, dass alle Installationsaktivitäten bei der Installation der BlueXP Klassifizierung protokolliert werden. Wenn während der Installation Probleme auftreten, können Sie den Inhalt des Audit-Protokolls für die Installation anzeigen. Es ist geschrieben `/opt/netapp/install_logs/`. "Weitere Details finden Sie hier".

Was Sie benötigen

- Vergewissern Sie sich, dass Ihr Linux-System die erfüllt Host-Anforderungen erfüllt.
- Überprüfen Sie, ob auf dem System die beiden erforderlichen Softwarepakete installiert sind (Docker Engine oder Podman und Python 3).
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.
- Wenn Sie einen Proxy für den Zugriff auf das Internet verwenden:
  - Sie benötigen die Proxy-Server-Informationen (IP-Adresse oder Hostname, Verbindungsport, Verbindungsschema: https oder http, Benutzername und Passwort).
  - Wenn der Proxy TLS abfängt, müssen Sie den Pfad auf dem BlueXP Klassifizierungs-Linux-System kennen, auf dem die TLS-CA-Zertifikate gespeichert sind.
  - Der Proxy muss nicht transparent sein - wir unterstützen derzeit keine transparenten Proxys.
  - Der Benutzer muss ein lokaler Benutzer sein. Domänenbenutzer werden nicht unterstützt.

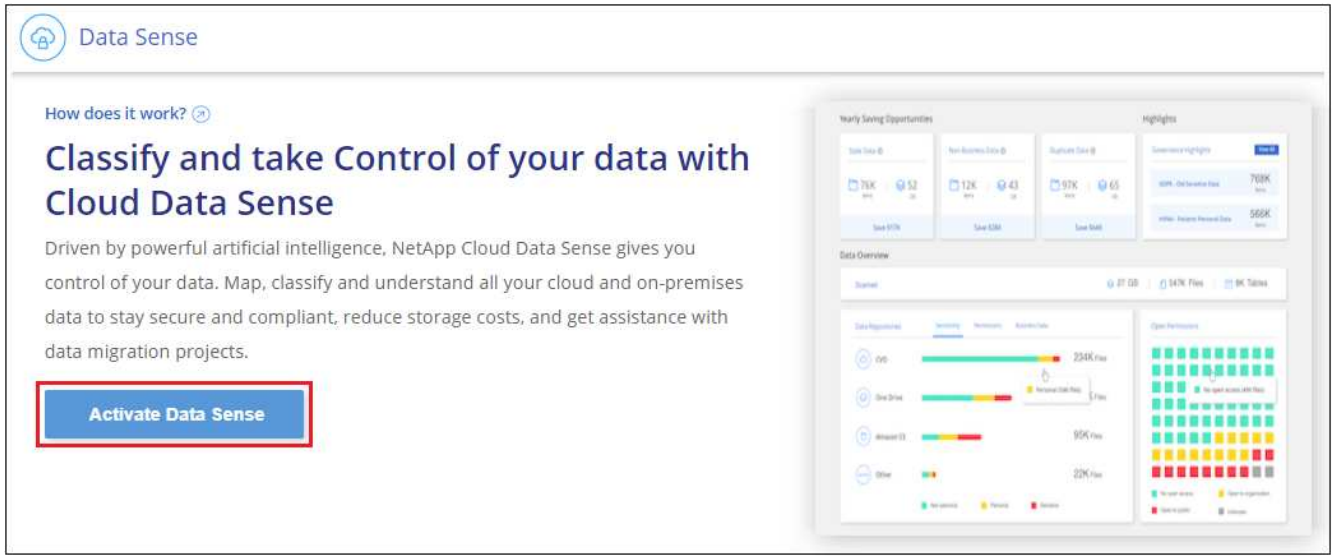
- Vergewissern Sie sich, dass die erforderliche Offline-Umgebung erfüllt ist Berechtigungen und Konnektivität.

Schritte

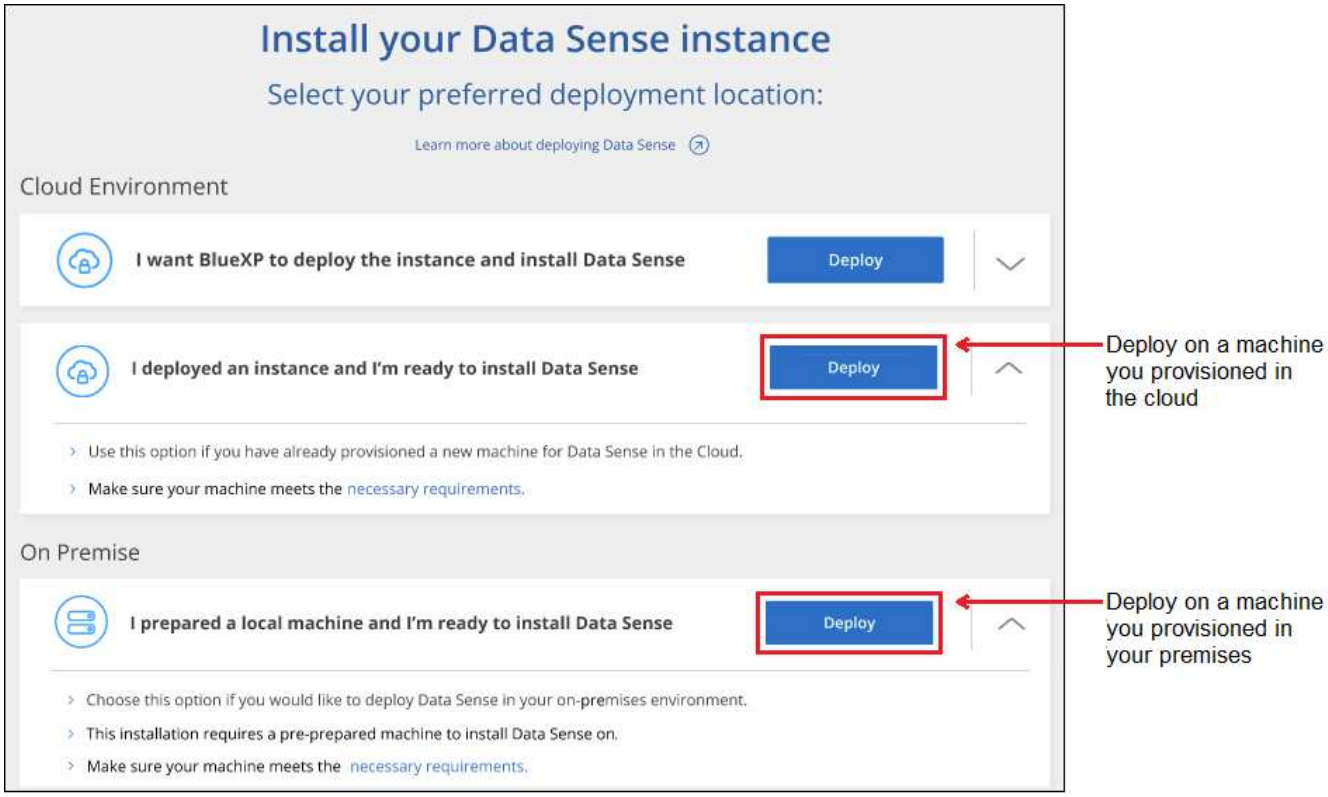
1. Laden Sie die BlueXP Klassifizierungssoftware von herunter "NetApp Support Website". Die ausgewählte Datei heißt **DATASENSE-INSTALLER-<Version>.tar.gz**.
2. Kopieren Sie die Installationsdatei auf den Linux-Host, den Sie verwenden möchten (mit `scp` Oder eine andere Methode).
3. Entpacken Sie die Installationsdatei auf dem Hostcomputer, z. B.:

```
tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
```

4. Wählen Sie in BlueXP die Option **Governance > Klassifizierung** aus.
5. Klicken Sie Auf **Datensense Aktivieren**.



6. Je nachdem, ob Sie die BlueXP-Klassifizierung auf einer Instanz installieren, die Sie in der Cloud vorbereitet haben, oder auf einer Instanz, die Sie vor Ort vorbereitet haben, klicken Sie auf die entsprechende Schaltfläche **Deploy**, um die BlueXP-Klassifikationsinstallation zu starten.



7. Das Dialogfeld *Deploy Data Sense on premise* wird angezeigt. Kopieren Sie den angegebenen Befehl (z. B.: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`) Und fügen Sie sie in eine Textdatei ein, damit Sie sie später verwenden können. Klicken Sie dann auf **Schließen**, um das Dialogfeld zu schließen.
8. Geben Sie auf dem Hostcomputer den kopierten Befehl ein, und folgen Sie dann einer Reihe von Eingabeaufforderungen. Alternativ können Sie den vollständigen Befehl einschließlich aller erforderlichen Parameter als Befehlszeilenargumente bereitstellen.

   Beachten Sie, dass das Installationsprogramm eine Vorprüfung durchführt, um sicherzustellen, dass Ihre System- und Netzwerkanforderungen für eine erfolgreiche Installation erfüllt werden. "Hier geht's zum Video" Um die Pre-Check-Meldungen und -Auswirkungen zu verstehen.

Geben Sie die Parameter wie aufgefordert ein:	Geben Sie den vollständigen Befehl ein:
a. Fügen Sie den Befehl ein, den Sie aus Schritt 7 kopiert haben: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` Wenn Sie die Installation auf einer Cloud-Instanz (nicht vor Ort) ausführen, fügen Sie hinzu `--manual-cloud-install <cloud_provider>`. b. Geben Sie die IP-Adresse oder den Hostnamen der Host-Maschine der BlueXP Klassifizierung ein, damit das Connector-System darauf zugreifen kann. c. Geben Sie die IP-Adresse oder den Host-Namen der BlueXP Connector Host Machine ein, damit das BlueXP Klassifizierungssystem darauf zugreifen kann. d. Geben Sie die Proxy-Details wie aufgefordert ein. Wenn Ihr BlueXP Connector bereits einen Proxy verwendet, müssen Sie diese Informationen hier nicht erneut eingeben, da die BlueXP Klassifizierung automatisch den vom Connector verwendeten Proxy verwendet.	Alternativ können Sie den gesamten Befehl vorab erstellen und die erforderlichen Host- und Proxy-Parameter bereitstellen: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --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>`

Variablenwerte:

- *Account_id* = NetApp Konto-ID
- *Client_id* = Konnektor-Client-ID (fügen Sie der Client-ID das Suffix „Clients“ hinzu, falls es noch nicht vorhanden ist)
- *User_Token* = JWT-Benutzer-Zugriffstoken
- *ds_Host* = IP-Adresse oder Hostname des BlueXP Klassifizierungs-Linux-Systems.
- *Cm_Host* = IP-Adresse oder Hostname des BlueXP Connector-Systems.
- *Cloud_Provider* = Geben Sie bei der Installation auf einer Cloud-Instanz je nach Cloud-Provider „AWS“, „Azure“ oder „GCP“ ein.
- *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. Der Benutzer muss ein lokaler Benutzer sein – Domänenbenutzer werden nicht unterstützt.
- *Proxy_Password* = Passwort für den von Ihnen angegebenen Benutzernamen.
- *Ca_cert_dir* = Pfad auf dem BlueXP-Klassifizierungs-Linux-System mit zusätzlichen TLS-CA-Zertifikatbundles. Nur erforderlich, wenn der Proxy TLS Abfangen durchführt.

Ergebnis

Das BlueXP Klassifizierungs-Installationsprogramm installiert Pakete, registriert die Installation und installiert die BlueXP Klassifizierung. Die Installation dauert 10 bis 20 Minuten.

Wenn Konnektivität über Port 8080 zwischen der Host-Maschine und der Connector-Instanz besteht, wird der Installationsfortschritt auf der Registerkarte BlueXP Klassifizierung in BlueXP angezeigt.

Nächste Schritte

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

BlueXP Klassifizierung auf einem Linux-Host ohne Internetzugang installieren

Führen Sie einige Schritte aus, um die BlueXP Klassifizierung auf einem Linux-Host an einem lokalen Standort ohne Internetzugang zu installieren – auch als *Private Mode* bezeichnet. Diese Art der Installation ist perfekt für Ihre sicheren Standorte.

"Informieren Sie sich über die verschiedenen Implementierungsmodi für die BlueXP Connector und BlueXP Klassifizierung".

Beachten Sie, dass Sie auch können "Implementieren Sie die BlueXP Klassifizierung auf einer lokalen Website mit Internetzugang".

Das BlueXP Klassifizierungs-Installationsskript wird zunächst überprüft, ob das System und die Umgebung die erforderlichen Voraussetzungen erfüllen. Wenn alle Voraussetzungen erfüllt sind, wird die Installation gestartet. Wenn Sie die Voraussetzungen unabhängig vom Ausführen der BlueXP Klassifizierungssysteminstallation überprüfen möchten, steht Ihnen ein separates Softwarepaket zur Verfügung, das nur auf die Voraussetzungen testet. "Erfahren Sie, wie Sie überprüfen können, ob Ihr Linux-Host bereit ist, die BlueXP Klassifizierung zu installieren".

> Informationen zu älteren Versionen 1.30 und älteren Versionen finden Sie unter, wenn Sie BlueXP Klassifizierung auf mehreren Hosts installieren müssen "Installieren Sie die BlueXP Klassifizierung auf mehreren Hosts ohne Internetzugang".

Unterstützte Datenquellen

Bei installierter Private-Mode (manchmal auch „offline“ oder „dunkle“ Site genannt) kann die BlueXP Klassifizierung nur Daten aus Datenquellen scannen, die auch lokal am lokalen Standort gespeichert sind. Die BlueXP Klassifizierung kann derzeit die folgenden **lokalen** Datenquellen scannen:

- On-Premises ONTAP Systeme
- Datenbankschemas

Wenn die BlueXP Klassifizierung im privaten Modus implementiert wird, wird derzeit keine Unterstützung für das Scannen von Cloud Volumes ONTAP-, Azure NetApp Files- oder FSX-Konten für ONTAP angeboten.

Einschränkungen

Die meisten BlueXP Klassifizierungsfunktionen sind verfügbar, wenn sie an einem Standort ohne Internetzugang implementiert werden. Bestimmte Funktionen, für die ein Internetzugang erforderlich ist, werden jedoch nicht unterstützt, z. B.:

- Festlegen von BlueXP-Rollen für unterschiedliche Benutzer (z. B. Account Admin oder Compliance Viewer)

- Quelldateien werden mittels BlueXP Kopier- und Synchronisierungsfunktion kopiert und synchronisiert
- Automatisierte Software-Upgrades von BlueXP

  Sowohl der BlueXP Connector als auch die BlueXP Klassifizierung erfordern regelmäßige manuelle Upgrades zur Aktivierung neuer Funktionen. Die BlueXP Klassifizierungsversion wird unten auf den BlueXP Klassifizierungs-UI-Seiten angezeigt. Prüfen Sie die "BlueXP Klassifizierung – Versionshinweise" Um sich die neuen Funktionen in jeder Version und deren Wunsch nach jenen Funktionen ansehen zu können. Anschließend können Sie die Schritte befolgen "Upgrade des BlueXP Connector" Und Upgrade Ihrer BlueXP Klassifizierungssoftware.

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 im privaten Modus installiert haben, "Den Stecker einsetzen" Jetzt auf einem Linux-Host.

2 **Voraussetzungen für die BlueXP Klassifizierung prüfen**

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 die BlueXP Klassifizierung herunter und implementieren Sie sie**

Laden Sie die BlueXP Klassifizierungssoftware von der NetApp Support-Website herunter und kopieren Sie die Installer-Datei auf den geplanten Linux-Host. Starten Sie dann den Installationsassistenten und befolgen Sie die Anweisungen zur Implementierung der BlueXP Klassifizierungsinstanz.

Installieren Sie den BlueXP-Anschluss

Wenn Sie noch keinen BlueXP Connector im privaten Modus installiert haben, "Den Stecker einsetzen" Auf einem Linux-Host in Ihrer Offline-Site.

Bereiten Sie das Linux-Hostsystem vor

Die BlueXP Klassifizierungssoftware muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Software-Anforderungen usw. erfüllt.

