Implementieren Sie die BlueXP Klassifizierung

BlueXP classification

NetApp
July 25, 2024

Inhalt

Implementieren Sie die BlueXP Klassifizierung

Welche BlueXP Klassifizierungs-Implementierung sollten Sie verwenden?

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

Die BlueXP Klassifizierung kann wie folgt implementiert werden:

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

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

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

Implementieren Sie die BlueXP Klassifizierung in der Cloud mit BlueXP

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

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

Schnellstart

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

1 **Einen Konnektor erstellen**

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

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

2 Voraussetzungen prüfen

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

3 Implementieren Sie die BlueXP Klassifizierung

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

Einen Konnektor erstellen

Falls Sie noch keinen Connector haben, erstellen Sie bei Ihrem Cloud-Provider einen Connector. Siehe "Erstellen eines Konnektors in AWS" Oder "Erstellen eines Connectors in Azure", Oder "Erstellen eines Konnektors in GCP". In den meisten Fällen ist wahrscheinlich vor der Aktivierung der BlueXP Klassifizierung ein Connector eingerichtet "Für BlueXP-Funktionen ist ein Connector erforderlich", Aber es gibt Fälle, in denen Sie müssen, um eine Einrichtung jetzt.

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

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

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

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

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

Unterstützung für Regierungsregionen

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

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

Voraussetzungen prüfen

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

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

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

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

Erforderliche Endpunkte für AWS

Endpunkte	Zweck
https://api.bluexp.netapp.com	Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der BlueXP-Website zur zentralen Benutzerauthentifizierung.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	Die BlueXP Klassifizierung ermöglicht den Zugriff auf Manifeste und Vorlagen sowie das Senden von Protokollen und Kennzahlen.

Erforderliche Endpunkte für Azure

Endpunkte	Zweck
https://api.bluexp.netapp.com	Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der BlueXP-Website zur zentralen Benutzerauthentifizierung.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden.
https://support.compliance.api.bluexp.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.

Erforderliche Endpunkte für GCP

Endpunkte	Zweck
https://api.bluexp.netapp.com	Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der BlueXP-Website zur zentralen Benutzerauthentifizierung.

Endpunkte	Zweck
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden.
https://support.compliance.api.bluexp.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.

Stellen Sie sicher, dass BlueXP über die erforderlichen Berechtigungen verfügt

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

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

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

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

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

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

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

Webbrowser-Konnektivität zur BlueXP Klassifizierung sicherstellen

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

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

Überprüfen Sie Ihre vCPU-Limits

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

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

- "AWS Dokumentation: Amazon EC2 Service Quotas"

- "Azure Dokumentation: VCPU Kontingente von Virtual Machines"
- "Google Cloud Dokumentation: Ressourcenkontingente"

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

Implementieren Sie die BlueXP Klassifizierung in der Cloud

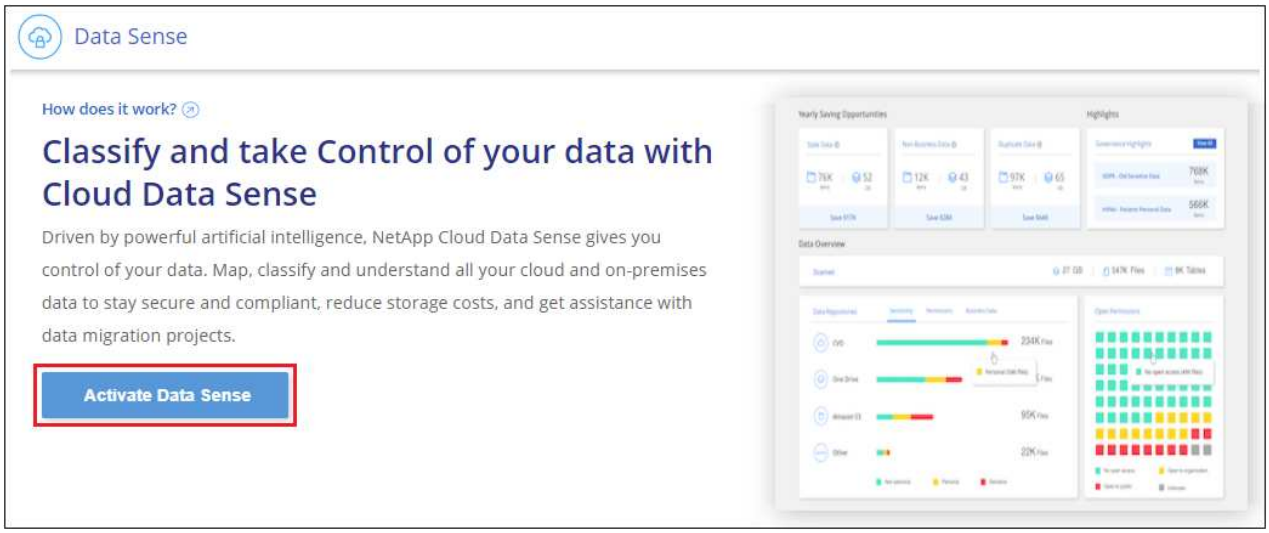
Führen Sie diese Schritte aus, um eine Instanz der BlueXP Klassifizierung in der Cloud zu implementieren. Der Connector implementiert die Instanz in der Cloud und installiert dann die BlueXP Klassifizierungssoftware auf dieser Instanz.

