Los geht's

BlueXP classification

NetApp
August 11, 2025

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.

Ab Version 1.31 ist die BlueXP -Klassifizierung als Kernfunktion bei BlueXP verfügbar. Es fallen keine zusätzlichen Gebühren an. Es ist keine Lizenz zur Klassifizierung oder kein Abonnement erforderlich. + Wenn Sie die ältere Version 1.30 oder eine frühere Version verwendet haben, ist diese Version verfügbar, bis Ihr Abonnement abläuft. "Siehe eine Liste der veralteten Features".

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

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

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, 4.0 und 4.1 sowie CIFS-Versionen 1.x, 2.0, 2.1 und 3.0.

Kosten

Die BlueXP -Klassifizierung ist frei zu verwenden. 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.

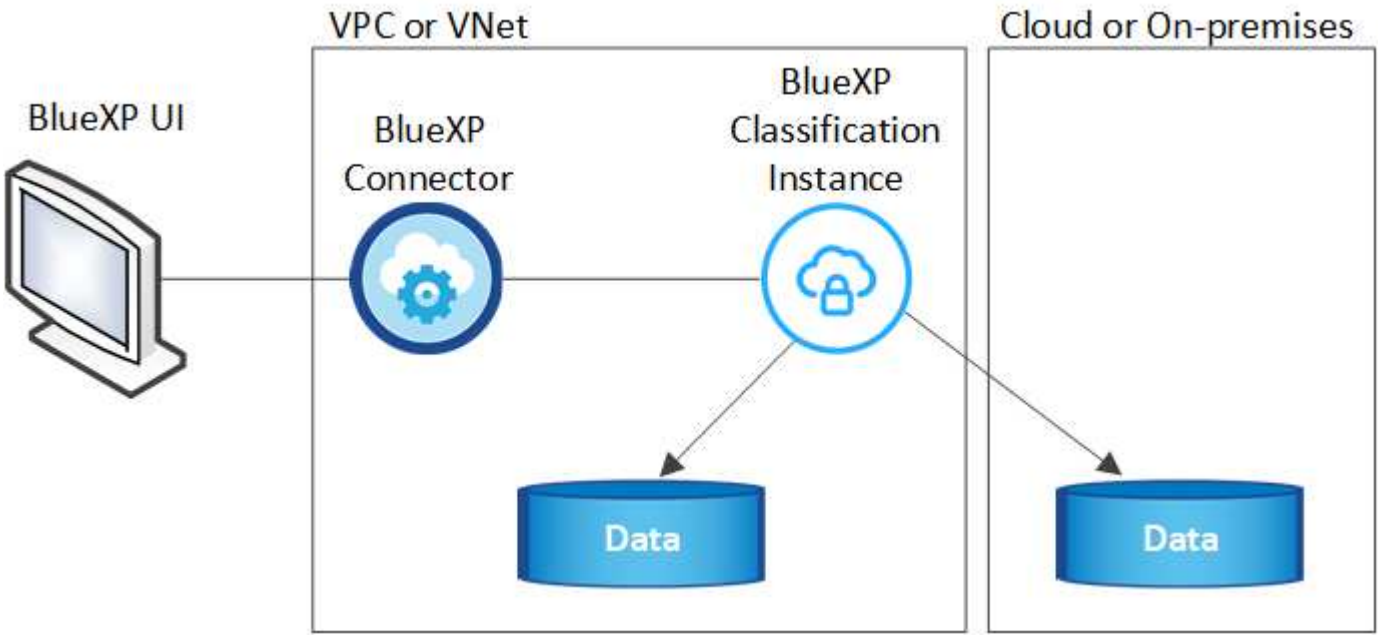
Datentransferkosten

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 einem mit einer Festplatte von 500 gib ausgeführt"Standard_D16s_v3 VM". Das Betriebssystem-Image ist Ubuntu 22.04.
- In GCP wird die BlueXP -Klassifizierung auf einer persistenten Standardfestplatte mit 500 gib ausgeführt"n2-Standard-16-VM". Das Betriebssystem-Image ist Ubuntu 22.04.
- 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-Klassifizierungssoftware werden automatisiert, solange die Instanz über Internetzugang verfügt.

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

Einsatz auf verschiedenen Instanztypen

Überprüfen Sie die folgenden Spezifikationen für Instanztypen:

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.

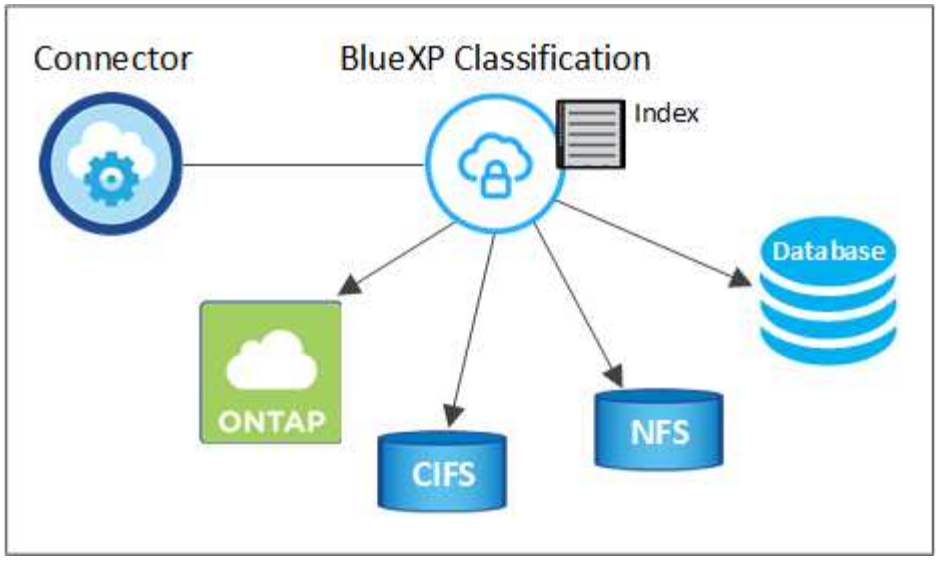
So funktioniert das Scannen der BlueXP -Klassifizierung

Auf hoher Ebene funktioniert das Scannen der BlueXP -Klassifizierung wie folgt:

1. Sie implementieren eine Instanz der BlueXP Klassifizierung in BlueXP.
2. Sie aktivieren High-Level-Mapping (nur *Mapping* Scans genannt) oder Deep-Level-Scan (*Map & Classify* Scans genannt) für eine oder mehrere 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.

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 dem Round Robin-Verfahren, um inkrementelle Änderungen zu erkennen. Aus diesem Grund ist es wichtig, dass die Instanz weiterhin ausgeführt wird.

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

> Die BlueXP classification begrenzt die Datenmenge nicht. Jeder Connector unterstützt das Scannen und Anzeigen von 500 TiB Daten. Um mehr als 500 TiB Daten zu scannen, "einen anderen Connector installieren" Dann "eine weitere Klassifizierungsinstanz bereitstellen" . + Die BlueXP -Benutzeroberfläche zeigt Daten eines einzelnen Konnektors an. Tipps zur Anzeige von Daten mehrerer Konnektoren finden Sie unter "Arbeiten Sie mit mehreren Anschlüssen" .

Was ist der Unterschied zwischen Mapping und Classification Scans

Sie können zwei Arten von Scans in der BlueXP -Klassifizierung durchführen:

- **Nur Mapping-Scans** bieten nur einen allgemeinen Überblick über Ihre Daten und werden an ausgewählten Datenquellen durchgeführt. Reine Mapping-Scans benötigen weniger Zeit als Mapping- und Klassifizierungs-Scans, da sie nicht auf Dateien zugreifen, um die darin enthaltenen Daten anzuzeigen. Sie sollten dies zunächst tun, um Forschungsbereiche zu identifizieren und dann einen Map & Classify-Scan für diese Bereiche durchzuführen.
- **Map & Classify Scans** ermöglichen ein tiefes Scannen Ihrer Daten.

Einzelheiten zu den Unterschieden zwischen Mapping- und Classification-Scans finden Sie unter "Was ist der Unterschied zwischen Mapping- und Classification-Scans?".

Informationen, die durch die BlueXP -Klassifizierung kategorisiert werden

Die BlueXP -Klassifizierung erfasst, indiziert und weist den folgenden Daten Kategorien zu:

- **Standardmetadaten** über Dateien: Der Dateityp, seine Größe, Erstellungs- und Änderungsdaten, und so weiter.
- **Personenbezogene Daten**: Personenbezogene Daten (PII) wie E-Mail-Adressen, Identifikationsnummern oder Kreditkartennummern, die durch die BlueXP -Klassifizierung anhand bestimmter Wörter, Zeichenfolgen und Muster in den Dateien identifiziert werden. "Weitere Informationen zu personenbezogenen Daten".

- **Sensible personenbezogene Daten**: Besondere Arten von sensiblen personenbezogenen Daten (SPII), wie Gesundheitsdaten, ethnische Herkunft oder politische Meinungen, wie sie in der Datenschutz-Grundverordnung (DSGVO) und anderen 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".
- **Namensentity Recognition**: BlueXP Classification verwendet KI, um natürliche Namen von Menschen aus Dokumenten zu extrahieren. "Informieren Sie sich über die Reaktion auf Zugriffsanfragen von Betroffenen".

Netzwerkübersicht

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. Dadurch wird eine Unterstützung für Multi-Cloud-, Cloud-, Private-Cloud- und On-Premises-Umgebungen möglich.

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, und 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 auf die BlueXP classification

Sie können über NetApp BlueXP auf den BlueXP classification zugreifen.

Um sich bei BlueXP anzumelden, können Sie Ihre Anmeldeinformationen für die NetApp Support-Site verwenden oder sich mit Ihrer E-Mail-Adresse und einem Kennwort für eine NetApp Cloud-Anmeldung registrieren. "Erfahren Sie mehr über die Anmeldung bei BlueXP".

Bestimmte Aufgaben erfordern bestimmte BlueXP Benutzerrollen. "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Bevor Sie beginnen

- "Sie sollten einen BlueXP Connector hinzufügen."
- "Finden Sie heraus, welcher Bereitstellungsstil der BlueXP classification zu Ihrer Arbeitslast passt."

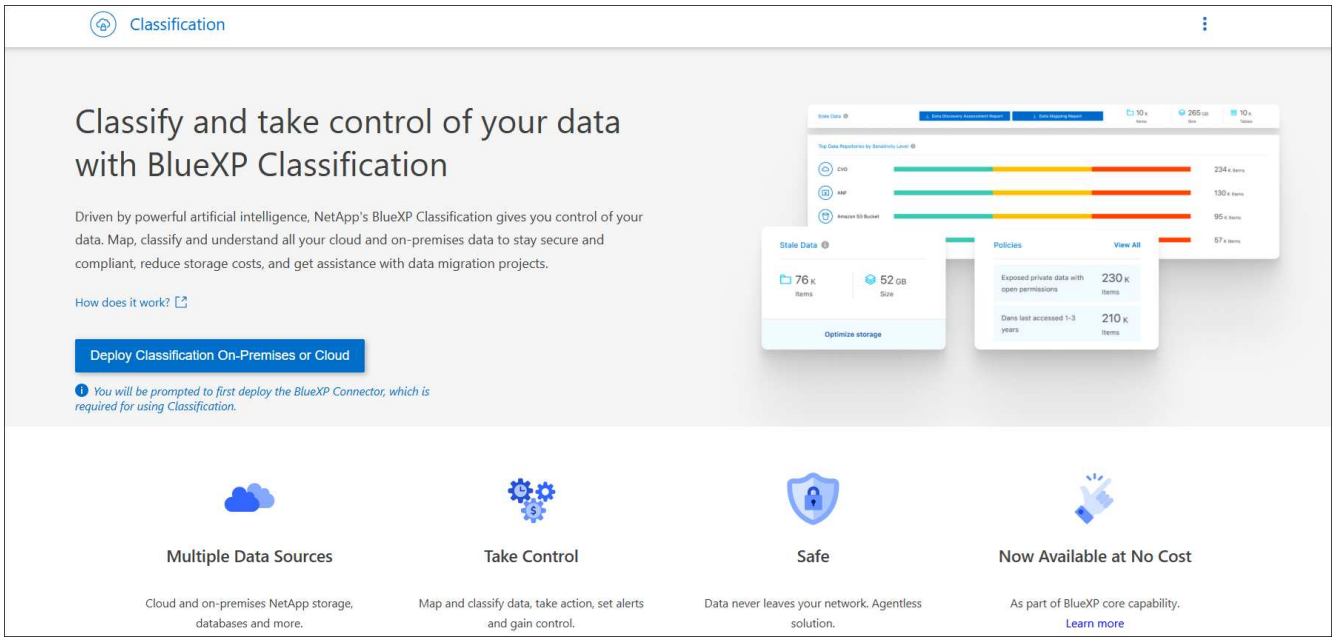
Schritte

1. Navigieren Sie in einem Webbrowser zu "BlueXP-Konsole" .

   Die Anmeldeseite für NetApp BlueXP wird angezeigt.

2. Sign in bei BlueXP an.
3. Wählen Sie im linken Navigationsmenü von BlueXP **Governance** > **Klassifizierung**.
4. Wenn Sie zum ersten Mal auf die BlueXP classification zugreifen, wird die Zielseite angezeigt.

   Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**, um mit der Bereitstellung Ihrer Klassifizierungsinstanz zu beginnen. Weitere Informationen finden Sie unter "Welche BlueXP Klassifizierungs-Implementierung sollten Sie verwenden?"



   Andernfalls wird das BlueXP classification -Dashboard angezeigt.

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, hat keine Verbindung zur BlueXP

SaaS Schicht.

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.

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.

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.

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".

Die BlueXP classification begrenzt die Datenmenge nicht. Jeder Connector unterstützt das Scannen und Anzeigen von 500 TiB Daten. Um mehr als 500 TiB Daten zu scannen, "einen anderen Connector installieren" Dann "eine weitere Klassifizierungsinstanz bereitstellen" . + Die BlueXP -Benutzeroberfläche zeigt Daten eines einzelnen Konnektors an. Tipps zur Anzeige von Daten mehrerer Konnektoren finden Sie unter "Arbeiten Sie mit mehreren Anschlüssen" .

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. Transparente Proxys werden derzeit nicht unterstützt.

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 die Berechtigung zum Bereitstellen von Ressourcen und Erstellen von Sicherheitsgruppen für die BlueXP classification verfügt.

- "Google Cloud-Berechtigungen"
- "AWS-Berechtigungen"
- "Azure-Berechtigungen"

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"

Implementieren Sie die BlueXP Klassifizierung in der Cloud

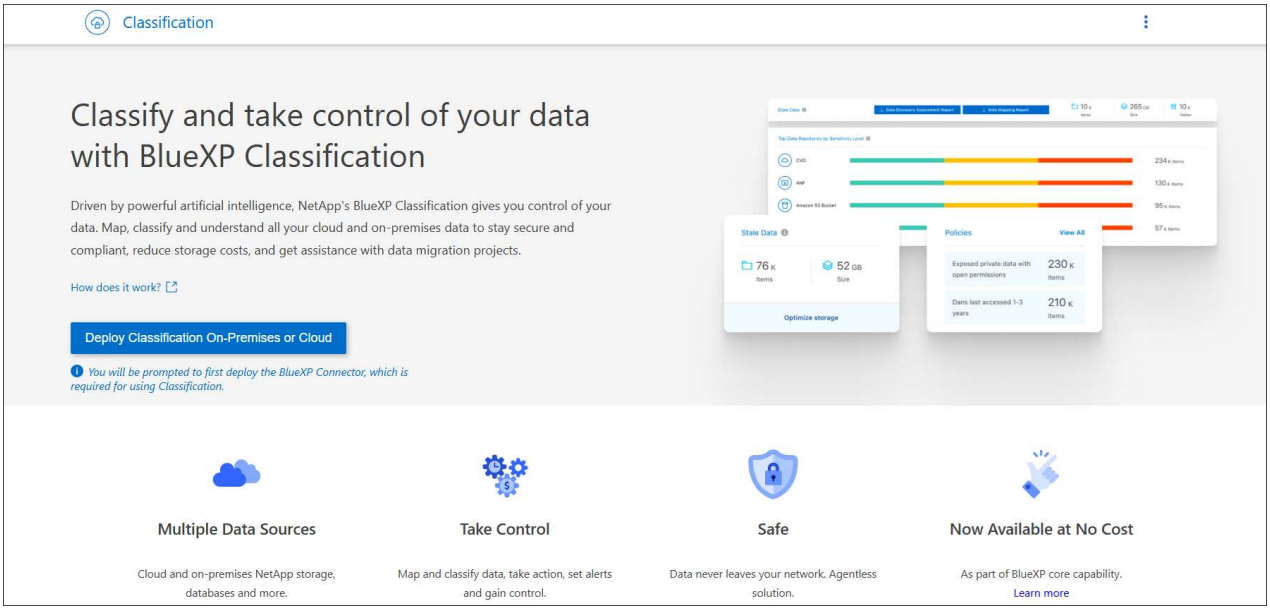
Führen Sie diese Schritte aus, um eine Instanz der BlueXP Klassifizierung in der Cloud zu implementieren. Der Connector implementiert die Instanz in der Cloud und installiert dann die BlueXP Klassifizierungssoftware auf dieser Instanz.

