



Implementieren Sie die BlueXP Klassifizierung

BlueXP classification

NetApp
April 03, 2024

Inhalt

- Implementieren Sie die BlueXP Klassifizierung 1
 - Welche BlueXP Klassifizierungs-Implementierung sollten Sie verwenden? 1
 - Implementieren Sie die BlueXP Klassifizierung in der Cloud mit BlueXP 1
 - Installieren Sie die BlueXP Klassifizierung auf einem Host mit Internetzugang 11
 - BlueXP Klassifizierung auf einem Linux-Host ohne Internetzugang installieren 31
 - Stellen Sie sicher, dass Ihr Linux Host bereit ist, die BlueXP Klassifizierung zu installieren 43

Implementieren Sie die BlueXP Klassifizierung

Welche BlueXP Klassifizierungs-Implementierung sollten Sie verwenden?

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

Die BlueXP Klassifizierung kann wie folgt implementiert werden:

- ["Implementieren Sie mit BlueXP in der Cloud"](#). BlueXP implementiert die BlueXP Klassifizierungsinstanz im selben Cloud-Provider-Netzwerk wie der BlueXP Connector.
- ["Installation auf einem Linux-Host mit Internetzugang"](#). Installieren Sie die BlueXP Klassifizierung auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud mit Internetzugang. Diese Art der Installation ist möglicherweise eine gute Option, wenn Sie lokale ONTAP Systeme mit einer BlueXP Klassifizierungsinstanz scannen möchten, die sich auch vor Ort befindet. Das ist jedoch keine Anforderung.
- ["Installation auf einem Linux-Host an einem Standort ohne Internetzugang"](#), Auch bekannt als *privater Modus*. Diese Art der Installation, die ein Installationsskript verwendet, ist gut für Ihre sicheren Seiten.

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

Siehe ["Stellen Sie sicher, dass Ihr Linux Host bereit ist, die BlueXP Klassifizierung zu installieren"](#).

Implementieren Sie die BlueXP Klassifizierung in der Cloud mit BlueXP

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

Beachten Sie, dass Sie auch können ["Installieren Sie die BlueXP Klassifizierung auf einem Linux-Host mit Internetzugang"](#). Diese Art der Installation ist möglicherweise eine gute Option, wenn Sie lokale ONTAP Systeme mit einer BlueXP Klassifizierungsinstanz scannen möchten, die sich auch vor Ort befindet. Das ist jedoch keine Anforderung. Die Software funktioniert unabhängig von der gewählten Installationsmethode genau auf die gleiche Weise.

Schnellstart

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



Einen Konnektor erstellen

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

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

2

Voraussetzungen prüfen

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

3

Implementieren Sie die BlueXP Klassifizierung

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

4

Abonnieren Sie den BlueXP Klassifizierungsservice

Die ersten 1 TB an Daten, die die BlueXP Klassifizierung in BlueXP scannt, sind 30 Tage lang kostenlos. Um die Daten nach diesem Zeitpunkt weiterhin zu scannen, ist ein BlueXP Abonnement über Ihren Cloud-Provider Marketplace oder eine BYOL-Lizenz von NetApp erforderlich.

Einen Konnektor erstellen

Falls Sie noch keinen Connector haben, erstellen Sie bei Ihrem Cloud-Provider einen Connector. Siehe ["Erstellen eines Konnektors in AWS"](#) Oder ["Erstellen eines Connectors in Azure"](#), Oder ["Erstellen eines Konnektors in GCP"](#). In den meisten Fällen 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:

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

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

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

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

Unterstützung für Regierungsregionen

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

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

["Weitere Informationen zur Bereitstellung des Connectors in einer Regierungsregion finden Sie unter"](#).

Voraussetzungen prüfen

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

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

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

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

Erforderliche Endpunkte für AWS

Endpunkte	Zweck
https://api.bluexp.netapp.com	Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der BlueXP-Website zur zentralen Benutzerauthentifizierung.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	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://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden.
https://support.compliance.api.bluexp.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.

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.blueexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden.
https://support.compliance.api.blueexp.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.

Stellen Sie sicher, dass BlueXP über die erforderlichen Berechtigungen verfügt

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

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

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

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

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

Sorgen Sie dafür, dass die BlueXP Klassifizierung weiter ausgeführt werden kann

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

Webbrowser-Konnektivität zur BlueXP Klassifizierung sicherstellen

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

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

Überprüfen Sie Ihre vCPU-Limits

Stellen Sie sicher, dass die vCPU-Begrenzung Ihres Cloud-Providers die Bereitstellung einer Instanz mit der erforderlichen Anzahl an Kernen ermöglicht. Sie müssen das vCPU-Limit für die jeweilige Instanzfamilie in der Region, in der BlueXP ausgeführt wird, überprüfen. ["Siehe die erforderlichen Instanztypen"](#).

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

- ["AWS Dokumentation: Amazon EC2 Service Quotas"](#)

- ["Azure Dokumentation: VCPU Kontingente von Virtual Machines"](#)
- ["Google Cloud Dokumentation: Ressourcenkontingente"](#)

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

Implementieren Sie die BlueXP Klassifizierung in der Cloud

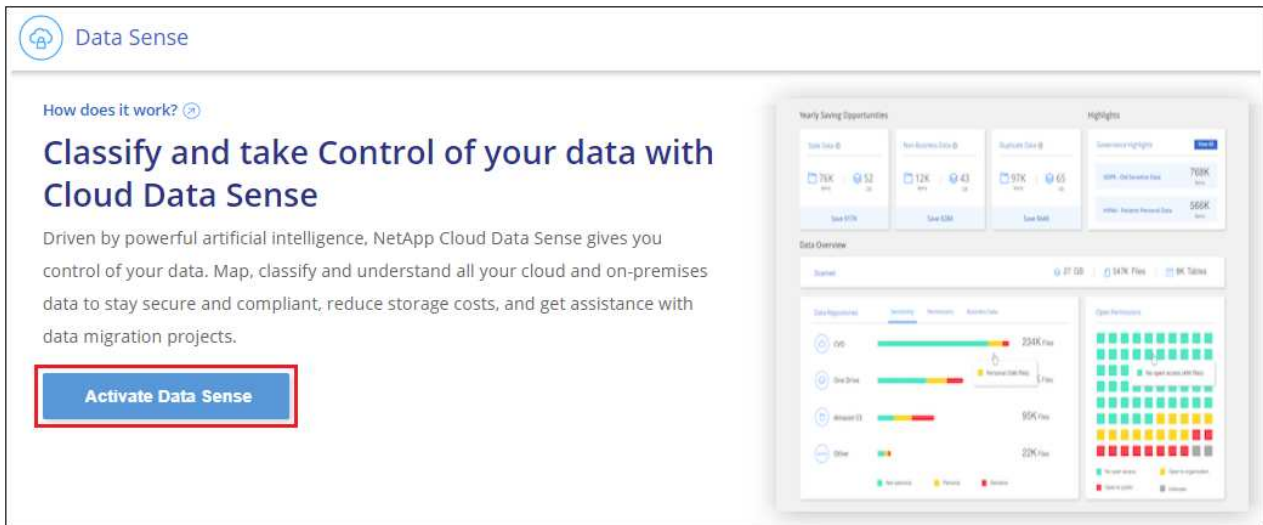
Führen Sie diese Schritte aus, um eine Instanz der BlueXP Klassifizierung in der Cloud zu implementieren. Der Connector implementiert die Instanz in der Cloud und installiert dann die BlueXP Klassifizierungssoftware auf dieser Instanz.

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

Implementieren in AWS

Schritte

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



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



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

Implementieren in Azure

Schritte

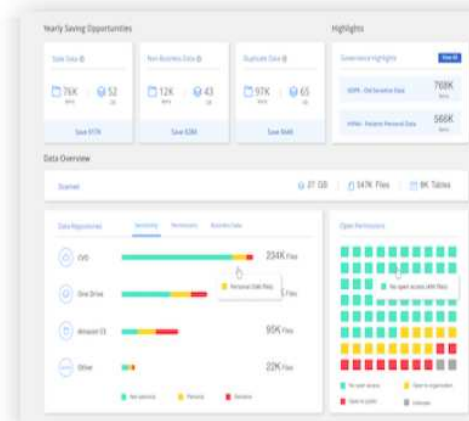
1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung**.
2. Klicken Sie Auf **Datensense Aktivieren**.

How does it work? ⓘ

Classify and take Control of your data with Cloud Data Sense

Driven by powerful artificial intelligence, NetApp Cloud Data Sense gives you control of your data. Map, classify and understand all your cloud and on-premises data to stay secure and compliant, reduce storage costs, and get assistance with data migration projects.

Activate Data Sense



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

Install your Data Sense instance

Select your preferred deployment location:

[Learn more about deploying Data Sense ⓘ](#)

Cloud Environment

I want BlueXP to deploy the instance and install Data Sense

Deploy

- > BlueXP will deploy a new machine automatically in the chosen cloud environment.
- > You will be taken to an installation wizard where you can configure your Data Sense installation.