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

Implementieren in AWS

Schritte

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



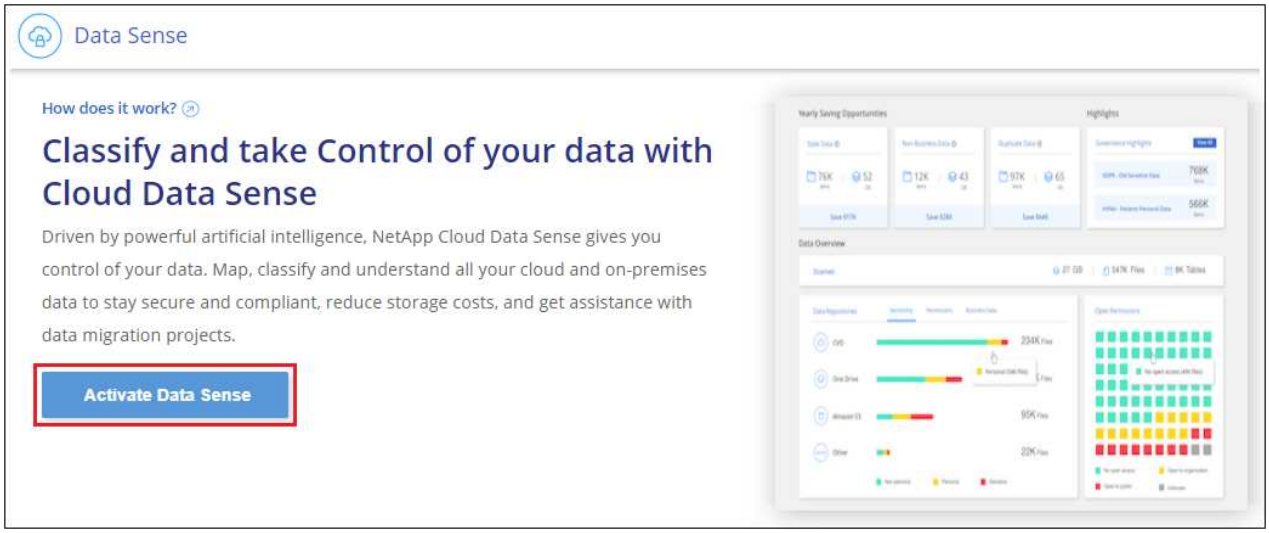
2. Klicken Sie Auf **Datensense Aktivieren**.
3. Klicken Sie auf der Seite *Installation* auf **Deploy > Deploy**, um die „große“ Instanzgröße zu verwenden und den Cloud-Bereitstellungsassistenten zu starten.
4. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Es wird angehalten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