- Die BlueXP Klassifizierung wird auf einem Host, der mit anderen Applikationen gemeinsam genutzt wird, nicht unterstützt – der Host muss ein dedizierter Host sein.
- Wenn Sie das Host-System an Ihrem Standort aufbauen, können Sie zwischen diesen Systemgrößen wählen, je nach Größe des Datensatzes, den Sie die BlueXP Klassifizierung scannen möchten.

Systemgröße	CPU	RAM (Swap-Speicher muss deaktiviert sein)	Festplatte
Extra Groß	32 CPUs	128 GB RAM	1 tib SSD auf /, oder - 100 gib verfügbar auf /opt - 895 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Groß	16 CPUs	64 GB RAM	500 gib SSD auf /, oder - 100 gib verfügbar auf /opt - 395 gib verfügbar auf /var/lib/docker oder für Podman /var/lib/Containers oder für Podman /var/lib/Containers - 5 gib auf /tmp

- Bei der Implementierung einer Computing-Instanz in der Cloud für Ihre BlueXP Klassifizierungsinstallation empfehlen wir ein System, das die oben genannten „großen“ Systemanforderungen erfüllt:
  - **Amazon Elastic Compute Cloud (Amazon EC2) Instanztyp**: Wir empfehlen "m6i.4xlarge". "Siehe zusätzliche AWS-Instanztypen".
  - **Größe der Azure VM**: Wir empfehlen „Standard_D16s_v3“. "Siehe zusätzliche Azure-Instanztypen".
  - **GCP-Maschinentyp**: Wir empfehlen "n2-Standard-16". "Weitere GCP-Instanztypen finden Sie unter".
- **UNIX-Ordnerberechtigungen**: Folgende UNIX-Mindestberechtigungen sind erforderlich:

Ordner	Mindestberechtigungen
/Tmp	`rwxrwxrwt`
/Opt	`rwxr-xr-x`
/Var/lib/Docker	`rwx------`
/Usr/lib/systemd/System	`rwxr-xr-x`

- **Betriebssystem**:
  - Für die folgenden Betriebssysteme ist die Verwendung der Docker Container-Engine erforderlich:
    - Red hat Enterprise Linux Version 7.8 und 7.9
    - CentOS Version 7.8 und 7.9
    - Ubuntu 22.04 (BlueXP Klassifikation ab Version 1.23 erforderlich)
  - Die folgenden Betriebssysteme erfordern die Verwendung der Podman Container-Engine. Sie erfordern eine BlueXP Klassifikation der Version 1.30 oder höher:
    - Red hat Enterprise Linux Version 8.8, 9.0, 9.1, 9.2 und 9.3

      Beachten Sie, dass die folgenden Funktionen derzeit nicht unterstützt werden, wenn RHEL 8.x und RHEL 9.x verwendet werden:

      - Installation an einem dunklen Ort
      - Verteiltes Scannen; Verwendung eines Master-Scanner-Knotens und Remote-Scanner-Knoten
- **Red hat Subscription Management**: Der Host muss bei Red hat Subscription Management registriert

sein. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.

- **Zusätzliche Software**: Sie müssen die folgende Software auf dem Host installieren, bevor Sie die BlueXP-Klassifizierung installieren:
  - Je nach verwendetem Betriebssystem müssen Sie eine der Container-Engines installieren:
    - Docker Engine ab Version 19.3.1. "Installationsanweisungen anzeigen".

      "Hier geht's zum Video" Eine kurze Demo zur Installation von Docker auf CentOS.

    - Podman Version 4 oder höher. Um Podman zu installieren, geben Sie) ein (`sudo yum install podman netavark -y`.
- Python Version 3.6 oder höher. "Installationsanweisungen anzeigen".
  - **NTP-Überlegungen**: NetApp empfiehlt die Konfiguration des BlueXP Klassifizierungssystems für die Verwendung eines NTP-Dienstes (Network Time Protocol). Die Zeit muss zwischen dem BlueXP Klassifizierungssystem und dem BlueXP Connector System synchronisiert werden.
  - **Firewalld Überlegungen**: Wenn Sie planen zu verwenden `firewalld`, Wir empfehlen, dass Sie es aktivieren, bevor Sie BlueXP Klassifizierung installieren. Führen Sie die folgenden Befehle zum Konfigurieren aus `firewalld` Damit es mit der BlueXP Klassifizierung 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
    ```

    Beachten Sie, dass Sie Docker oder Podman neu starten müssen, wenn Sie aktivieren oder aktualisieren `firewalld` Einstellungen.

> Die IP-Adresse des Host-Systems für die BlueXP Klassifizierung kann nach der Installation nicht mehr geändert werden.

Voraussetzungen für die Klassifizierung von BlueXP und BlueXP prüfen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass vor der Implementierung der BlueXP Klassifizierung eine unterstützte Konfiguration vorhanden ist.

- Stellen Sie sicher, dass der Connector über die Berechtigungen zum Implementieren von Ressourcen und zum Erstellen von Sicherheitsgruppen für die BlueXP Klassifizierungsinstanz verfügt. Die neuesten BlueXP-Berechtigungen finden Sie in "Die von NetApp bereitgestellten Richtlinien".
- Sorgen Sie dafür, dass die BlueXP Klassifizierung weiter ausgeführt werden kann. Die BlueXP Klassifizierungs-Instanz muss aktiviert bleiben, um Ihre Daten kontinuierlich zu scannen.
- Webbrowser-Konnektivität zur BlueXP Klassifizierung sicherstellen Nachdem die Klassifizierung von BlueXP aktiviert ist, stellen Sie sicher, dass Benutzer von einem Host, der über eine Verbindung zur BlueXP Klassifizierungsinstanz verfügt, auf die BlueXP Schnittstelle zugreifen.

  Die BlueXP Klassifizierungsinstanz verwendet eine private IP-Adresse, um sicherzustellen, dass andere

nicht auf die indizierten Daten zugreifen können. 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 selben Netzwerk wie die BlueXP Klassifizierungsinstanz befindet.

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

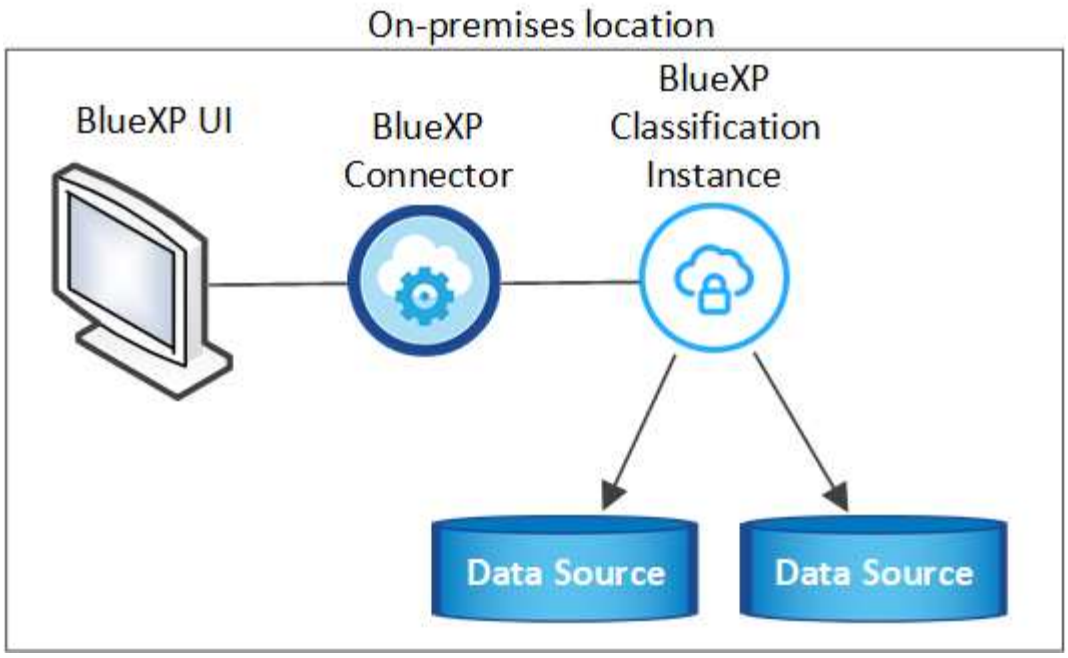
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 6000 (TCP), 443 (TCP) UND 80	Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über die Ports 6000 und 443 zur und von der BlueXP Klassifizierungsinstanz zulassen. • Port 6000 ist erforderlich, damit die BYOL-Lizenz für die BlueXP Klassifizierung an einem Dark Site funktioniert. • Port 8080 sollte offen sein, damit Sie den Installationsfortschritt in BlueXP sehen können.
Connector <> ONTAP-Cluster (NAS)	443 (TCP)	BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen: • 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.

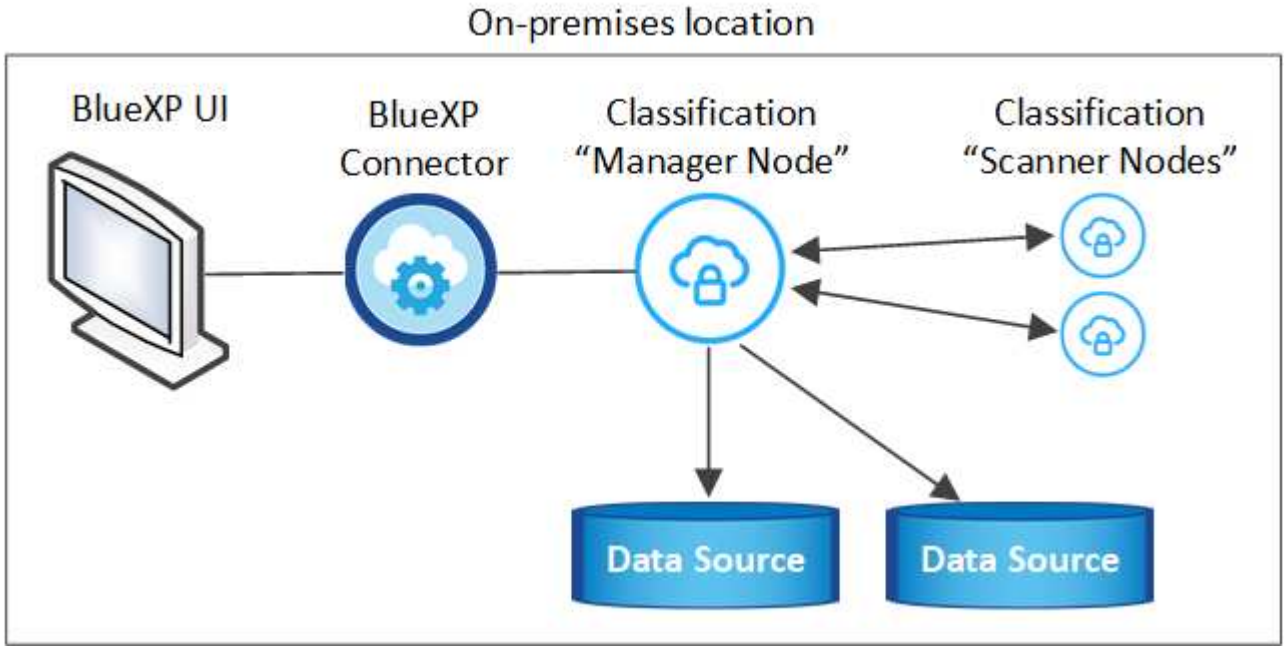
Verbindungstyp	Ports	Beschreibung
BlueXP Klassifizierung <> ONTAP Cluster	• Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS - 139 (TCP\UDP) und 445 (TCP\UDP)	Für die BlueXP Klassifizierung benötigen Sie eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder Ihrem lokalen ONTAP System. Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind: • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.
BlueXP Klassifizierung <> Active Directory	389 (TCP & UDP), 636 (TCP), 3268 (TCP) UND 3269 (TCP)	Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben. Darüber hinaus sind für die BlueXP Klassifizierung Active Directory Anmeldeinformationen erforderlich, um CIFS-Volumes zu scannen. Sie müssen über die folgenden Informationen für das Active Directory verfügen: • 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 BlueXP Klassifizierungs-Hosts nutzen, um eine zusätzliche Rechenleistung zum Scannen Ihrer Datenquellen zu bieten, müssen Sie zusätzliche Ports/Protokolle aktivieren. "Siehe zusätzliche Anschlussanforderungen".

BlueXP Klassifizierung auf dem lokalen Linux-Host installieren

Für typische Konfigurationen installieren Sie die Software auf einem einzigen Host-System.





Installation mit einem Host für typische Konfigurationen

Folgen Sie diesen Schritten, wenn Sie die BlueXP Klassifizierungssoftware auf einem einzelnen lokalen Host in einer Offline-Umgebung installieren.

Beachten Sie, dass alle Installationsaktivitäten bei der Installation der BlueXP Klassifizierung protokolliert werden. Wenn während der Installation Probleme auftreten, können Sie den Inhalt des Audit-Protokolls für die Installation anzeigen. Es ist geschrieben `/opt/netapp/install_logs/`. "Weitere Details finden Sie hier".

Was Sie benötigen

- Vergewissern Sie sich, dass Ihr Linux-System die erfüllt Host-Anforderungen erfüllt.
- Überprüfen Sie, ob Sie die beiden erforderlichen Softwarepakete (Docker Engine oder Podman 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 die BlueXP Klassifizierungssoftware auf einem internetkonfigurierten System von der 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 im privaten Modus verwenden möchten.
3. Entpacken Sie das Installationspaket auf dem Hostcomputer, z. B.:

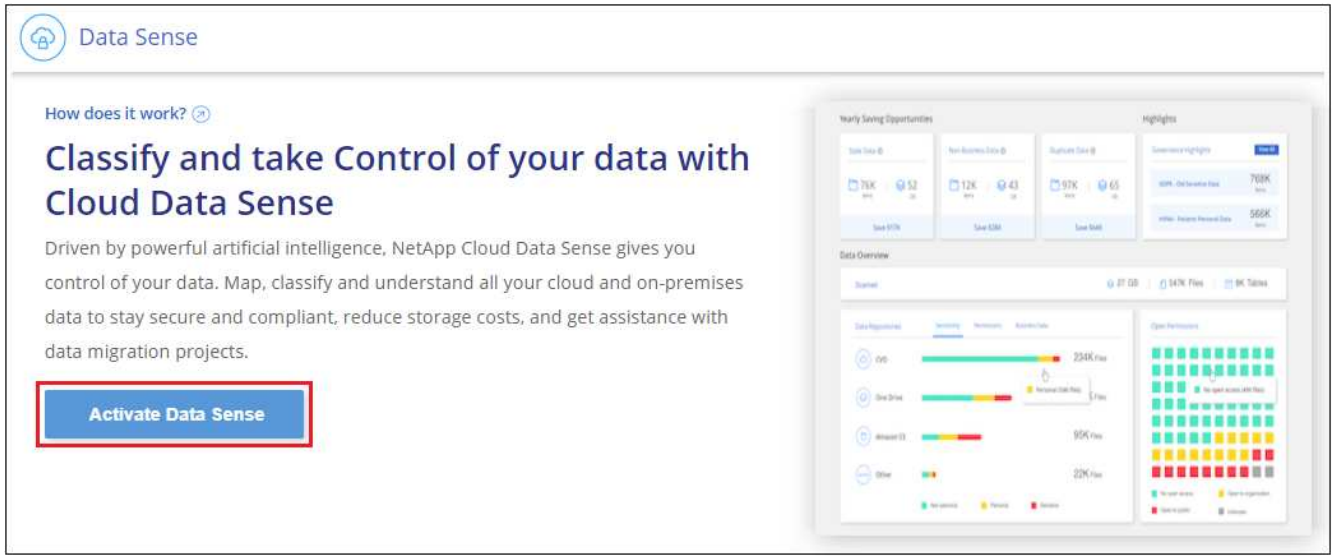
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

   Diese extrahiert erforderliche Software und die eigentliche Installationsdatei **cc_onprem_Installer.tar.gz**.