I deployed an instance and I'm ready to install Data Sense

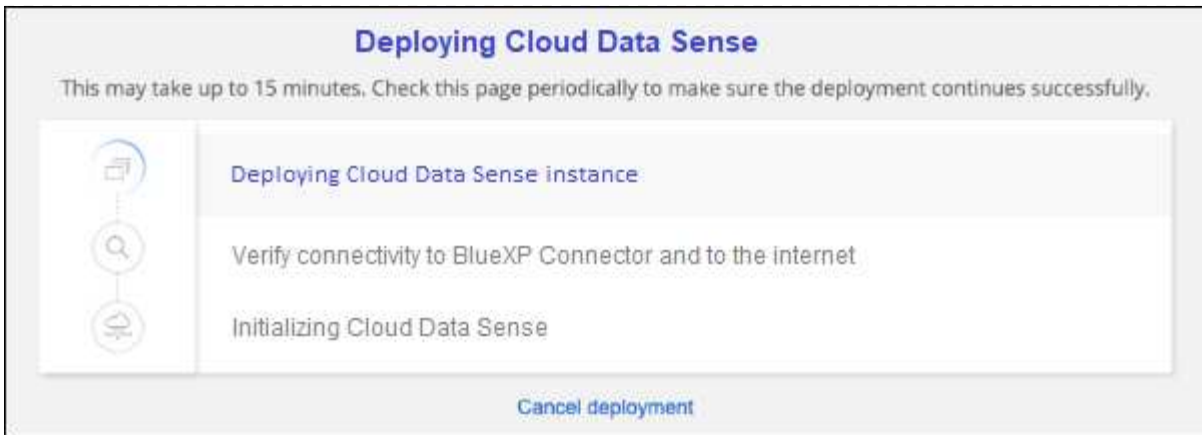
Deploy

On Premise

I prepared a local machine and I'm ready to install Data Sense

Deploy

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

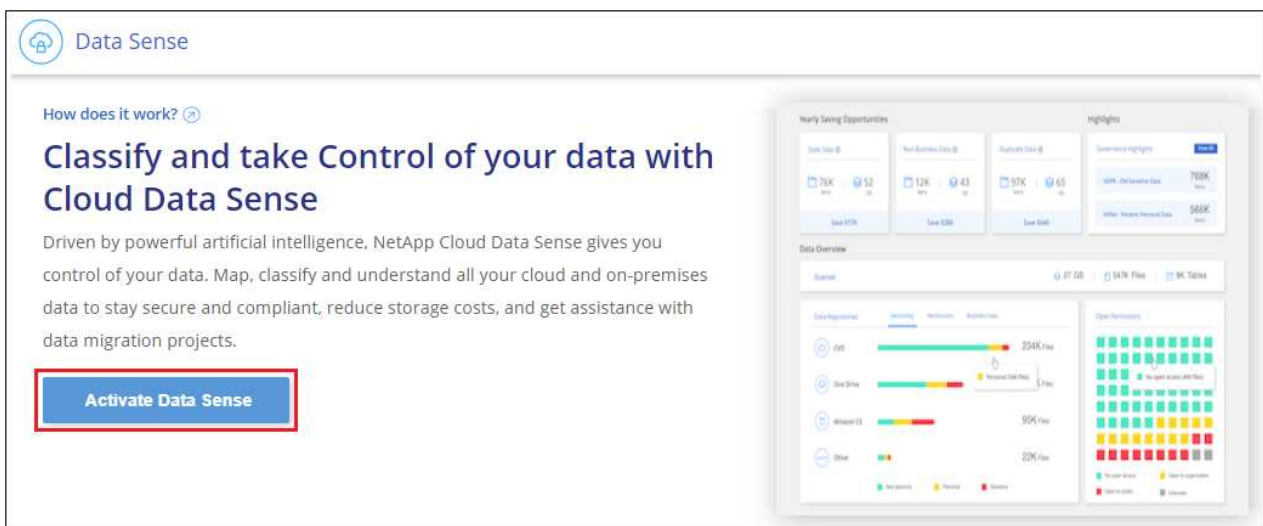


5. Wenn die Instanz bereitgestellt und die BlueXP-Klassifizierung installiert ist, klicken Sie auf **Weiter zur Konfiguration**, um zur Seite *Configuration* zu gelangen.

Implementieren in Google Cloud

Schritte

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




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

Install your Data Sense instance

Select your preferred deployment location:

[Learn more about deploying Data Sense](#)

Cloud Environment




I want BlueXP to deploy the instance and install Data Sense

> BlueXP will deploy a new machine automatically in the chosen cloud environment.
> You will be taken to an installation wizard where you can configure your Data Sense installation.

Deploy

^




I deployed an instance and I'm ready to install Data Sense

Deploy

v

On Premise



I prepared a local machine and I'm ready to install Data Sense

Deploy

v

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

Deploying Cloud Data Sense

This may take up to 15 minutes. Check this page periodically to make sure the deployment continues successfully.







Deploying Cloud Data Sense instance

Verify connectivity to BlueXP Connector and to the internet

Initializing Cloud Data Sense

Cancel deployment

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

Ergebnis

BlueXP implementiert die BlueXP Klassifizierungsinstanz in Ihrem Cloud-Provider.

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

Nächste Schritte

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

Das können Sie auch ["Lizenzierung für die BlueXP Klassifizierung einrichten"](#) Derzeit. Sie werden erst nach Ablauf der 30-tägigen kostenlosen Testversion belastet.

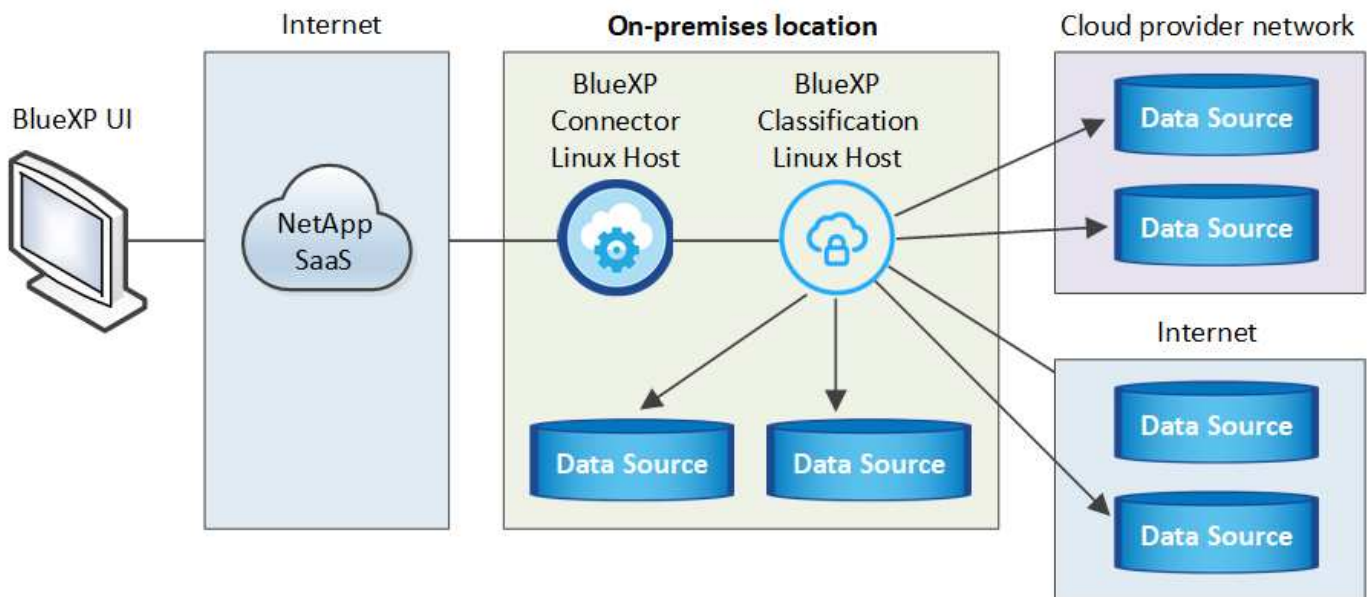
Installieren Sie die BlueXP Klassifizierung auf einem Host mit Internetzugang

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

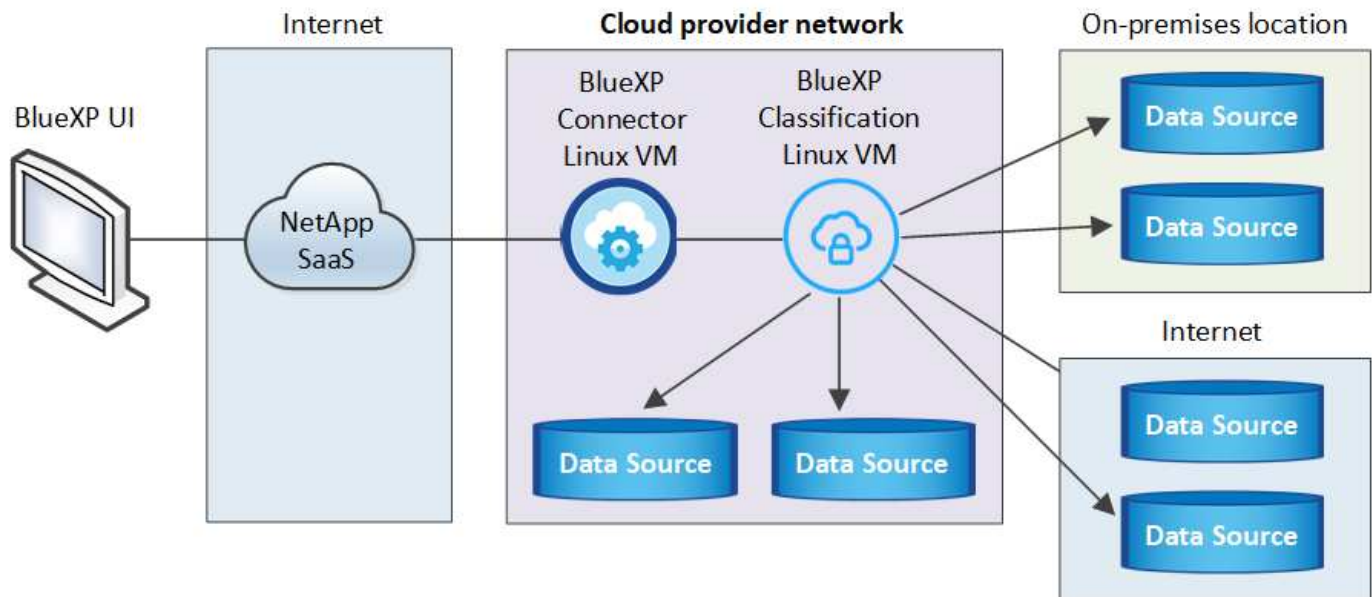
Die On-Premises-Installation ist möglicherweise eine gute Option, wenn Sie On-Premises-ONTAP Systeme mit einer BlueXP Klassifizierungsinstanz scannen möchten, die sich auch vor Ort befindet – dies ist jedoch keine Anforderung. Die Software funktioniert unabhängig von der gewählten Installationsmethode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

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

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



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



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

Beachten Sie, dass Sie auch können ["Installieren Sie die BlueXP Klassifizierung auf einer lokalen Website ohne Internetzugang"](#) Für vollständig sichere Standorte.