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

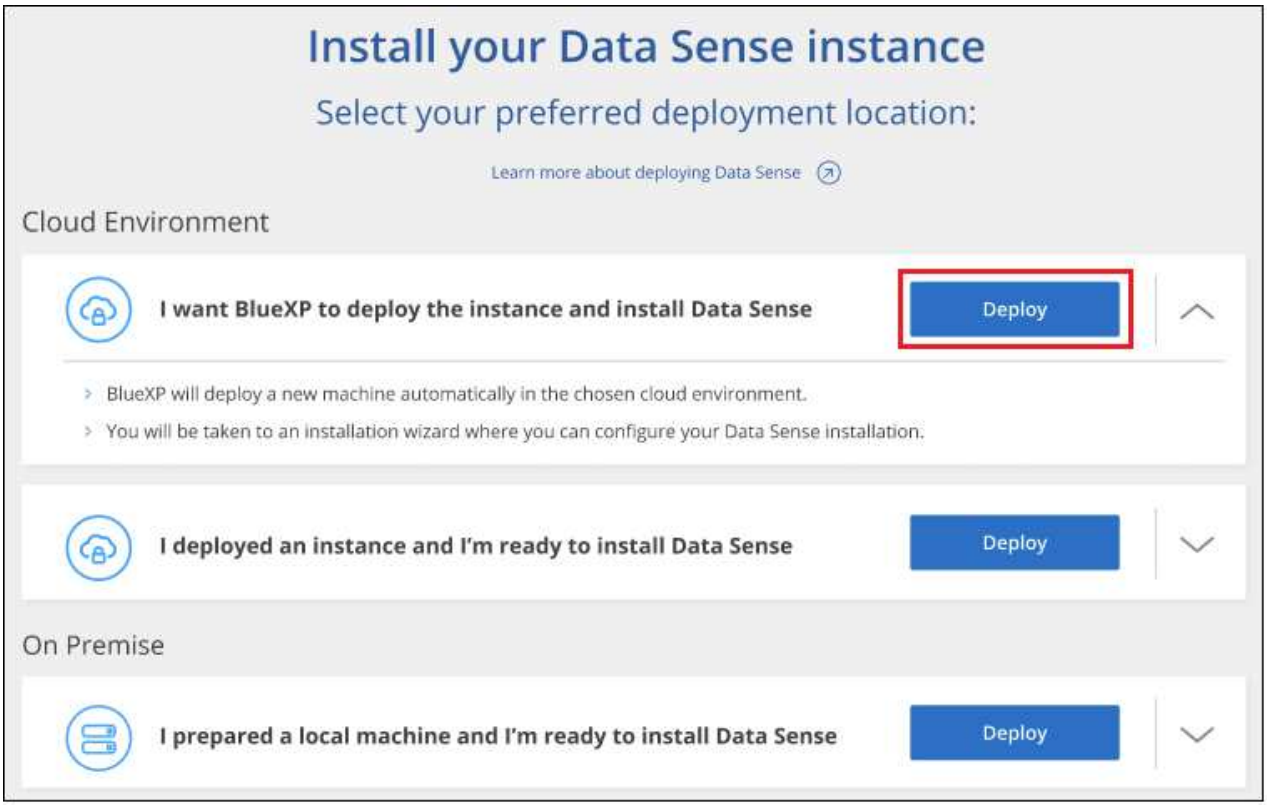
Implementieren in Azure

Schritte

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



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



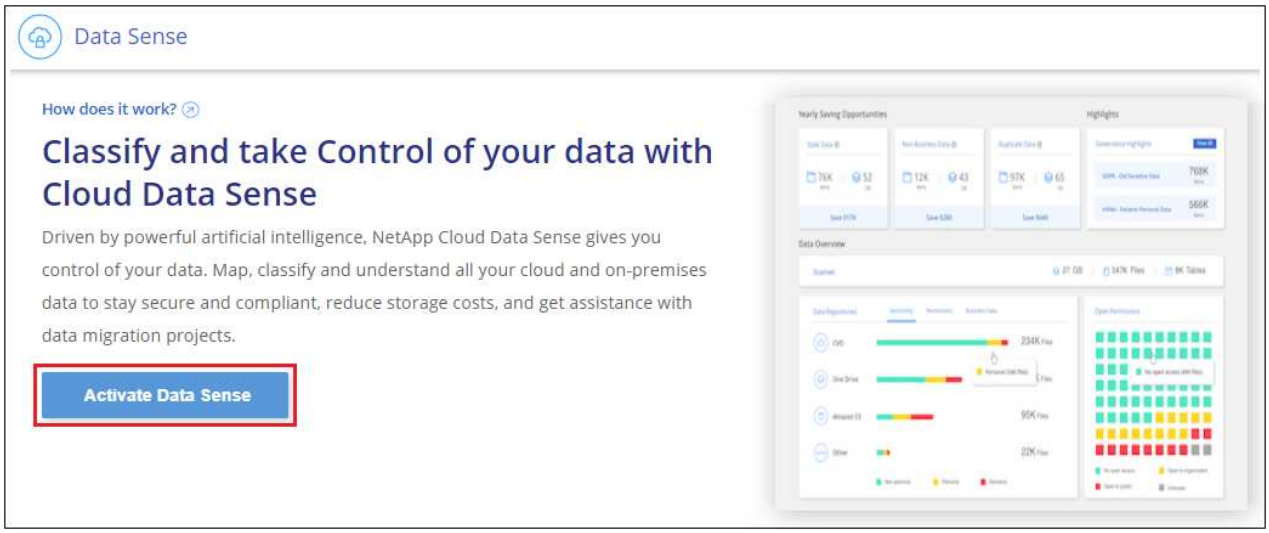
4. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Es wird angehalten und zur Eingabe aufgefordert, wenn Probleme auftreten.

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

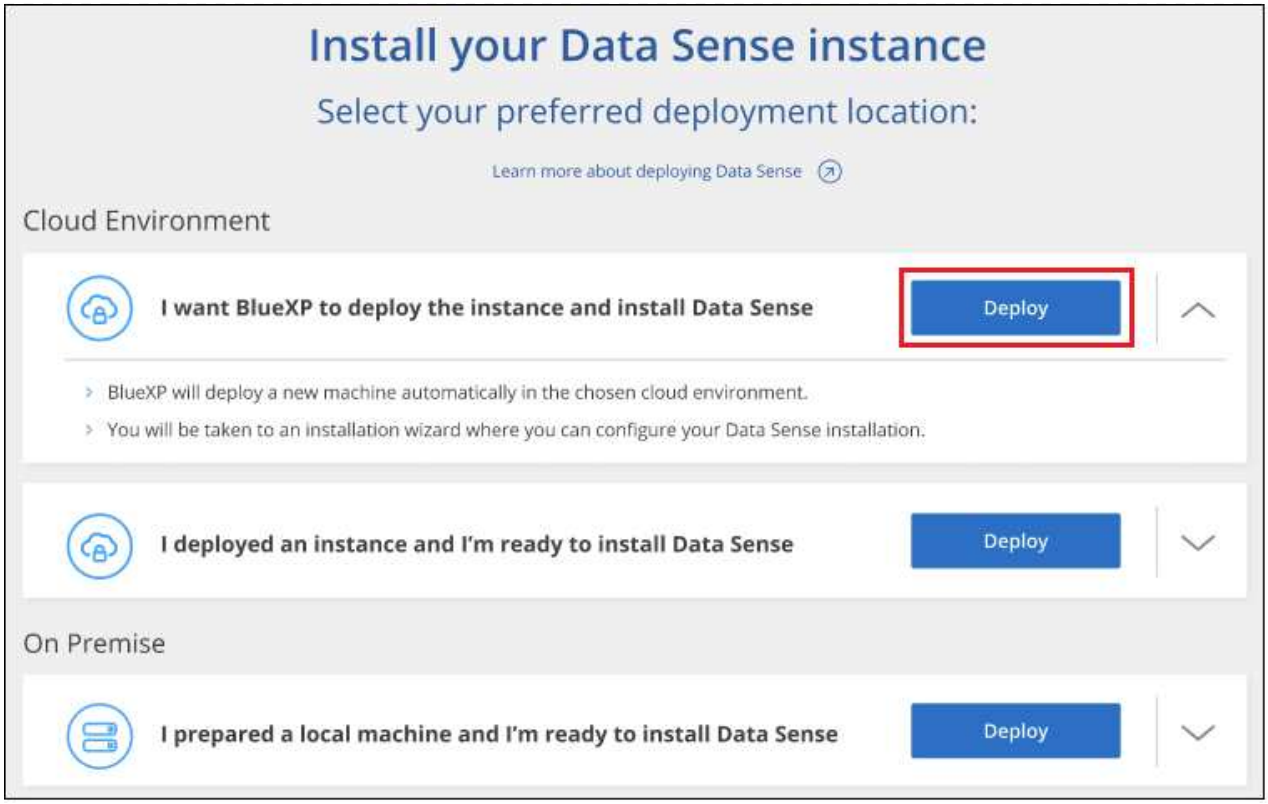
Implementieren in Google Cloud

Schritte

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



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



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

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

Ergebnis

BlueXP implementiert die BlueXP Klassifizierungsinstanz in Ihrem Cloud-Provider.