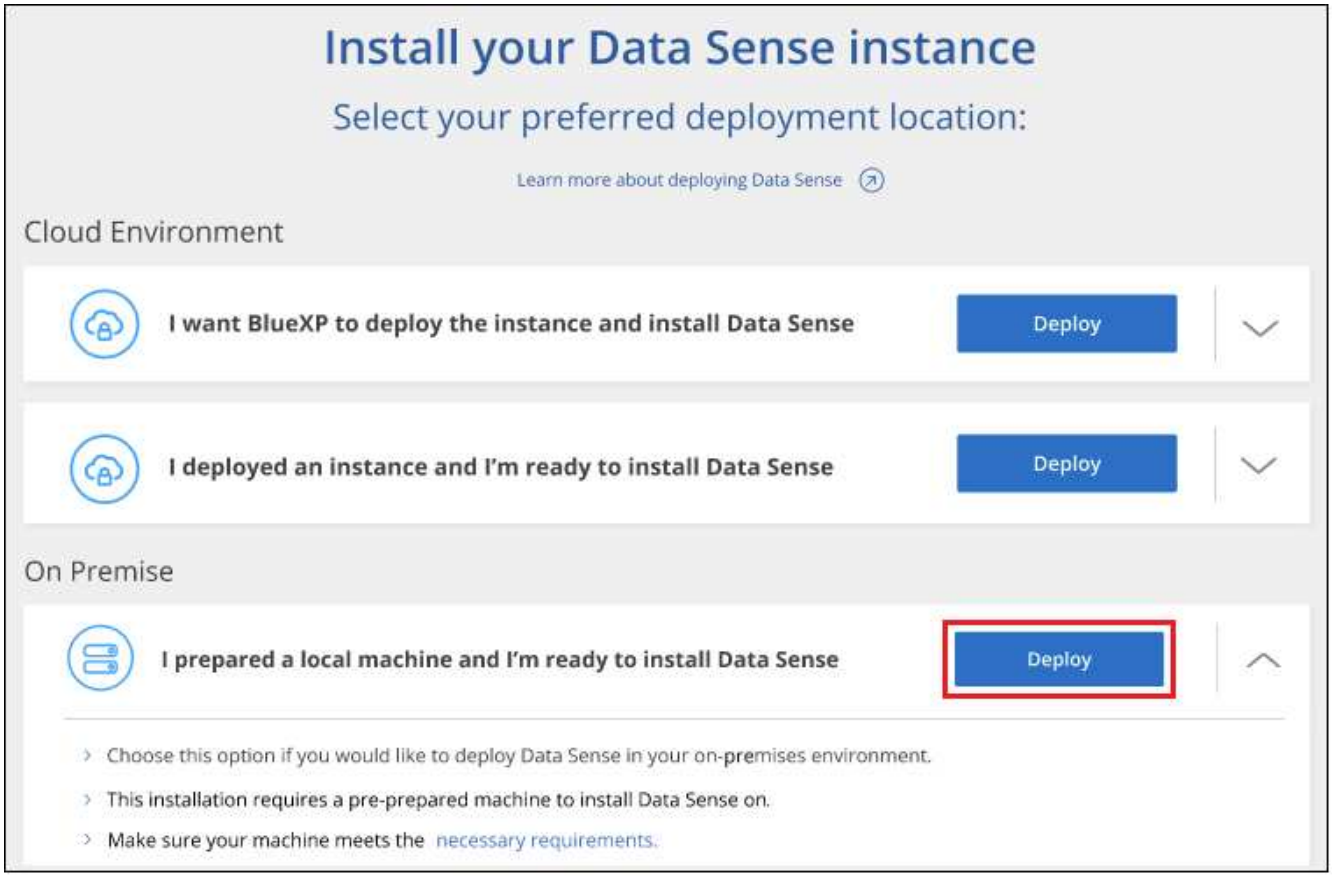
4. Entpacken Sie die Installationsdatei auf dem Host-Rechner, z. B.:

```
tar -xzf cc_onprem_installer.tar.gz
```

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



7. Klicken Sie auf **Deploy**, um die On-Premises-Installation zu starten.



8. Das Dialogfeld *Deploy Data Sense on premise* wird angezeigt. Kopieren Sie den angegebenen Befehl (z. B.: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`) Und fügen Sie sie in eine Textdatei ein, damit Sie sie später verwenden können. Klicken Sie dann auf **Schließen**, um das Dialogfeld zu schließen.
9. Geben Sie auf dem Hostcomputer den kopierten Befehl ein, und folgen Sie dann einer Reihe von Eingabeaufforderungen. Alternativ können Sie den vollständigen Befehl einschließlich aller erforderlichen Parameter als Befehlszeilenargumente bereitstellen.

   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:
a. Fügen Sie die Informationen ein, die Sie aus Schritt 8 kopiert haben: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite` b. Geben Sie die IP-Adresse oder den Hostnamen der Host-Maschine der BlueXP Klassifizierung ein, damit das Connector-System darauf zugreifen kann. c. Geben Sie die IP-Adresse oder den Host-Namen der BlueXP Connector Host Machine ein, damit das BlueXP Klassifizierungssystem darauf zugreifen kann.	Alternativ können Sie den gesamten Befehl vorab erstellen und die erforderlichen Host-Parameter bereitstellen: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

Variablenwerte:

- *Account_id* = NetApp Konto-ID
- *Client_id* = Konnektor-Client-ID (fügen Sie der Client-ID das Suffix „Clients“ hinzu, falls es noch nicht vorhanden ist)
- *User_Token* = JWT-Benutzer-Zugriffstoken
- *ds_Host* = IP-Adresse oder Host-Name des BlueXP Klassifizierungssystems.
- *Cm_Host* = IP-Adresse oder Hostname des BlueXP Connector-Systems.

Ergebnis

Das BlueXP Klassifizierungs-Installationsprogramm installiert Pakete, registriert die Installation und installiert die BlueXP Klassifizierung. Die Installation dauert 10 bis 20 Minuten.

Wenn Konnektivität über Port 8080 zwischen der Host-Maschine und der Connector-Instanz besteht, wird der Installationsfortschritt auf der Registerkarte BlueXP Klassifizierung in BlueXP angezeigt.

Nächste Schritte

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

Upgrade der BlueXP Klassifizierungssoftware

Da die BlueXP Klassifizierungssoftware regelmäßig mit neuen Funktionen aktualisiert wird, sollten Sie regelmäßig auf neue Versionen überprüfen, um sicherzustellen, dass Sie die neueste Software und Funktionen verwenden. Sie müssen die BlueXP Klassifizierungssoftware manuell aktualisieren, da für ein automatisches Upgrade keine Internetverbindung besteht.

Bevor Sie beginnen

- Wir empfehlen ein Upgrade Ihrer BlueXP Connector Software auf die neueste verfügbare Version. "Siehe die Schritte zur Aktualisierung des Connectors".
- Ab der BlueXP Klassifizierungsversion 1.24 können Sie Upgrades auf jede beliebige zukünftige Softwareversion durchführen.

  Wenn Ihre BlueXP Klassifizierungssoftware eine Version vor 1.24 verwendet, können Sie jeweils nur eine Hauptversion aktualisieren. Wenn Sie beispielsweise Version 1.21.x installiert haben, können Sie nur auf 1.22.x aktualisieren Wenn Sie einige Hauptversionen hinter sich haben, müssen Sie die Software mehrmals aktualisieren.

Schritte

1. Laden Sie die BlueXP Klassifizierungssoftware auf einem internetkonfigurierten System von der 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 die BlueXP Klassifizierung am Dark Site installiert ist.
3. Entpacken Sie das Software-Bundle auf dem Host-Rechner, zum Beispiel:

   ```
   tar -xvf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   Dadurch wird die Installationsdatei **cc_onprem_Installer.tar.gz** extrahiert.

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

```
tar -xzf cc_onprem_installer.tar.gz
```

   Dadurch wird das Upgrade-Skript **Start_darchsite_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 BlueXP Klassifizierungssoftware wird auf Ihrem Host aktualisiert. Die Aktualisierung kann 5 bis 10 Minuten dauern.

Sie können überprüfen, ob die Software aktualisiert wurde, indem Sie die Version unten auf den BlueXP Klassifizierungs-UI-Seiten überprüfen.

Stellen Sie sicher, dass Ihr Linux Host bereit ist, die BlueXP Klassifizierung zu installieren

Bevor Sie die BlueXP-Klassifizierung manuell auf einem Linux-Host installieren, können Sie ein Skript auf dem Host ausführen, um zu überprüfen, ob alle Voraussetzungen für die Installation der BlueXP Klassifizierung vorhanden sind. Sie können dieses Skript auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud ausführen. Der Host kann mit dem Internet verbunden werden, oder der Host kann sich auf einer Site befinden, die keinen Internetzugang hat (eine *dunkle Seite*).

Es gibt auch ein Test-Skript mit Voraussetzung, das Teil des BlueXP Klassifizierungsskripts für die Installation ist. Das hier beschriebene Skript wurde speziell für Benutzer entwickelt, die den Linux-Host unabhängig von der Ausführung des BlueXP Klassifizierungsskripts überprüfen möchten.

Erste Schritte

Sie führen die folgenden Aufgaben aus.

1. Optional können Sie einen BlueXP Connector installieren, wenn noch keiner installiert ist. Sie können das Testskript ausführen, ohne einen Connector installiert zu haben, aber das Skript überprüft die Verbindung zwischen dem Connector und der BlueXP-Klassifikationshost-Maschine - daher wird empfohlen, dass Sie einen Connector haben.
2. Bereiten Sie den Host-Rechner vor und überprüfen Sie, ob er alle Anforderungen erfüllt.
3. Aktivieren Sie Outbound-Internetzugriff über die Host-Maschine der BlueXP Klassifizierung.
4. Vergewissern Sie sich, dass alle erforderlichen Ports auf allen Systemen aktiviert sind.
5. Laden Sie das Skript für den Voraussetzungstest herunter, und führen Sie es aus.

Einen Konnektor erstellen

Ein BlueXP Connector ist erforderlich, bevor Sie die BlueXP Klassifizierung installieren und verwenden können. Sie können jedoch das Skript Voraussetzungen ohne Connector ausführen.

Das können Sie "Installieren Sie den Steckverbinder vor Ort" Auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud. Einige Benutzer, die die BlueXP Klassifizierung lokal installieren möchten, können den Connector möglicherweise auch On-Premises installieren.

Informationen zum Erstellen eines Connectors in der Umgebung Ihres Cloud-Providers finden Sie unter "Erstellen eines Konnektors in AWS", "Erstellen eines Connectors in Azure", Oder "Erstellen eines Konnektors in GCP".

Sie benötigen die IP-Adresse oder den Hostnamen des Connector-Systems, wenn Sie das Skript Voraussetzungen ausführen. 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**.

Host-Anforderungen prüfen

Die BlueXP Klassifizierungssoftware muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Software-Anforderungen usw. erfüllt.

- Die BlueXP Klassifizierung wird auf einem Host, der mit anderen Applikationen gemeinsam genutzt wird, nicht unterstützt – der Host muss ein dedizierter Host sein.
- Wenn Sie das Host-System an Ihrem Standort aufbauen, können Sie zwischen diesen Systemgrößen wählen, je nach Größe des Datensatzes, den Sie die BlueXP Klassifizierung scannen möchten.

Systemgröße	CPU	RAM (Swap-Speicher muss deaktiviert sein)	Festplatte
Extra Groß	32 CPUs	128 GB RAM	1 tib SSD auf /, oder - 100 gib verfügbar auf /opt - 895 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Groß	16 CPUs	64 GB RAM	500 gib SSD auf /, oder - 100 gib verfügbar auf /opt - 395 gib verfügbar auf /var/lib/docker oder für Podman /var/lib/Containers oder für Podman /var/lib/Containers - 5 gib auf /tmp

- Bei der Implementierung einer Computing-Instanz in der Cloud für Ihre BlueXP Klassifizierungsinstallation empfehlen wir ein System, das die oben genannten „großen“ Systemanforderungen erfüllt:
  - **Amazon Elastic Compute Cloud (Amazon EC2) Instanztyp**: Wir empfehlen "m6i.4xlarge". "Siehe zusätzliche AWS-Instanztypen".
  - **Größe der Azure VM**: Wir empfehlen „Standard_D16s_v3“. "Siehe zusätzliche Azure-Instanztypen".
  - **GCP-Maschinentyp**: Wir empfehlen "n2-Standard-16". "Weitere GCP-Instanztypen finden Sie unter".

- **UNIX-Ordnerberechtigungen**: Folgende UNIX-Mindestberechtigungen sind erforderlich:

Ordner	Mindestberechtigungen
/Tmp	`rwxrwxrwt`
/Opt	`rwxr-xr-x`
/Var/lib/Docker	`rwx------`
/Usr/lib/systemd/System	`rwxr-xr-x`

- **Betriebssystem**:
  - Für die folgenden Betriebssysteme ist die Verwendung der Docker Container-Engine erforderlich:
    - Red hat Enterprise Linux Version 7.8 und 7.9
    - CentOS Version 7.8 und 7.9
    - Ubuntu 22.04 (BlueXP Klassifikation ab Version 1.23 erforderlich)
  - Die folgenden Betriebssysteme erfordern die Verwendung der Podman Container-Engine. Sie erfordern eine BlueXP Klassifikation der Version 1.30 oder höher:
    - Red hat Enterprise Linux Version 8.8, 9.0, 9.1, 9.2 und 9.3

      Beachten Sie, dass die folgenden Funktionen derzeit nicht unterstützt werden, wenn RHEL 8.x und RHEL 9.x verwendet werden:

      - Installation an einem dunklen Ort
      - Verteiltes Scannen; Verwendung eines Master-Scanner-Knotens und Remote-Scanner-Knoten
- **Red hat Subscription Management**: Der Host muss bei Red hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.
- **Zusätzliche Software**: Sie müssen die folgende Software auf dem Host installieren, bevor Sie die BlueXP-Klassifizierung installieren:
  - Je nach verwendetem Betriebssystem müssen Sie eine der Container-Engines installieren:
    - Docker Engine ab Version 19.3.1. "Installationsanweisungen anzeigen".

      "Hier geht's zum Video" Eine kurze Demo zur Installation von Docker auf CentOS.

    - Podman Version 4 oder höher. Um Podman zu installieren, geben Sie) ein (`sudo yum install podman netavark -y`.
- Python Version 3.6 oder höher. "Installationsanweisungen anzeigen".

  - **NTP-Überlegungen**: NetApp empfiehlt die Konfiguration des BlueXP Klassifizierungssystems für die Verwendung eines NTP-Dienstes (Network Time Protocol). Die Zeit muss zwischen dem BlueXP Klassifizierungssystem und dem BlueXP Connector System synchronisiert werden.
  - **Firewalld Überlegungen**: Wenn Sie planen zu verwenden `firewalld`, Wir empfehlen, dass Sie es aktivieren, bevor Sie BlueXP Klassifizierung installieren. Führen Sie die folgenden Befehle zum Konfigurieren aus `firewalld` Damit es mit der BlueXP Klassifizierung 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 BlueXP Klassifizierungs-Hosts als Scanner-Nodes (in einem verteilten Modell) zu verwenden, fügen Sie derzeit diese Regeln Ihrem Primärsystem 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
```

+
Beachten Sie, dass Sie Docker oder Podman neu starten müssen, wenn Sie aktivieren oder aktualisieren `firewalld` Einstellungen.

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

Für die BlueXP Klassifizierung ist Outbound-Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxy-Server für den Internetzugang verwendet, stellen Sie sicher, dass die BlueXP Klassifizierungsinstanz über Outbound-Internetzugang verfügt, um die folgenden Endpunkte zu kontaktieren.

Dieser Abschnitt ist für Hostsysteme, die an Standorten ohne Internetverbindung installiert sind, nicht erforderlich.

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://dseasb33srnrn.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	Enthält die erforderlichen Pakete für die Installation von Dockern.

Endpunkte	Zweck
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 erforderlichen Pakete für die CentOS-Installation.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Enthält die erforderlichen Pakete für die Ubuntu-Installation.