Schnellstart

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

1

Einen Konnektor erstellen

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

4

Abonnieren Sie den BlueXP Klassifizierungsservice

Die ersten 1 TB an Daten, die die BlueXP Klassifizierung in BlueXP scannt, sind 30 Tage lang kostenlos. Um die Daten nach diesem Zeitpunkt weiterhin zu scannen, benötigen Sie ein Abonnement für Ihren Cloud-Provider Marketplace oder eine BYOL-Lizenz von NetApp.

Einen Konnektor erstellen

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:

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

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

Beachten Sie, dass Sie auch können ["Stellen Sie den Connector vor Ort bereit"](#) Auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host 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"](#).

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, haben Sie die Wahl zwischen drei Systemgrößen, je nach Größe des Datensatzes, den Sie die BlueXP Klassifizierung scannen möchten.

Systemgröße	CPU	RAM (Swap-Speicher muss deaktiviert sein)	Festplatte
Extra Groß	32 CPUs	128 GB RAM	1 tib SSD auf /, oder - 100 gib verfügbar auf /opt - 895 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Groß	16 CPUs	64 GB RAM	500 gib SSD auf /, oder - 100 gib verfügbar auf /opt - 395 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Mittel	8 CPUs	32 GB RAM	200 gib SSD auf /, oder - 50 gib verfügbar auf /opt - 145 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Klein	8 CPUs	16 GB RAM	100 gib SSD auf /, oder - 50 gib verfügbar auf /opt - 45 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp

Beachten Sie, dass es bei der Verwendung der kleineren Systeme Einschränkungen gibt. Siehe ["Verwenden eines kleineren Instanztyps"](#) Entsprechende Details.

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

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

- **Betriebssystem:**

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

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

- Installation an einem dunklen Ort
- Verteiltes Scannen; Verwendung eines Master-Scanner-Knotens und Remote-Scanner-Knoten

- **Red hat Subscription Management:** Der Host muss bei Red hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.
- **Zusätzliche Software:** Sie müssen die folgende Software auf dem Host installieren, bevor Sie die BlueXP-Klassifizierung installieren:

- Je nach verwendetem Betriebssystem müssen Sie eine der Container-Engines installieren:
 - Docker Engine ab Version 19.3.1. "[Installationsanweisungen anzeigen](#)".

"[Hier geht's zum Video](#)" Eine kurze Demo zur Installation von Docker auf CentOS.

- Podman Version 4 oder höher. Um Podman zu installieren, aktualisieren Sie die Systempakete (`sudo yum update -y`), und installieren Sie dann Podman (`sudo yum install 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://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden.
https://support.compliance.api.bluexp.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://github.com/docker https://download.docker.com	Enthält die erforderlichen Pakete für die Installation von Dockern.
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Enthält die erforderlichen Pakete für die CentOS-Installation.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Enthält die erforderlichen Pakete für die Ubuntu-Installation.

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

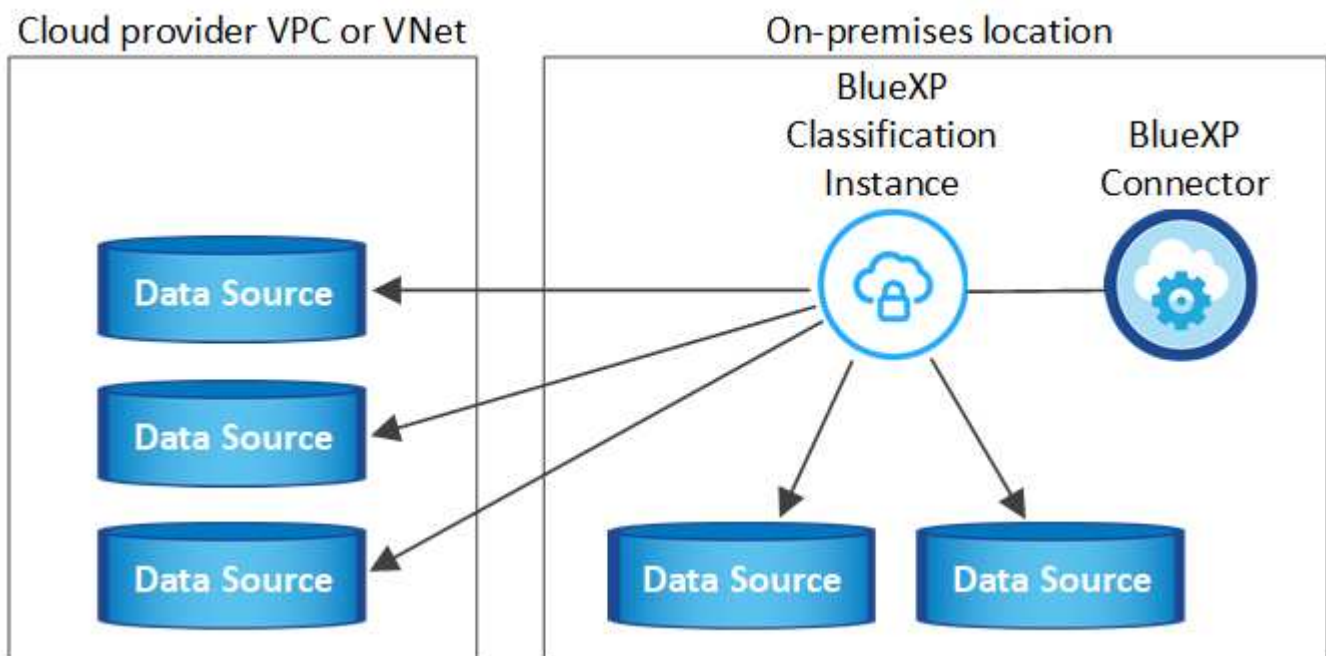
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 443 (TCP) und 80	Die Firewall- oder Routing-Regeln für den Connector müssen ein- und ausgehenden Datenverkehr über Port 443 zur und von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass Port 8080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

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

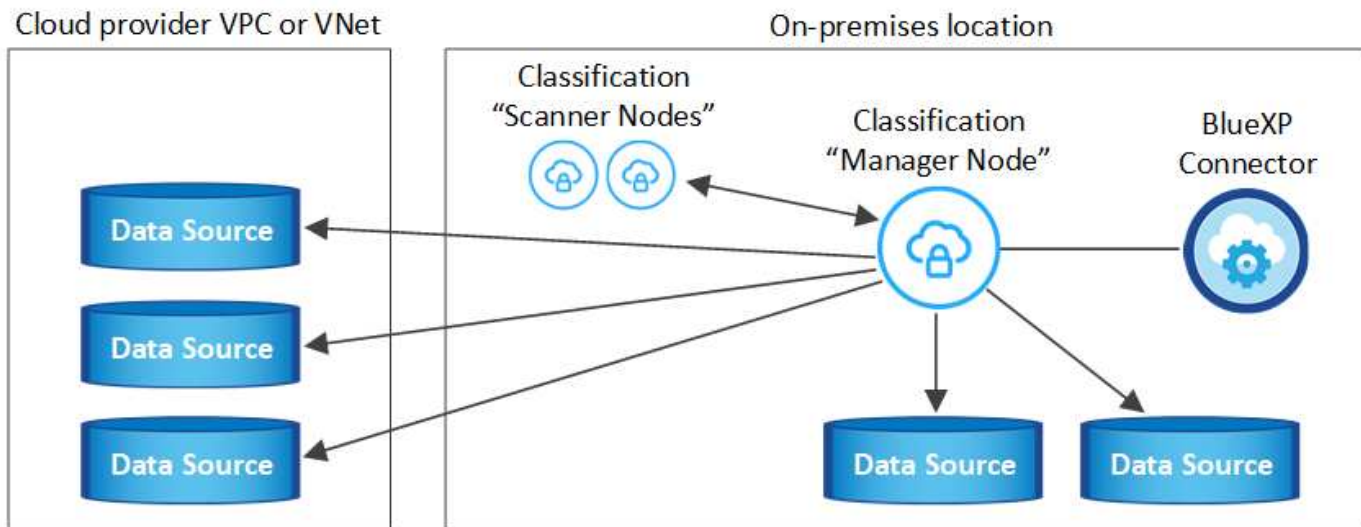
Wenn Sie mehrere BlueXP Klassifizierungs-Hosts nutzen, um eine zusätzliche Rechenleistung zum Scannen Ihrer Datenquellen zu bieten, müssen Sie zusätzliche Ports/Protokolle aktivieren. ["Siehe zusätzliche Anschlussanforderungen"](#).

BlueXP Klassifizierung auf dem Linux-Host installieren

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



Bei sehr großen Konfigurationen, bei denen Sie Petabyte an Daten scannen, können Sie mehrere Hosts einschließen, um zusätzliche Verarbeitungsleistung zu schaffen. [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"](#) Informationen zur Installation der BlueXP Klassifizierung.

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

Was Sie benötigen

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

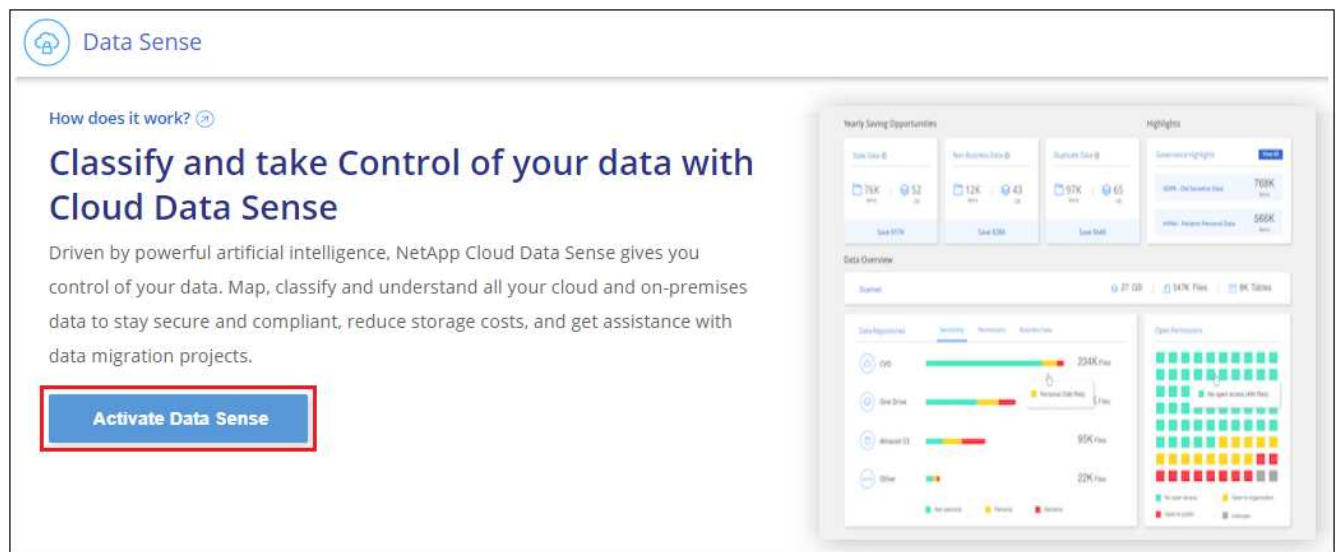
- Der Benutzer muss ein lokaler Benutzer sein. Domänenbenutzer werden nicht unterstützt.
- Vergewissern Sie sich, dass die erforderliche Offline-Umgebung erfüllt ist [Berechtigungen und Konnektivität](#).