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

Nächste Schritte

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

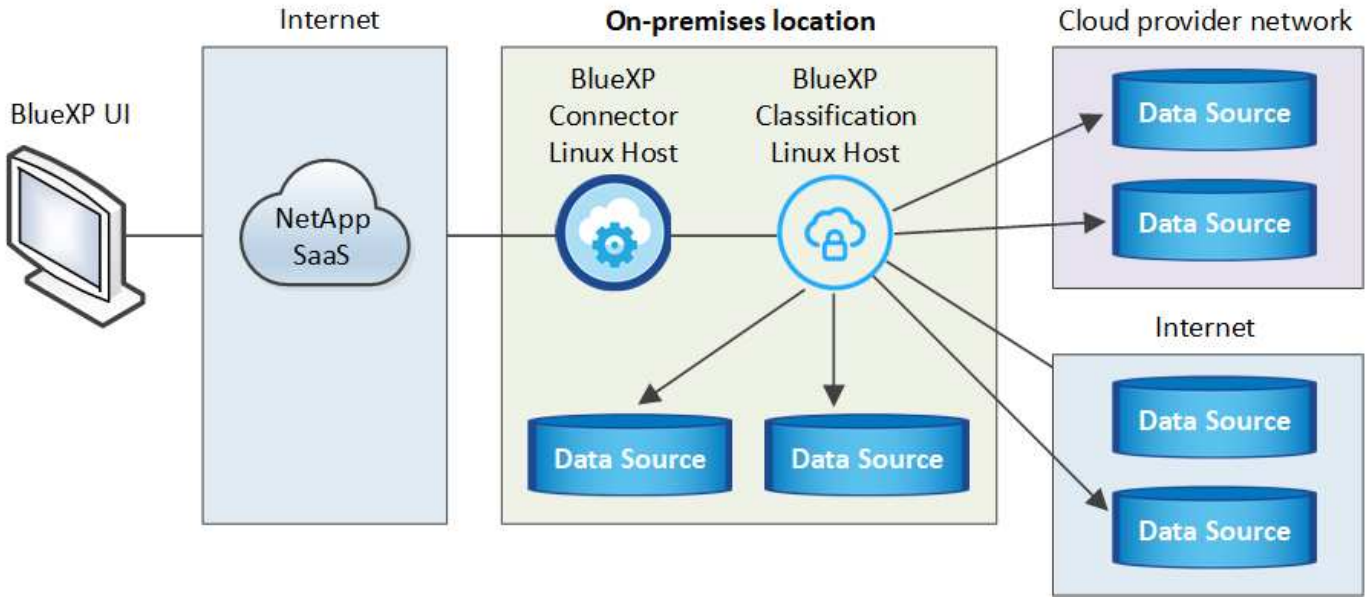
Installieren Sie die BlueXP Klassifizierung auf einem Host mit Internetzugang

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

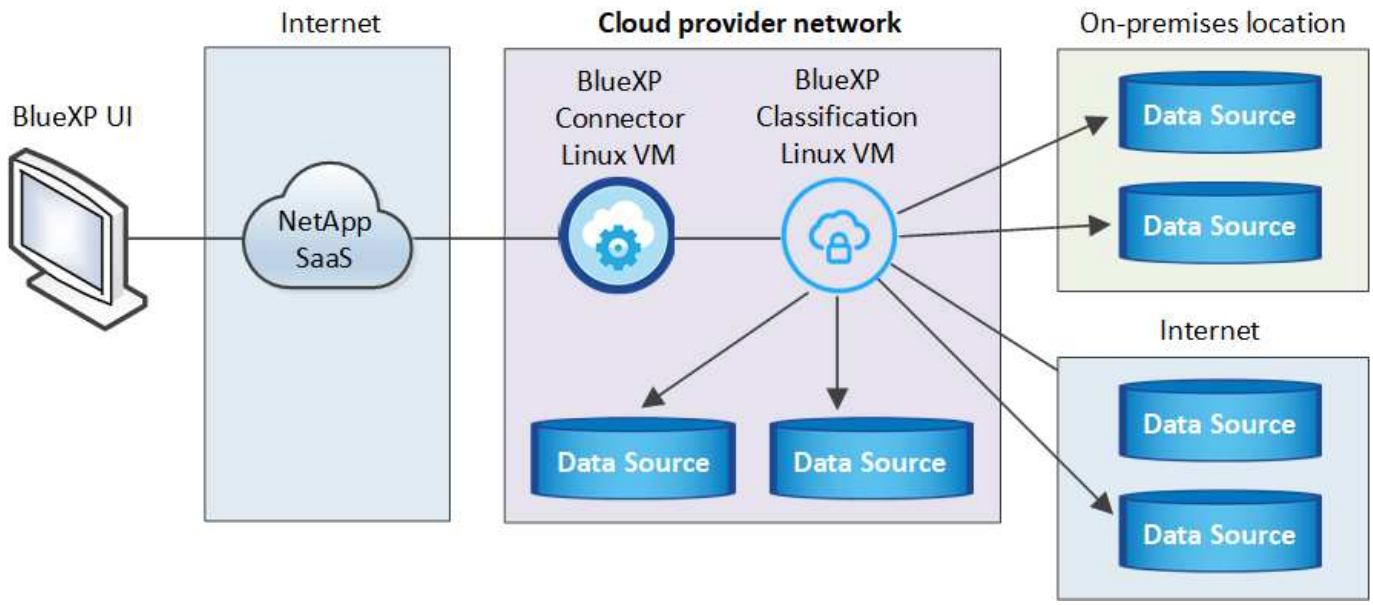
Die On-Premises-Installation ist möglicherweise eine gute Option, wenn Sie On-Premises-ONTAP Systeme mit einer BlueXP Klassifizierungsinstanz scannen möchten, die sich auch vor Ort befindet – dies ist jedoch keine Anforderung. Die Software funktioniert unabhängig von der gewählten Installationsmethode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

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

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



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



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

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

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

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

Schnellstart

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

1 Einen Konnektor erstellen

Falls Sie noch keinen Connector haben, "Stellen Sie den Connector vor Ort bereit" Auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud.

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

2 Voraussetzungen prüfen

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

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

3 Laden Sie die BlueXP Klassifizierung herunter und implementieren Sie sie

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

Einen Konnektor erstellen

Ein BlueXP Connector ist erforderlich, bevor Sie die BlueXP Klassifizierung installieren und verwenden können. In den meisten Fällen ist wahrscheinlich vor der Aktivierung der BlueXP Klassifizierung ein Connector eingerichtet. Die meisten dieser Funktionen sind jedoch vorhanden "Für BlueXP-Funktionen ist ein Connector erforderlich", Aber es gibt Fälle, in denen Sie müssen, um eine Einrichtung jetzt.

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

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

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

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

- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP wird ein Connector in GCP verwendet.

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

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

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

Bereiten Sie das Linux-Hostsystem vor

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

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

- Die BlueXP Klassifizierung wird auf einem Host, der mit anderen Applikationen gemeinsam genutzt wird,

nicht unterstützt – der Host muss ein dedizierter Host sein.