In Regionen, in denen der Standardinstanztyp nicht verfügbar ist, wird die BlueXP -Klassifizierung auf einem ausgeführt"Alternativer Instanztyp".

Implementieren in AWS

Schritte

1. Wählen Sie im linken Navigationsmenü von BlueXP **Governance > Klassifizierung**.
2. Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



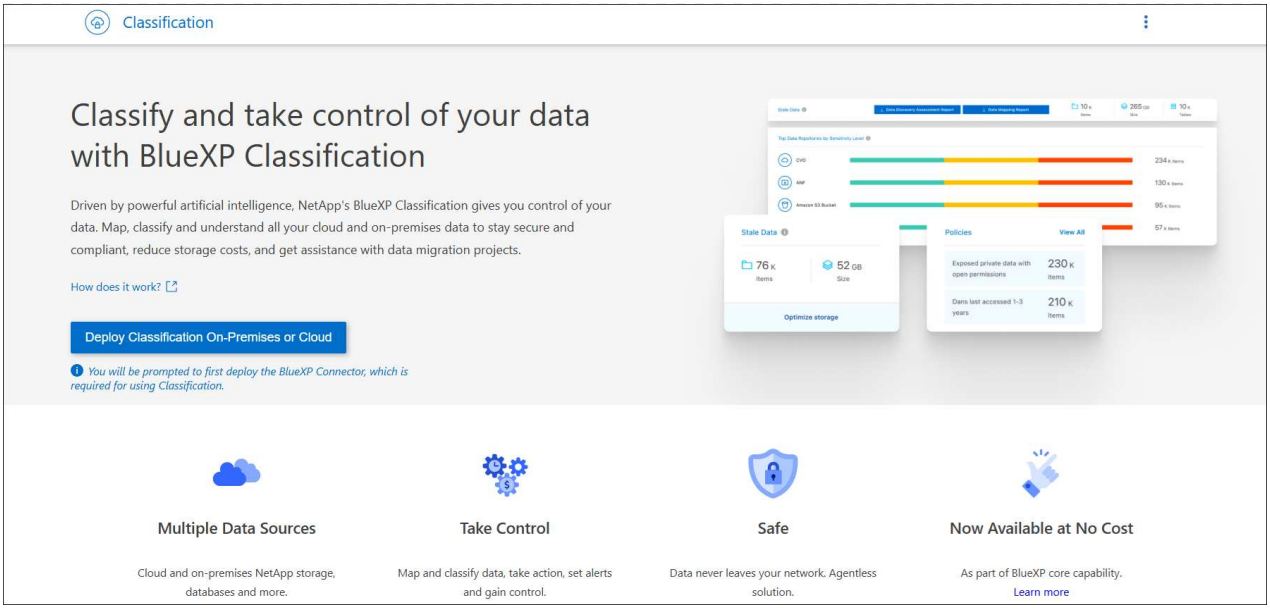
3. Wählen Sie auf der Seite „Installation“ die Option „Bereitstellen > Bereitstellen“ aus, um die Instanzgröße „Groß“ zu verwenden und den Cloud-Bereitstellungsassistenten zu starten.
4. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Es wird angehalten und zur Eingabe aufgefordert, wenn Probleme auftreten.

5. Wenn die Instanz bereitgestellt und die BlueXP classification installiert ist, wählen Sie **Weiter zur Konfiguration**, um zur Seite *Konfiguration* zu gelangen.

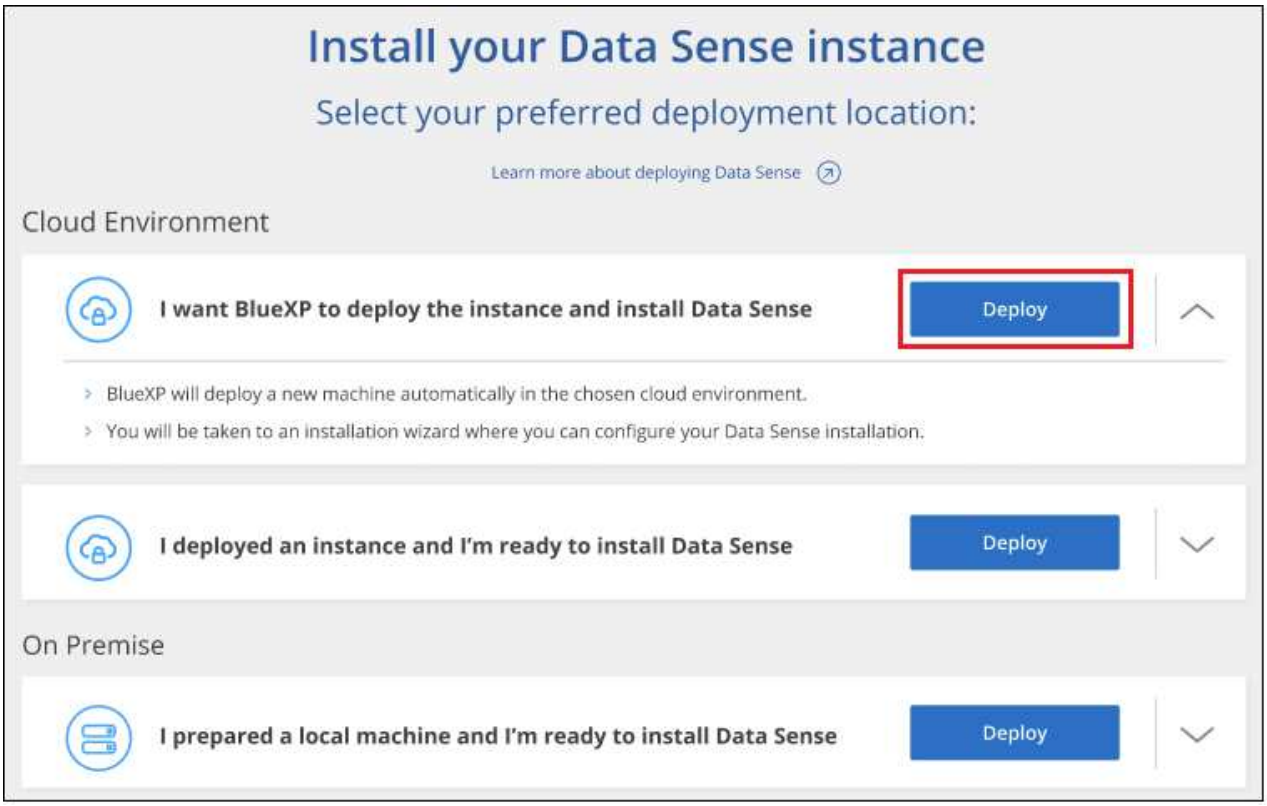
Implementieren in Azure

Schritte

1. Wählen Sie im linken Navigationsmenü von BlueXP **Governance > Klassifizierung**.
2. Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



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



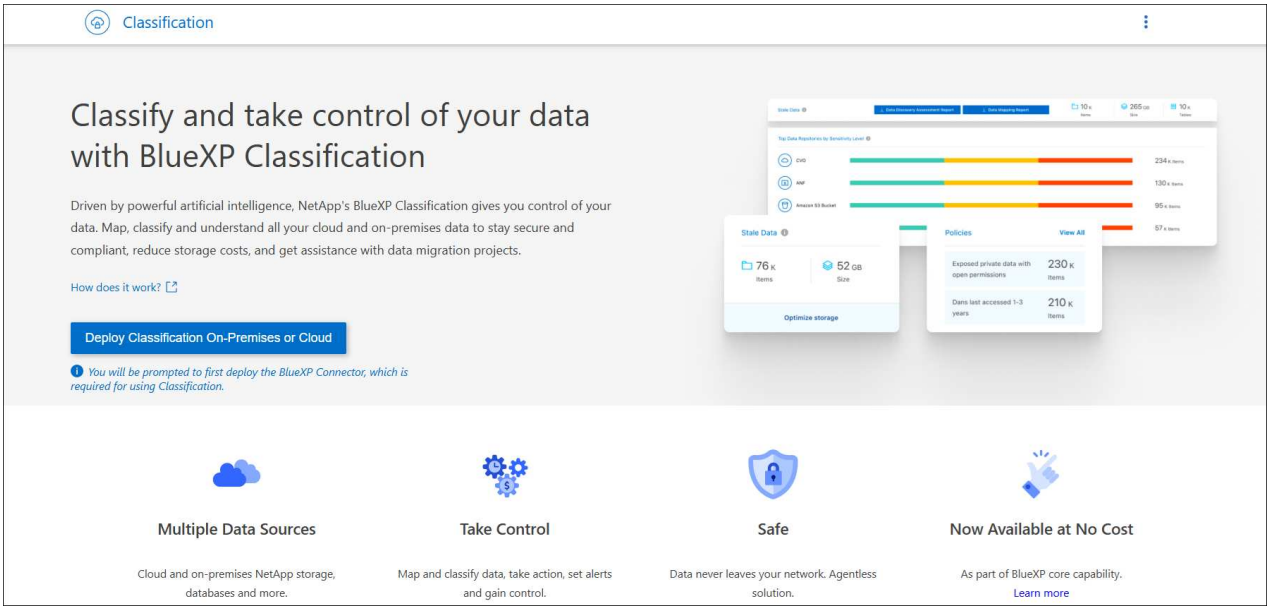
4. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Es wird angehalten und zur Eingabe aufgefordert, wenn Probleme auftreten.

5. Wenn die Instanz bereitgestellt und die BlueXP classification installiert ist, wählen Sie **Weiter zur Konfiguration**, um zur Seite *Konfiguration* zu gelangen.

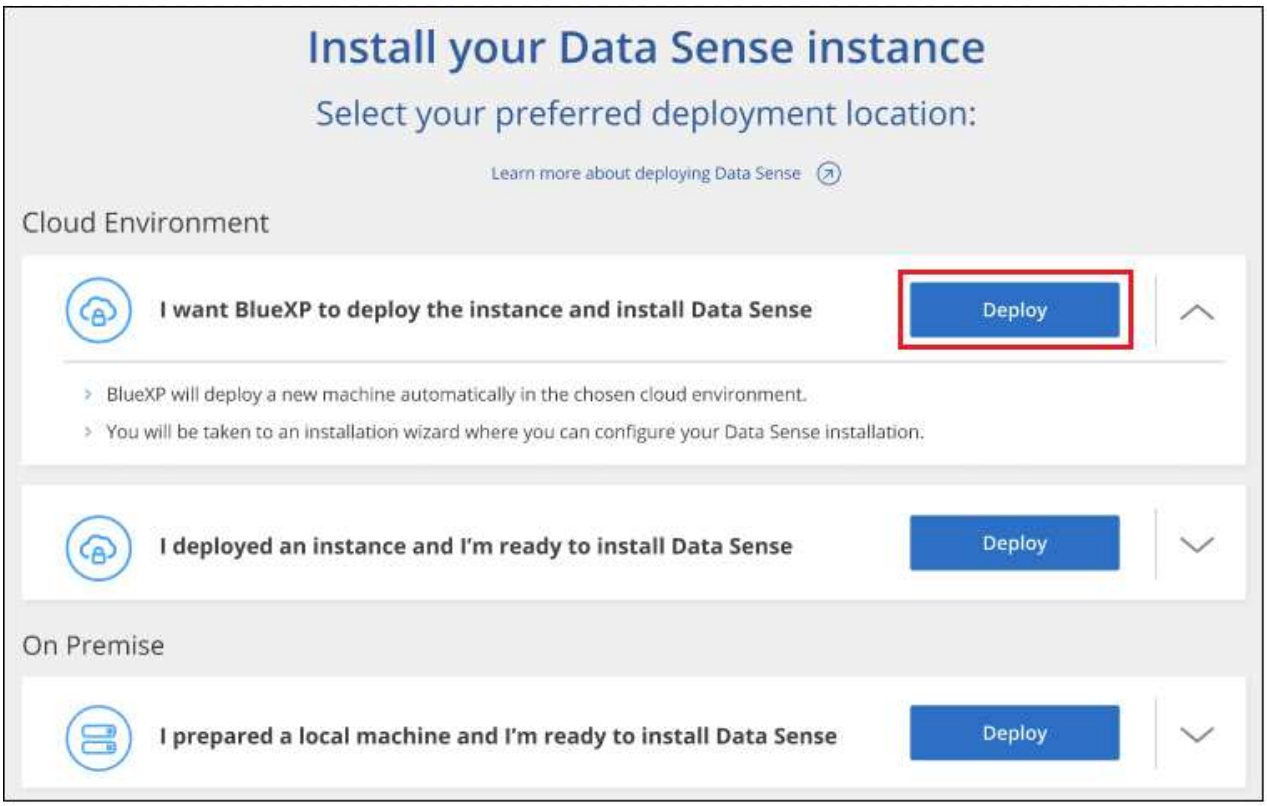
Implementieren in Google Cloud

Schritte

1. Wählen Sie im linken Navigationsmenü von BlueXP **Governance > Klassifizierung**.
2. Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



3. Wählen Sie **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 classification installiert ist, wählen Sie **Weiter zur Konfiguration**, um zur Seite *Konfiguration* 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.

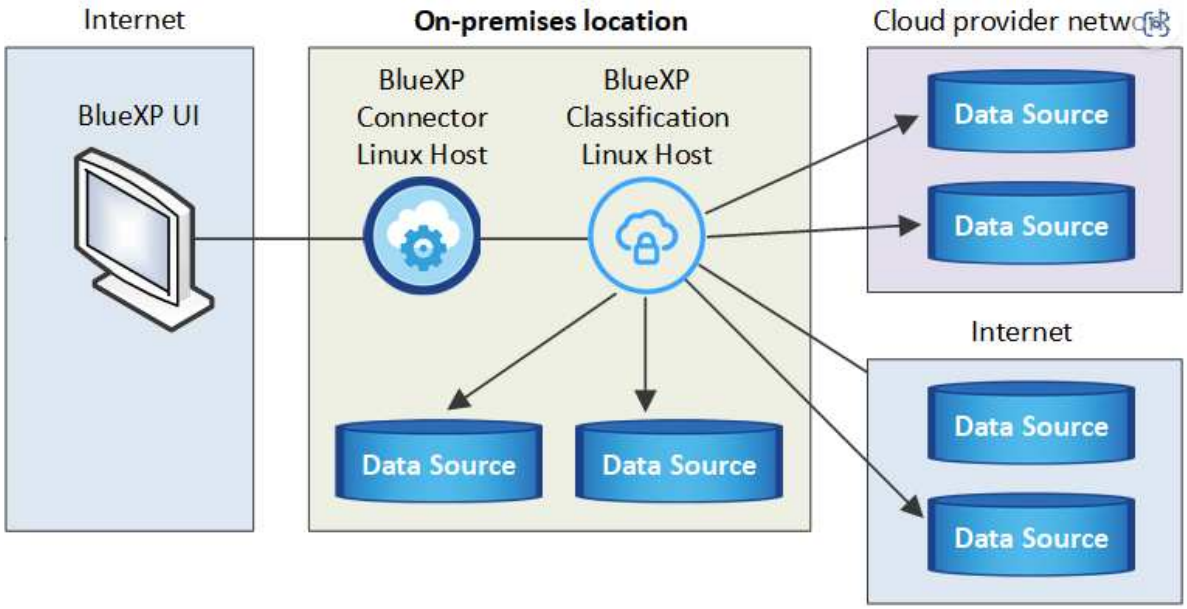
Installieren Sie die BlueXP Klassifizierung auf einem Host mit Internetzugang

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.