Schritte

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

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

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



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

Install your Data Sense instance

Select your preferred deployment location:

[Learn more about deploying Data Sense](#)

Cloud Environment

I want BlueXP to deploy the instance and install Data Sense

Deploy

I deployed an instance and I'm ready to install Data Sense

Deploy

> Use this option if you have already provisioned a new machine for Data Sense in the Cloud.
 > Make sure your machine meets the [necessary requirements](#).

On Premise

I prepared a local machine and I'm ready to install Data Sense

Deploy

> Choose this option if you would like to deploy Data Sense in your on-premises environment.
 > This installation requires a pre-prepared machine to install Data Sense on.
 > Make sure your machine meets the [necessary requirements](#).

Deploy on a machine you provisioned in the cloud

Deploy on a machine you provisioned in your premises

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

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

Geben Sie die Parameter wie aufgefordert ein:	Geben Sie den vollständigen Befehl ein:
<p>a. Fügen Sie den Befehl ein, den Sie aus Schritt 7 kopiert haben:</p> <pre>sudo ./install.sh -a <account_id> -c <client_id> -t <user_token></pre> <p>Wenn Sie die Installation auf einer Cloud-Instanz (nicht vor Ort) ausführen, fügen Sie hinzu <code>--manual-cloud-install</code> <code><cloud_provider></code>.</p> <p>b. Geben Sie die IP-Adresse oder den Hostnamen der Host-Maschine der BlueXP Klassifizierung ein, damit das Connector-System darauf zugreifen kann.</p> <p>c. Geben Sie die IP-Adresse oder den Host-Namen der BlueXP Connector Host Machine ein, damit das BlueXP Klassifizierungssystem darauf zugreifen kann.</p> <p>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.</p>	<p>Alternativ können Sie den gesamten Befehl vorab erstellen und die erforderlichen Host- und Proxy-Parameter bereitstellen:</p> <pre>sudo ./install.sh -a <account_id> -c <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></pre>

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-Zertifikatbündeln. 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.

Das können Sie auch "[Lizenzierung für die BlueXP Klassifizierung einrichten](#)" Derzeit. Sie werden erst nach Ablauf der 30-tägigen kostenlosen Testversion belastet.

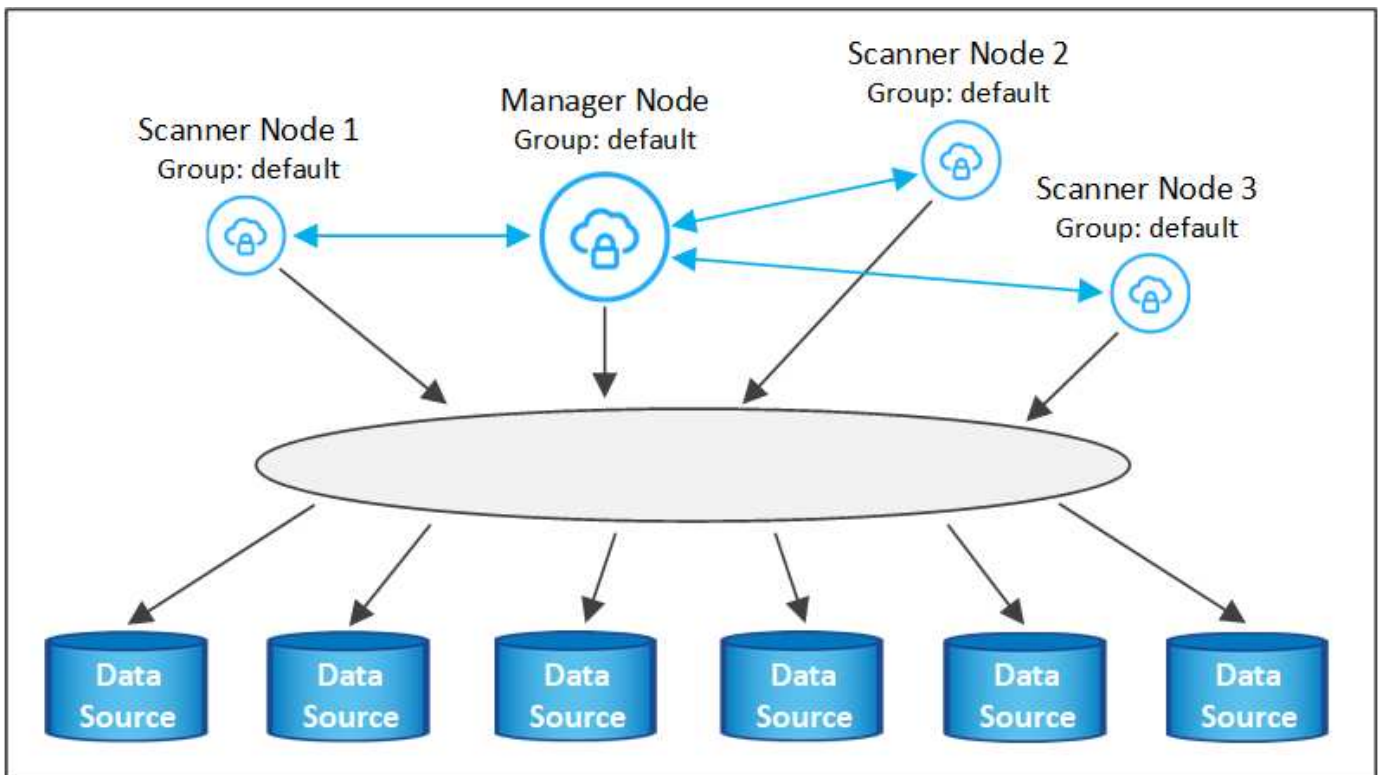
Fügen Sie Scannerknoten zu einer vorhandenen Implementierung hinzu

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

Es gibt zwei Möglichkeiten, weitere Scanner-Knoten hinzuzufügen:

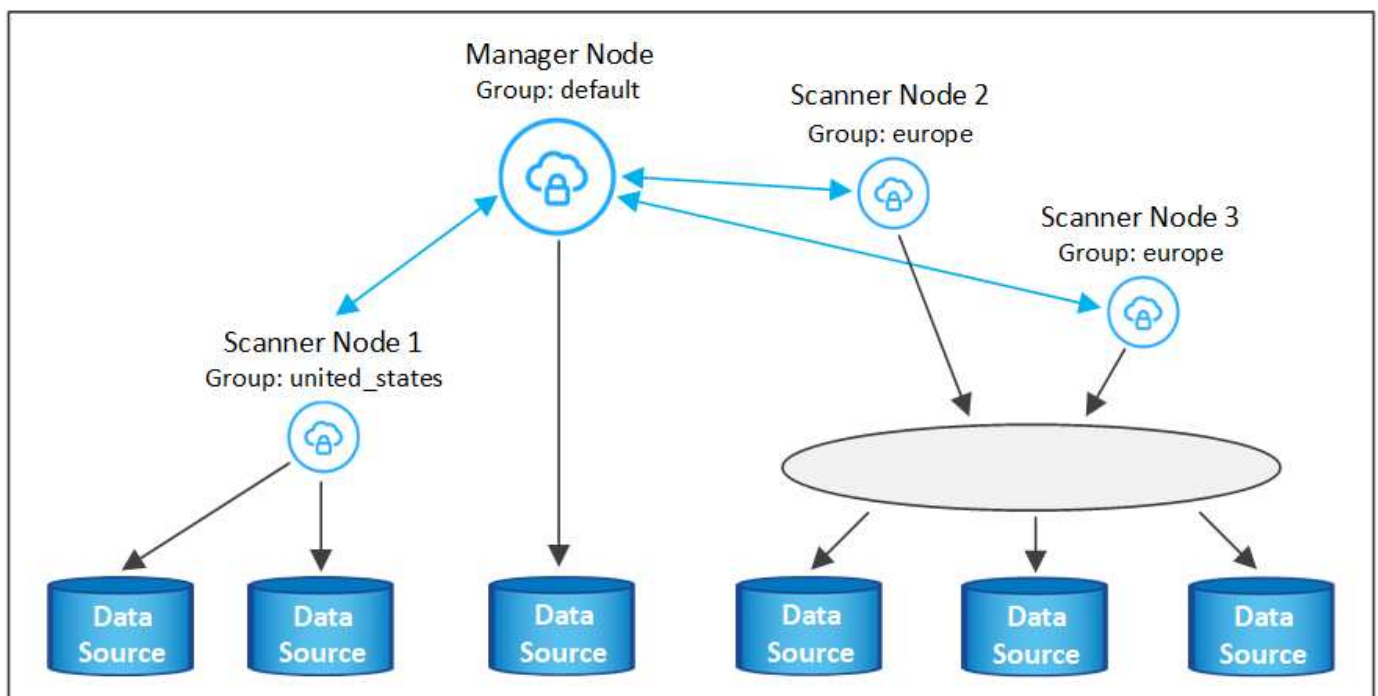
- Fügen Sie einen Knoten hinzu, um das Scannen aller Datenquellen zu unterstützen
- Fügen Sie einen Knoten hinzu, um das Scannen einer bestimmten Datenquelle oder einer bestimmten Gruppe von Datenquellen zu unterstützen (typischerweise basierend auf dem Speicherort).