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 443 (TCP) und 80	Die Firewall- oder Routing-Regeln für den Connector müssen ein- und ausgehenden Datenverkehr über Port 443 zur und von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass Port 8080 geöffnet ist, damit Sie den Installationsfortschritt in BlueXP sehen können.
Connector <> ONTAP-Cluster (NAS)	443 (TCP)	BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewallrichtlinien verwenden, muss der Connector-Host ausgehenden HTTPS-Zugriff über Port 443 zulassen. Wenn sich der Connector in der Cloud befindet, ist die gesamte ausgehende Kommunikation durch vordefinierte Firewall- oder Routingregeln zulässig.

Führen Sie das Skript für die Klassifizierungsvoraussetzungen von BlueXP aus

Führen Sie diese Schritte aus, um das Skript für die Voraussetzungen der BlueXP Klassifizierung auszuführen.

"Hier geht's zum Video" Anleitung zum Ausführen des Skripts „Voraussetzungen“ und zum Interpretieren der Ergebnisse.

Was Sie benötigen

- Vergewissern Sie sich, dass Ihr Linux-System die erfüllt Host-Anforderungen erfüllt.
- Überprüfen Sie, ob auf dem System die beiden erforderlichen Softwarepakete installiert sind (Docker Engine oder Podman und Python 3).
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.

Schritte

1. Laden Sie das Skript für die BlueXP Klassifizierungs-Voraussetzungen von herunter "NetApp Support Website". Die Datei, die Sie auswählen sollten, heißt **Standalone-pre-requisite-Tester-<version>**.
2. Kopieren Sie die Datei auf den Linux-Host, den Sie verwenden möchten (mit `scp` Oder eine andere Methode).

3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x standalone-pre-requisite-tester-v1.25.0
```

4. Führen Sie das Skript mit dem folgenden Befehl aus.