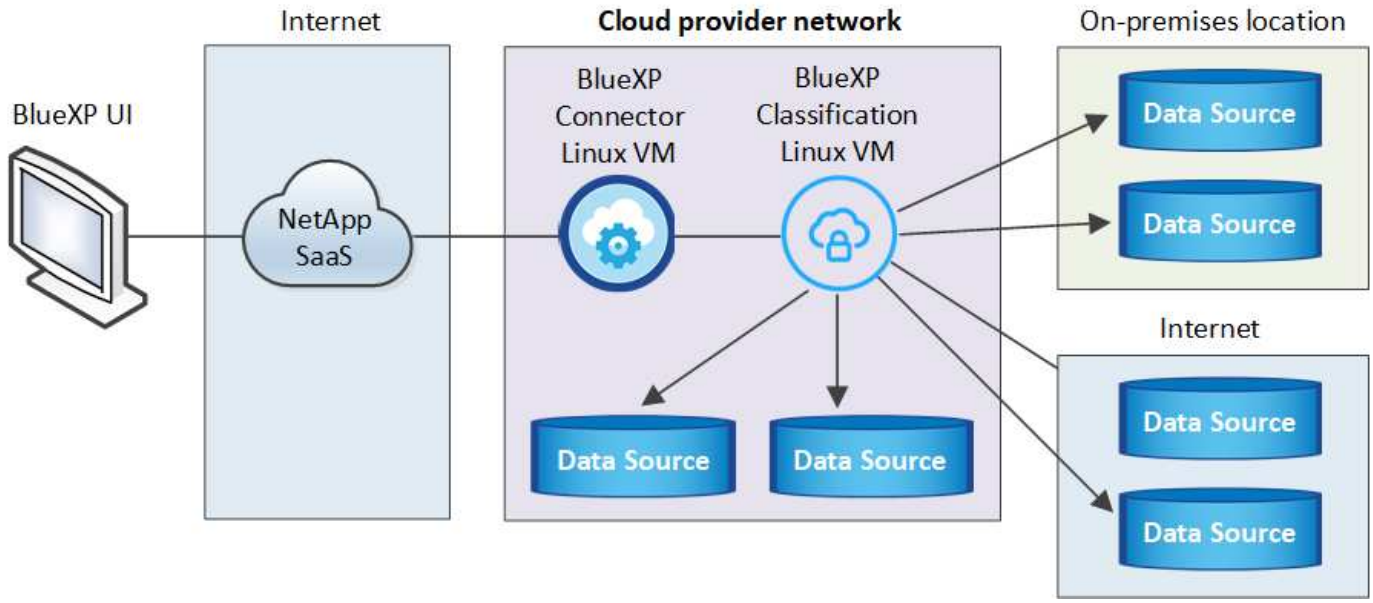
Die On-Premises-Installation ist möglicherweise eine gute Option, wenn Sie lokale ONTAP Systeme lieber mit einer BlueXP Klassifizierungsinstanz scannen möchten, die sich auch vor Ort befindet - dies ist jedoch keine Anforderung. Die Software funktioniert unabhängig von der gewählten Installationsmethode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



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".

Sie können auch "Installieren Sie die BlueXP Klassifizierung auf einer lokalen Website ohne Internetzugang".

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 auf /opt verfügbar • 895 gib verfügbar für /var/lib/Docker • 5 gib auf /tmp • **Für Podman, 5 GB auf /tmp** • **Für Podman, 30 GB auf /var/tmp**
Groß	16 CPUs	64 GB RAM	• 500 gib SSD auf / oder 100 gib auf /opt verfügbar • 395 gib verfügbar auf /var/lib/Docker oder für Podman /var/lib/Containers oder für Podman /var/lib/Containers • 5 gib auf /tmp • **Für Podman, 5 GB auf /tmp** • **Für Podman, 30 GB auf /var/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
    - Ubuntu 22.04 (BlueXP Klassifikation ab Version 1.23 erforderlich)

        - Ubuntu 24.04 (erfordert BlueXP -Klassifizierung Version 1.23 oder höher)
    - 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, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 und 9.6.
    - Advanced Vector Extensions (AVX2) muss auf dem Hostsystem aktiviert sein.
- **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".
        - 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://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.

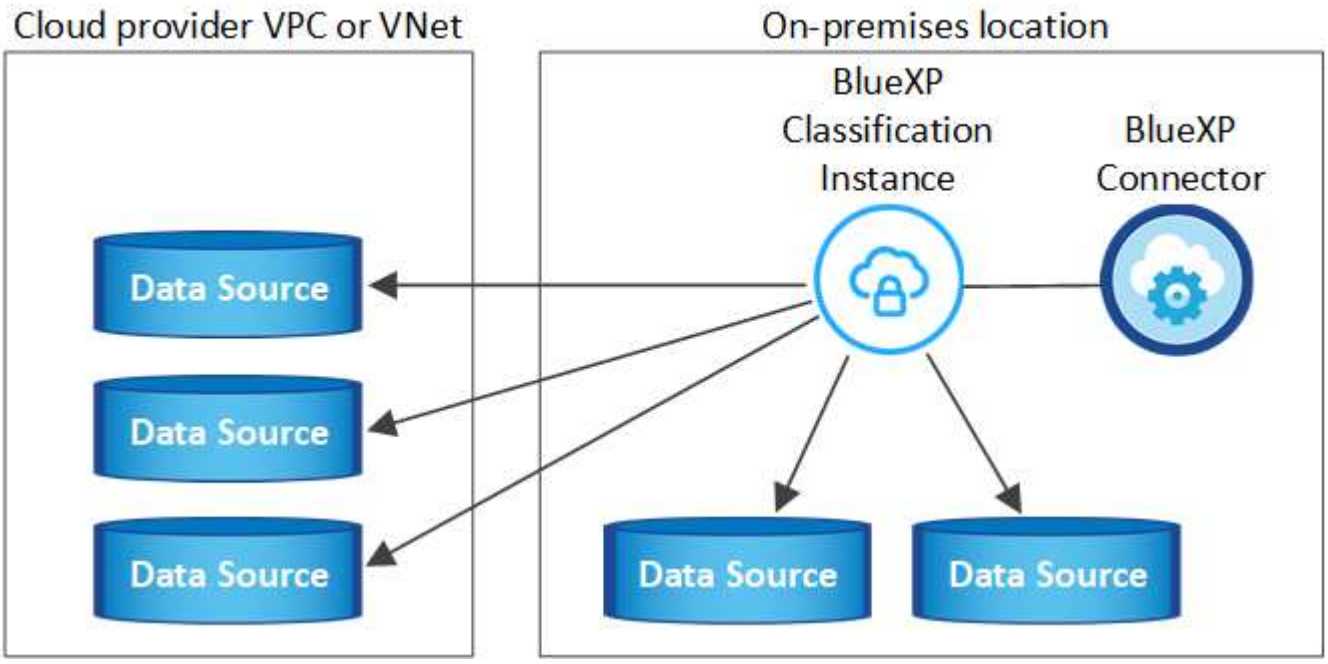
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 443 (TCP) und 80. 9000	Die Firewall- oder Routing-Regeln für den Connector müssen ein- und ausgehenden Datenverkehr über Port 443 zur und von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass Port 8080 geöffnet ist, damit Sie den Installationsfortschritt in BlueXP sehen können. Wenn eine Firewall auf dem Linux-Host verwendet wird, ist Port 9000 für interne Prozesse innerhalb eines Ubuntu-Servers erforderlich.

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.



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" Um zu sehen, wie die BlueXP -Klassifizierung installiert wird.

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".

Bevor Sie beginnen

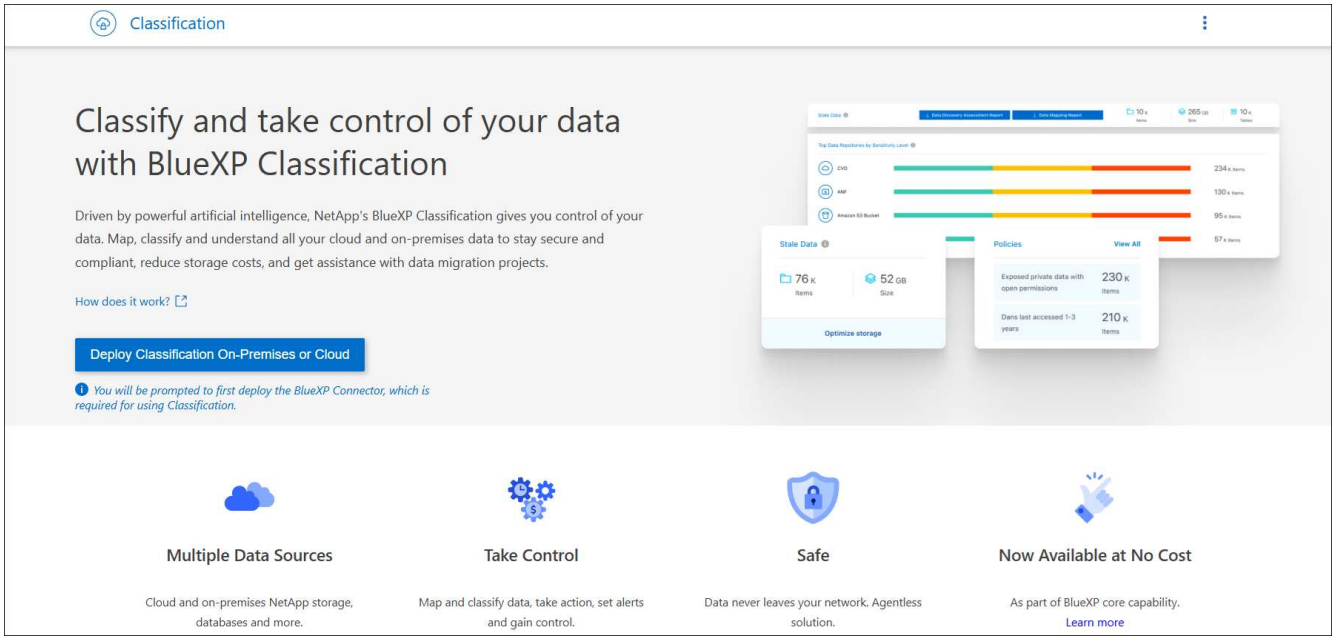
- Vergewissern Sie sich, dass Ihr Linux-System die erfüllt Host-Anforderungen erfüllt.
- Überprüfen Sie, ob auf dem System die beiden erforderlichen Softwarepakete installiert sind (Docker Engine oder Podman und Python 3).
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.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

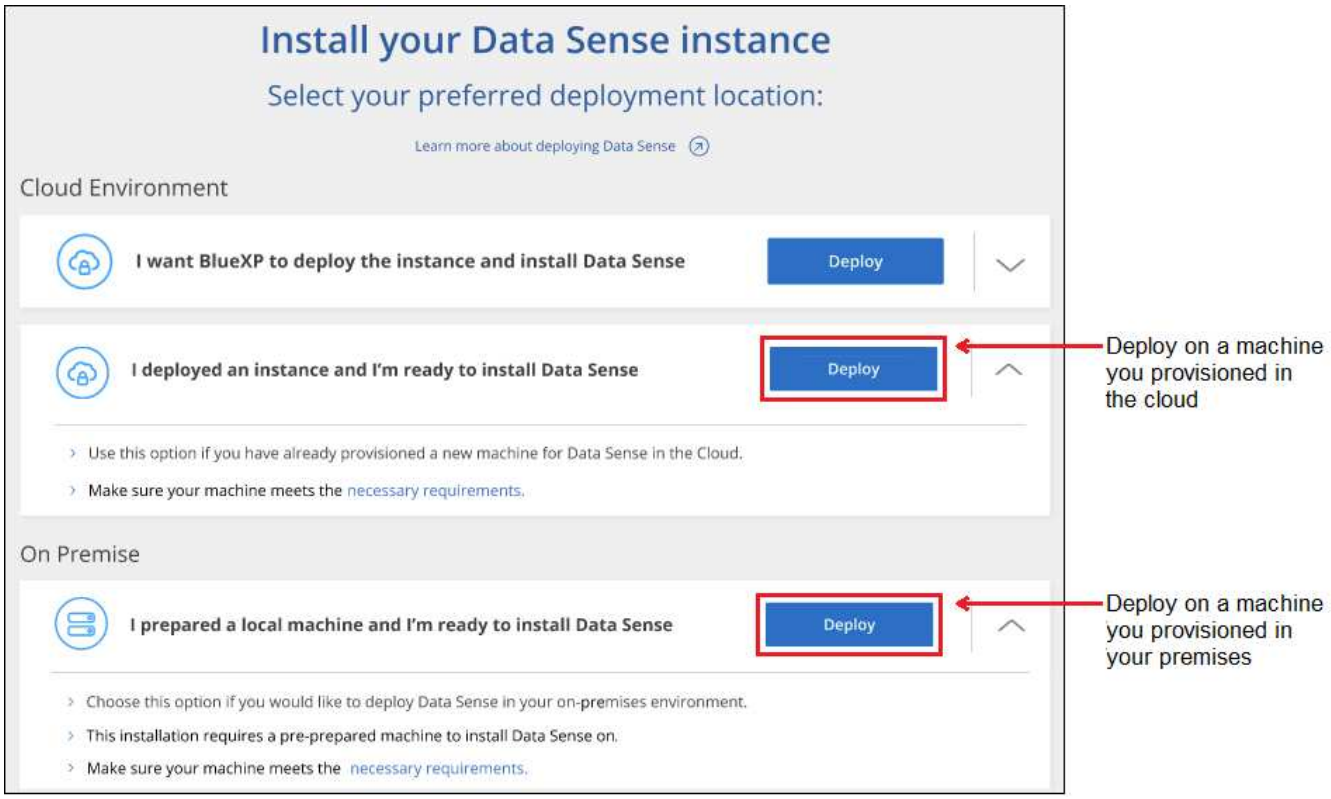
1. Laden Sie die BlueXP Klassifizierungssoftware von herunter "NetApp Support Website". Die ausgewählte Datei heißt **DATASENSE-INSTALLER-<Version>.tar.gz**.
2. Kopieren Sie die Installationsdatei auf den Linux-Host, den Sie verwenden möchten (mit `scp` Oder eine andere Methode).
3. Entpacken Sie die 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. Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



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 Vorabprüfung durchführt, um sicherzustellen, dass Ihre System- und Netzwerkanforderungen für eine erfolgreiche Installation vorhanden sind. "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. Bei diesem Installationstyp, der ein Installationsskript verwendet, besteht keine Verbindung zur BlueXP -SaaS-Schicht.

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

Sie können auch "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.

Installieren Sie den BlueXP-Anschluss

Wenn Sie noch keinen Connector im privaten Modus installiert haben, "Den Stecker einsetzen" Jetzt auf einem Linux-Host.

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.

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 auf /opt verfügbar • 895 gib verfügbar für /var/lib/Docker • 5 gib auf /tmp • **Für Podman, 5 GB auf /tmp** • **Für Podman, 30 GB auf /var/tmp**
Groß	16 CPUs	64 GB RAM	• 500 gib SSD auf / oder 100 gib auf /opt verfügbar • 395 gib verfügbar auf /var/lib/Docker oder für Podman /var/lib/Containers oder für Podman /var/lib/Containers • 5 gib auf /tmp • **Für Podman, 5 GB auf /tmp** • **Für Podman, 30 GB auf /var/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
        - Ubuntu 22.04 (BlueXP Klassifikation ab Version 1.23 erforderlich)
        - Ubuntu 24.04 (erfordert BlueXP -Klassifizierung Version 1.23 oder höher)
    - 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, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 und 9.6.
    - Advanced Vector Extensions (AVX2) muss auf dem Hostsystem aktiviert sein.
- **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".
        - 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.

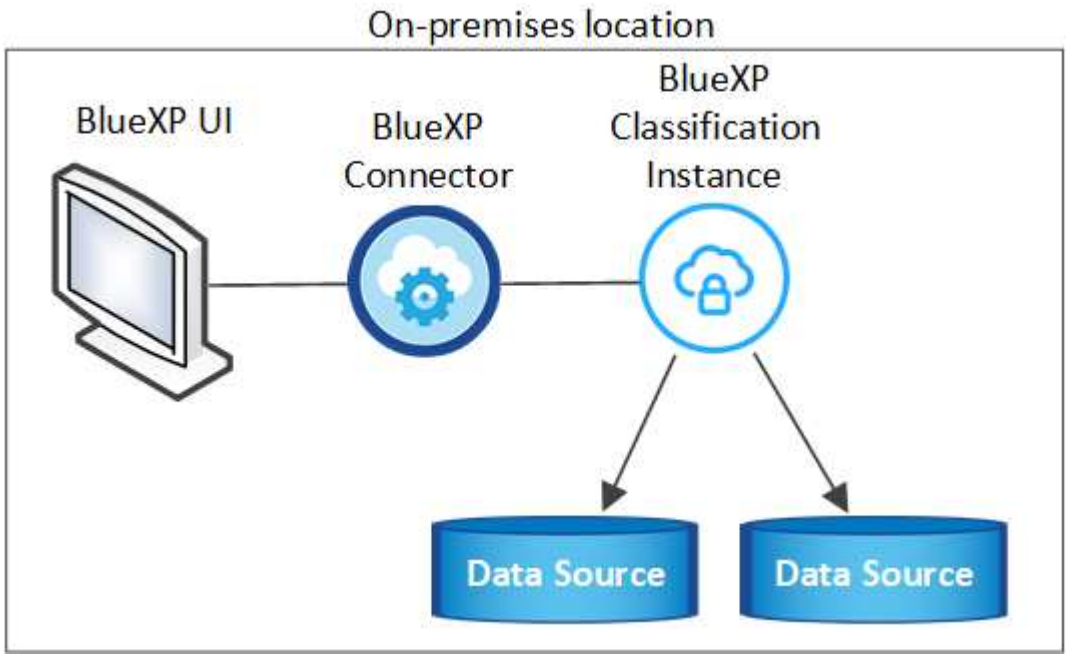
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 6000 (TCP), 443 (TCP) UND 80. 9000	Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über die Ports 6000 und 443 zur und von der BlueXP Klassifizierungsinstanz zulassen. • Port 6000 ist erforderlich, 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. • Wenn eine Firewall auf dem Linux-Host verwendet wird, ist Port 9000 für interne Prozesse innerhalb eines Ubuntu-Servers erforderlich.