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



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

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



BlueXP Klassifizierungs-Scannergruppen sind separate geografische Bereiche, in denen Ihre Daten gespeichert sind. Es können weltweit mehrere BlueXP Klassifizierungs-Scanner-Nodes implementiert und für jeden Node eine Scannergruppe ausgewählt werden. Auf diese Weise scannt jeder Scanner-Knoten die Daten, die ihm am nächsten sind. Je näher der Scanner-Knoten an den Daten liegt, desto besser, da er die Netzwerklatenz so weit wie möglich beim Scannen der Daten reduziert.

Sie können auswählen, welche Scannergruppen zur BlueXP Klassifizierung hinzugefügt werden sollen, und ihre Namen festlegen. Durch die Klassifizierung von BlueXP wird nicht erzwungen, dass ein Node, der einer Scannergruppe namens „europa“ zugeordnet ist, in Europa implementiert wird.

Gehen Sie folgendermaßen vor, um zusätzliche BlueXP Klassifizierungs-Scanner-Nodes zu installieren:

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

Was Sie benötigen

- Stellen Sie sicher, dass alle Linux-Systeme für Scanner-Knoten den erfüllen [Host-Anforderungen erfüllt](#).
- Überprüfen Sie, ob auf den Systemen die beiden erforderlichen Softwarepakete installiert sind (Docker Engine oder Podman und Python 3).
- Stellen Sie sicher, dass Sie auf den Linux-Systemen über Root-Rechte verfügen.
- Vergewissern Sie sich, dass Ihre Umgebung den erforderlichen Anforderungen entspricht [Berechtigungen und Konnektivität](#).
- Sie müssen über die IP-Adressen der Scanner-Knoten-Hosts verfügen, die Sie hinzufügen.
- Sie müssen über die IP-Adresse des Node-Host-Systems von BlueXP Classification Manager verfügen
- Sie müssen über die IP-Adresse oder den Hostnamen des Connector-Systems, Ihre NetApp Account-ID, Connector Client-ID und Benutzer-Zugriffstoken verfügen. Wenn Sie planen, Scannergruppen zu verwenden, müssen Sie die ID der Arbeitsumgebung für jede Datenquelle in Ihrem Konto kennen. Weitere Informationen finden Sie unten unter **Voraussetzungen Schritte**.
- Die folgenden Ports und Protokolle müssen auf allen Hosts aktiviert sein:

Port	Protokolle	Beschreibung
2377	TCP	Cluster-Management-Kommunikation
7946	TCP, UDP	Kommunikation zwischen den Knoten
4789	UDP	Overlay-Netzwerk-Traffic
50	ESP	Verschlüsselter ESP-Datenverkehr (IPsec Overlay Network)

Port	Protokolle	Beschreibung
111	TCP, UDP	NFS-Server für die gemeinsame Nutzung von Dateien zwischen den Hosts (benötigt von jedem Scanner-Knoten zu Manager-Knoten)
2049	TCP, UDP	NFS-Server für die gemeinsame Nutzung von Dateien zwischen den Hosts (benötigt von jedem Scanner-Knoten zu Manager-Knoten)

- Wenn Sie verwenden `firewalld` Auf Ihren BlueXP Klassifizierungs-Machines empfehlen wir, sie zu aktivieren, bevor Sie die BlueXP Klassifizierung installieren. Führen Sie die folgenden Befehle zum Konfigurieren aus `firewalld` Damit es mit der BlueXP Klassifizierung kompatibel ist:

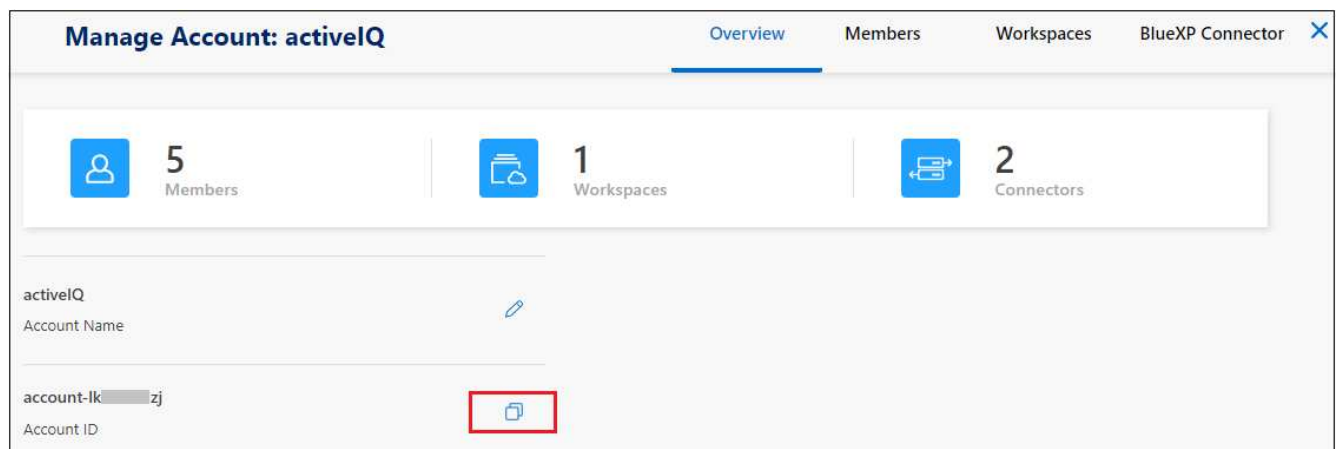
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp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

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

Erforderliche Schritte

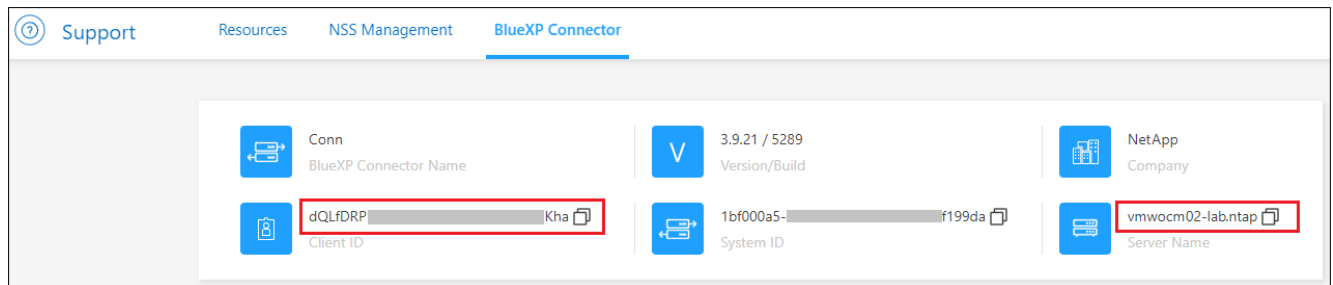
Führen Sie diese Schritte aus, um die NetApp Account ID, die Connector Client ID, den Connector Server-Namen und das Token für den Benutzerzugriff zu erhalten, die erforderlich sind, um Scanner-Nodes hinzuzufügen.

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

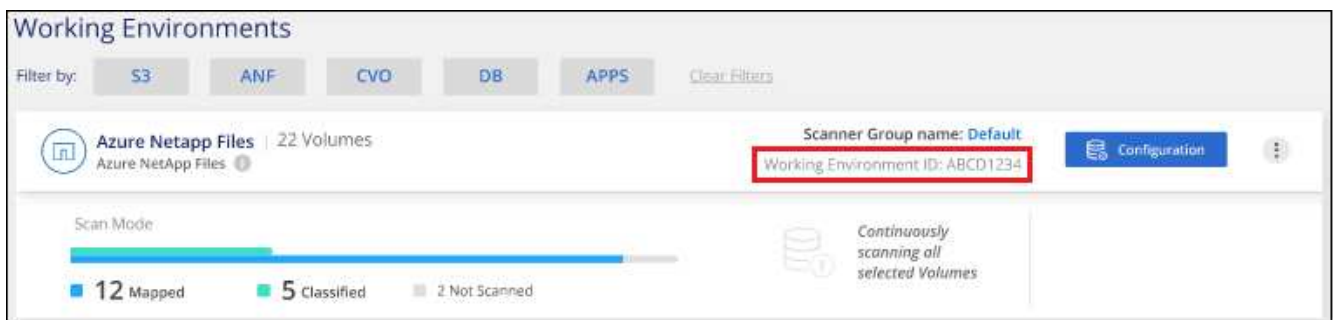


2. Kopieren Sie die *Konto-ID*.

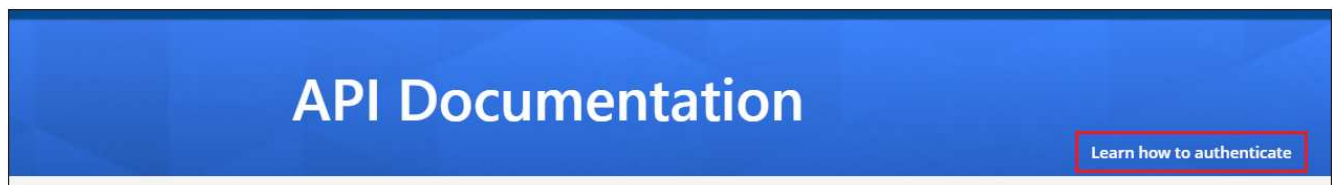
3. Klicken Sie in der Menüleiste von BlueXP auf **Hilfe > Support > BlueXP Connector**.



4. Kopieren Sie die Konnektor_Client-ID_ und die *Servername*.
5. Wenn Sie planen, Scannergruppen zu verwenden, kopieren Sie auf der Registerkarte BlueXP Classification Configuration die Arbeitsumgebungs-ID für jede Arbeitsumgebung, die Sie einer Scannergruppe hinzufügen möchten.



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



7. Befolgen Sie die Authentifizierungsanweisungen, indem Sie den Benutzernamen und das Passwort des Kontoadministrators in den Parametern „Benutzername“ und „Passwort“ verwenden.
8. Kopieren Sie dann das *Access-Token* aus der Antwort.