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

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

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

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

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

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

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

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

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

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

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

      Wenn Sie planen, zusätzliche BlueXP Klassifizierungs-Hosts als Scanner-Nodes zu verwenden, fügen Sie diese Regeln derzeit Ihrem Primärsystem hinzu:

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

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

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

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

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

Endpunkte	Zweck
https://api.bluexp.netapp.com	Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der BlueXP-Website zur zentralen Benutzerauthentifizierung.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden.
https://support.compliance.api.bluexp.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://github.com/docker https://download.docker.com	Enthält die erforderlichen Pakete für die Installation von Dockern.
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Enthält die erforderlichen Pakete für die CentOS-Installation.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Enthält die erforderlichen Pakete für die Ubuntu-Installation.

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

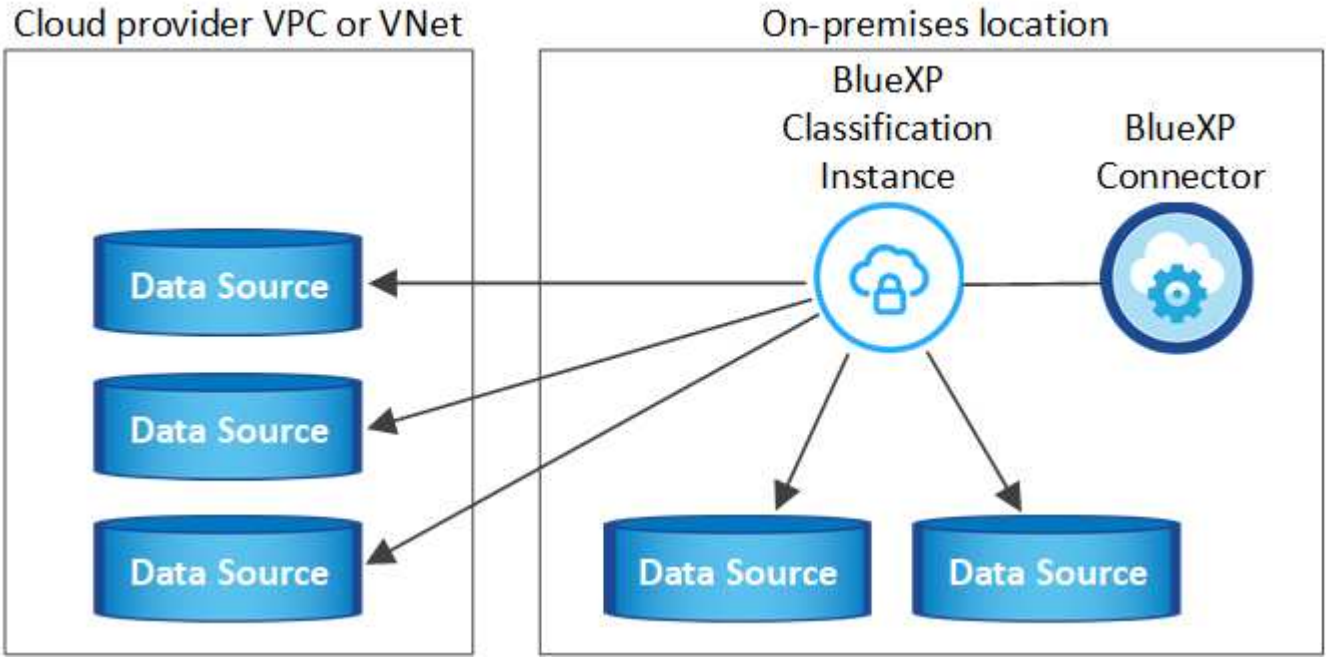
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 443 (TCP) und 80	Die Firewall- oder Routing-Regeln für den Connector müssen ein- und ausgehenden Datenverkehr über Port 443 zur und von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass Port 8080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

Verbindungstyp	Ports	Beschreibung
Connector <> ONTAP-Cluster (NAS)	443 (TCP)	BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen: • Der Connector-Host muss ausgehenden HTTPS-Zugriff über Port 443 ermöglichen. Wenn sich der Connector in der Cloud befindet, ist die gesamte ausgehende Kommunikation durch vordefinierte Firewall- oder Routingregeln zulässig. • Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen. Die standardmäßige "mgmt"-Firewall-Richtlinie ermöglicht eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert haben oder wenn Sie eine eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff über den Connector-Host aktivieren.
BlueXP Klassifizierung <> ONTAP Cluster	• Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS - 139 (TCP\UDP) und 445 (TCP\UDP)	Für die BlueXP Klassifizierung benötigen Sie eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder Ihrem lokalen ONTAP System. Firewalls oder Routingregeln für Cloud Volumes ONTAP müssen eingehende Verbindungen von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind: • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.

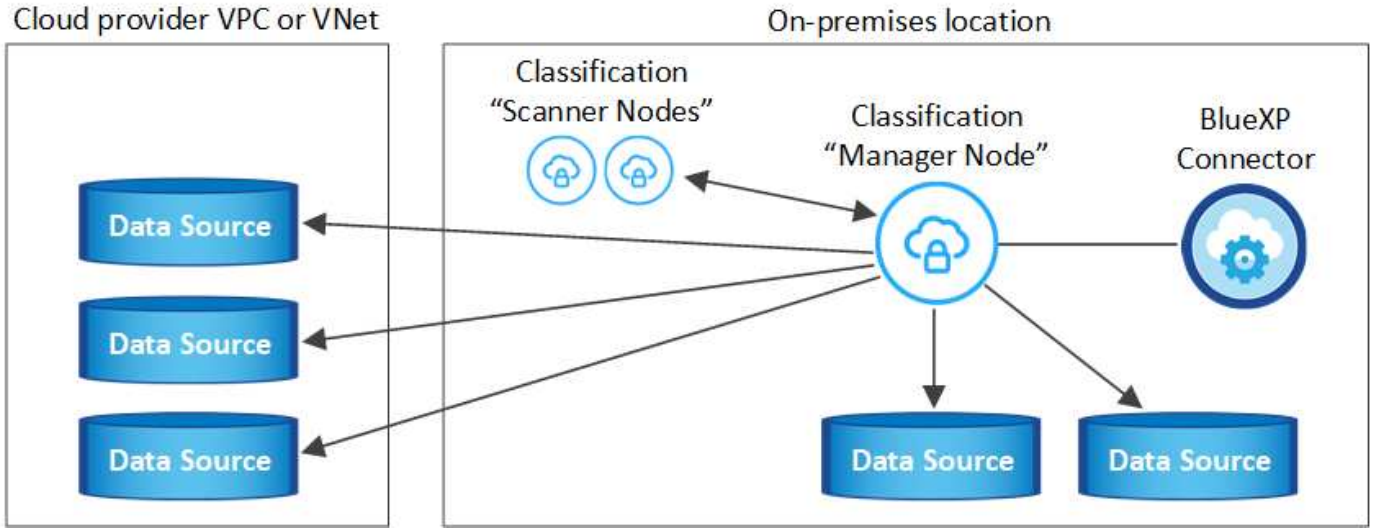
Verbindungstyp	Ports	Beschreibung
BlueXP Klassifizierung <> Active Directory	389 (TCP & UDP), 636 (TCP), 3268 (TCP) UND 3269 (TCP)	Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben. Darüber hinaus sind für die BlueXP Klassifizierung Active Directory Anmeldeinformationen erforderlich, um CIFS-Volumes zu scannen. Sie müssen über die folgenden Informationen für das Active Directory verfügen: • DNS-Server-IP-Adresse oder mehrere IP-Adressen • Benutzername und Kennwort für den Server • Domain-Name (Active Directory-Name) • Ob Sie Secure LDAP (LDAPS) verwenden oder nicht • LDAP-Server-Port (normalerweise 389 für LDAP und 636 für sicheres LDAP)