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 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.
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.

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)
Wenn eine Firewall auf Linux-Host verwendet wird	9000	Wird für interne Prozesse innerhalb eines Ubuntu-Servers benötigt.

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".

Bevor Sie beginnen

- 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.:

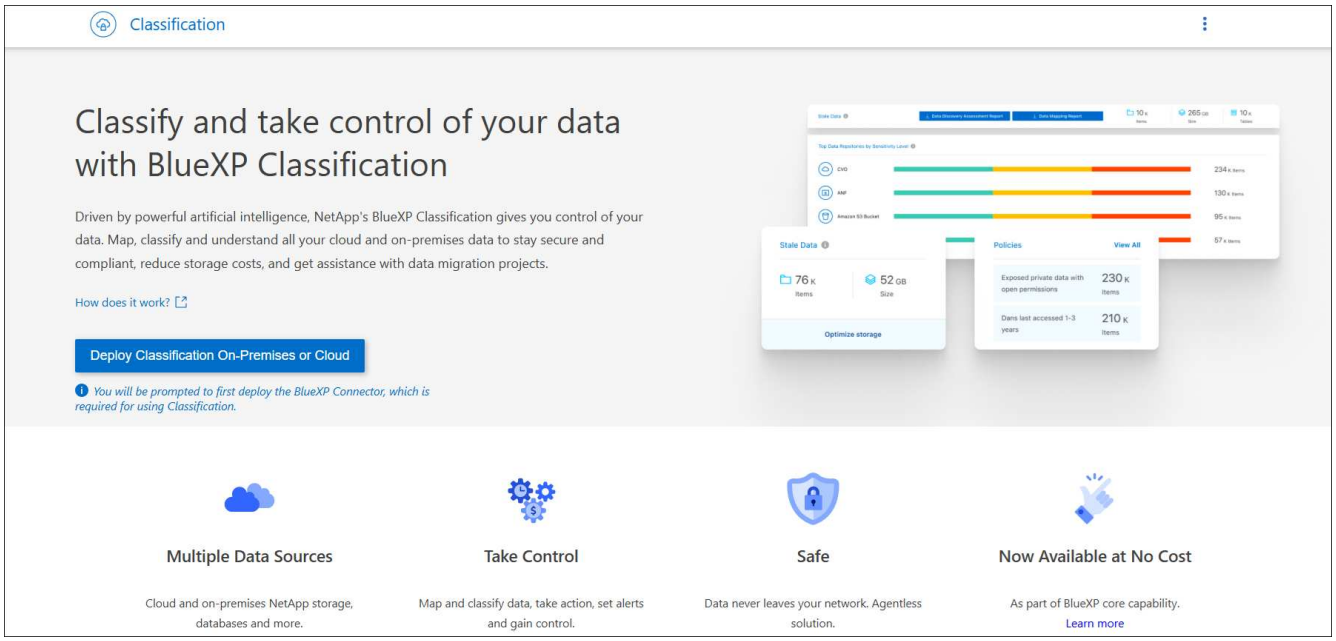
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

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

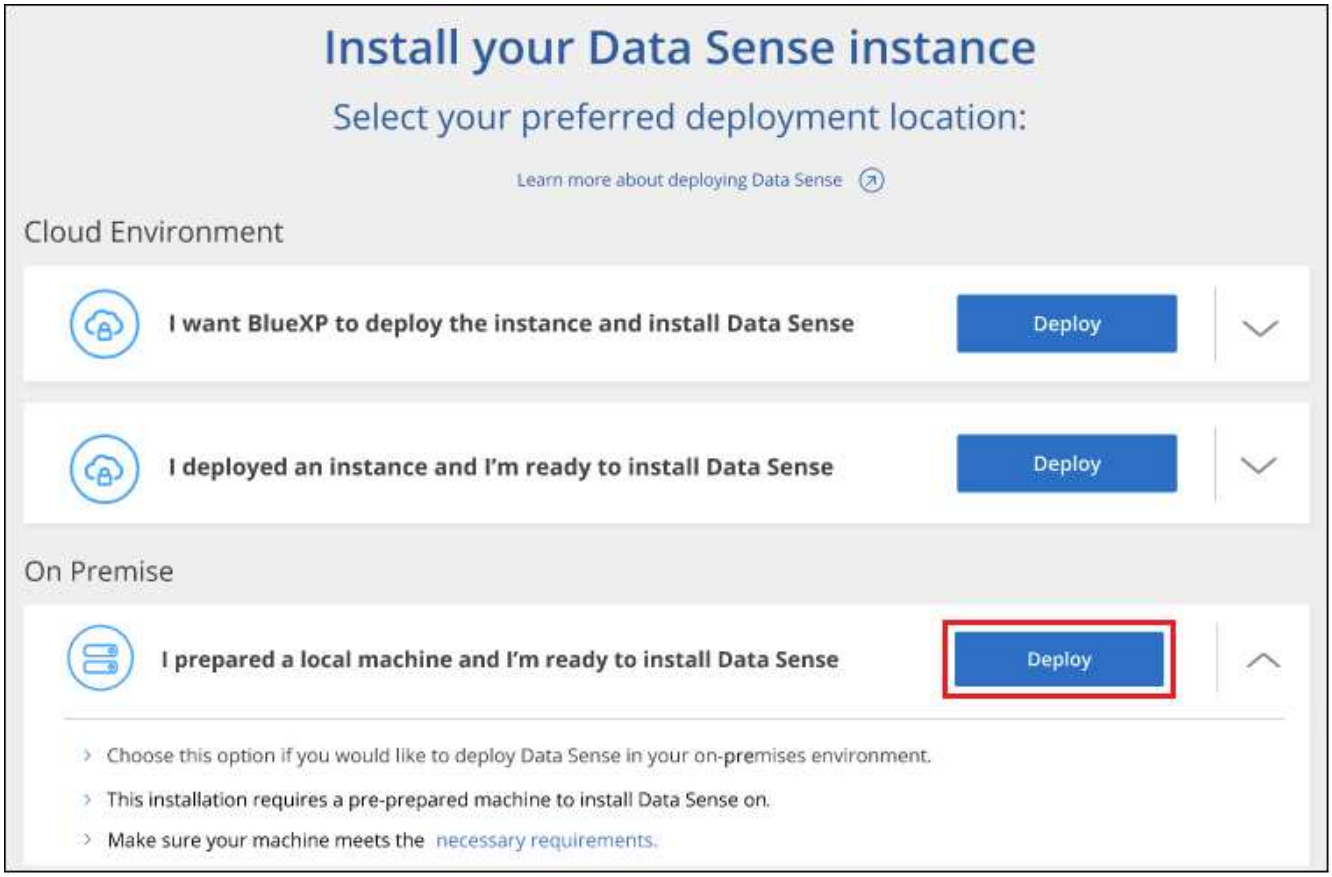
4. Entpacken Sie die Installationsdatei auf dem Host-Rechner, z. B.:

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

5. Starten Sie BlueXP, und wählen Sie **Governance > Klassifizierung**.
6. Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



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

Führen Sie vor der manuellen Installation der BlueXP -Klassifizierung auf einem Linux-Host optional ein Skript auf dem Host aus, 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 auf /opt verfügbar • 895 gib verfügbar für /var/lib/Docker • 5 gib auf /tmp • **Für Podman, 5 GB auf /tmp** • **Für Podman, 30 GB auf /var/tmp**
Groß	16 CPUs	64 GB RAM	• 500 gib SSD auf / oder 100 gib auf /opt verfügbar • 395 gib verfügbar auf /var/lib/Docker oder für Podman /var/lib/Containers oder für Podman /var/lib/Containers • 5 gib auf /tmp • **Für Podman, 5 GB auf /tmp** • **Für Podman, 30 GB auf /var/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
    - Ubuntu 22.04 (BlueXP Klassifikation ab Version 1.23 erforderlich)

        - Ubuntu 24.04 (erfordert BlueXP -Klassifizierung Version 1.23 oder höher)
    - 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, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 und 9.6.
    - Advanced Vector Extensions (AVX2) muss auf dem Hostsystem aktiviert sein.
- **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".
        - 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.
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. 9000	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. Wenn eine Firewall auf dem Linux-Host verwendet wird, ist Port 9000 für interne Prozesse innerhalb eines Ubuntu-Servers erforderlich.
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.

Bevor Sie beginnen

- 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

Übersicht über Scandatenquellen mit BlueXP -Klassifizierung

Durch die BlueXP -Klassifizierung werden die von Ihnen ausgewählten Daten in den Repositorys (Volumes, Datenbankschemas oder andere Benutzerdaten) gescannt, um personenbezogene und sensible Daten zu identifizieren. Die BlueXP -Klassifizierung bildet dann Ihre Unternehmensdaten ab, kategorisiert jede Datei und identifiziert vordefinierte Muster in den Daten. Das Ergebnis des Scans ist ein Index von persönlichen Daten, sensiblen persönlichen Daten, Datenkategorien und Dateitypen.

Nach dem ersten Scan scannt die BlueXP -Klassifizierung Ihre Daten fortlaufend und nach dem Round Robin-Verfahren, um inkrementelle Änderungen zu erkennen. Aus diesem Grund ist es wichtig, dass die Instanz weiterhin ausgeführt wird.

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

Was ist der Unterschied zwischen Mapping und Classification Scans

Sie können zwei Arten von Scans in der BlueXP -Klassifizierung durchführen:

- **Nur Mapping-Scans** bieten nur einen allgemeinen Überblick über Ihre Daten und werden an ausgewählten Datenquellen durchgeführt. Nur-Mapping-Scans benötigen weniger Zeit als Map und klassifizieren Scans, da die nicht auf Dateien zugreifen, um die Daten darin zu sehen. Sie sollten dies zunächst tun, um Forschungsbereiche zu identifizieren und dann einen Map & Classify-Scan für diese Bereiche durchzuführen.
- **Map & Classify Scans** ermöglichen ein tiefes Scannen Ihrer Daten.

In der folgenden Tabelle sind einige Unterschiede aufgeführt:

Merkmal	Scans zuordnen und klassifizieren	Nur-Mapping-Scans
Scangeschgeschwindigkeit	Langsam	Schnell
Preisgestaltung	Kostenlos	Kostenlos
Kapazität	Begrenzt auf 500 TiB*	Begrenzt auf 500 TiB*
Liste der Dateitypen und der genutzten Kapazität	Ja.	Ja.
Anzahl der Dateien und genutzte Kapazität	Ja.	Ja.
Alter und Größe der Dateien	Ja.	Ja.
Fähigkeit, eine auszuführen "Datenzuordnungsbericht"	Ja.	Ja.
Datenuntersuchung, um Dateidetails anzuzeigen	Ja.	Nein
Suche nach Namen in Dateien	Ja.	Nein

Merkmal	Scans zuordnen und klassifizieren	Nur-Mapping-Scans
Erstellen"Gespeicherte Suchvorgänge", die benutzerdefinierte Suchergebnisse liefern	Ja.	Nein
Möglichkeit zur Ausführung anderer Berichte	Ja.	Nein
Fähigkeit, Metadaten aus Dateien zu sehen*	Nein	Ja.

{Sternchen} include::_include/connector-limit.adoc[]

*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 gespeicherte Suchen	Ja.	Nein
Standardmäßig gespeicherte Suchen	Ja.	Ja.
DDA-Bericht	Ja.	Ja.
Zuordnungsbericht	Ja.	Ja.
Erkennung des Empfindlichkeitsniveaus	Ja.	Nein
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 in der Compliance-Konsole:

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

Unterschiede bei den Untersuchungsfiltern:

Merkmal	Zuordnen Und Klassifizieren	Karte
Gespeicherte Suchvorgänge	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
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 nur-Mapping-Scans kann die BlueXP -Klassifizierung zwischen 100-150 TIBS Daten pro Tag scannen.
- Bei der Durchführung von Map & Classify Scans kann die BlueXP -Klassifizierung zwischen 15-40 TIBS Daten pro Tag scannen.

Scannen Sie Azure NetApp Files Volumes mit BlueXP -Klassifizierung

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

Ermitteln Sie das Azure NetApp Files-System, 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.

Ermöglichen Sie die 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**.
2. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.

3. 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, wählen Sie **Alle Volumes zuordnen**.
   - Um alle Volumes zuzuordnen und zu klassifizieren, wählen Sie **Alle Volumes zuordnen und klassifizieren**.

- Um die Scanvorgänge für jedes Volume anzupassen, wählen Sie **oder wählen Sie den Scantyp für jedes Volume** aus, und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

  Weitere Informationen finden Sie unter Aktivieren und deaktivieren Sie Compliance-Scans auf Volumes .

4. Wählen Sie im Bestätigungsdialogfeld **approve** aus, damit die BlueXP -Klassifikation 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. Sie können den Fortschritt der ersten Messung verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die Konfiguration **Arbeitsumgebung** auswählen. Der Fortschritt jeder Messung wird als Fortschrittsbalken angezeigt. Sie können auch den Mauszeiger über die Fortschrittsleiste bewegen, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen.

- 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".

Vergewissern Sie sich, dass die BlueXP -Klassifizierung Zugriff auf Volumes hat

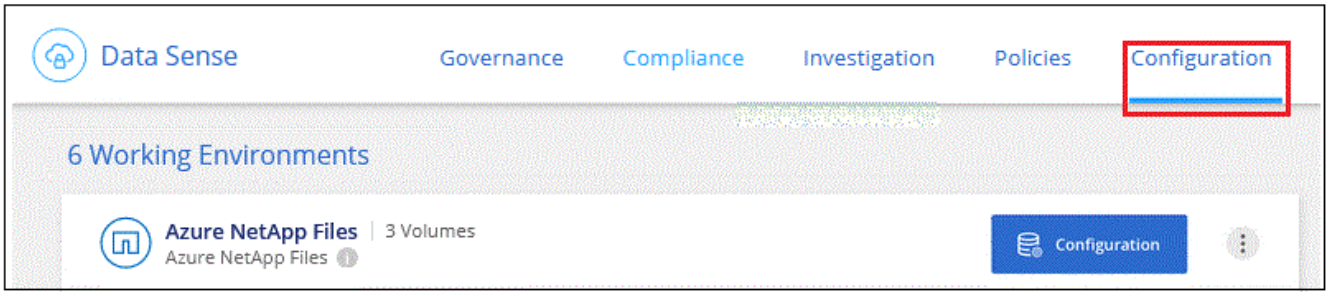
Vergewissern Sie sich, dass die BlueXP Klassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen und Exportrichtlinien prüfen. Sie müssen BlueXP mit CIFS-Anmeldedaten klassifizieren, um auf CIFS Volumes zugreifen zu können.

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

Schritte

1. Stellen Sie sicher, dass eine Netzwerkverbindung zwischen der BlueXP Klassifizierungsinstanz und jedem Netzwerk, das Volumes für Azure NetApp Files umfasst, besteht.
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. Wählen Sie im linken Navigationsmenü von BlueXP **Governance > Klassifizierung**.
5. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.

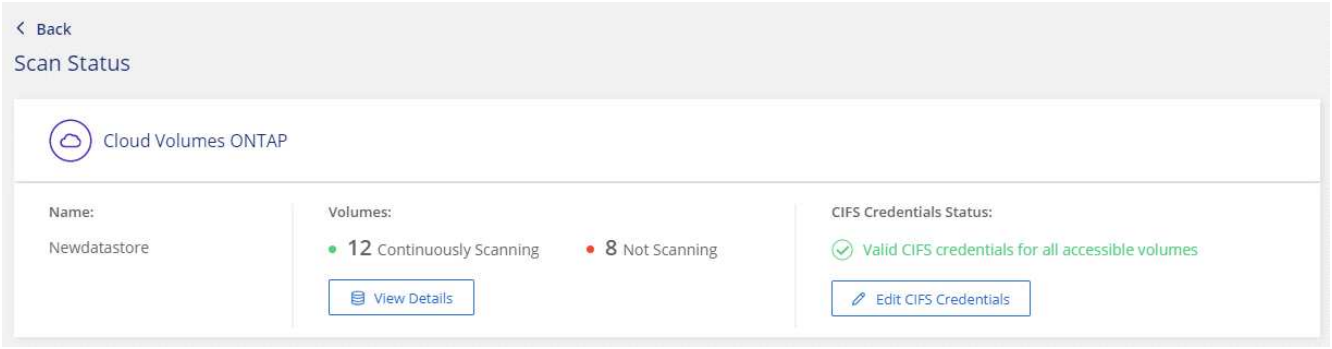


   a. Wählen Sie für jede Arbeitsumgebung **Edit CIFS Credentials** aus und geben Sie den Benutzernamen und das Passwort ein, den die BlueXP -Klassifizierung für den Zugriff auf CIFS-Volumes auf dem System benötigt.