Schritte

1. Führen Sie auf dem BlueXP Classification Manager Node das Skript „add_Scanner_Node.sh“ aus. Mit diesem Befehl werden beispielsweise 2 Scannerknoten hinzugefügt:

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

Variablenwerte:

- *Account_id* = NetApp Konto-ID
- *Client_id* = Konnektor-Client-ID (fügen Sie das Suffix „Clients“ der Client-ID hinzu, die Sie in den erforderlichen Schritten kopiert haben)

- *Cm_Host* = IP-Adresse oder Hostname des Steckverbindersystems
 - *ds_Manager_ip* = Private IP-Adresse des Node-Systems BlueXP Classification Manager
 - *Node_Private_ip* = IP-Adressen der BlueXP Klassifizierungsscanner Node-Systeme (mehrere Scanner-Node-IPs werden durch ein Komma getrennt)
 - *User_Token* = JWT-Benutzer-Zugriffstoken
2. Bevor das Skript `add_Scanner_Node` abgeschlossen wird, wird in einem Dialogfeld der Installationsbefehl angezeigt, der für die Scanner-Knoten benötigt wird. Kopieren Sie den Befehl (z. B.: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`) Und in einer Textdatei speichern.
3. Auf * jedem Scanner-Knoten-Host:
- a. Kopieren Sie die Data Sense Installer-Datei (**DATASENSE-INSTALLER-<Version>.tar.gz**) auf den Host-Rechner (mit `scp` Oder eine andere Methode).
 - b. Entpacken Sie die Installationsdatei.
 - c. Fügen Sie den Befehl ein, den Sie in Schritt 2 kopiert haben, und führen Sie ihn aus.
 - d. Wenn Sie einen Scannerknoten zu einer "Scannergruppe" hinzufügen möchten, fügen Sie dem Befehl den Parameter **-r <Scanner_Group_Name>** hinzu. Andernfalls wird der Scannerknoten zur Gruppe „Standard“ hinzugefügt.
- Wenn die Installation auf allen Scanner-Knoten abgeschlossen ist und sie mit dem Manager-Knoten verbunden wurden, wird das Skript „`add_Scanner_Node.sh`“ ebenfalls beendet. Die Installation dauert 10 bis 20 Minuten.
4. Wenn Sie Scannerknoten zu einer Scannergruppe hinzugefügt haben, kehren Sie zum Manager-Knoten zurück und führen Sie die folgenden beiden Aufgaben aus:
- a. Öffnen Sie die Datei `„/opt/netapp/config/Custom_Configuration/working_environment_to_Scanner_Group_config.yml“` und geben Sie die Zuordnung ein, für welche Scannergruppen bestimmte Arbeitsumgebungen scannen sollen. Sie benötigen die *Working Environment ID* für jede Datenquelle. Die folgenden Einträge fügen beispielsweise 2 Arbeitsumgebungen zur Scanner-Gruppe „europa“ und 2 zur Scannergruppe „united_States“ hinzu:

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

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

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

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

Ergebnis

Die BlueXP Klassifizierung wird mit Manager- und Scanner-Nodes eingerichtet, um alle Datenquellen zu scannen.

Nächste Schritte

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

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

The screenshot shows the 'Working Environments' configuration page. At the top, there are filter buttons for 'S3', 'ANF', 'CVO', 'DB', and 'APPS', along with a 'Clear Filters' link. Below this, the 'Azure Netapp Files' section is visible, showing '22 Volumes'. A red box highlights the 'Scanner Group name: Default' and 'Working Environment ID: ABCD1234'. To the right is a 'Configuration' button. Below the filter section, a 'Scan Mode' progress bar is shown, with '12 Mapped' (blue), '5 Classified' (green), and '2 Not Scanned' (grey). To the right of the progress bar, it says 'Continuously scanning all selected Volumes'.

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

The screenshot shows the 'Scanner Groups' configuration page. At the top, there is a search bar. Below it, the 'Scanner Group: Default' section is expanded, showing '2 Scanner nodes'. A table lists the scanner nodes with columns: 'Scanner node host name', 'IP', 'Last active time', 'Status', and 'Error'. The table shows two nodes, both with 'Active' status. Below this, the 'Scanner Group: United_States' section is also expanded, showing '2 Scanner nodes' with a similar table. At the bottom, the 'Scanner Group: Europe' section is partially visible.

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

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

Das können Sie "[Lizenzierung für die BlueXP Klassifizierung einrichten](#)" Derzeit. Sie werden erst nach Ablauf der 30-tägigen kostenlosen Testversion belastet.

Installation mit mehreren Hosts für große Konfigurationen

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

Befolgen Sie diese Schritte, wenn Sie die BlueXP Klassifizierungssoftware gleichzeitig auf mehreren lokalen Hosts installieren. Beachten Sie, dass Sie bei der Bereitstellung mehrerer Hosts keine „Scannergruppen“ verwenden können.

Was Sie benötigen

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

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

Schritte

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

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

Mit diesem Befehl werden beispielsweise 3 Scannerknoten hinzugefügt:

```
sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host  
<ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy
```



```
-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme>  
--proxy-user <proxy_user> --proxy-password <proxy_password>
```

3. Bevor die Installation des Manager-Node abgeschlossen ist, wird in einem Dialogfeld der für die Scanner-Knoten erforderliche Installationsbefehl angezeigt. Kopieren Sie den Befehl (z. B. `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) Und in einer Textdatei speichern.
4. Auf * jedem Scanner-Knoten-Host:
 - a. Kopieren Sie die Data Sense Installer-Datei (**DATASENSE-INSTALLER-<Version>.tar.gz**) auf den Host-Rechner (mit `scp` Oder eine andere Methode).
 - b. Entpacken Sie die Installationsdatei.
 - c. Fügen Sie den Befehl ein, den Sie in Schritt 3 kopiert haben, und führen Sie ihn aus.

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

Ergebnis

Das BlueXP Klassifizierungs-Installationsprogramm schließt die Installation der Pakete ab und registriert die Installation. Die Installation dauert 10 bis 20 Minuten.

Nächste Schritte

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

Das können Sie auch ["Lizenzierung für die BlueXP Klassifizierung einrichten"](#) Derzeit. Sie werden erst nach Ablauf der 30-tägigen kostenlosen Testversion belastet.

BlueXP Klassifizierung auf einem Linux-Host ohne Internetzugang installieren

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

["Informieren Sie sich über die verschiedenen Implementierungsmodi für die BlueXP Connector und BlueXP Klassifizierung"](#).

Beachten Sie, dass Sie auch können ["Implementieren Sie die BlueXP Klassifizierung auf einer lokalen Website mit Internetzugang"](#).

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

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

Derzeit wird Cloud Volumes ONTAP, Azure NetApp Files, FSX für ONTAP, AWS S3 oder Google Drive nicht unterstützt, OneDrive- oder SharePoint Online-Konten, wenn die BlueXP Klassifizierung im privaten Modus bereitgestellt wird.

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.:

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

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

Schnellstart

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

1

Installieren Sie den BlueXP-Anschluss

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

2

Voraussetzungen für die BlueXP Klassifizierung prüfen

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

3

Laden Sie die BlueXP Klassifizierung herunter und implementieren Sie sie

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

4

Abonnieren Sie den BlueXP Klassifizierungsservice

Die ersten 1 TB an Daten, die die BlueXP Klassifizierung in BlueXP scannt, sind 30 Tage lang kostenlos. Nach diesem Zeitpunkt ist eine BYOL-Lizenz von NetApp erforderlich, um das Scannen von Daten fortzusetzen.

Installieren Sie den BlueXP-Anschluss

Wenn Sie noch keinen BlueXP Connector 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, haben Sie die Wahl zwischen drei Systemgrößen, je nach Größe des Datensatzes, den Sie die BlueXP Klassifizierung scannen möchten.

Systemgröße	CPU	RAM (Swap-Speicher muss deaktiviert sein)	Festplatte
Extra Groß	32 CPUs	128 GB RAM	1 tib SSD auf /, oder - 100 gib verfügbar auf /opt - 895 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Groß	16 CPUs	64 GB RAM	500 gib SSD auf /, oder - 100 gib verfügbar auf /opt - 395 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Mittel	8 CPUs	32 GB RAM	200 gib SSD auf /, oder - 50 gib verfügbar auf /opt - 145 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Klein	8 CPUs	16 GB RAM	100 gib SSD auf /, oder - 50 gib verfügbar auf /opt - 45 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp

Beachten Sie, dass es bei der Verwendung der kleineren Systeme Einschränkungen gibt. Siehe ["Verwenden eines kleineren Instanztyps"](#) Entsprechende Details.

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

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

- **Betriebssystem:**
 - Für die folgenden Betriebssysteme ist die Verwendung der Docker Container-Engine erforderlich:
 - Red hat Enterprise Linux Version 7.8 und 7.9
 - CentOS Version 7.8 und 7.9
 - Ubuntu 22.04 (BlueXP Klassifikation ab Version 1.23 erforderlich)

- Die folgenden Betriebssysteme erfordern die Verwendung der Podman Container-Engine. Sie erfordern eine BlueXP Klassifikation der Version 1.30 oder höher:

- Red hat Enterprise Linux Version 8.8, 9.0, 9.1, 9.2 und 9.3

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

- Installation an einem dunklen Ort
- Verteiltes Scannen; Verwendung eines Master-Scanner-Knotens und Remote-Scanner-Knoten

- **Red hat Subscription Management:** Der Host muss bei Red hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.
- **Zusätzliche Software:** Sie müssen die folgende Software auf dem Host installieren, bevor Sie die BlueXP-Klassifizierung installieren:
 - Je nach verwendetem Betriebssystem müssen Sie eine der Container-Engines installieren:
 - Docker Engine ab Version 19.3.1. ["Installationsanweisungen anzeigen"](#).

["Hier geht's zum Video"](#) Eine kurze Demo zur Installation von Docker auf CentOS.
 - Podman Version 4 oder höher. Um Podman zu installieren, aktualisieren Sie die Systempakete (`sudo yum update -y`), und installieren Sie dann Podman (`sudo yum install 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.