```
./standalone-pre-requisite-tester-v1.25.0 <--darksite>
```

   Fügen Sie die Option "--darksite" nur hinzu, wenn Sie das Skript auf einem Host ausführen, der keinen Internetzugang hat. Bestimmte Voraussetzungstests werden übersprungen, wenn der Host nicht mit dem Internet verbunden ist.

5. Das Skript fordert Sie zur Eingabe der IP-Adresse der BlueXP Klassifizierungs-Host-Maschine auf.
   - Geben Sie die IP-Adresse oder den Hostnamen ein.
6. Das Skript fordert Sie auf, zu fragen, ob Sie einen BlueXP Connector installiert haben.
   - Geben Sie **N** ein, wenn kein Connector installiert ist.
   - Geben Sie **Y** ein, wenn Sie einen Connector installiert haben. Geben Sie dann die IP-Adresse oder den Hostnamen des BlueXP Connector ein, damit das Testskript diese Konnektivität testen kann.
7. Das Skript führt eine Vielzahl von Tests auf dem System aus und zeigt die Ergebnisse im weiteren Verlauf an. Nach Abschluss der Sitzung wird ein Protokoll der Sitzung in eine Datei mit dem Namen geschrieben `prerequisites-test-<timestamp>.log` Im Verzeichnis `/opt/netapp/install_logs`.

Ergebnis

Wenn alle Voraussetzungstests erfolgreich durchgeführt wurden, können Sie die BlueXP Klassifizierung auf dem Host installieren, wenn Sie bereit sind.

Wenn Probleme entdeckt wurden, werden sie als „empfohlen“ oder „erforderlich“ kategorisiert, um behoben zu werden. Empfohlene Probleme sind in der Regel Elemente, die das Scannen und Kategorisieren von BlueXP verlangsamen würden. Diese Elemente müssen nicht korrigiert werden - aber Sie können sie ansprechen.

Wenn Sie „erforderliche“ Probleme haben, sollten Sie die Probleme beheben und das Testskript „Voraussetzungen“ erneut ausführen.

Aktivieren Sie das Scannen Ihrer Datenquellen

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

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

Schnellstart

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

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"

Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

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

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

Zugriff auf Volumes sicherstellen

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

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

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

Verwalten Sie die Volumes, die Sie scannen möchten

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

Ermitteln der Datenquellen, die gescannt werden sollen

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

Ihre Cloud Volumes ONTAP-Systeme sollten bereits auf dem Canvas in BlueXP verfügbar sein. Bei ONTAP

Systemen vor Ort ist ein muss erforderlich "BlueXP ermittelt diese Cluster".

Implementieren der BlueXP Klassifizierungsinstanz

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

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

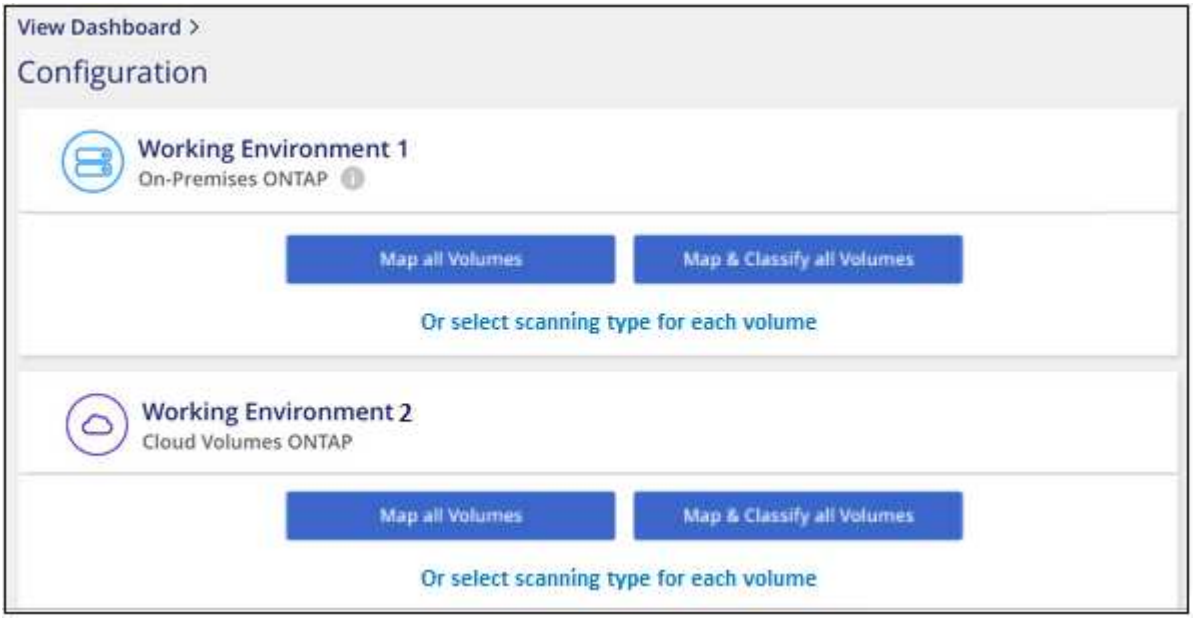
Wenn Sie lokale ONTAP-Systeme scannen, die in einer dunklen Site installiert wurden und über keinen Internetzugang verfügen, müssen Sie sie überprüfen "Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang". Dazu ist auch die Implementierung des BlueXP Connectors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

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

Ermöglichen der BlueXP Klassifizierung in Ihren Arbeitsumgebungen

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

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



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

     Siehe Aktivieren und Deaktivieren von Compliance-Scans auf Volumes Entsprechende Details.

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

Ergebnis

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

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

Überprüfung, ob die BlueXP Klassifizierung Zugriff auf Volumes hat

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

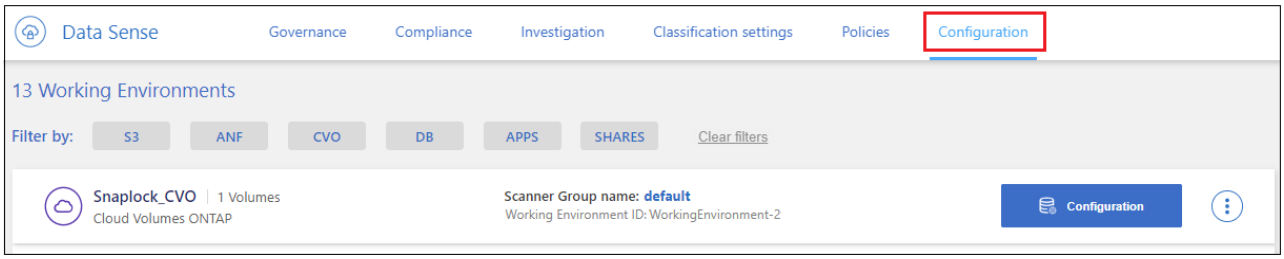
Schritte

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

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

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

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

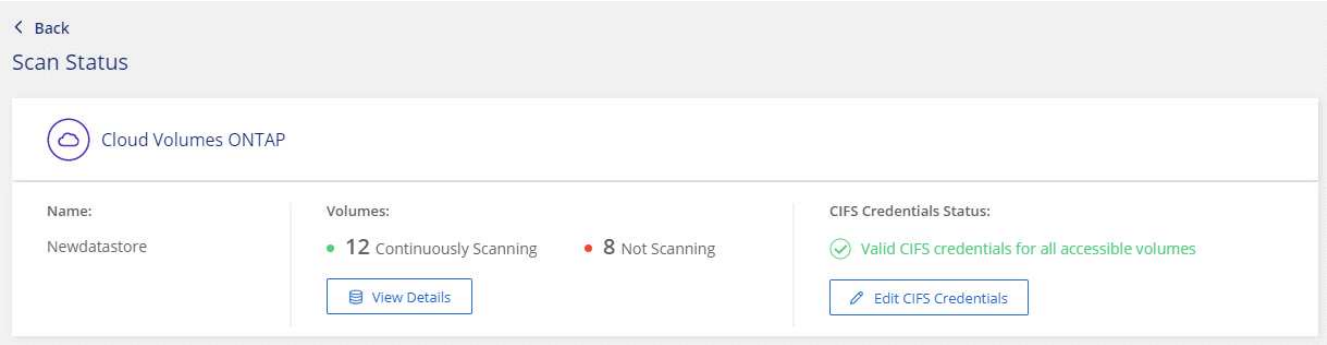


b. Klicken Sie für jede Arbeitsumgebung auf **Edit CIFS Credentials** und geben Sie den Benutzernamen und das Passwort ein, die die BlueXP Klassifizierung für den Zugriff auf CIFS Volumes auf dem System benötigt.

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

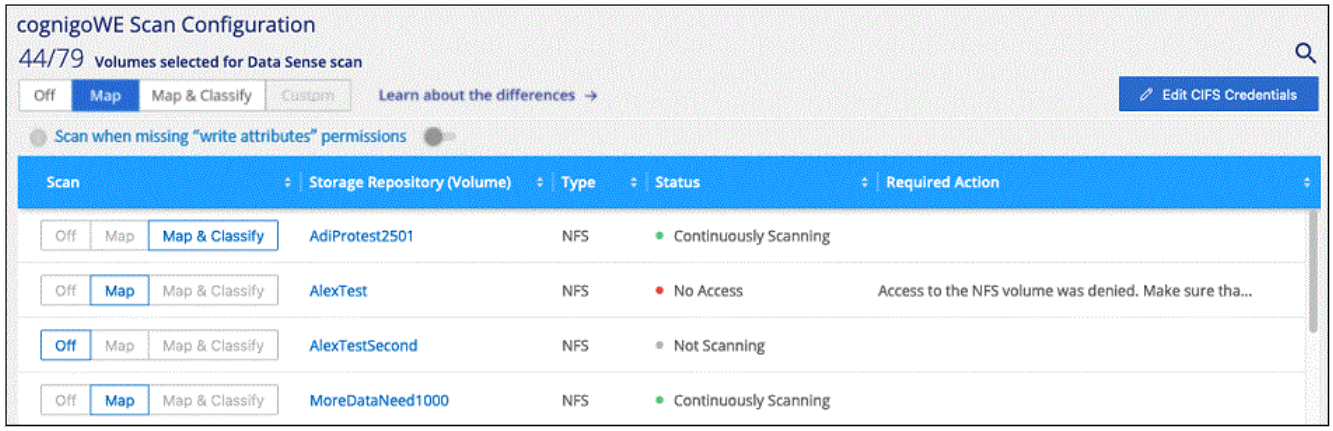
   Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten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

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



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

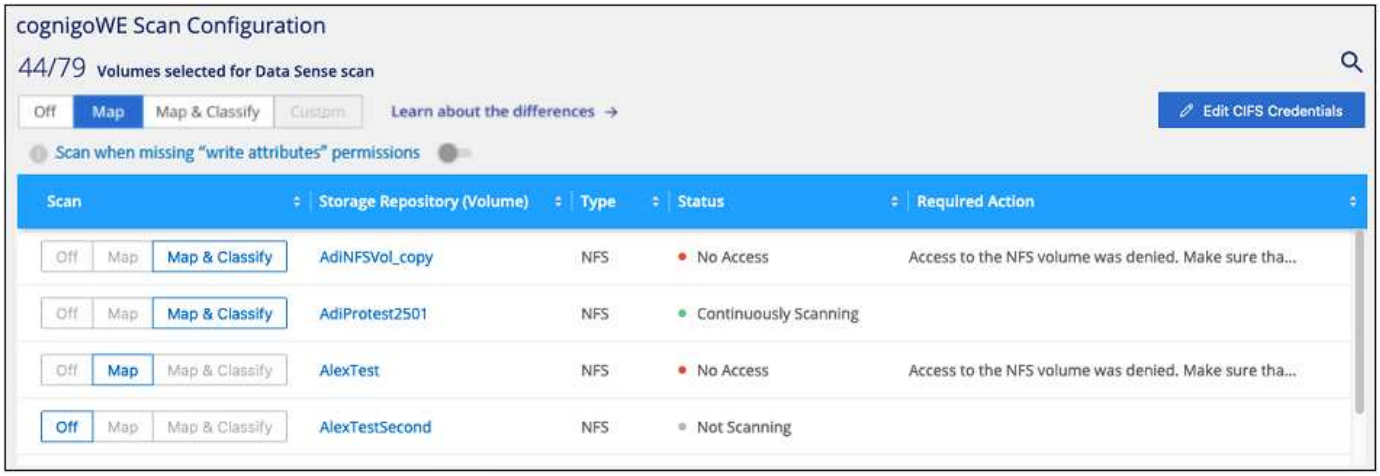
   Das folgende Bild zeigt beispielsweise vier Volumes. Eine davon kann aufgrund von Netzwerkverbindungsproblemen zwischen der BlueXP Klassifizierungsinstanz und dem Volume nicht mit der BlueXP Klassifizierung gescannt werden.



Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

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

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Weitere Informationen .".



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

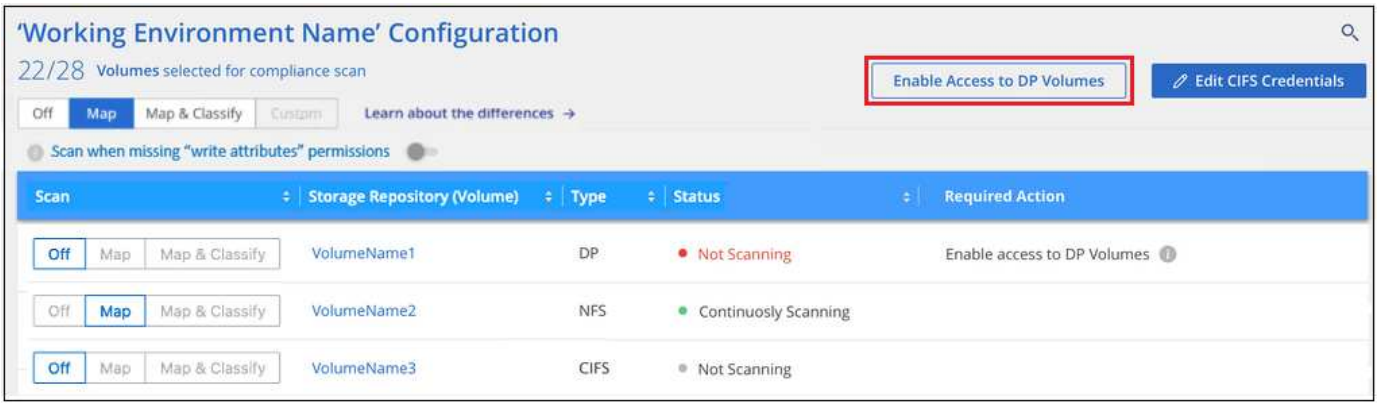
An:	Tun Sie dies:
Aktivieren Sie das vollständige Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf **Karte & Klassieren**
Deaktivieren Sie das Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf **aus**

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

Scannen von Datensicherungs-Volumes

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

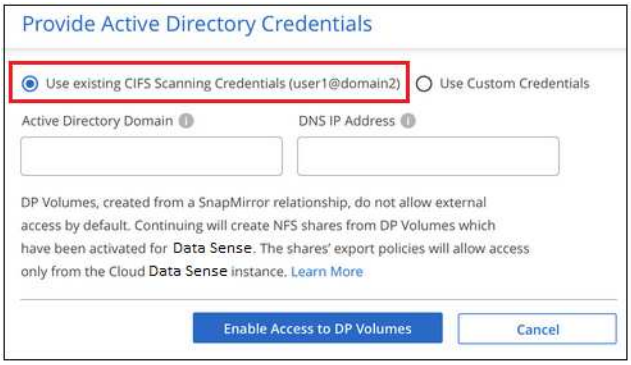
Zunächst erkennt die Volume-Liste diese Volumes als *Type* **DP** mit dem *Status* **Not Scanning** und der *required Action* **Enable Access to DP Volumes**.

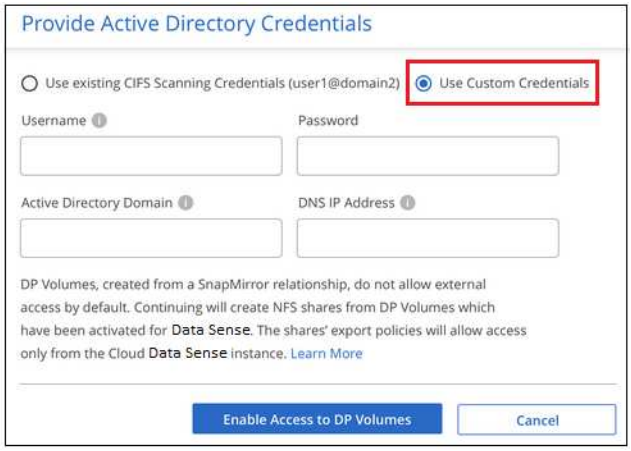


Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

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





3. Aktivieren Sie jedes zu scannenden DP-Volume Auf die gleiche Weise haben Sie andere Volumes aktiviert.

Ergebnis

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

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

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

Erste Schritte mit der BlueXP Klassifizierung für Azure NetApp Files

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

Schnellstart

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

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

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

2 Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung in BlueXP" Falls noch keine Instanz implementiert wurde.

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

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

4 Zugriff auf Volumes sicherstellen

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

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

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

5 Verwalten Sie die Volumes, die Sie scannen möchten

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

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

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

"Erfahren Sie, wie Sie das Azure NetApp Files-System in BlueXP entdecken".

Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

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

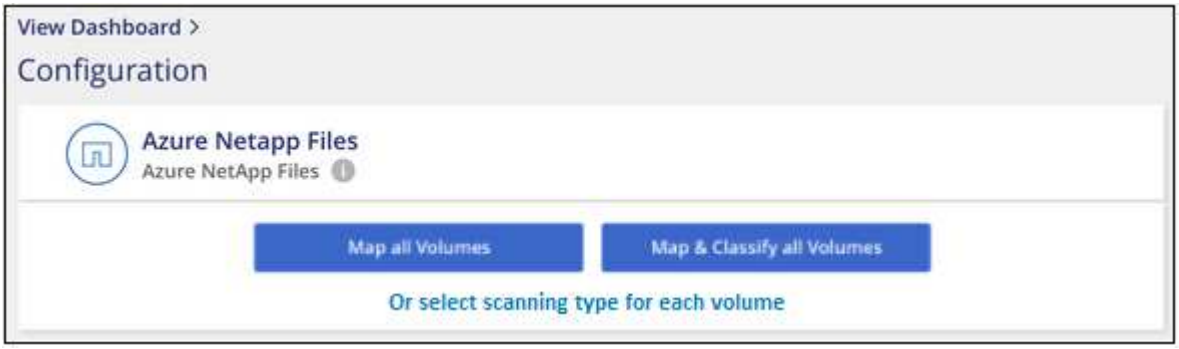
Hinweis: die Implementierung der BlueXP Klassifizierung an einem lokalen Standort wird derzeit beim Scannen von Azure NetApp Files Volumes nicht unterstützt.

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

Ermöglichen der BlueXP Klassifizierung in Ihren Arbeitsumgebungen

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

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



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

     Siehe Aktivieren und Deaktivieren von Compliance-Scans auf Volumes Entsprechende Details.

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

Ergebnis

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

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

Überprüfung, ob die BlueXP Klassifizierung Zugriff auf Volumes hat

Vergewissern Sie sich, dass die BlueXP Klassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-,

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

Schritte

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

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

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

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

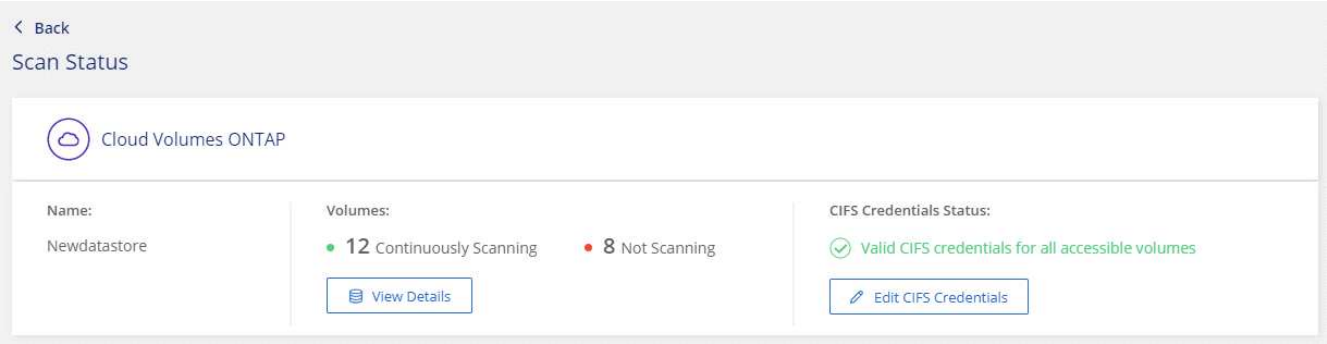
   

   b. Klicken Sie für jede Arbeitsumgebung auf **Edit CIFS Credentials** und geben Sie den Benutzernamen und das Passwort ein, die die BlueXP Klassifizierung für den Zugriff auf CIFS Volumes auf dem System benötigt.

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

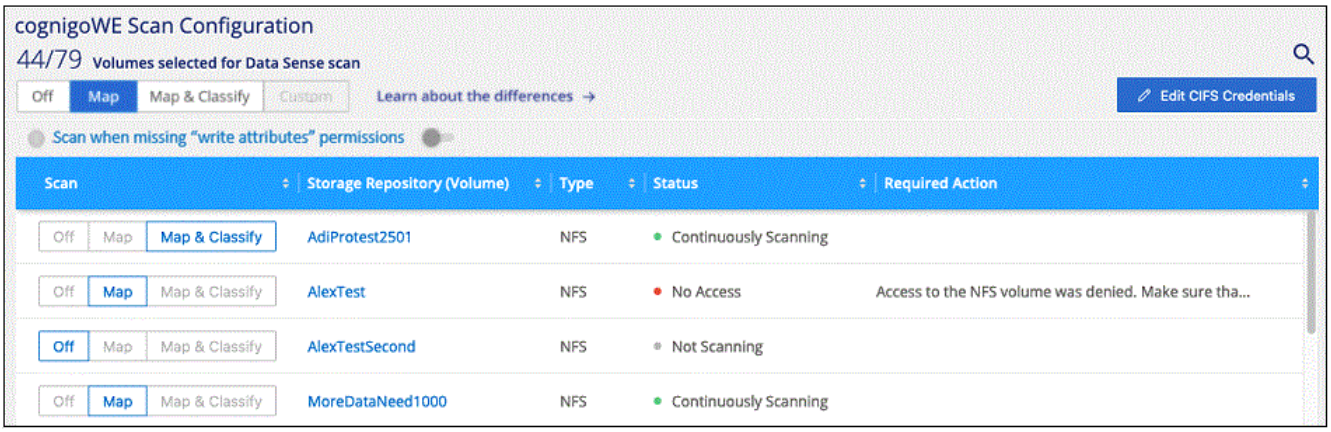
      Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten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

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



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

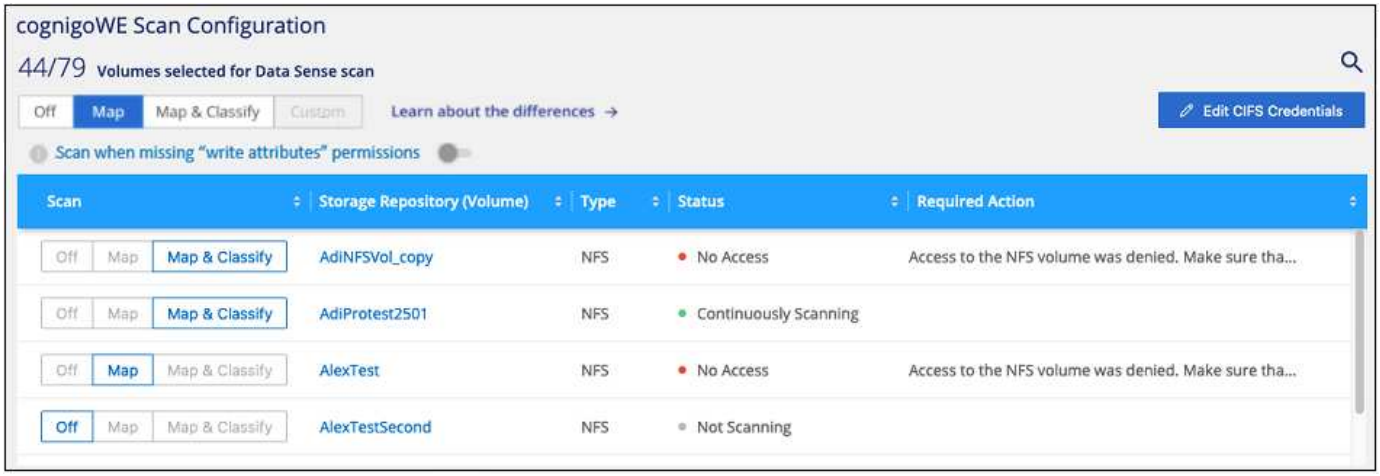
   Das folgende Bild zeigt beispielsweise vier Volumes. Eine davon kann aufgrund von Netzwerkverbindungsproblemen zwischen der BlueXP Klassifizierungsinstanz und dem Volume nicht mit der BlueXP Klassifizierung gescannt werden.



Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

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

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Weitere Informationen .".



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

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

Erste Schritte mit der BlueXP Klassifizierung für Amazon FSX for ONTAP

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

Bevor Sie beginnen

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

  "AWS Sicherheitsgruppen für Linux Instanzen"

"AWS Sicherheitsgruppen für Windows Instanzen"

"Elastische AWS Netzwerkschnittstellen (ENI)"