      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.

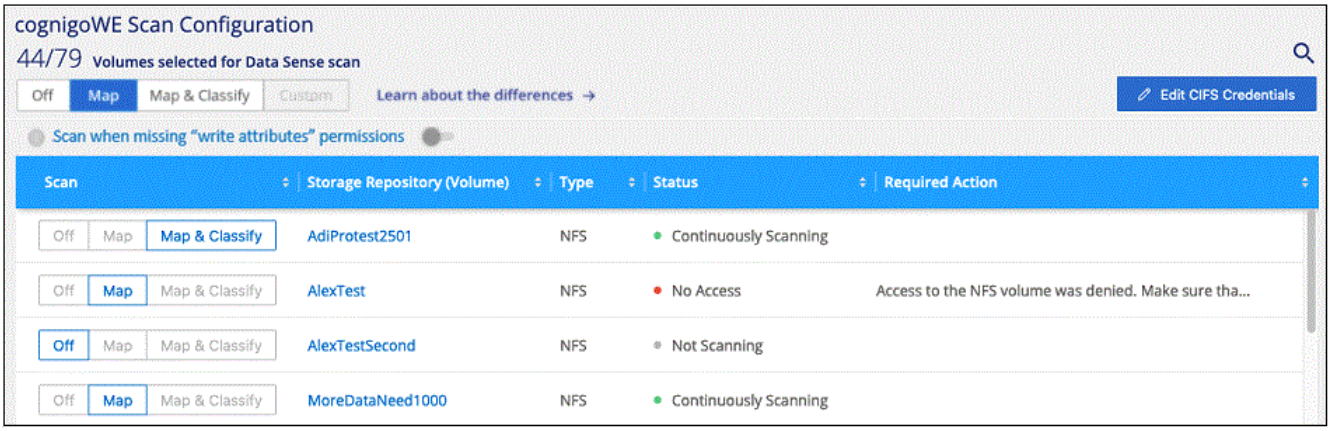
      Um sicherzustellen, dass die Zugriffszeiten Ihrer Dateien durch BlueXP classification Klassifizierungsscans unverändert bleiben, empfiehlt es sich, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

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



6. Wählen Sie auf der Konfigurationsseite **View Details** aus, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und etwaige Fehler zu korrigieren.

   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.

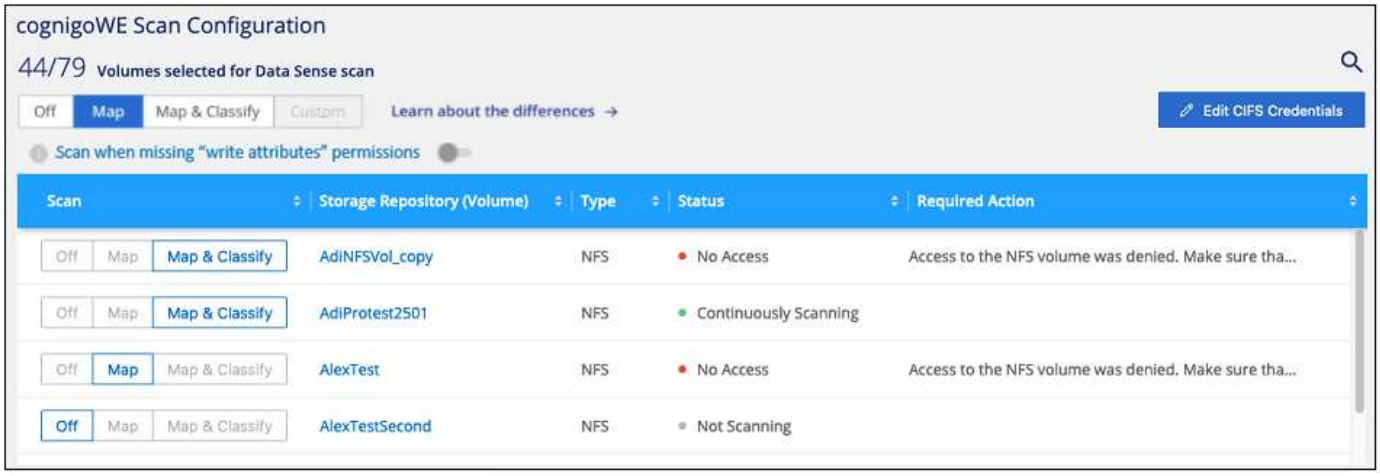


Aktivieren und deaktivieren Sie Compliance-Scans auf Volumes

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.

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.

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 .".



Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Führen Sie einen der folgenden Schritte aus:
   - Um nur-Mapping-Scans auf einem Volume zu aktivieren, wählen Sie im Volume-Bereich **Map**. Um auf

allen Volumes zu aktivieren, wählen Sie im Überschriftenbereich **Karte**.

- Um das vollständige Scannen auf einem Volume zu aktivieren, wählen Sie im Volumenbereich **Zuordnen & Klassifizieren**. Um auf allen Volumes zu aktivieren, wählen Sie im Überschriftenbereich **Map & Classify**.
- Um das Scannen auf einem Volume zu deaktivieren, wählen Sie im Lautstärkebereich **aus**. Um das Scannen auf allen Volumes zu deaktivieren, wählen Sie im Überschriftenbereich **aus**.

Scannen Sie Amazon FSX nach ONTAP Volumes mit BlueXP -Klassifizierung

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)"

- 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.

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.

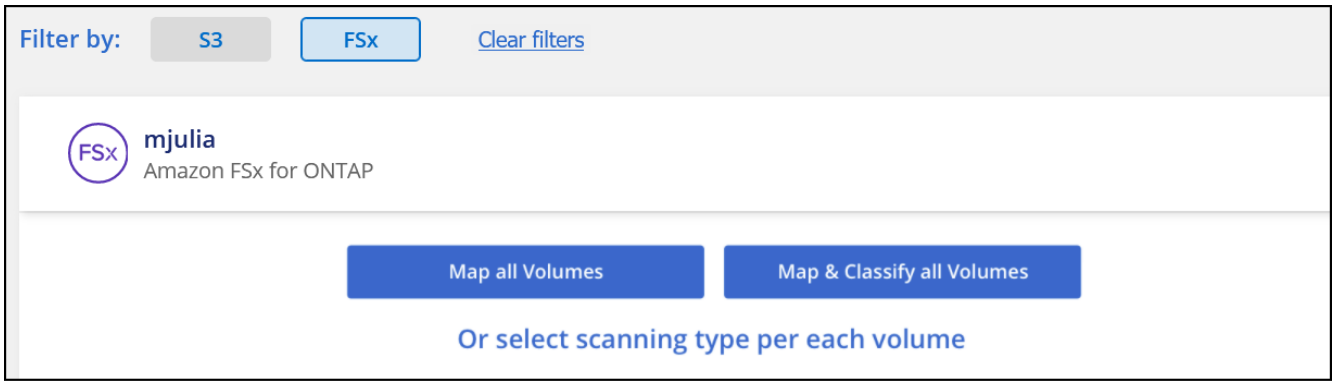
Hinweis: die Implementierung der BlueXP Klassifizierung an einem lokalen Standort wird derzeit beim Scannen von FSX Volumes nicht unterstützt.

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

Ermöglichen Sie die BlueXP -Klassifizierung in Ihren Arbeitsumgebungen

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

1. Wählen Sie im linken Navigationsmenü von BlueXP **Governance > Klassifizierung**.
2. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.



3. 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.
4. 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. Sie können den Fortschritt der ersten Messung verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die Konfiguration **Arbeitsumgebung** auswählen. Der Fortschritt jeder Messung wird als Fortschrittsbalken angezeigt. Sie können auch den Mauszeiger über die Fortschrittsleiste bewegen, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen.

- 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".

Vergewissern Sie sich, dass die BlueXP -Klassifizierung Zugriff auf Volumes hat

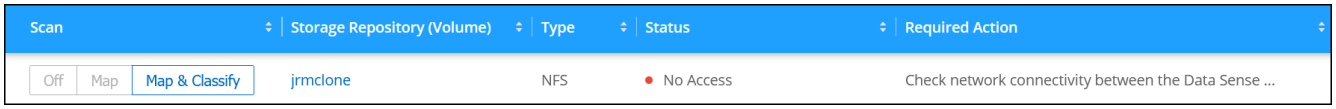
Sorgen Sie dafür, dass die BlueXP Klassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen und Exportrichtlinien prüfen.

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

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie auf der Konfigurationsseite **Details anzeigen** aus, um den Status zu überprüfen und etwaige Fehler zu korrigieren.

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



3. 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.

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. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
   b. Wählen Sie für jede Arbeitsumgebung **Edit CIFS Credentials** aus und geben Sie den Benutzernamen und das Passwort ein, den 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.

      Um sicherzustellen, dass die Zugriffszeiten Ihrer Dateien durch BlueXP classification Klassifizierungsscans unverändert bleiben, empfiehlt es sich, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

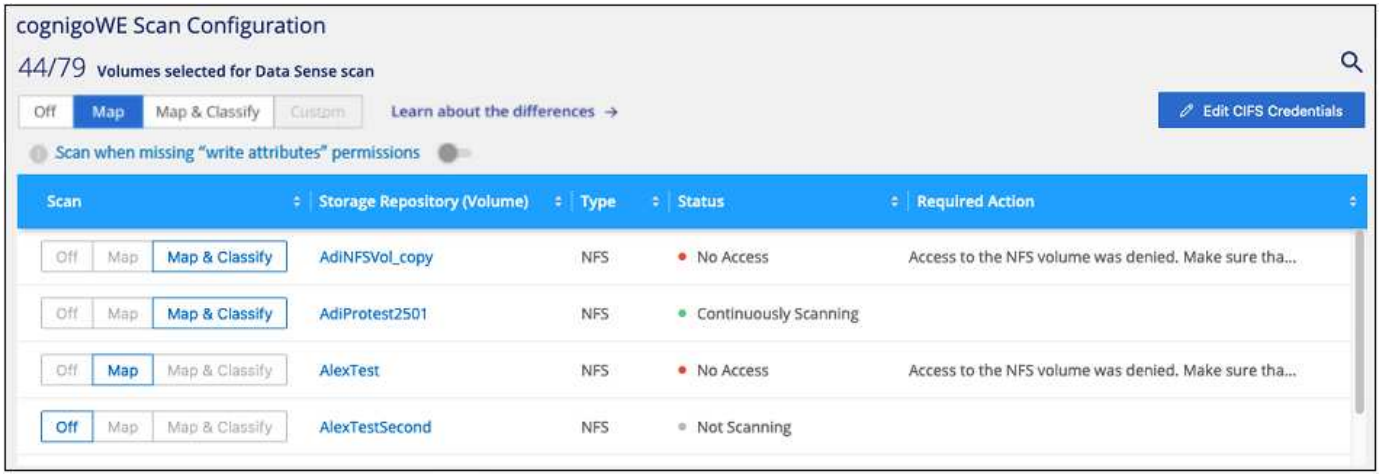
   Nach Eingabe der Anmeldedaten sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.

Aktivieren und deaktivieren Sie 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 .".



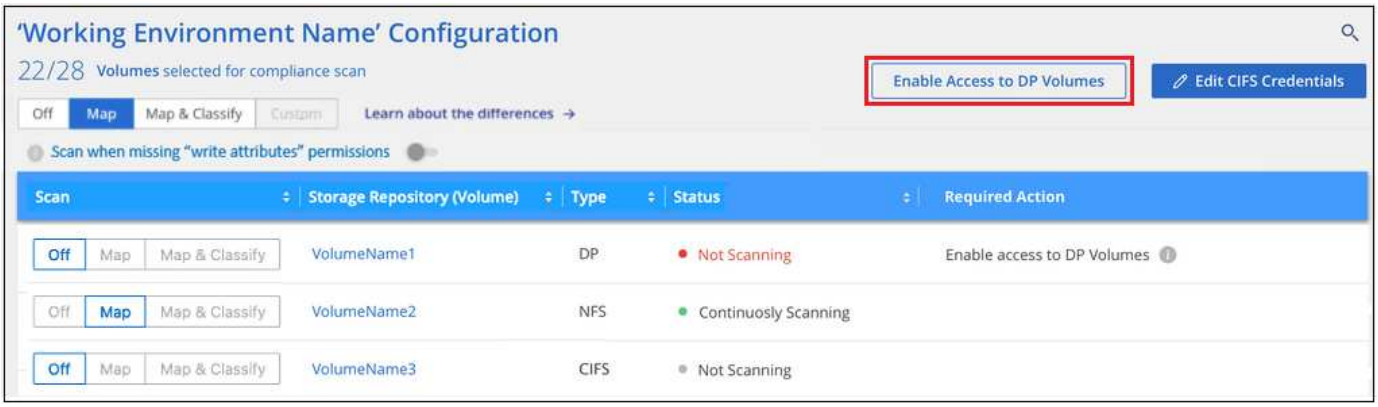
1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Suchen Sie auf der Seite Konfiguration die Arbeitsumgebung mit den Volumes, die Sie scannen möchten.
3. Führen Sie einen der folgenden Schritte aus:
   - Um nur-Mapping-Scans auf einem Volume zu aktivieren, wählen Sie im Volume-Bereich **Map**. Oder, um auf allen Volumes zu aktivieren, wählen Sie im Überschriftenbereich **Karte**. Um das vollständige Scannen auf einem Volume zu aktivieren, wählen Sie im Volumenbereich **Zuordnen & Klassifizieren**. Oder, um auf allen Volumes zu aktivieren, wählen Sie im Überschriftenbereich **Map & Classify**.
   - Um das Scannen auf einem Volume zu deaktivieren, wählen Sie im Lautstärkebereich **aus**. Um das Scannen auf allen Volumes zu deaktivieren, wählen Sie im Überschriftenbereich **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 Sie Datensicherungsvolumes

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.

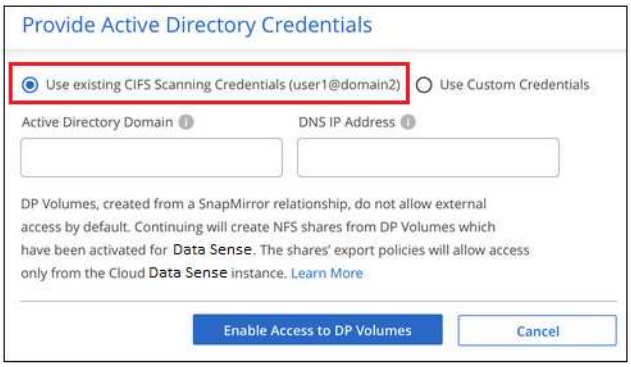
Zunächst erkennt die Volume-Liste diese Volumes als *Type* **DP** mit dem *Status* **Not Scanning** und der *required Action* **Enable Access to DP Volumes**.

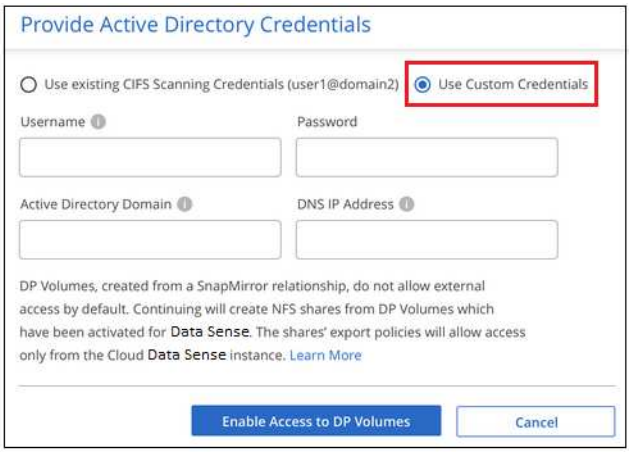


Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie **Zugriff auf DP-Volumes aktivieren** oben auf der Seite aus.
3. Überprüfen Sie die Bestätigungsmeldung und wählen Sie erneut **Zugriff auf DP-Volumes aktivieren**.
   - 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.





4. Aktivieren Sie jedes DP-Volume, das Sie scannen möchten.

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.