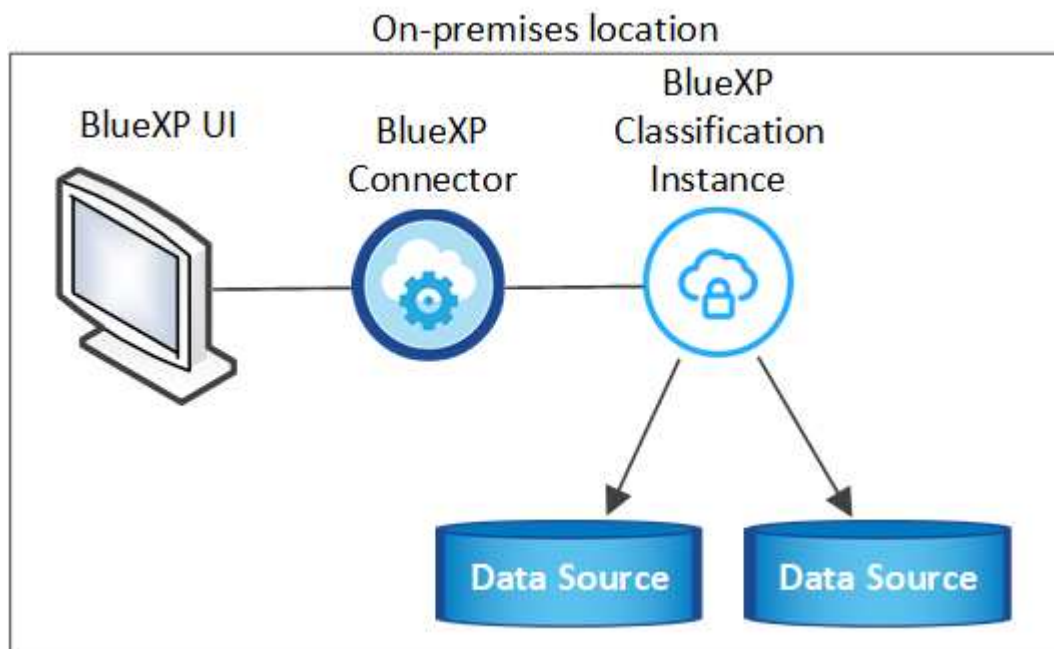
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 6000 (TCP), 443 (TCP) UND 80	<p>Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über die Ports 6000 und 443 zur und von der BlueXP Klassifizierungsinstanz zulassen.</p> <ul style="list-style-type: none"> • Port 6000 ist erforderlich, damit die BYOL-Lizenz für die BlueXP Klassifizierung an einem Dark Site funktioniert. • Port 8080 sollte offen sein, damit Sie den Installationsfortschritt in BlueXP sehen können.
Connector <> ONTAP-Cluster (NAS)	443 (TCP)	<p>BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen:</p> <ul style="list-style-type: none"> • Der Connector-Host muss ausgehenden HTTPS-Zugriff über Port 443 ermöglichen. Wenn sich der Connector in der Cloud befindet, ist die gesamte ausgehende Kommunikation durch die vordefinierte Sicherheitsgruppe zulässig. • Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen. Die standardmäßige "mgmt"-Firewall-Richtlinie ermöglicht eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert haben oder wenn Sie eine eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff über den Connector-Host aktivieren.
BlueXP Klassifizierung <> ONTAP Cluster	<ul style="list-style-type: none"> • Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS - 139 (TCP\UDP) und 445 (TCP\UDP) 	<p>Für 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.</p> <p>Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind:</p> <ul style="list-style-type: none"> • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 <p>NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.</p>

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

Wenn Sie mehrere BlueXP Klassifizierungs-Hosts nutzen, um eine zusätzliche Rechenleistung zum Scannen Ihrer Datenquellen zu bieten, müssen Sie zusätzliche Ports/Protokolle aktivieren. ["Siehe zusätzliche Anschlussanforderungen"](#).

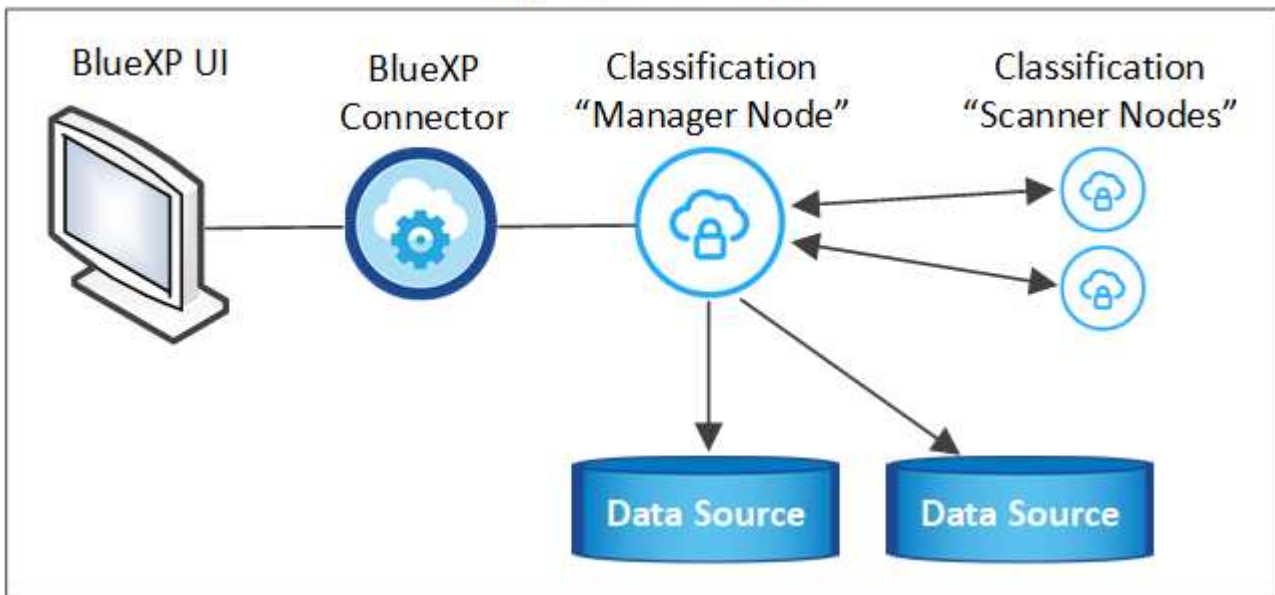
BlueXP Klassifizierung auf dem lokalen Linux-Host installieren

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



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

On-premises location



Installation mit einem Host für typische Konfigurationen

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

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

Was Sie benötigen

- Vergewissern Sie sich, dass Ihr Linux-System die erfüllt [Host-Anforderungen](#) erfüllt.
- Überprüfen Sie, ob Sie die beiden erforderlichen Softwarepakete (Docker Engine oder Podman und Python 3) installiert haben.
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.
- Vergewissern Sie sich, dass die erforderliche Offline-Umgebung erfüllt ist [Berechtigungen und Konnektivität](#).

Schritte

1. Laden Sie die BlueXP Klassifizierungssoftware auf einem internetkonfigurierten System von der herunter ["NetApp Support Website"](#). Die ausgewählte Datei heißt **DataSense-offline-Bundle-<Version>.tar.gz**.
2. Kopieren Sie das Installationspaket auf den Linux-Host, den Sie im privaten Modus verwenden möchten.
3. Entpacken Sie das Installationspaket auf dem Hostcomputer, z. B.:

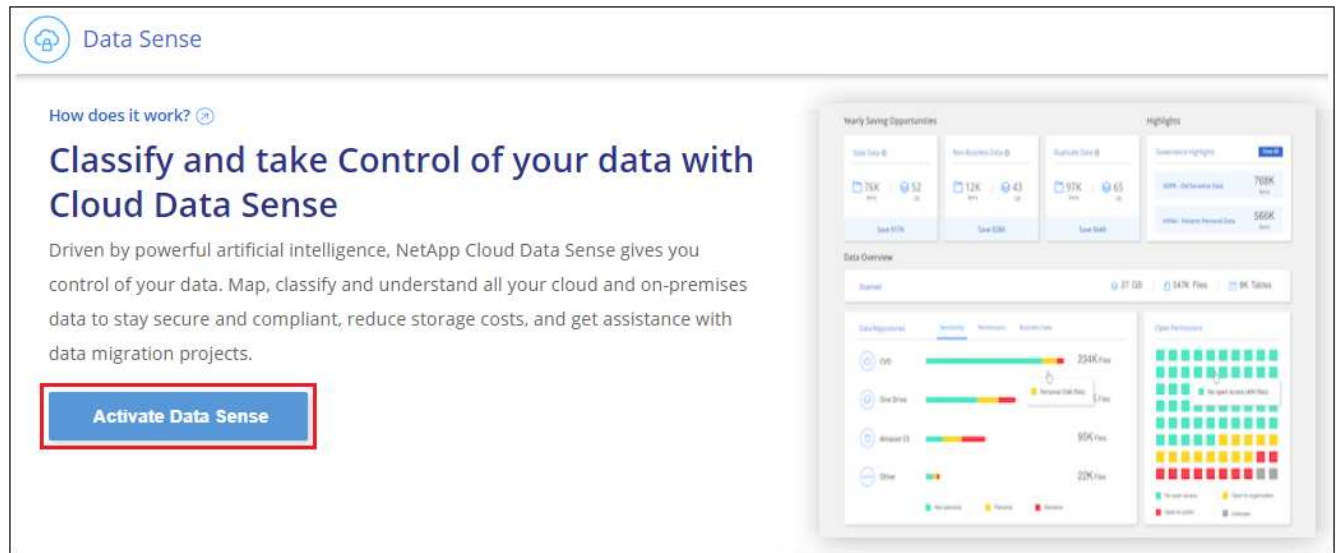
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