BlueXP Klassifizierung auf dem Linux-Host installieren

Für typische Konfigurationen installieren Sie die Software auf einem einzigen Host-System. Siehe diese Schritte hier.



Bei sehr großen Konfigurationen, bei denen Sie Petabyte an Daten scannen, können Sie mehrere Hosts einschließen, um zusätzliche Verarbeitungsleistung zu schaffen. Weitere Informationen Link:Task-deploy-multi-Host-install-dark-site.HTML> über die Installation auf mehreren Hosts für große Konfigurationen.



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

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

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

Installation mit einem Host für typische Konfigurationen

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

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

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

Was Sie benötigen

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

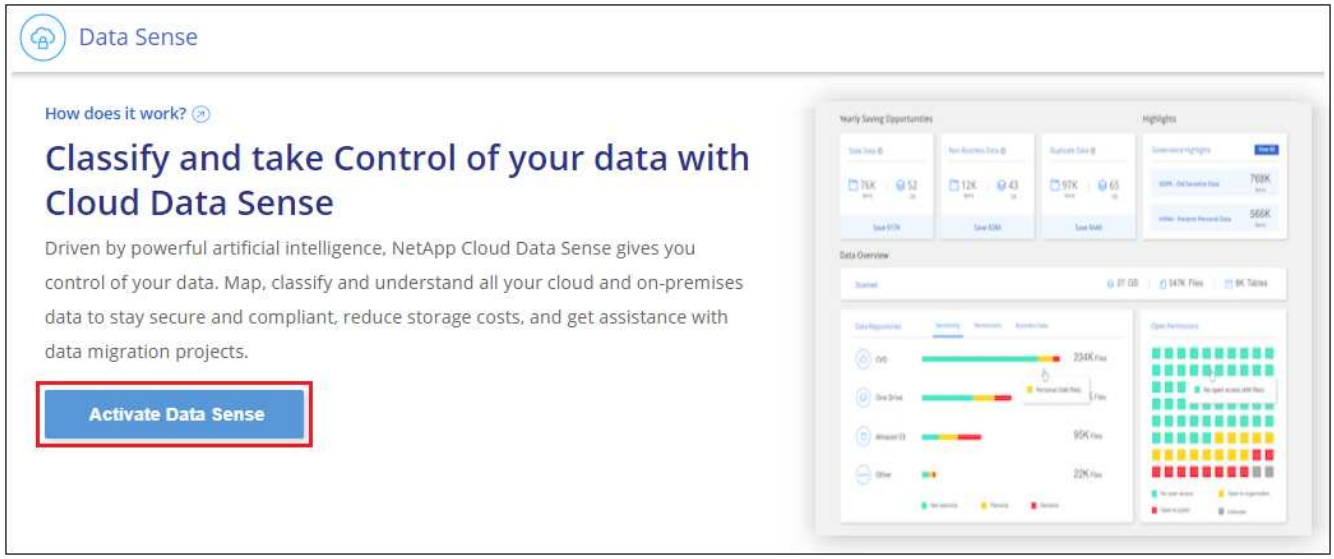
- Vergewissern Sie sich, dass die erforderliche Offline-Umgebung erfüllt ist Berechtigungen und Konnektivität.