Wenn Sie keine CIFS Data Protection Volumes hatten, als Sie den Zugriff auf DP-Volumes aktiviert haben, und später einige hinzufügen, wird oben auf der Konfigurationsseite die Schaltfläche **Enable Access to CIFS DP** angezeigt. Wählen Sie diese Schaltfläche aus, und fügen Sie CIFS-Anmeldeinformationen hinzu, um den Zugriff auf diese CIFS-DP-Volumes zu aktivieren.

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

Scannen Sie Cloud Volumes ONTAP und lokale ONTAP Volumes mit BlueXP - Klassifizierung

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

Voraussetzungen

Bevor Sie die BlueXP -Klassifizierung aktivieren, stellen Sie sicher, dass eine unterstützte Konfiguration vorhanden ist.

- Wenn Sie Scannen Cloud Volumes ONTAP und On-Premises ONTAP-Systeme, die über das Internet zugänglich sind, können Sie "Implementieren Sie die BlueXP Klassifizierung in der Cloud"oder "In einer Anlage mit Internetzugang".
- Wenn Sie On-Premises ONTAP-Systeme scannen, die in einer dunklen Seite installiert wurden, die keinen Internetzugang hat, müssen Sie "Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

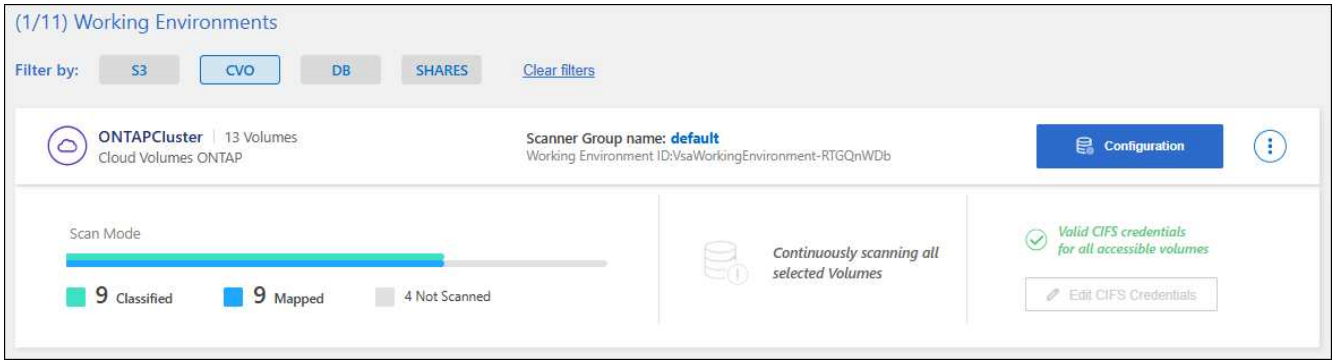
Ermöglichen Sie das Scannen der BlueXP -Klassifizierung in Ihren Arbeitsumgebungen

Sie können das Scannen der BlueXP -Klassifizierung auf Cloud Volumes ONTAP Systemen bei jedem unterstützten Cloud-Provider oder in lokalen ONTAP Clustern aktivieren.

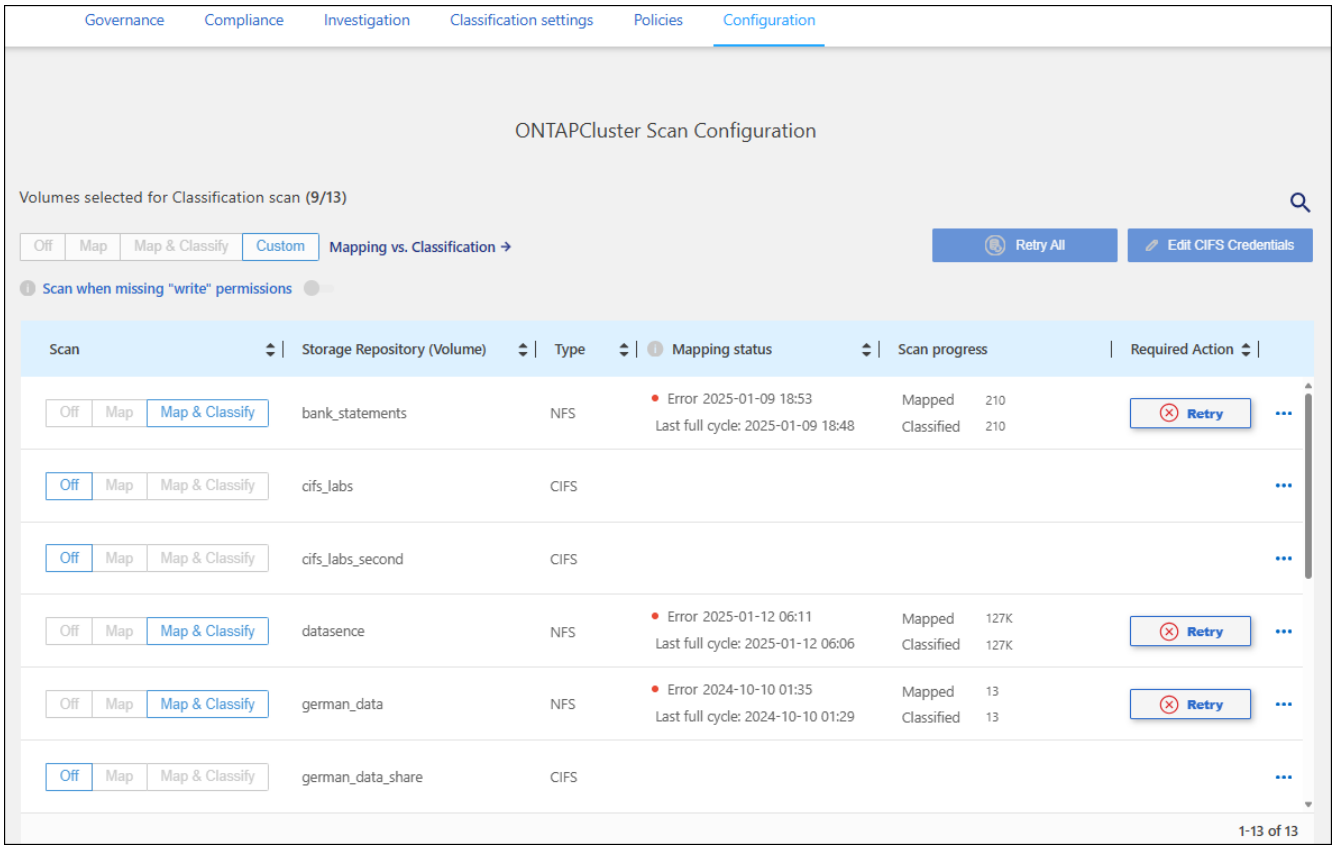
Schritte

1. Wählen Sie im linken Navigationsmenü von BlueXP **Governance > Klassifizierung**.
2. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.

   Auf der Seite Konfiguration werden mehrere Arbeitsumgebungen angezeigt.



3. Wählen Sie eine Arbeitsumgebung aus und wählen Sie **Konfiguration**.



4. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter **Scan bei fehlenden "Schreibattributen"-Berechtigungen** EIN und alle Dateien werden unabhängig von den Berechtigungen gescannt.

   Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributberechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dass das System die Dateien nicht klassifizieren wird, weil die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. "Weitere Informationen .".

5. 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, wählen Sie **Map**.
   - Um alle Volumes zuzuordnen und zu klassifizieren, wählen Sie **Map & Classify**.
   - Um die Scanvorgänge für jedes Volume anzupassen, wählen Sie **Custom** aus, und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.
6. Wählen Sie im Bestätigungsdialogfeld **approve** aus, damit die BlueXP -Klassifikation mit dem Scannen Ihrer Volumes beginnt.

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen in der Arbeitsumgebung ausgewählten Volumes. Die Ergebnisse werden im Compliance-Dashboard angezeigt, sobald die BlueXP -Klassifizierung den Scan startet. Die benötigte Zeit hängt von der Datenmenge ab – sie kann einige Minuten oder Stunden dauern.

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".

Vergewissern Sie sich, dass 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

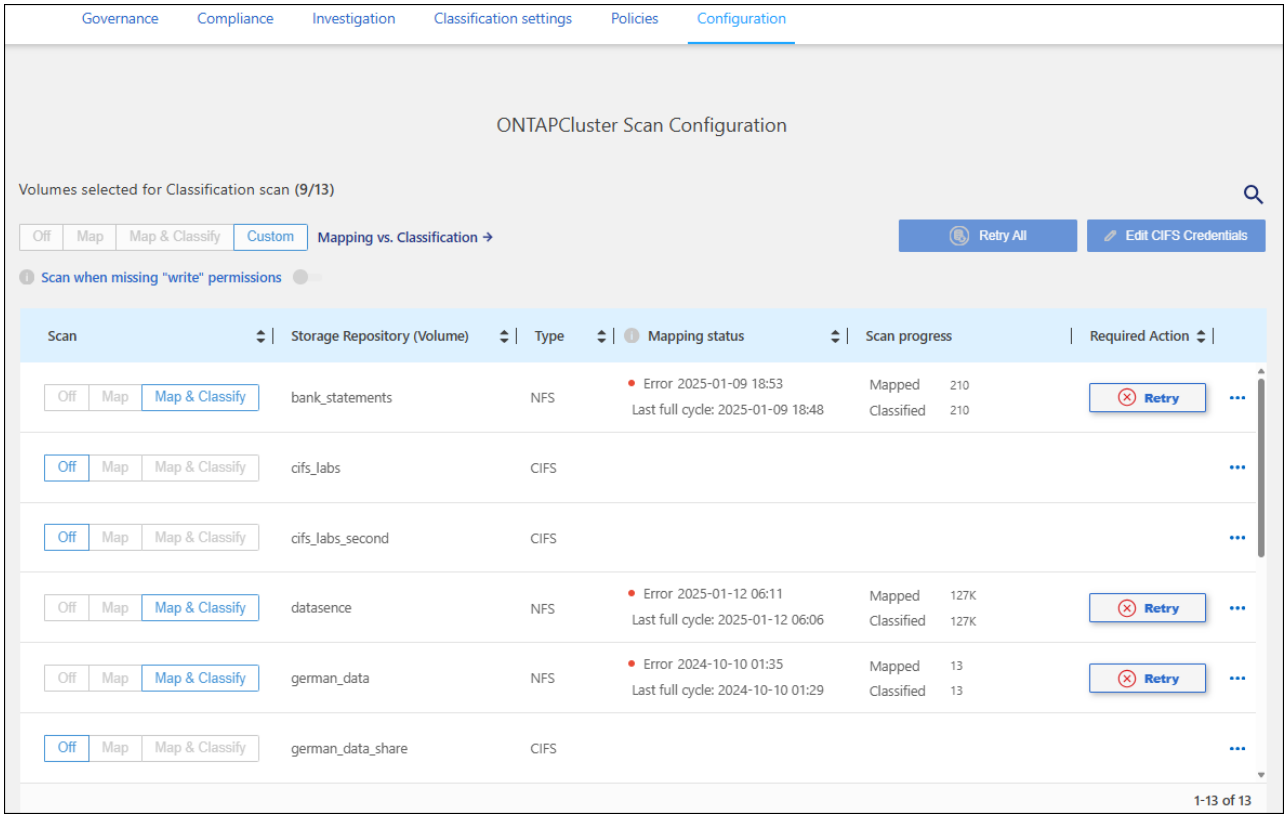
1. Stellen Sie sicher, dass eine Netzwerkverbindung zwischen der BlueXP Klassifizierungsinstanz und jedem Netzwerk, das Volumes für Cloud Volumes ONTAP- oder lokale ONTAP-Cluster umfasst, besteht.
2. Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr von der 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. 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. Wählen Sie im linken Navigationsmenü von BlueXP **Governance > Klassifizierung**.

   b. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.



c. Wählen Sie für jede Arbeitsumgebung **Edit CIFS Credentials** aus und geben Sie den Benutzernamen und das Passwort ein, den 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.

   Um sicherzustellen, dass die Zugriffszeiten Ihrer Dateien durch BlueXP classification Klassifizierungsscans unverändert bleiben, empfiehlt es sich, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

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

5. Wählen Sie auf der Konfigurationsseite **Konfiguration** aus, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und eventuelle Fehler zu korrigieren.

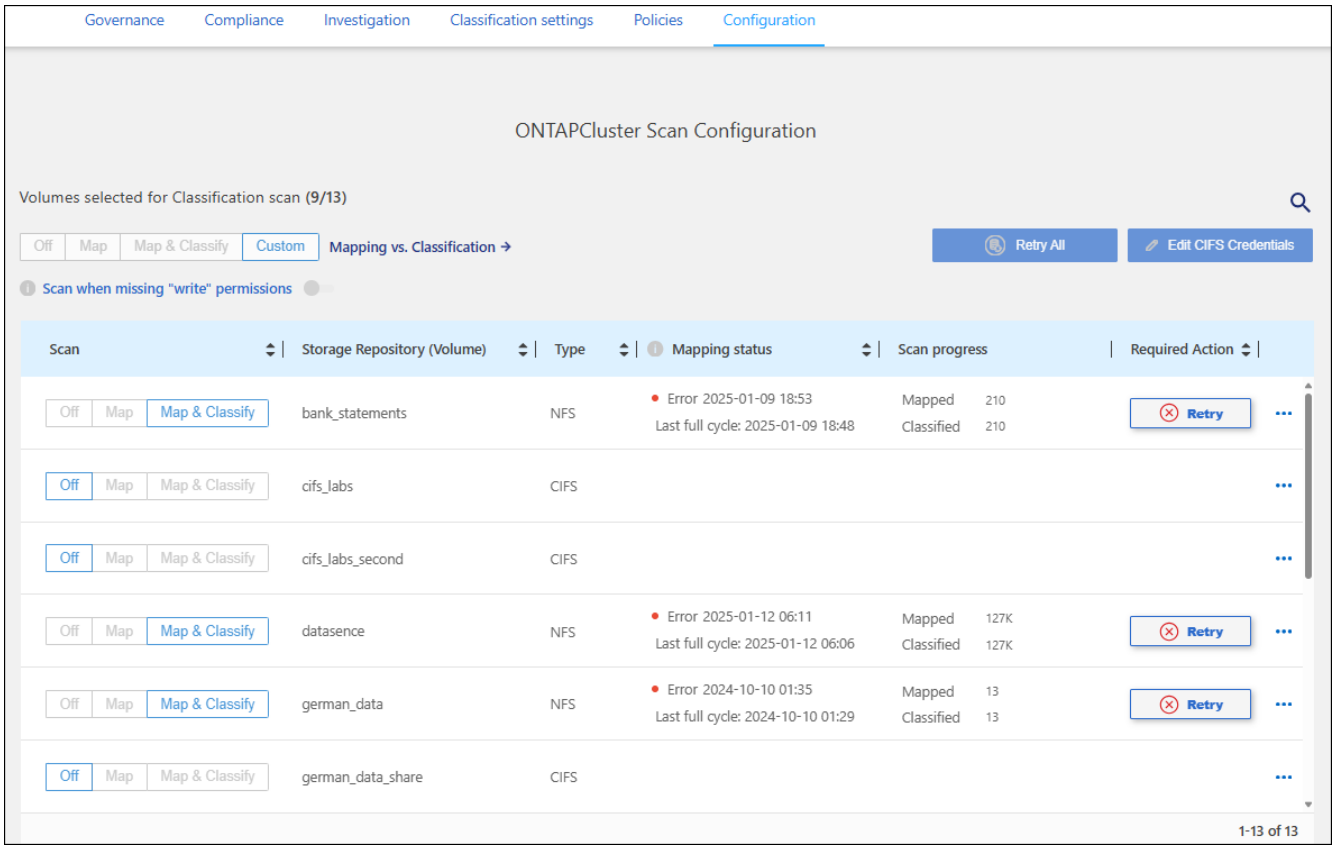
Deaktivieren Sie Compliance-Scans auf Volumes

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.

Neue Volumen, die der Arbeitsumgebung hinzugefügt wurden, werden automatisch nur gescannt, wenn Sie die Einstellung **Karte** oder **Karte & Klassieren** im Steuerkursbereich festgelegt haben. Wenn die Option im Überschriftenbereich auf **Custom** oder **Off** eingestellt ist, müssen Sie die Zuordnung und/oder das vollständige Scannen jedes neuen Volumens aktivieren, das Sie in der Arbeitsumgebung hinzufügen.

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie die Schaltfläche **Konfiguration** für die Arbeitsumgebung, die Sie ändern möchten.



3. Führen Sie einen der folgenden Schritte aus:
   - Um das Scannen auf einem Volume zu deaktivieren, wählen Sie im Lautstärkebereich **aus**.
   - Um das Scannen auf allen Volumes zu deaktivieren, wählen Sie im Überschriftenbereich **aus**.

Datenbankschemas mit BlueXP -Klassifizierung scannen

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

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.