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

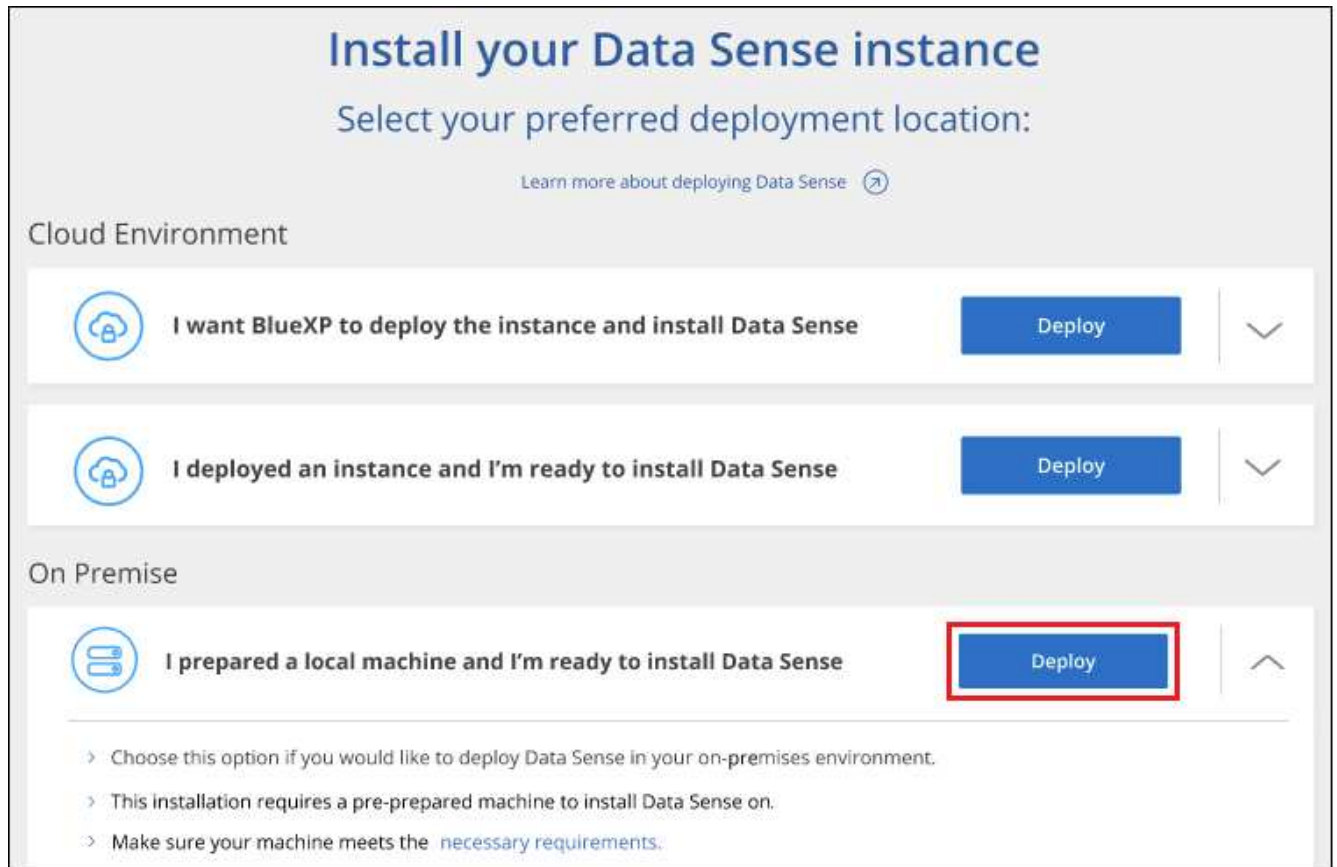
4. Entpacken Sie die Installationsdatei auf dem Host-Rechner, z. B.:


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

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



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



8. Das Dialogfeld *Deploy Data Sense on premise* wird angezeigt. Kopieren Sie den angegebenen Befehl (z.

B.: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`) Und fügen Sie sie in eine Textdatei ein, damit Sie sie später verwenden können. Klicken Sie dann auf **Schließen**, um das Dialogfeld zu schließen.

9. Geben Sie auf dem Hostcomputer den kopierten Befehl ein, und folgen Sie dann einer Reihe von Eingabeaufforderungen. Alternativ können Sie den vollständigen Befehl einschließlich aller erforderlichen Parameter als Befehlszeilenargumente bereitstellen.

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

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

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.

Das können Sie auch ["Byol-Lizenzierung für die BlueXP Klassifizierung einrichten"](#) Von der BlueXP Digital-Wallet-Seite aus. Sie werden erst nach Ablauf der 30-tägigen kostenlosen Testversion belastet.

Installation mit mehreren Hosts für große Konfigurationen

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

Befolgen Sie diese Schritte, wenn Sie die BlueXP Klassifizierungssoftware auf mehreren lokalen Hosts in einer Offline-Umgebung installieren.

Was Sie benötigen

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

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

Schritte

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

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

Mit diesem Befehl werden beispielsweise 3 Scannerknoten hinzugefügt:

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

3. Bevor die Installation des Manager-Node abgeschlossen ist, wird in einem Dialogfeld der für die Scanner-Knoten erforderliche Installationsbefehl angezeigt. Kopieren Sie den Befehl (z. B.: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) Und in einer Textdatei speichern.
4. Auf * jedem Scanner-Knoten-Host:
 - a. Kopieren Sie die Data Sense Installer-Datei (**cc_onprem_Installer.tar.gz**) auf den Host-Rechner.
 - b. Entpacken Sie die Installationsdatei.
 - c. Fügen Sie den Befehl ein, den Sie in Schritt 3 kopiert haben, und führen Sie ihn aus.

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

Ergebnis

Das BlueXP Klassifizierungs-Installationsprogramm schließt die Installation der Pakete ab und registriert die Installation. Die Installation dauert 15 bis 25 Minuten.

Nächste Schritte

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

Das können Sie auch ["Byol-Lizenzierung für die BlueXP Klassifizierung einrichten"](#) Von der BlueXP Digital-Wallet-Seite aus. Sie werden erst nach Ablauf der 30-tägigen kostenlosen Testversion belastet.

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_darksite_Upgrade.sh** und jede erforderliche Software von Drittanbietern extrahiert.

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

```
start_darksite_upgrade.sh
```

Ergebnis

Die BlueXP Klassifizierungssoftware wird auf Ihrem Host aktualisiert. Die Aktualisierung kann 5 bis 10 Minuten dauern.

Beachten Sie, dass für Scanner-Nodes kein Upgrade erforderlich ist, wenn Sie die BlueXP Klassifizierung auf mehreren Host-Systemen zum Scannen sehr großer Konfigurationen implementiert haben.

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

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

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

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

Erste Schritte

Sie führen die folgenden Aufgaben aus.

1. Optional können Sie einen BlueXP Connector installieren, wenn noch keiner installiert ist. Sie können das Testskript ausführen, ohne einen Connector installiert zu haben, aber das Skript überprüft die Verbindung zwischen dem Connector und der BlueXP-Klassifikationshost-Maschine - daher wird empfohlen, dass Sie

einen Connector haben.

2. Bereiten Sie den Host-Rechner vor und überprüfen Sie, ob er alle Anforderungen erfüllt.
3. Aktivieren Sie Outbound-Internetzugriff über die Host-Maschine der BlueXP Klassifizierung.
4. Vergewissern Sie sich, dass alle erforderlichen Ports auf allen Systemen aktiviert sind.
5. Laden Sie das Skript für den Voraussetzungstest herunter, und führen Sie es aus.

Einen Konnektor erstellen

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

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

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

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

Host-Anforderungen prüfen

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

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

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

Systemgröße	CPU	RAM (Swap-Speicher muss deaktiviert sein)	Festplatte
Mittel	8 CPUs	32 GB RAM	200 gib SSD auf /, oder - 50 gib verfügbar auf /opt - 145 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp
Klein	8 CPUs	16 GB RAM	100 gib SSD auf /, oder - 50 gib verfügbar auf /opt - 45 gib verfügbar auf /var/lib/docker - 5 gib auf /tmp

Beachten Sie, dass es bei der Verwendung der kleineren Systeme Einschränkungen gibt. Siehe ["Verwenden eines kleineren Instanztyps"](#) Entsprechende Details.

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

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

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

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

- Installation an einem dunklen Ort
- Verteiltes Scannen; Verwendung eines Master-Scanner-Knotens und Remote-Scanner-Knoten

- **Red hat Subscription Management:** Der Host muss bei Red hat Subscription Management registriert

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

- **Zusätzliche Software:** Sie müssen die folgende Software auf dem Host installieren, bevor Sie die BlueXP-Klassifizierung installieren:

- Je nach verwendetem Betriebssystem müssen Sie eine der Container-Engines installieren:

- Docker Engine ab Version 19.3.1. "[Installationsanweisungen anzeigen](#)".

"[Hier geht's zum Video](#)" Eine kurze Demo zur Installation von Docker auf CentOS.

- Podman Version 4 oder höher. Um Podman zu installieren, aktualisieren Sie die Systempakete (`sudo yum update -y`), und installieren Sie dann Podman (`sudo yum install 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://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden.
https://support.compliance.api.bluexp.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://github.com/docker https://download.docker.com	Enthält die erforderlichen Pakete für die Installation von Dockern.
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Enthält die erforderlichen Pakete für die CentOS-Installation.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Enthält die erforderlichen Pakete für die Ubuntu-Installation.

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

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

Führen Sie das Skript für die Klassifizierungsvoraussetzungen von BlueXP aus

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

["Hier geht's zum Video"](#) Anleitung zum Ausführen des Skripts „Voraussetzungen“ und zum Interpretieren der Ergebnisse.

Was Sie benötigen

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

Schritte

1. Laden Sie das Skript für die BlueXP Klassifizierungs-Voraussetzungen von [herunter "NetApp Support Website"](#). Die Datei, die Sie auswählen sollten, heißt **Standalone-pre-requisite-tester-<version>**.
2. Kopieren Sie die Datei auf den Linux-Host, den Sie verwenden möchten (mit `scp` Oder eine andere Methode).
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

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

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

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

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

Ergebnis

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

Wenn Probleme entdeckt wurden, werden sie als „empfohlen“ oder „erforderlich“ kategorisiert, um behoben zu werden. Empfohlene Probleme sind in der Regel Elemente, die das Scannen und Kategorisieren von BlueXP

verlangsamen würden. Diese Elemente müssen nicht korrigiert werden - aber Sie können sie ansprechen.

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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.