Schritte

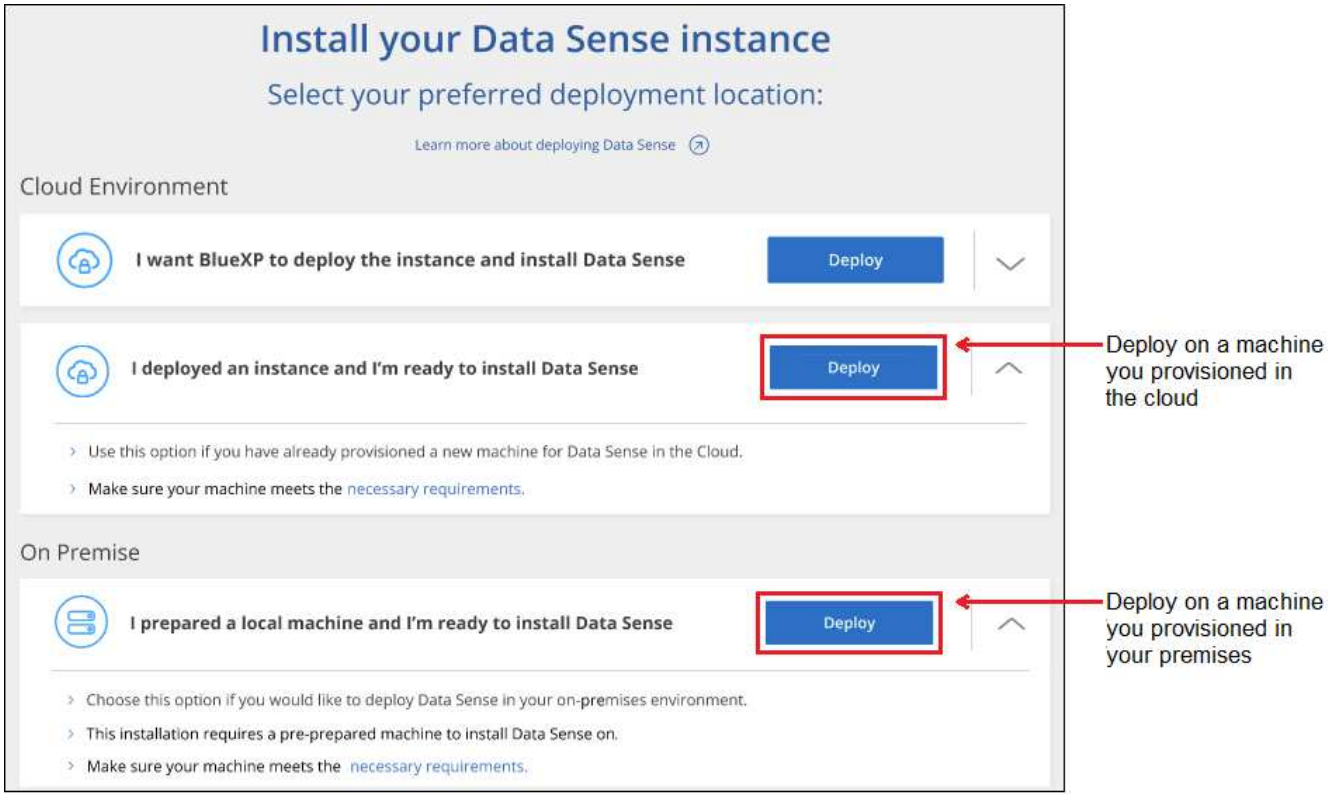
1. Laden Sie die BlueXP Klassifizierungssoftware von herunter "NetApp Support Website". Die ausgewählte Datei heißt **DATASENSE-INSTALLER-<Version>.tar.gz**.
2. Kopieren Sie die Installationsdatei auf den Linux-Host, den Sie verwenden möchten (mit `scp` Oder eine andere Methode).
3. Entpacken Sie die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

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

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



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



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

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

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

Variablenwerte:

- *Account_id* = NetApp Konto-ID
- *Client_id* = Konnektor-Client-ID (fügen Sie der Client-ID das Suffix „Clients“ hinzu, falls es noch nicht vorhanden ist)
- *User_Token* = JWT-Benutzer-Zugriffstoken
- *ds_Host* = IP-Adresse oder Hostname des BlueXP Klassifizierungs-Linux-Systems.
- *Cm_Host* = IP-Adresse oder Hostname des BlueXP Connector-Systems.
- *Cloud_Provider* = Geben Sie bei der Installation auf einer Cloud-Instanz je nach Cloud-Provider „AWS“, „Azure“ oder „GCP“ ein.
- *Proxy_Host* = IP oder Hostname des Proxy-Servers, wenn sich der Host hinter einem Proxy-Server befindet.
- *Proxy_Port* = Port zur Verbindung mit dem Proxy-Server (Standard 80).
- *Proxy_Schema* = Verbindungsschema: https oder http (Standard http).
- *Proxy_User* = authentifizierter Benutzer zur Verbindung mit dem Proxy-Server, falls eine grundlegende Authentifizierung erforderlich ist. Der Benutzer muss ein lokaler Benutzer sein – Domänenbenutzer werden nicht unterstützt.
- *Proxy_Password* = Passwort für den von Ihnen angegebenen Benutzernamen.
- *Ca_cert_dir* = Pfad auf dem BlueXP-Klassifizierungs-Linux-System mit zusätzlichen TLS-CA-Zertifikatbundles. Nur erforderlich, wenn der Proxy TLS Abfangen durchführt.

Ergebnis

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

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

Nächste Schritte

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

BlueXP Klassifizierung auf einem Linux-Host ohne Internetzugang installieren

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

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

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

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

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

Unterstützte Datenquellen

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

- On-Premises ONTAP Systeme
- Datenbankschemas

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

Einschränkungen

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

- Festlegen von BlueXP-Rollen für unterschiedliche Benutzer (z. B. Account Admin oder Compliance Viewer)
- Quelldateien werden mittels BlueXP Kopier- und Synchronisierungsfunktion kopiert und synchronisiert
- Automatisierte Software-Upgrades von BlueXP

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

Schnellstart

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

1 **Installieren Sie den BlueXP-Anschluss**

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

2 **Voraussetzungen für die BlueXP Klassifizierung prüfen**

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

3 **Laden Sie die BlueXP Klassifizierung herunter und implementieren Sie sie**

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

Installieren Sie den BlueXP-Anschluss

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

Bereiten Sie das Linux-Hostsystem vor

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Voraussetzungen für die Klassifizierung von BlueXP und BlueXP prüfen

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

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

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

nicht auf die indizierten Daten zugreifen können. Daher muss der Webbrowser, den Sie für den Zugriff auf BlueXP verwenden, über eine Verbindung mit dieser privaten IP-Adresse verfügen. Diese Verbindung kann von einem Host stammen, der sich im selben Netzwerk wie die BlueXP Klassifizierungsinstanz befindet.