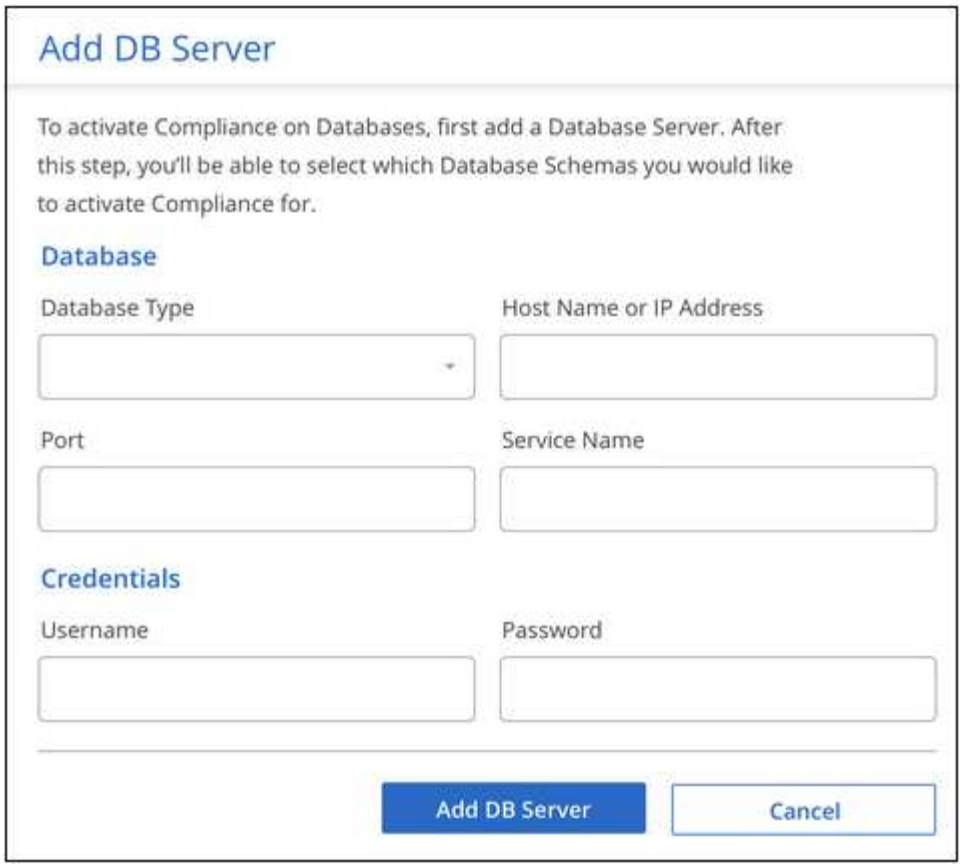
Wenn Sie Datenbankschemas scannen, die über das Internet zugänglich sind, können Sie dies tun "Implementieren Sie die BlueXP Klassifizierung in der Cloud" Oder "Implementieren Sie die BlueXP Klassifizierung an einem lokalen Standort mit Internetzugang".

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.

Fügen Sie den Datenbankserver hinzu

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

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie auf der Konfigurationsseite **Arbeitsumgebung hinzufügen** > **Datenbankserver hinzufügen**.
3. 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.

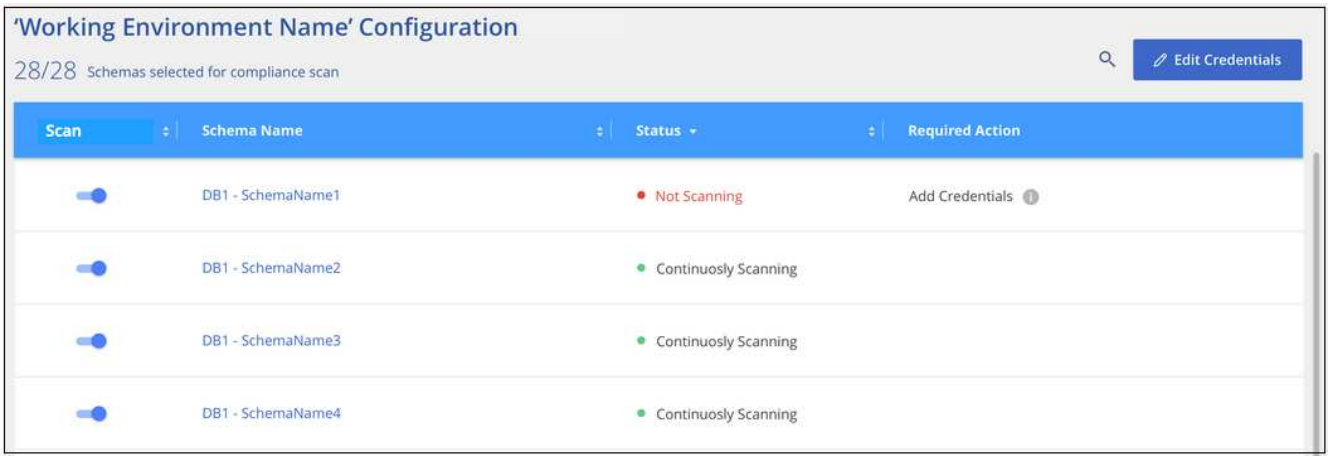
Aktivieren und deaktivieren Sie Compliance-Scans für Datenbankschemas

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

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

1. Wählen Sie auf der Konfigurationsseite die Schaltfläche **Konfiguration** für die Datenbank, die Sie konfigurieren möchten.

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. Sie können den Fortschritt der ersten Messung verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die Konfiguration **Arbeitsumgebung** auswählen. Der Fortschritt jeder Messung wird als Fortschrittsbalken angezeigt. Sie können auch den Mauszeiger über die Fortschrittsleiste bewegen, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen. 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 kontinuierlich gescannt.

Scannen Sie Dateifreigaben mit BlueXP -Klassifizierung

Um Dateifreigaben zu scannen, müssen Sie zunächst eine Dateifreigabegruppe in der BlueXP classification erstellen. Dateifreigabegruppen sind für NFS- oder CIFS-Freigaben (SMB) vorgesehen, die vor Ort oder in der Cloud gehostet werden.

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

Voraussetzungen

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.
  - Die BlueXP classification kann keine Berechtigungen oder die „letzte Zugriffszeit“ aus 7-Mode-Systemen extrahieren.
  - Aufgrund eines bekannten Problems zwischen einigen Linux-Versionen und CIFS-Freigaben auf 7-Mode-Systemen müssen Sie die Freigabe so konfigurieren, dass nur SMBv1 mit aktivierter NTLM-Authentifizierung verwendet wird.
- Zwischen der BlueXP Klassifizierungsinstanz und den Freigaben muss eine Netzwerkverbindung bestehen.
- Sie können eine DFS-Freigabe (Distributed File System) als reguläre CIFS-Freigabe hinzufügen. Da die

BlueXP classification nicht erkennt, dass die Freigabe auf mehreren Servern/Volumes basiert, die zu einer einzigen CIFS-Freigabe zusammengefasst sind, erhalten Sie möglicherweise Berechtigungs- oder Verbindungsfehler bezüglich der Freigabe, obwohl die Meldung tatsächlich nur für einen der Ordner/Freigaben gilt, der sich auf einem anderen Server/Volume befindet.

- 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.

  Um sicherzustellen, dass die Zugriffszeiten Ihrer Dateien durch BlueXP classification Klassifizierungsscans unverändert bleiben, empfiehlt es sich, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

- Alle CIFS-Dateifreigaben in einer Gruppe müssen dieselben Active Directory-Anmeldeinformationen verwenden.
- Sie können NFS- und CIFS-Freigaben (mit Kerberos oder NTLM) kombinieren. Sie müssen die Freigaben separat zur Gruppe hinzufügen. Das heißt, Sie müssen den Vorgang zweimal durchführen – einmal pro Protokoll.
  - Sie können keine Dateifreigabegruppe erstellen, die CIFS-Authentifizierungstypen (Kerberos und NTLM) mischt.
- Wenn Sie CIFS mit Kerberos-Authentifizierung verwenden, stellen Sie sicher, dass die angegebene IP-Adresse für den BlueXP classification zugänglich ist. Die Dateifreigaben können nicht hinzugefügt werden, wenn die IP-Adresse nicht erreichbar ist.

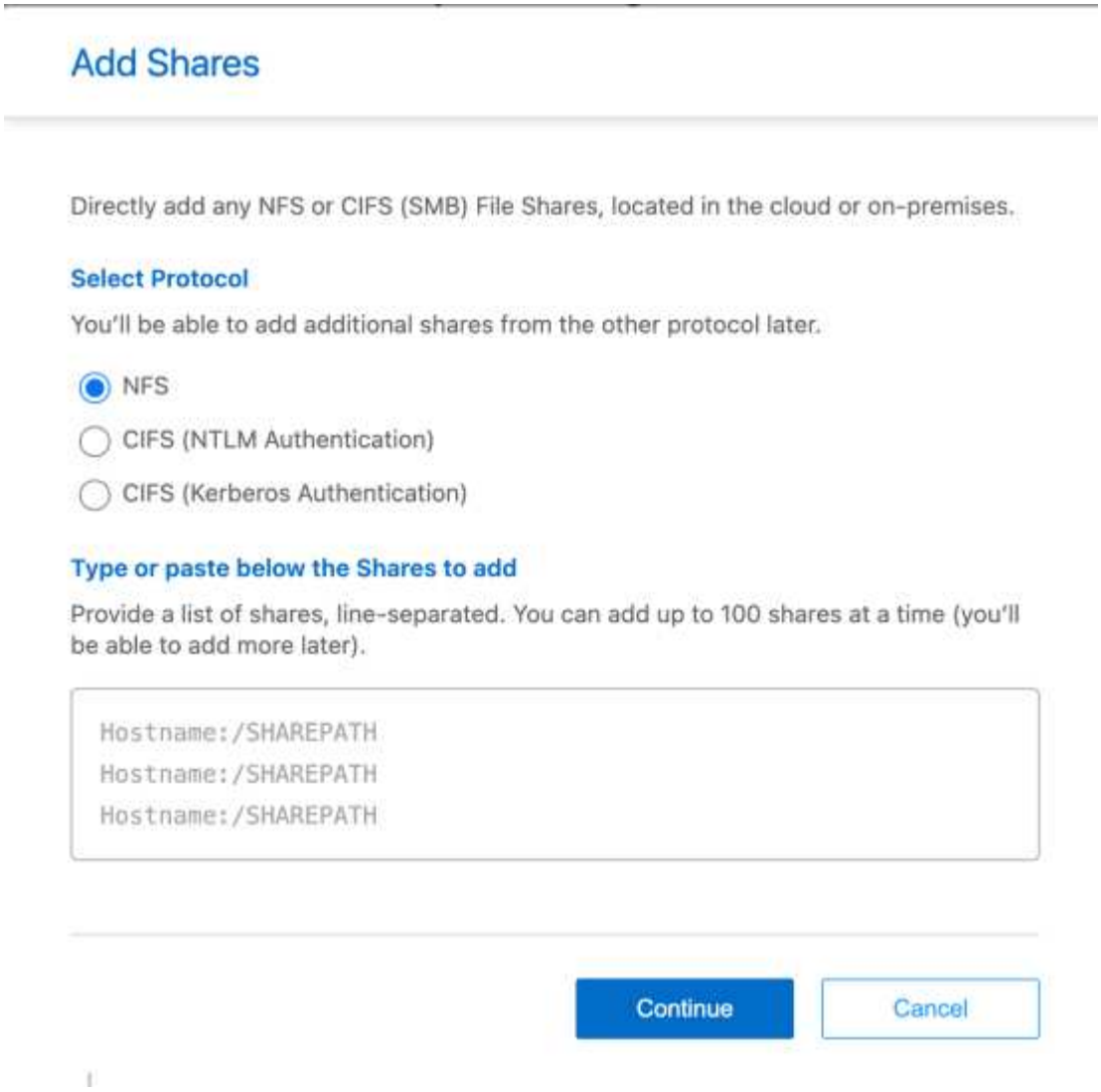
Erstellen einer Dateifreigabegruppe

Wenn Sie Dateifreigaben zur Gruppe hinzufügen, müssen Sie das Format verwenden `<host_name>:/<share_path>` .

+ Sie können Dateifreigaben einzeln hinzufügen oder eine zeilengetrennte Liste der Dateifreigaben eingeben, die Sie scannen möchten. Sie können bis zu 100 Shares gleichzeitig hinzufügen.

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie auf der Konfigurationsseite **Arbeitsumgebung hinzufügen** > **Gruppe mit Dateifreigaben hinzufügen**.
3. Geben Sie im Dialogfeld „Dateifreigabegruppe hinzufügen“ den Namen für die Freigabegruppe ein und wählen Sie dann **Weiter** aus.
4. Wählen Sie das Protokoll für die Dateifreigaben aus, die Sie hinzufügen möchten.



Wenn Sie CIFS-Freigaben mit NTLM-Authentifizierung hinzufügen, geben Sie die Active Directory-Anmeldeinformationen ein, um auf die CIFS-Volumes zuzugreifen. Obwohl schreibgeschützte Anmeldeinformationen unterstützt werden, wird empfohlen, Vollzugriff mit Administratoranmeldeinformationen zu gewähren. Wählen Sie Speichern.

1. Fügen Sie die zu scannenden Dateifreigaben hinzu (eine Dateifreigabe pro Zeile). Wählen Sie dann **Weiter**.
2. 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. Wenn das Problem eine Namenskonvention betrifft, können Sie die Freigabe mit einem korrigierten Namen erneut hinzufügen.

3. Konfigurieren Sie das Scannen auf dem Volume:
   - Um Mapping-only-Scans auf Dateifreigaben zu aktivieren, wählen Sie **Karte**.
   - Um vollständige Scans auf Dateifreigaben zu aktivieren, wählen Sie **Map & Classify**.
   - Um das Scannen auf Dateifreigaben zu deaktivieren, wählen Sie **aus**.

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet: Wenn die BlueXP classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, scannt das System die Dateien nicht, da die BlueXP classification den letzten Zugriffszeitpunkt nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. + Wenn Sie **Scannen bei fehlenden Schreibberechtigungen für Attribute** auf **Ein** schalten, setzt der Scan den letzten Zugriffszeitpunkt zurück und scannt alle Dateien unabhängig von den Berechtigungen. + Weitere Informationen zum letzten Zugriffszeitstempel finden Sie unter xref:./"Metadaten, die aus Datenquellen in BlueXP -Klassifizierung erfasst wurden" .

Ergebnis

Die BlueXP classification beginnt mit dem Scannen der Dateien in den von Ihnen hinzugefügten Dateifreigaben. Sie können Verfolgen Sie den Scanfortschritt und sehen Sie sich die Ergebnisse des Scans im **Dashboard** an.

Wenn der Scan für eine CIFS-Konfiguration mit Kerberos-Authentifizierung nicht erfolgreich abgeschlossen wird, überprüfen Sie die Registerkarte **Konfiguration** auf Fehler.

Bearbeiten einer Dateifreigabegruppe

Nachdem Sie eine Dateifreigabegruppe erstellt haben, können Sie das CIFS-Protokoll bearbeiten oder Dateifreigaben hinzufügen und entfernen.