Schnellstart

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

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

Bevor Sie FSX für ONTAP Volumes scannen können, "Sie benötigen eine FSX-Arbeitsumgebung mit konfigurierten Volumes".

2 **Implementieren der BlueXP Klassifizierungsinstanz**

"Implementieren Sie die BlueXP Klassifizierung in BlueXP" Falls noch keine Instanz implementiert wurde.

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

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

4 **Zugriff auf Volumes sicherstellen**

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

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

5 **Verwalten Sie die Volumes, die Sie scannen möchten**

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

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

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

"Lesen Sie, wie Sie das Dateisystem FSX für ONTAP in BlueXP erkennen oder erstellen".

Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

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

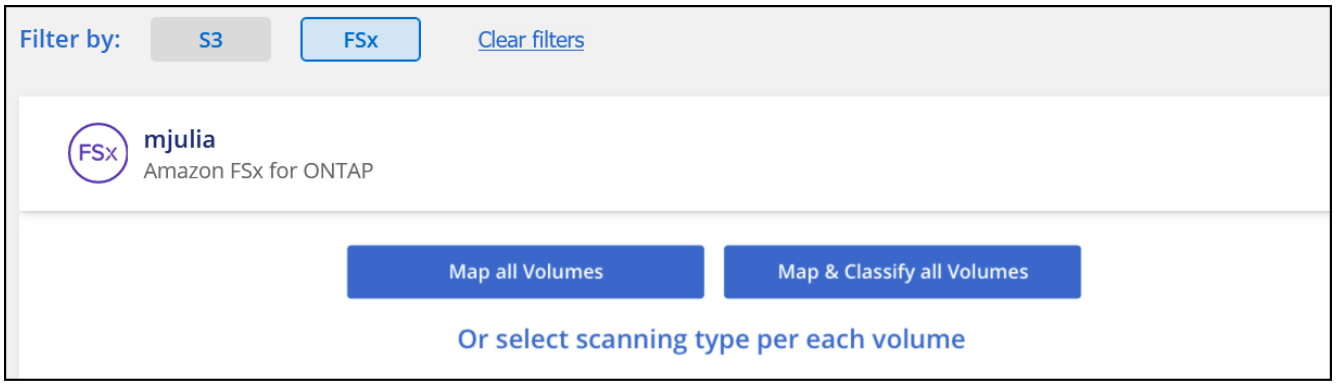
Hinweis: die Implementierung der BlueXP Klassifizierung an einem lokalen Standort wird derzeit beim Scannen von FSX Volumes nicht unterstützt.

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

Ermöglichen der BlueXP Klassifizierung in Ihren Arbeitsumgebungen

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

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



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

     Siehe Aktivieren und Deaktivieren von Compliance-Scans auf Volumes Entsprechende Details.

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

Ergebnis

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

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

Überprüfung, ob die BlueXP Klassifizierung Zugriff auf Volumes hat

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

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

Schritte

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

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

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	No Access	Check network connectivity between the Data Sense ...

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

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

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

System benötigt.

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

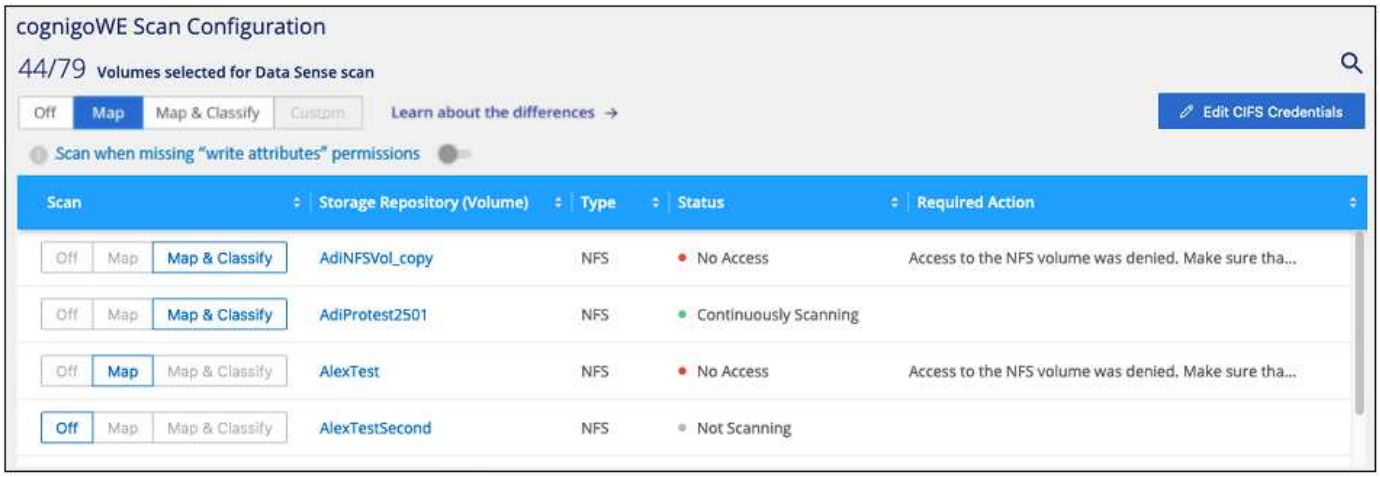
Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten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

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

Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

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

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Weitere Informationen .".



An:	Tun Sie dies:
Aktivieren von mappinggeschützten Scans auf einem Volume	Klicken Sie im Volumenbereich auf **Karte**
Aktivieren Sie das vollständige Scannen auf einem Volume	Klicken Sie im Volumenbereich auf **Karte & Klassieren**
Deaktivieren Sie das Scannen auf einem Volume	Klicken Sie im Volumenbereich auf **aus**

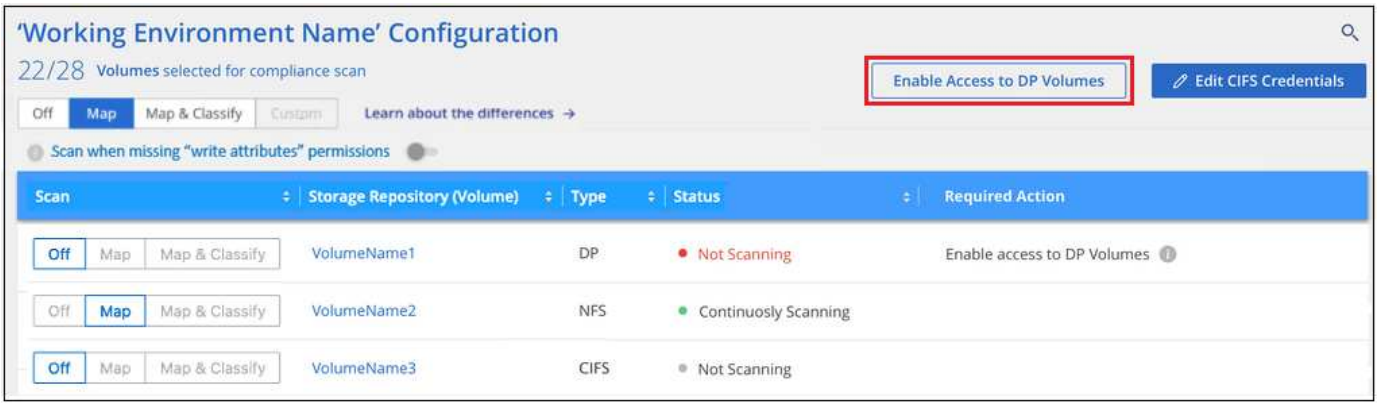
An:	Tun Sie dies:
Aktivieren Sie ausschließlich mappingbare Scans auf allen Volumes	Klicken Sie im Steuerkursbereich auf **Karte**
Aktivieren Sie das vollständige Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf **Karte & Klassieren**
Deaktivieren Sie das Scannen auf allen Volumes	Klicken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

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

Scannen von Datensicherungs-Volumes

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

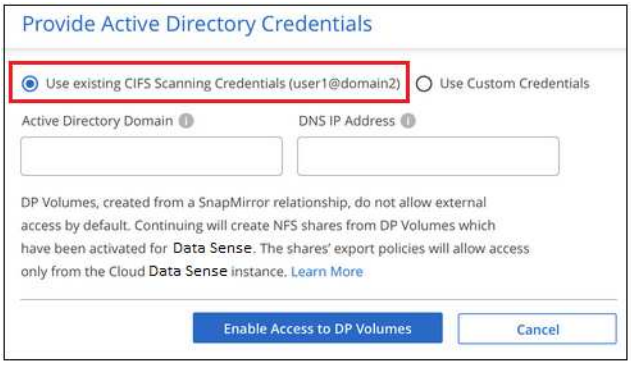
Zunächst erkennt die Volume-Liste diese Volumes als *Type* **DP** mit dem *Status* **Not Scanning** und der *required Action* **Enable Access to DP Volumes**.

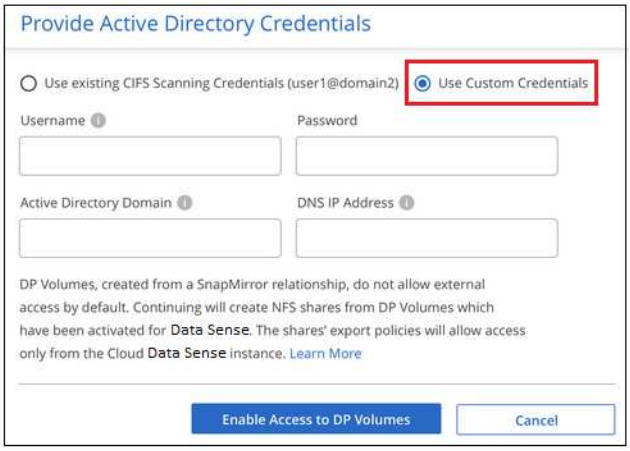


Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

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





3. Aktivieren Sie jedes zu scannenden DP-Volume Auf die gleiche Weise haben Sie andere Volumes aktiviert.

Ergebnis

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

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

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

Datenbankschemas scannen

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

Schnellstart

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

1 Datenbankvoraussetzungen prüfen

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

2 Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

Fügen Sie den Datenbankserver hinzu

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

Wählen Sie die Schemas aus

Wählen Sie die Schemata aus, die Sie scannen möchten.

Voraussetzungen prüfen

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

Unterstützte Datenbanken

Die BlueXP Klassifizierung kann Schemata aus den folgenden Datenbanken scannen:

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

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

Datenbankanforderungen erfüllt

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

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

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

Hinweis: für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

Implementieren der BlueXP Klassifizierungsinstanz

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

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

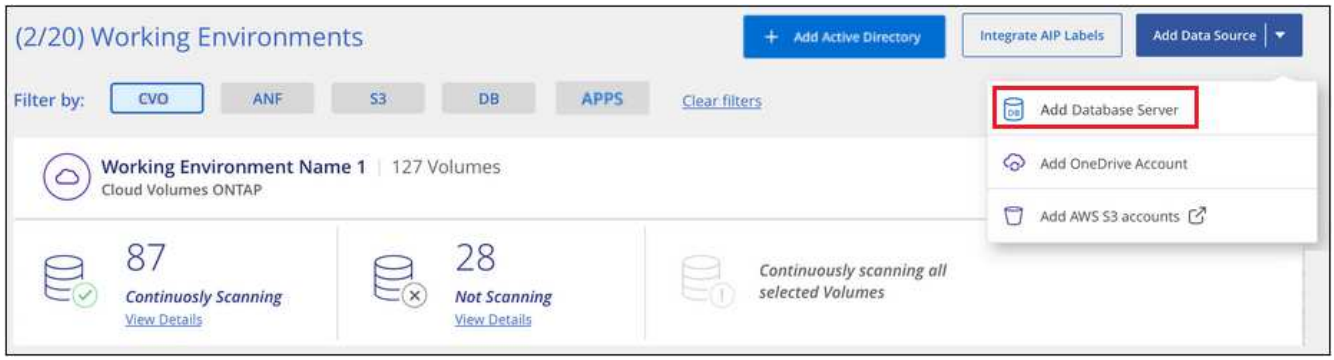
Wenn Sie Datenbankschemas scannen, die in einer dunklen Site installiert wurden, die keinen Internetzugang hat, müssen Sie dies tun "Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort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

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

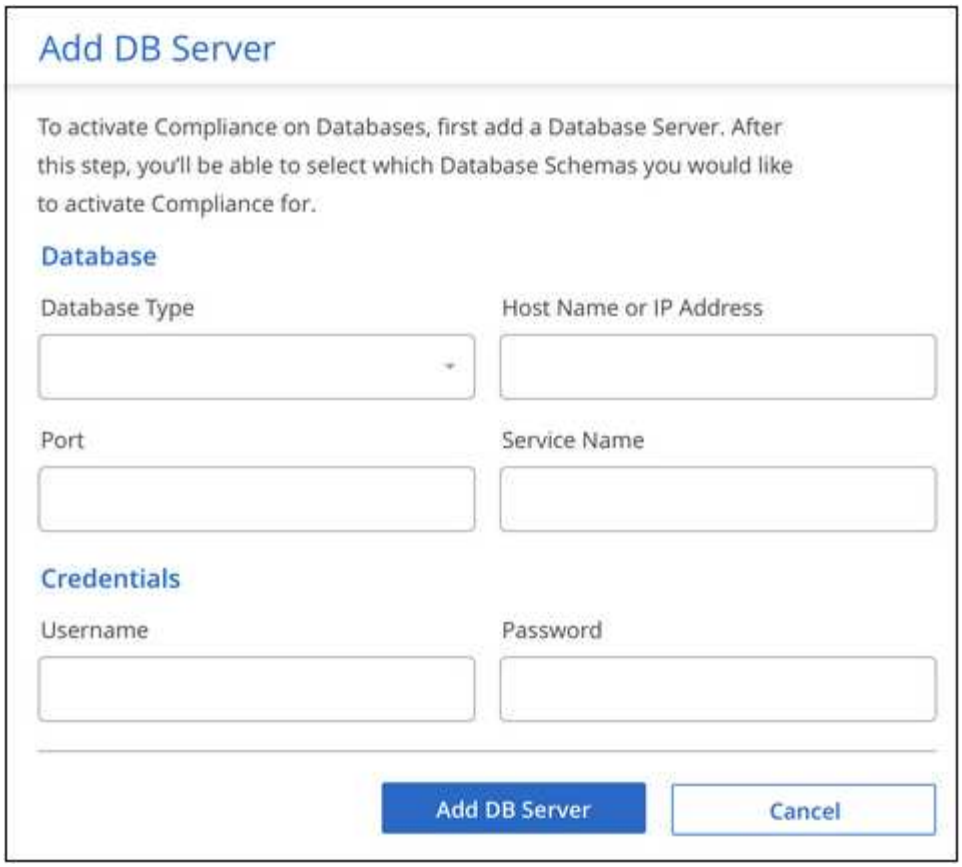
Fügen Sie den Datenbankserver hinzu

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

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



2. Geben Sie die erforderlichen Informationen ein, um den Datenbankserver zu identifizieren.
   a. Wählen Sie den Datenbanktyp aus.
   b. Geben Sie den Port und den Hostnamen oder die IP-Adresse ein, um eine Verbindung zur Datenbank herzustellen.
   c. Geben Sie für Oracle-Datenbanken den Dienstnamen ein.
   d. Geben Sie die Zugangsdaten ein, damit die BlueXP Klassifizierung auf den Server zugreifen kann.
   e. Klicken Sie auf **DB-Server hinzufügen**.



Die Datenbank wird zur Liste der Arbeitsumgebungen hinzugefügt.

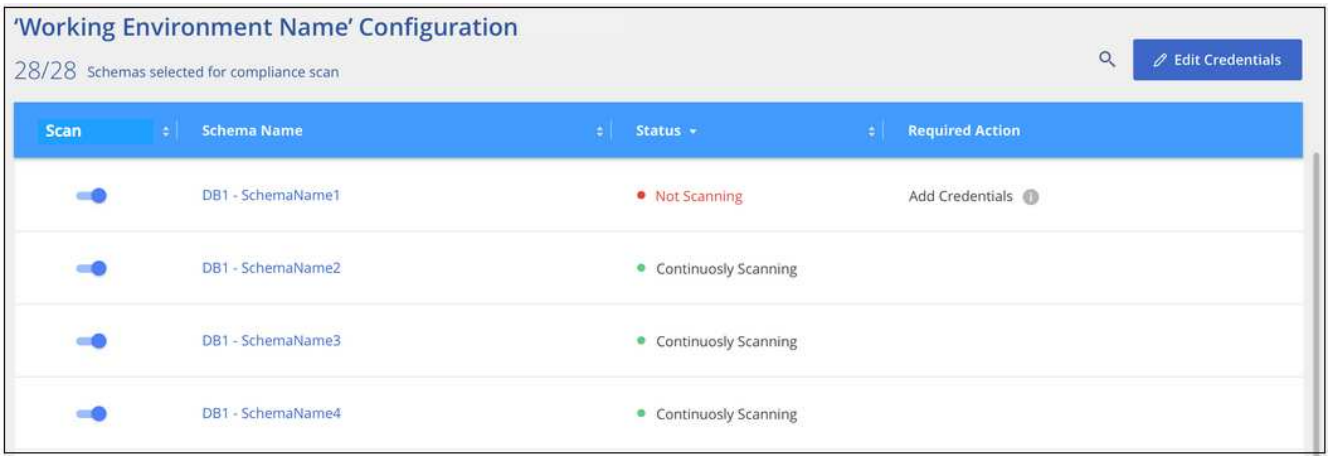
Aktivieren und deaktivieren Sie Compliance-Scans für Datenbankschemas

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

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

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

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



Ergebnis

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

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

Scannen von Dateifreigaben

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

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

Schnellstart

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

1. **Prüfen Sie die Voraussetzungen für die Dateifreigabe**

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

2. **Implementieren der BlueXP Klassifizierungsinstanz**

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

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

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

4 Fügen Sie die Dateifreigaben der Gruppe hinzu

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

Prüfen der Anforderungen für die Dateifreigabe

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

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

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

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

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

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

Implementieren der BlueXP Klassifizierungsinstanz

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

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

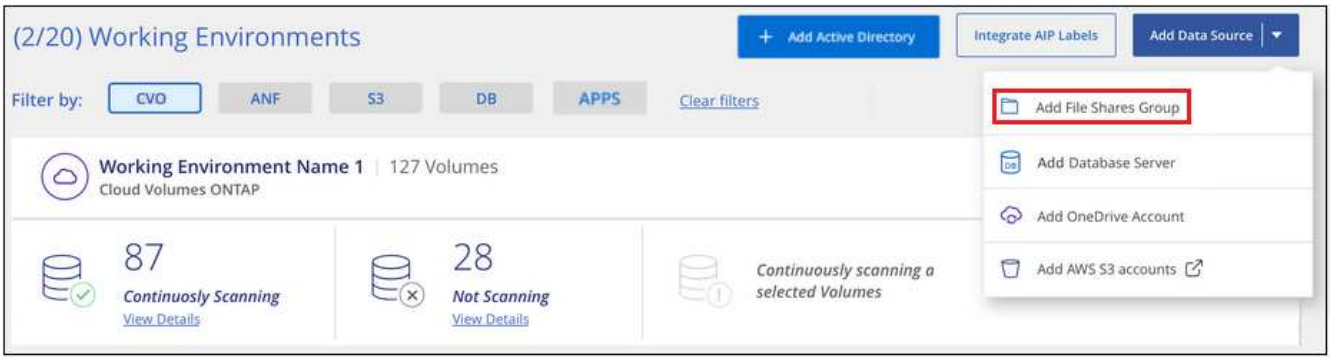
Erstellen der Gruppe für die Dateifreigaben

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

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

Schritte

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



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

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

Hinzufügen von Dateifreigaben zu einer Gruppe

Sie fügen der Dateifreigaben-Gruppe Dateifreigaben hinzu, damit die Dateien in diesen Freigaben durch die BlueXP-Klassifizierung gescannt werden. Sie fügen die Freigaben im Format hinzu `<host_name>:/<share_path>`.

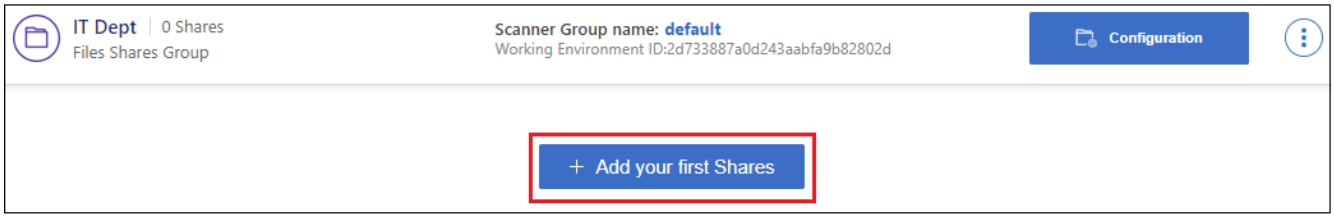
Sie können einzelne Dateifreigaben hinzufügen, oder Sie können eine Liste der Dateien, die Sie scannen möchten, mit einer Zeile eingeben. Sie können bis zu 100 Shares gleichzeitig hinzufügen.

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

Schritte

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

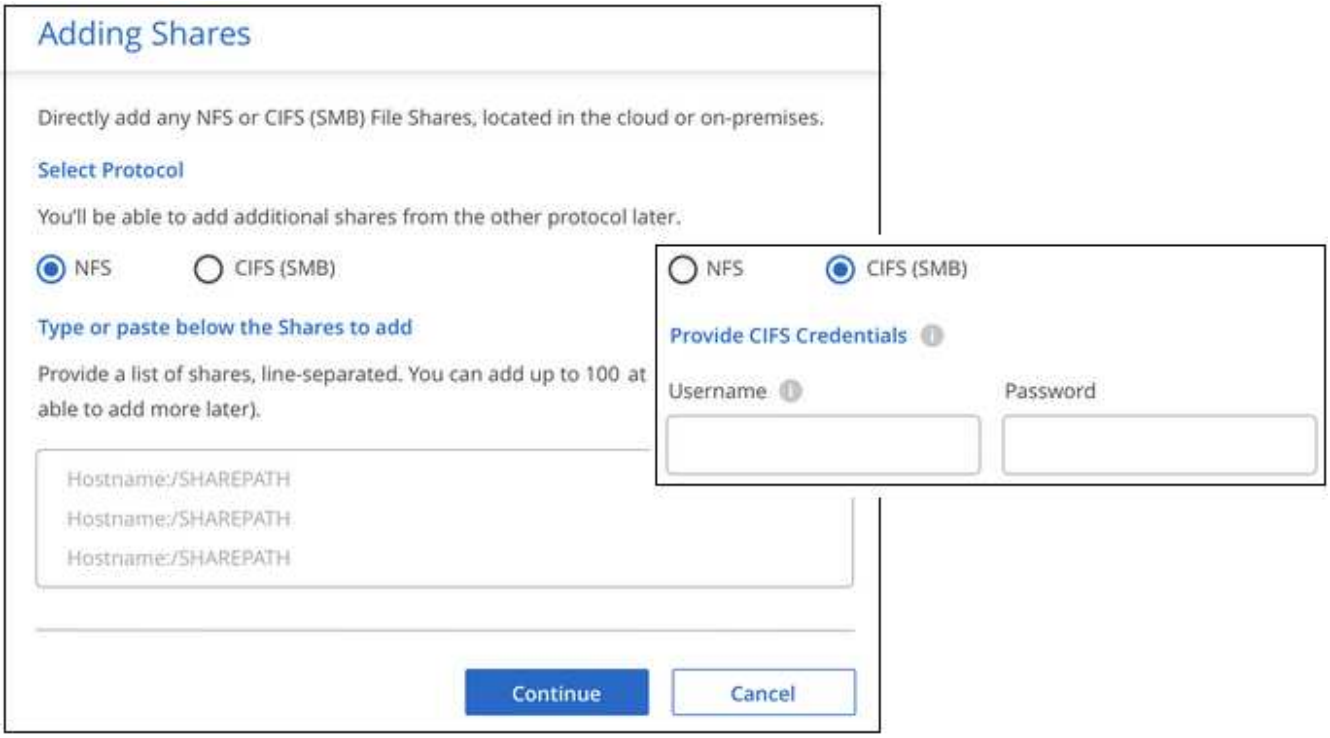
2. Wenn dies das erste Mal ist, um Dateifreigaben für diese File Shares-Gruppe hinzuzufügen, klicken Sie auf **erste Shares hinzufügen**.



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

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

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



Ein 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 mappingbare Scans oder Mappings und Klassifizierungen.

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

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Weitere Informationen .".

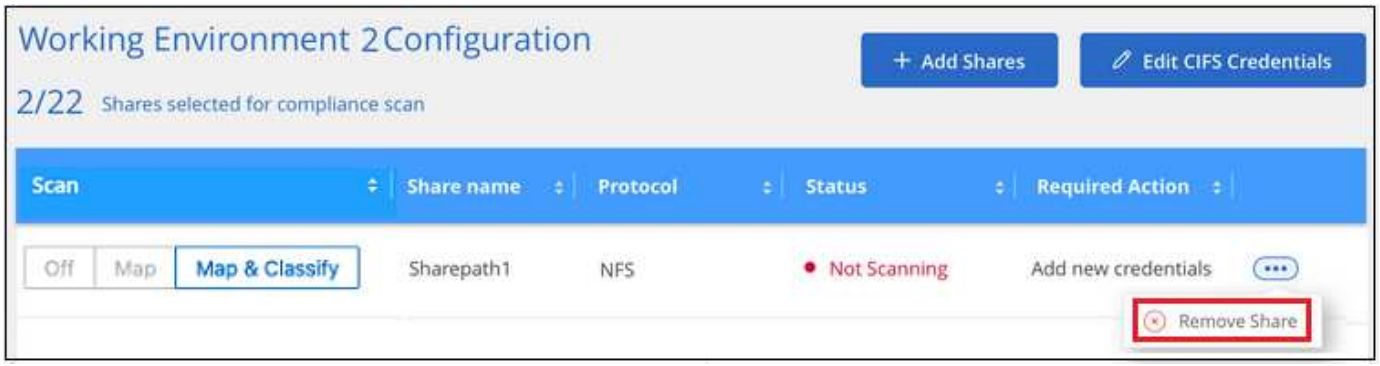
Ergebnis

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

Entfernen einer Dateifreigabe aus Compliance-Scans

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

entfernen.



Integrieren Sie Active Directory in die BlueXP Klassifizierung

Sie können eine globale Active Directory-Klassifizierung mit BlueXP integrieren und so die Ergebnisse verbessern, die BlueXP Klassifizierungen von Dateieigentümern meldet und die Benutzer und Gruppen Zugriff auf Ihre Dateien haben.

> Die Integration in Active Directory wird in der Kernversion der BlueXP Klassifizierung nicht unterstützt.

Wenn Sie bestimmte (unten aufgeführte) Datenquellen einrichten, müssen Sie Active Directory-Anmeldeinformationen eingeben, um die BlueXP Klassifizierung zum Scannen von CIFS-Volumes zu ermöglichen. Diese Integration ermöglicht die Klassifizierung von BlueXP mit Angaben zu Dateieigentümerrechten und Berechtigungen für die Daten in diesen Datenquellen. Das für diese Datenquellen eingegebene Active Directory unterscheidet sich möglicherweise von den globalen Active Directory-Anmeldeinformationen, die Sie hier eingeben. Die BlueXP Klassifizierung betrachtet in allen integrierten Active Directorys unter Angabe von Benutzer- und Berechtigungsdetails.

Diese Integration bietet zusätzliche Informationen an folgenden Standorten in der BlueXP Klassifizierung:

- Sie können den „Dateieigentümer“ verwenden. "Filtern" Und siehe die 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

Durch eine Active Directory Integration mit BlueXP Klassifizierung können Daten aus den folgenden Datenquellen identifiziert werden:

- On-Premises ONTAP Systeme

- Cloud Volumes ONTAP
- Azure NetApp Dateien
- FSX für ONTAP
- OneDrive-Konten und SharePoint-Konten (für ältere Versionen 1.30 und früher)

Es wird keine Unterstützung für das Identifizieren von Benutzer- und Berechtigungsinformationen aus Datenbankschemas, Google Drive-Konten, Amazon S3-Konten oder Objekt-Storage mit dem S3-Protokoll (Simple Storage Service) angeboten.

Stellen Sie eine Verbindung zu Ihrem Active Directory-Server her

Nachdem Sie die BlueXP Klassifizierung implementiert und das Scannen Ihrer Datenquellen aktiviert haben, können Sie die BlueXP Klassifizierung 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-Zugangsdaten können schreibgeschützt sein, allerdings ist durch die Angabe von Administratorberechtigungen sichergestellt, dass die BlueXP Klassifizierung alle Daten lesen kann, die erhöhte Berechtigungen erfordern. Die Zugangsdaten werden in der BlueXP Klassifizierungsinstanz gespeichert.

Wenn Sie bei CIFS Volumes/Dateifreigaben sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „zuletzt zugegriffen“ unverändert bleiben, empfehlen wir dem Benutzer die Berechtigung zum Schreiben von Attributen. 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

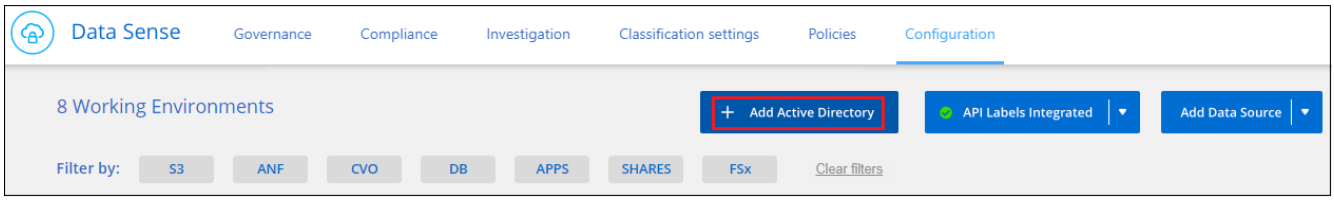
  LDAP-Server-IP-Adresse oder mehrere IP-Adressen

  - 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 Outbound-Kommunikation durch die BlueXP Klassifizierungsinstanz offen sein:

Protokoll	Port	Ziel	Zweck
TCP UND UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP über SSL
TCP	3268	Active Directory	Globaler Katalog
TCP	3269	Active Directory	Globaler Katalog über SSL

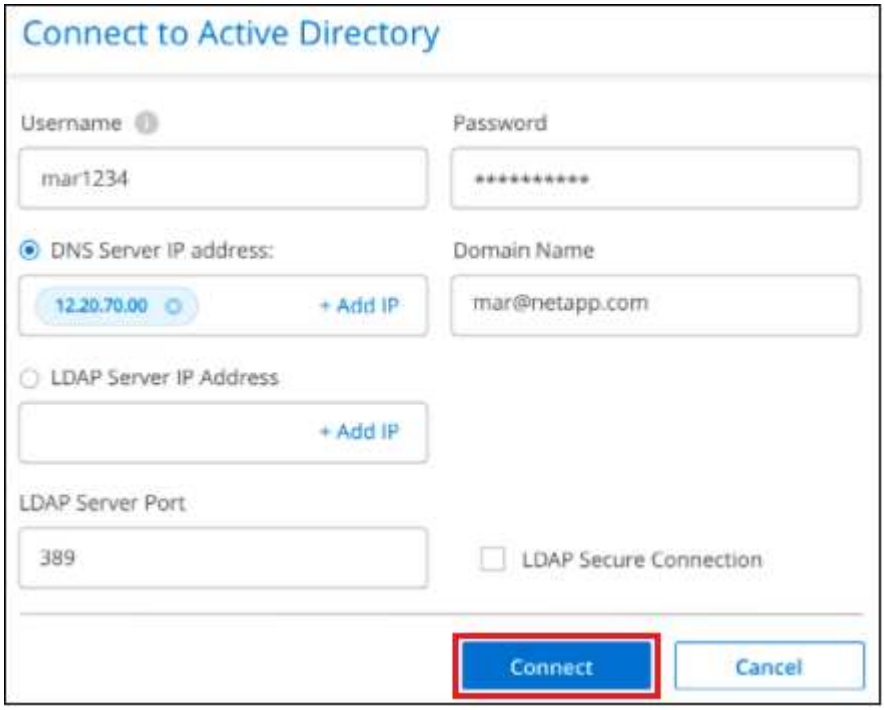
Schritte

1. Klicken Sie auf der Seite BlueXP Classification Configuration auf **Add Active Directory**.

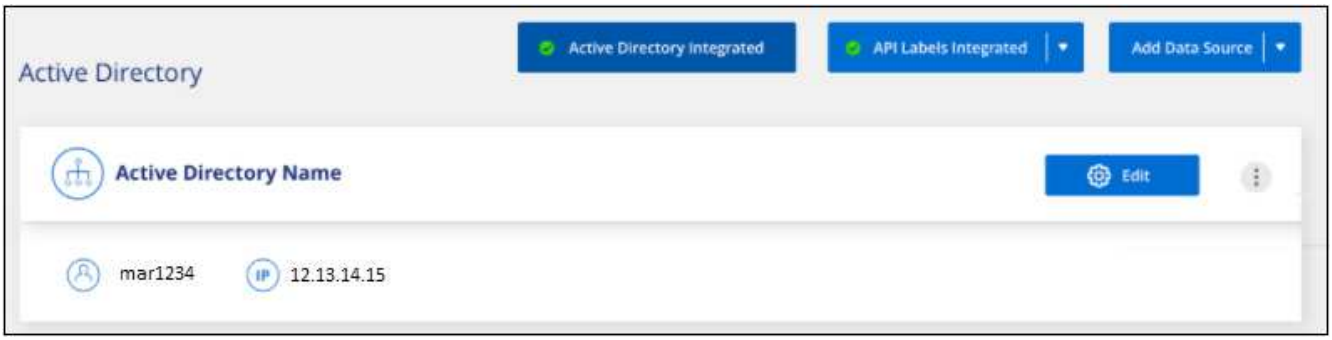


2. Geben Sie im Dialogfeld mit Active Directory verbinden die Active Directory-Details ein, und klicken Sie auf **Verbinden**.

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



   Die BlueXP Klassifizierung wird in Active Directory integriert. Anschließend wird der Konfigurationsseite ein neuer Abschnitt hinzugefügt.



Verwalten Sie Ihre 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**.

Häufig gestellte Fragen zur BlueXP Klassifizierung

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

BlueXP Klassifizierungsservice

Die folgenden Fragen bieten ein allgemeines Verständnis der BlueXP Klassifizierung.

Was ist die BlueXP Klassifizierung?

Die BlueXP Klassifizierung ist ein Cloud-Angebot, das auf KI-gestützter Technologie (künstliche Intelligenz) setzt, um den Datenkontext zu verstehen und sensible Daten in Ihren Storage-Systemen zu identifizieren. Bei den Systemen kann es sich um Arbeitsumgebungen handelt, die Sie in BlueXP Canvas hinzugefügt haben, sowie um viele Arten von Datenquellen, auf die BlueXP-Klassifizierung über Ihre Netzwerke zugreifen kann. "Die vollständige Liste finden Sie unten".

Die BlueXP Klassifizierung bietet vordefinierte Parameter (z. B. Arten von sensiblen Daten und Kategorien), um neue Daten-Compliance-Vorschriften für Datenschutz und -Sensibilität zu erfüllen, beispielsweise die DSGVO, CCPA oder HIPAA.

Wie funktioniert die BlueXP Klassifizierung?

Die BlueXP Klassifizierung implementiert eine weitere Schicht aus künstlicher Intelligenz zusammen mit Ihrem BlueXP System und Ihren Storage-Systemen. Anschließend werden die Daten auf Volumes, Buckets, Datenbanken und anderen Storage-Konten überprüft und die gefundenen Dateneinblicke indiziert. Die BlueXP Klassifizierung nutzt sowohl künstliche Intelligenz als auch natürliche Sprachverarbeitung, im Gegensatz zu alternativen Lösungen, die häufig auf regulären Ausdrücken und Mustervergleichen basieren.

Die BlueXP Klassifizierung verwendet KI, um ein kontextbezogenes Verständnis der Daten für eine genaue Erkennung und Klassifizierung zu ermöglichen. 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.

"Erfahren Sie mehr über die BlueXP Klassifizierung".

"Weitere Informationen zu Anwendungsfällen für die BlueXP Klassifizierung".

Wie sieht es mit der Architektur der BlueXP Klassifizierung aus?

Die BlueXP Klassifizierung implementiert einen einzelnen Server oder Cluster unabhängig von Ihrer Wahl – in der Cloud oder lokal. 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?

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

Verfügt die BlueXP Klassifizierung über EINE REST-API, die auch mit Tools von Drittanbietern funktioniert?

Nein, für die BlueXP Klassifizierung gibt es keine REST-API.

Ist die BlueXP Klassifizierung über die Marktplätze verfügbar?

Ja, die Klassifizierung von BlueXP und BlueXP kann auf den AWS, Azure und GCP Marketplace abgerufen werden.

BlueXP Klassifizierungsscan und -Analysen

Die folgenden Fragen beziehen sich auf die Scan-Performance der BlueXP Klassifizierung sowie auf die für Anwender verfügbaren Analysen.

Wie oft werden meine Daten durch die BlueXP Klassifizierung gescannt?

Während der erste Scan Ihrer Daten etwas Zeit in Anspruch nehmen kann, untersuchen nachfolgende Scans nur die inkrementellen Änderungen, was die Systemscanzeiten verkürzt. Die BlueXP Klassifizierung scannt Ihre Daten kontinuierlich nach Round Robin-Verfahren und bietet Ihnen sechs Repositorys gleichzeitig, sodass alle geänderten Daten sehr schnell klassifiziert werden.

"Lesen Sie, wie Scans funktionieren".

Beachten Sie, dass die BlueXP Klassifizierung Datenbanken nur einmal pro Tag scannt – Datenbanken werden nicht wie andere Datenquellen fortlaufend gescannt.

Datenscans haben keine nennenswerten Auswirkungen auf Ihre Storage-Systeme und Ihre Daten. Wenn Sie jedoch auch nur geringe Auswirkungen haben, können Sie die BlueXP-Klassifizierung für „langsame“ Scans konfigurieren. "Erfahren Sie, wie Sie die Scangeschwindigkeit verringern".

Kann ich meine Daten mithilfe der BlueXP Klassifizierung durchsuchen?

Die BlueXP Klassifizierung bietet umfangreiche Suchfunktionen, die das Suchen nach einer bestimmten Datei oder einem Datenelement über alle verbundenen Quellen hinweg erleichtern. Die BlueXP Klassifizierung ermöglicht Benutzern eine umfassendere Suche als nur die Inhalte der Metadaten. 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. Die BlueXP Klassifizierung verfügt außerdem über RBAC-Kontrollen. Damit können Dateien verschoben oder gelöscht werden, sofern entsprechende 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.

Bietet die BlueXP Klassifizierung Berichte?

Ja. Die durch die Klassifizierung von BlueXP angebotenen Informationen können für andere Beteiligte in Ihrem Unternehmen relevant sein. Deshalb ermöglichen wir Ihnen die Erstellung von Berichten und die damit verbundene Nutzung. Die folgenden Berichte sind für die BlueXP Klassifizierung verfügbar:

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 .".

Data Discovery Assessment-Bericht

Bietet eine allgemeine Analyse der gescannten Umgebung, um die Ergebnisse des Systems hervorzuheben und Problembereiche und mögliche Schritte zur Problembehebung aufzuzeigen. "Lernmodus".

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 BlueXP Klassifizierungsinstanz" Und "Implementieren der BlueXP Klassifizierung" 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".

BlueXP Klassifizierungsmanagement und Datenschutz

Die folgenden Fragen enthalten Informationen zum Management von BlueXP Klassifizierungs- und Datenschutzeinstellungen.

Wie lässt sich die BlueXP Klassifizierung aktivieren?

Zunächst müssen Sie eine Instanz der BlueXP Klassifizierung in BlueXP oder auf einem lokalen System implementieren. Sobald die Instanz ausgeführt wird, können Sie den Dienst auf vorhandenen Arbeitsumgebungen, Datenbanken und anderen Datenquellen über die Registerkarte **Konfiguration** oder durch Auswahl einer bestimmten Arbeitsumgebung aktivieren.

"Erste Schritte".

> Durch die Aktivierung der BlueXP Klassifizierung einer Datenquelle wird ein sofortiger erster Scan durchgeführt. Ergebnisse des Scans werden kurz danach angezeigt.

Wie deaktiviere ich die BlueXP-Klassifizierung?

Sie können die BlueXP Klassifizierung für das Scannen einzelner Arbeitsumgebungen, Datenbanken oder Dateifreigabegruppen auf der Seite BlueXP Klassifizierungskonfiguration deaktivieren.

"Weitere Informationen .".

> Um die BlueXP Klassifizierungsinstanz vollständig zu entfernen, können Sie die BlueXP Klassifizierungsinstanz manuell aus dem Portal Ihres Cloud-Providers oder Ihrem lokalen Standort entfernen.

Kann ich den Service an die Anforderungen meines Unternehmens anpassen?

Die BlueXP Klassifizierung bietet Einblick in Ihre Daten. Diese Erkenntnisse können extrahiert und für die Bedürfnisse Ihres Unternehmens verwendet werden.