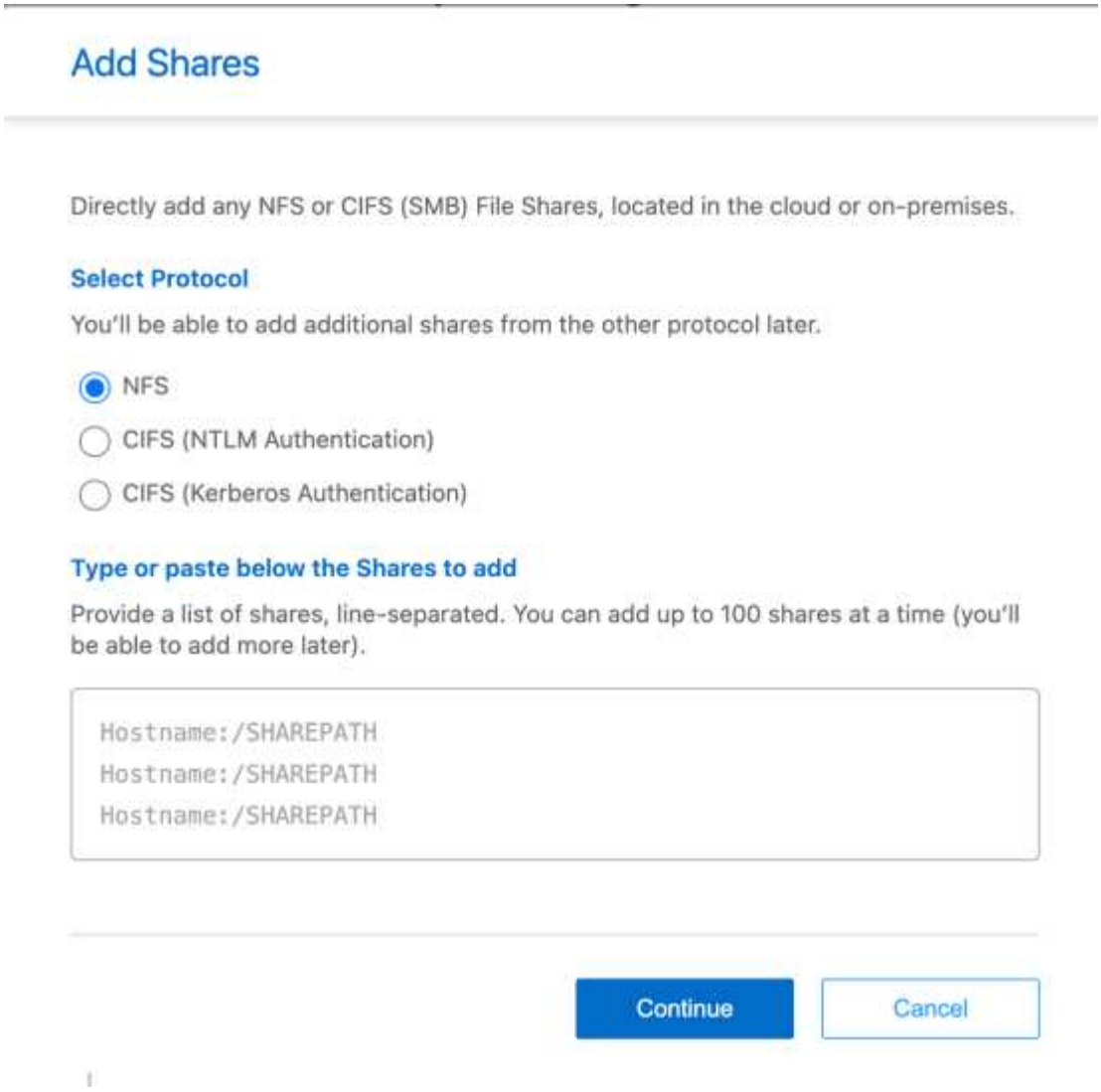
Bearbeiten Sie die CIFS-Protokollkonfiguration

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie auf der Konfigurationsseite die Dateifreigabegruppe aus, die Sie ändern möchten.
3. Wählen Sie **CIFS-Anmeldeinformationen bearbeiten**.

4. Wählen Sie die Authentifizierungsmethode: **NTLM** oder **Kerberos**.
5. Geben Sie den **Benutzernamen** und das **Passwort** des Active Directory ein.
6. Wählen Sie **Speichern**, um den Vorgang abzuschließen.

Dateifreigaben zu Compliance-Scans hinzufügen

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie auf der Konfigurationsseite die Dateifreigabegruppe aus, die Sie ändern möchten.
3. Wählen Sie **+ Freigaben hinzufügen**.
4. Wählen Sie das Protokoll für die Dateifreigaben aus, die Sie hinzufügen möchten.



Wenn Sie Dateifreigaben zu einem bereits konfigurierten Protokoll hinzufügen, sind keine Änderungen erforderlich.

Wenn Sie Dateifreigaben mit einem zweiten Protokoll hinzufügen, stellen Sie sicher, dass Sie die Authentifizierung ordnungsgemäß konfiguriert haben, wie im "Voraussetzungen" .

5. Fügen Sie die Dateifreigaben hinzu, die Sie scannen möchten (eine Dateifreigabe pro Zeile) im Format `<host_name>:/<share_path>` .
6. Wählen Sie **Weiter** aus, um das Hinzufügen der Dateifreigaben abzuschließen.

Entfernen einer Dateifreigabe aus Compliance-Scans

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie die Arbeitsumgebung aus, aus der Sie Dateifreigaben entfernen möchten.
3. Wählen Sie **Konfiguration**.
4. Wählen Sie auf der Seite Konfiguration die Aktionen für die Dateifreigabe aus ••• , die Sie entfernen möchten.
5. Wählen Sie im Menü Aktionen die Option **Freigabe entfernen**.

Verfolgen Sie den Scanfortschritt

Sie können den Fortschritt der ersten Messung verfolgen.

1. Wählen Sie das Menü **Konfiguration**.
2. Wählen Sie die **Arbeitsumgebungskonfiguration** aus.

   Der Fortschritt jeder Messung wird als Fortschrittsbalken angezeigt.

3. Bewegen Sie den Mauszeiger über die Fortschrittsleiste, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen.

Scannen Sie StorageGRID-Daten mit BlueXP -Klassifizierung

Führen Sie ein paar Schritte durch, um mit dem Scannen von Daten in StorageGRID direkt mit BlueXP -Klassifizierung zu beginnen.

StorageGRID-Anforderungen prüfen

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

- Es muss die Endpunkt-URL vorhanden sein, um eine Verbindung mit dem Objekt-Storage-Service herzustellen.
- Sie müssen über den Zugriffsschlüssel und den geheimen Schlüssel aus dem StorageGRID verfügen, damit die BlueXP -Klassifizierung auf die Buckets zugreifen kann.

Implementieren der BlueXP Klassifizierungsinstanz

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

Wenn Sie Daten von StorageGRID scannen, die über das Internet zugänglich ist, können Sie "Implementieren Sie die BlueXP Klassifizierung in der Cloud"oder "Implementieren Sie die BlueXP Klassifizierung an einem lokalen Standort mit Internetzugang".

Wenn Sie Daten von StorageGRID scannen, die in einer dunklen Seite installiert wurde, die keinen Internetzugang hat, müssen Sie "Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

Fügen Sie den StorageGRID-Service der BlueXP -Klassifizierung hinzu

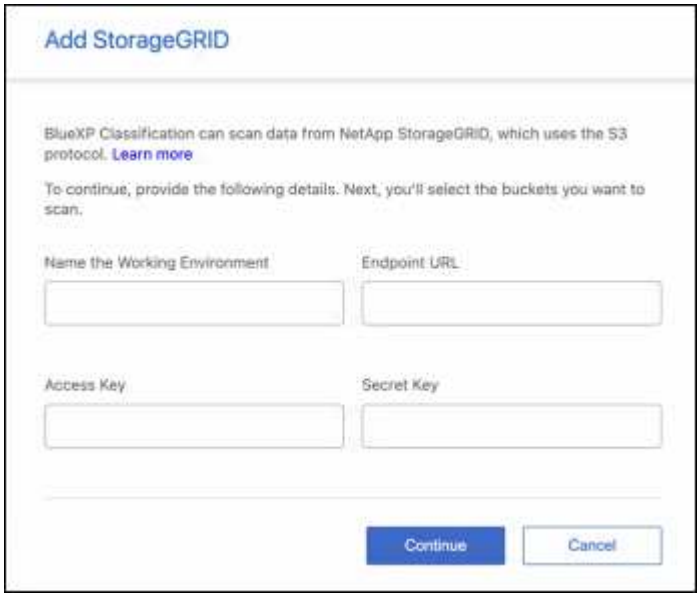
Fügen Sie den StorageGRID-Dienst hinzu.

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü die Option **Konfiguration**.
2. Wählen Sie auf der Konfigurationsseite **Arbeitsumgebung hinzufügen** > **StorageGRID hinzufügen**.
3. Geben Sie im Dialogfeld StorageGRID-Dienst hinzufügen die Details für den StorageGRID-Dienst ein und klicken Sie auf **Weiter**.
   a. Geben Sie den Namen ein, den Sie für die Arbeitsumgebung verwenden möchten. Dieser Name sollte den Namen des StorageGRID-Dienstes wiedergeben, mit dem Sie eine Verbindung herstellen.

b. Geben Sie die Endpunkt-URL ein, um auf den Objekt-Storage-Service zuzugreifen.

c. Geben Sie den Zugriffsschlüssel und den geheimen Schlüssel ein, damit die BlueXP -Klassifizierung auf die Buckets in StorageGRID zugreifen kann.



Ergebnis

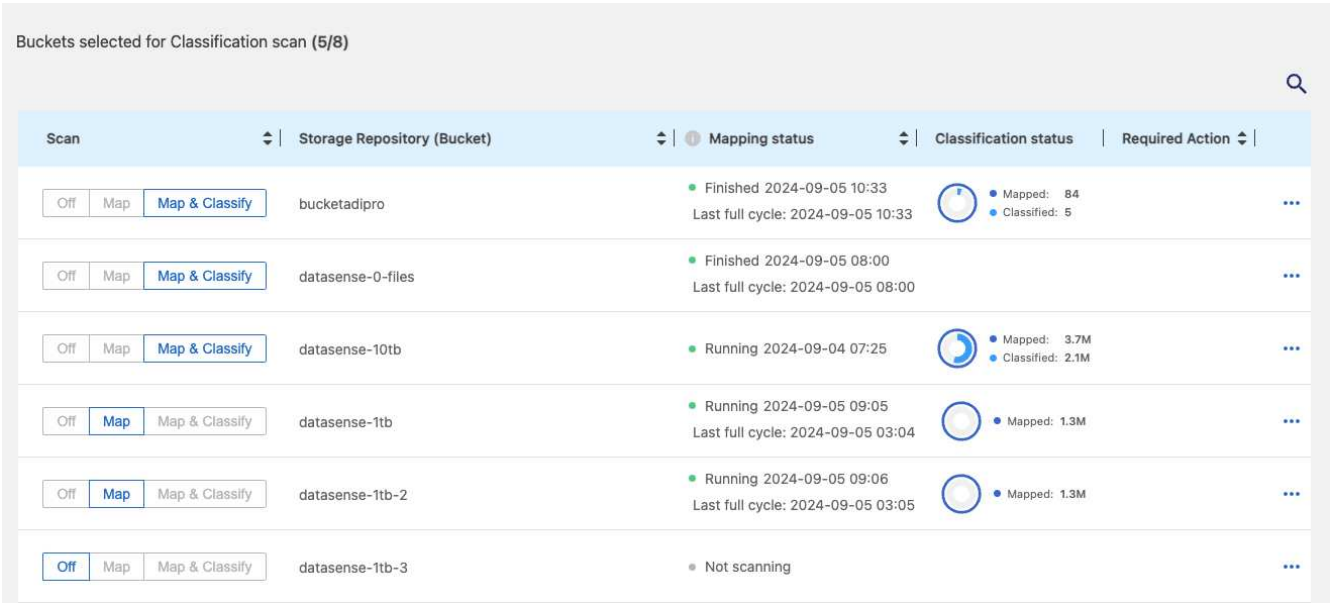
StorageGRID wird der Liste der Arbeitsumgebungen hinzugefügt.

Aktivieren und Deaktivieren von Compliance-Scans für StorageGRID Buckets

Nachdem Sie die BlueXP -Klassifizierung auf StorageGRID aktiviert haben, konfigurieren Sie die Buckets, die Sie scannen möchten. Die BlueXP Klassifizierung erkennt diese Buckets und zeigt sie in der von Ihnen erstellten Arbeitsumgebung an.

Schritte

1. Suchen Sie auf der Seite Konfiguration nach der StorageGRID-Arbeitsumgebung.
2. Wählen Sie auf der Kachel StorageGRID-Arbeitsumgebung **Konfiguration** aus.



3. Führen Sie einen der folgenden Schritte aus, um den Scanvorgang zu aktivieren oder zu deaktivieren:
    - Um nur-Mapping-Scans auf einem Bucket zu aktivieren, wählen Sie **Karte**.
    - Um vollständige Scans auf einem Bucket zu aktivieren, wählen Sie **Karte & klassifizieren**.
    - Um das Scannen auf einem Bucket zu deaktivieren, wählen Sie **aus**.

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen aktivierten Buckets. Sie können den Fortschritt der ersten Messung verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die Konfiguration **Arbeitsumgebung** auswählen. Der Fortschritt jeder Messung wird als Fortschrittsbalken angezeigt. Sie können auch den Mauszeiger über die Fortschrittsleiste bewegen, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen. Wenn Fehler auftreten, werden sie neben der erforderlichen Aktion zur Behebung des Fehlers in der Spalte Status angezeigt.

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.

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 die Ergebnisse in den Metadaten der Datei im Untersuchungsbereich anzeigen. Anstelle des Dateieigentümers, der den SID (Security Identifier) enthält, wird er mit dem tatsächlichen Benutzernamen gefüllt.

  Sie können auch weitere Details zum Dateibesitzer anzeigen: Kontoname, E-Mail-Adresse und SAM-Kontoname oder Elemente anzeigen, die diesem Benutzer gehören.

- Sie können für jede Datei und jedes Verzeichnis sehen"Volldateiberechtigungen", wenn Sie auf die Schaltfläche „Alle Berechtigungen anzeigen“ klicken.
- 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:

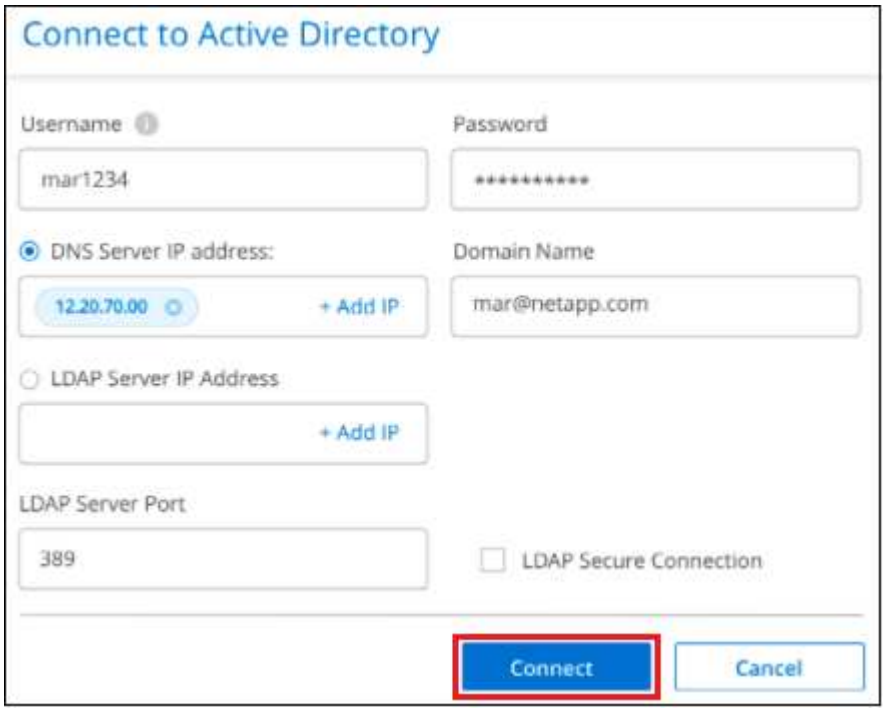
Protokoll	Port	Ziel	Zweck
TCP UND UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP über SSL
TCP	3268	Active Directory	Globaler Katalog
TCP	3269	Active Directory	Globaler Katalog über SSL

Schritte

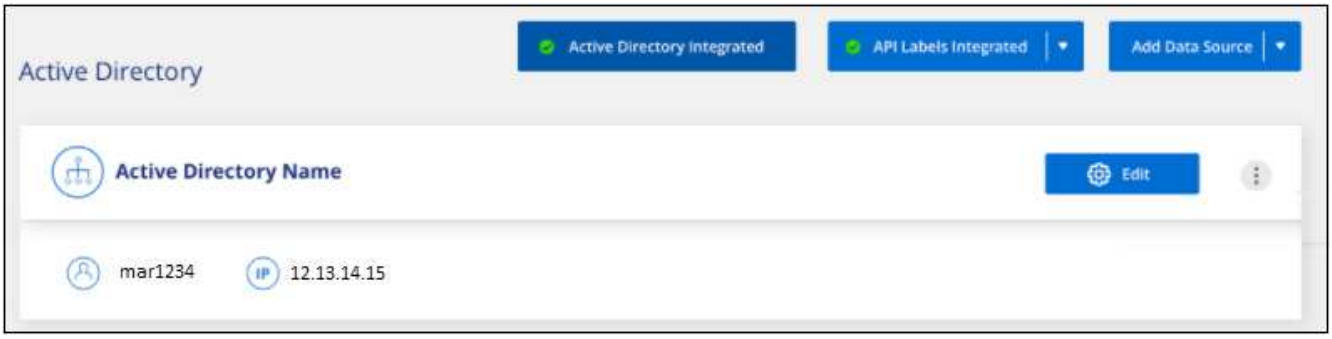
1. Klicken Sie auf der Seite BlueXP Classification Configuration auf **Add Active Directory**.

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, indem Sie auf die Schaltfläche dann **Active Directory entfernen** klicken.