Darüber hinaus bietet die BlueXP Klassifizierung Ihnen viele Möglichkeiten, eine benutzerdefinierte Liste mit „personenbezogenen Daten“ hinzuzufügen, die durch die BlueXP Klassifizierung in Scans identifiziert werden. So haben Sie alle Informationen darüber, wo sich potenziell sensible Daten in den Dateien 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 den Dienst anweisen, Scandaten in bestimmten Verzeichnissen auszuschließen?

Ja. Wenn die BlueXP Klassifizierung Scandaten in bestimmten Quellverzeichnissen ausschließen soll, können Sie der Klassifizierungs-Engine diese Liste bereitstellen. Nach Anwendung dieser Änderung schließt die BlueXP Klassifizierung Scandaten in den angegebenen Verzeichnissen aus.

"Weitere Informationen .".

Werden Snapshots gescannt, die sich auf ONTAP-Volumes befinden?

Nein Durch die BlueXP Klassifizierung werden Snapshots nicht gescannt, da der Inhalt mit dem Inhalt des Volume identisch ist.

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

Wenn die BlueXP Klassifizierung Volumes scannt, die kalte Daten in Objekt-Storage verschoben haben, scannt sie alle Daten auf lokalen Festplatten, während die kalten Daten in Objekt-Storage verschoben werden. Dies gilt auch für Produkte, die nicht von NetApp stammen und Tiering implementieren.

Der Scan heizt die kalten Daten nicht auf – sie bleiben kalt und verbleiben im Objekt-Storage.

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 der BlueXP Klassifizierung gescannt werden?

Die BlueXP Klassifizierung kann Daten aus Arbeitsumgebungen scannen, die Sie der BlueXP Leinwand hinzugefügt haben, sowie aus vielen Arten von strukturierten und unstrukturierten Datenquellen, auf die die BlueXP Klassifizierung über Ihre Netzwerke zugreifen kann.

Siehe "Unterstützte Arbeitsumgebungen und Datenquellen".

Gibt es Einschränkungen bei der Bereitstellung in einer Regierungsregion?

Die BlueXP Klassifizierung wird unterstützt, wenn der Connector in einer Regierungsregion (AWS GovCloud, Azure Gov oder Azure DoD) bereitgestellt wird – auch als „eingeschränkter Modus“ bezeichnet. Bei einer solchen Implementierung unterliegt die BlueXP Klassifizierung folgenden Einschränkungen:

> **HINWEIS** Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

- 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 die BlueXP-Klassifizierung auf einer Website ohne Internetzugang installiere?

Die BlueXP Klassifizierung kann nur Daten aus lokalen Datenquellen am lokalen Standort scannen. Derzeit kann die BlueXP Klassifizierung folgende lokale Datenquellen scannen – im „privaten Modus“, auch als „dunkle“ Site bezeichnet:

- On-Premises ONTAP Systeme
- Datenbankschemas
- Objekt-Storage, der das Simple Storage Service (S3)-Protokoll verwendet

Siehe "Unterstützte Arbeitsumgebungen und Datenquellen".

Welche Dateitypen werden unterstützt?

Die BlueXP Klassifizierung scannt alle Dateien nach Kategorien- und Metadaten und zeigt alle Dateitypen im Abschnitt „Dateitypen“ des Dashboards an.

Wenn die BlueXP Klassifizierung personenbezogene Daten 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 werden durch die BlueXP Klassifizierung erfasst?

Die BlueXP Klassifizierung ermöglicht Ihnen die Durchführung eines allgemeinen „Mapping“-Scans oder eines vollständigen „Klassifizierungs“-Scans für 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.

- **Data Mapping Scan**: Die BlueXP Klassifizierung 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.

- **Datenklassifizierung (Deep) Scan**: BlueXP Klassifizierungsscans mit Standardprotokollen und Lesezugriff in Ihren gesamten 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 zahlreiche zusätzliche BlueXP Klassifizierungsfunktionen, die Sie auf Ihre Daten anwenden können, beispielsweise das Anzeigen und Optimieren von Daten auf der Seite „Datenuntersuchung“, das Suchen nach Namen in Dateien, das Kopieren, Verschieben und Löschen von Quelldateien usw.

Die BlueXP Klassifizierung erfasst Metadaten wie z. B. Dateiname, -Berechtigungen, -Erstellungszeit, letzter Zugriff und letzte Änderung. Dies umfasst alle Metadaten, die auf der Seite „Datenermittlungsdetails“ und in „Datenermittlungsberichte“ angezeigt werden.

Durch die BlueXP Klassifizierung können viele Arten von privaten Daten identifiziert werden, wie z. B. personenbezogene Daten (PII) und sensible personenbezogene Daten (SPii). Weitere Informationen zu privaten Daten finden Sie unter "Kategorien von privaten Daten, die durch die BlueXP Klassifizierung gescannt werden".

Kann ich die BlueXP Klassifizierungsinformationen auf bestimmte Benutzer beschränken?

Ja, die BlueXP Klassifizierung ist vollständig in BlueXP integriert. BlueXP-Benutzer können nur Informationen für die Arbeitsumgebungen sehen, für die sie gemäß ihren Arbeitsbereichberechtigungen angezeigt werden können.

Wenn Sie bestimmten Benutzern darüber hinaus erlauben möchten, die Ergebnisse der BlueXP Klassifizierungsüberprüfung einfach anzuzeigen, ohne BlueXP Klassifizierungseinstellungen zu managen, können Sie diesen Benutzern die Rolle der Cloud Compliance Viewer zuweisen.

"Weitere Informationen .".

Kann jemand auf die privaten Daten zugreifen, die zwischen meinem Browser und der BlueXP Klassifizierung gesendet werden?

Nein Die privaten Daten, die zwischen Ihrem Browser und der BlueXP Klassifizierungsinstanz übertragen werden, sind durch End-to-End-Verschlüsselung mit TLS 1.2 geschützt. Das bedeutet, dass NetApp und andere Anbieter die Daten nicht lesen können. Die BlueXP Klassifizierung gibt keine Daten oder Ergebnisse an NetApp weiter, es sei denn, Sie beantragen und genehmigen den Zugriff.

Die gescannten Daten verbleiben in Ihrer Umgebung.

Wie werden sensible Daten behandelt?

NetApp hat keinen Zugriff auf sensible Daten und zeigt sie nicht in der Benutzeroberfläche an. Sensible Daten werden maskiert, beispielsweise werden die letzten vier Zahlen für Kreditkarteninformationen angezeigt.

Wo werden die Daten gespeichert?

Die Scan-Ergebnisse werden in Elasticsearch innerhalb der BlueXP Klassifizierungsinstanz gespeichert.

Wie wird auf die Daten zugegriffen?

Die BlueXP Klassifizierung greift über API-Aufrufe, die eine Authentifizierung erfordern und mit AES-128 verschlüsselt sind, auf in Elasticsearch gespeicherte Daten zu. Für den direkten Zugriff auf Elasticsearch ist Root-Zugriff erforderlich.

Lizenzen und Kosten

Die folgende Frage bezieht sich auf Lizenzierung und Kosten der Nutzung der BlueXP Klassifizierung.

Wie hoch sind die Kosten für die Klassifizierung von BlueXP?

Die BlueXP Klassifizierung ist eine BlueXP Kernfunktion. Sie ist kostenfrei.

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 implementieren, um die BlueXP-Klassifizierung zu verwenden.

Wo muss der Connector installiert werden?

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS oder Amazon FSX für ONTAP verwenden Sie einen Connector in AWS.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konnektor in Azure.
- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP wird ein Connector in GCP verwendet.
- Wenn Sie Daten in lokalen ONTAP Systemen, NetApp Dateifreigaben oder Datenbanken scannen, können Sie an jedem dieser Cloud-Standorte einen Connector verwenden.

Wenn die Daten an vielen dieser Standorte gespeichert sind, müssen Sie eventuell verwenden "Mehrere Anschlüsse".

Ist für die BlueXP Klassifizierung Zugriff auf Zugangsdaten erforderlich?

Die BlueXP Klassifizierung selbst ruft keine Storage-Anmeldedaten ab. Stattdessen werden sie im BlueXP Connector gespeichert.

Die BlueXP Klassifizierung verwendet Daten-Ebenen-Anmeldedaten, zum Beispiel CIFS-Zugangsdaten, um Freigaben vor dem Scannen zu mounten.

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 auf einem Host in der Cloud. Wenn Sie die BlueXP Klassifizierung lokal implementieren möchten, sollten Sie den Connector möglicherweise auch On-Premises installieren. Dies ist aber nicht erforderlich.

Verwendet die Kommunikation zwischen dem Dienst und dem Connector HTTP?

Ja, die BlueXP Klassifizierung kommuniziert über HTTP mit dem BlueXP Connector.

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 bereit, der keinen Internetzugang hat". "Dies wird auch als „Privatmodus“ bezeichnet.". Anschließend können Sie lokale ONTAP Cluster und andere lokale Datenquellen erkennen und die Daten mit der BlueXP Klassifizierung scannen.

Implementierung der BlueXP Klassifizierung

Die folgenden Fragen beziehen sich auf die separate BlueXP Klassifizierungsinstanz.

Welche Implementierungsmodelle werden von der BlueXP Klassifizierung unterstützt?

Mit BlueXP können Benutzer Systeme praktisch überall scannen und protokollieren, einschließlich On-Premises-, Cloud- und Hybridumgebungen. Die BlueXP Klassifizierung wird normalerweise mit einem SaaS-Modell implementiert. Bei diesem Modell ist der Service über die BlueXP Schnittstelle aktiviert, sodass keine Hardware- oder Softwareinstallation erforderlich ist. 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 Art von Instanz oder VM ist für die BlueXP Klassifizierung erforderlich?

Wenn "In der Cloud implementiert":

- In AWS wird die BlueXP Klassifizierung auf einer m6i.4xlarge-Instanz mit einer GP2-Festplatte mit 500 gib ausgeführt. Sie können während der Bereitstellung einen kleineren Instanztyp auswählen.
- In Azure wird die Klassifizierung von BlueXP auf einer Standard_D16s_v3 VM mit einer Festplatte von 500 gib ausgeführt.
- In GCP wird die BlueXP Klassifizierung auf einer VM gemäß n2-Standard-16 mit einer persistenten Standardfestplatte von 500 gib ausgeführt.

Beachten Sie, dass Sie die BlueXP Klassifizierung auf einem System mit weniger CPUs und weniger RAM

implementieren können. Bei der Nutzung dieser Systeme bestehen jedoch Einschränkungen. Siehe "Verwenden eines kleineren Instanztyps" Entsprechende Details.

"Erfahren Sie mehr über die BlueXP Klassifizierung".

Kann ich die BlueXP Klassifizierung auf meinem eigenen Host implementieren?

Ja. Sie können die BlueXP Klassifizierungs-Software auf einem Linux-Host mit Internetzugang in Ihrem Netzwerk oder in der Cloud installieren. Alles funktioniert gleich, und Sie verwalten Ihre Scankonfiguration und -Ergebnisse weiterhin mit BlueXP. Siehe "Implementierung der BlueXP Klassifizierung 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 die BlueXP Klassifizierung auf einer lokalen Website ohne Internetzugang" Für vollständig sichere Standorte.