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

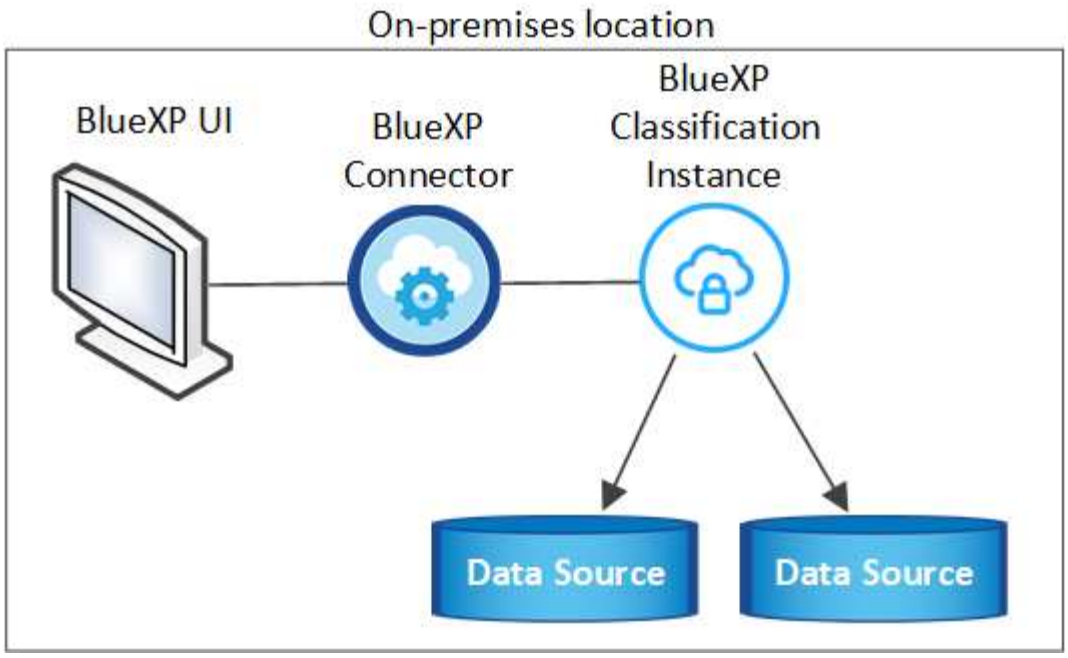
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 6000 (TCP), 443 (TCP) UND 80	Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über die Ports 6000 und 443 zur und von der BlueXP Klassifizierungsinstanz zulassen. • Port 6000 ist erforderlich, damit die BYOL-Lizenz für die BlueXP Klassifizierung an einem Dark Site funktioniert. • Port 8080 sollte offen sein, damit Sie den Installationsfortschritt in BlueXP sehen können.
Connector <> ONTAP-Cluster (NAS)	443 (TCP)	BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen: • Der Connector-Host muss ausgehenden HTTPS-Zugriff über Port 443 ermöglichen. Wenn sich der Connector in der Cloud befindet, ist die gesamte ausgehende Kommunikation durch die vordefinierte Sicherheitsgruppe zulässig. • Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen. Die standardmäßige "mgmt"-Firewall-Richtlinie ermöglicht eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert haben oder wenn Sie eine eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff über den Connector-Host aktivieren.

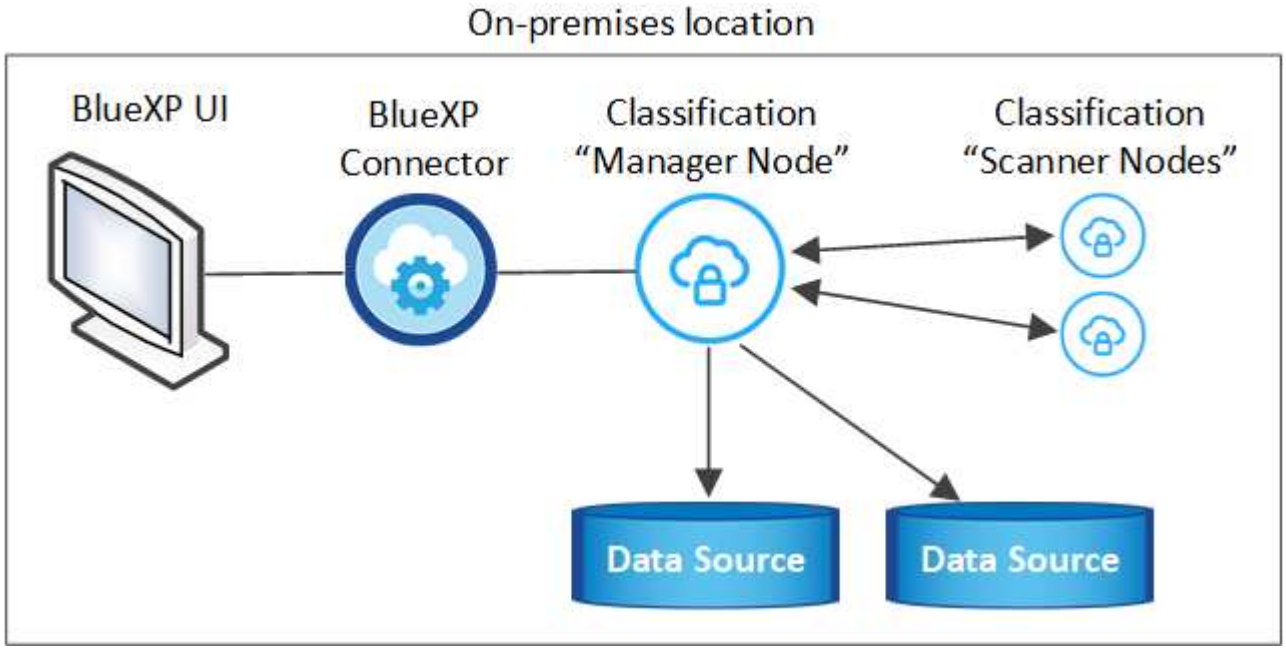
Verbindungstyp	Ports	Beschreibung
BlueXP Klassifizierung <> ONTAP Cluster	• Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS - 139 (TCP\UDP) und 445 (TCP\UDP)	Für die BlueXP Klassifizierung benötigen Sie eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder Ihrem lokalen ONTAP System. Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind: • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.
BlueXP Klassifizierung <> Active Directory	389 (TCP & UDP), 636 (TCP), 3268 (TCP) UND 3269 (TCP)	Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben. Darüber hinaus sind für die BlueXP Klassifizierung Active Directory Anmeldeinformationen erforderlich, um CIFS-Volumes zu scannen. Sie müssen über die folgenden Informationen für das Active Directory verfügen: • DNS-Server-IP-Adresse oder mehrere IP-Adressen • Benutzername und Kennwort für den Server • Domain-Name (Active Directory-Name) • Ob Sie Secure LDAP (LDAPS) verwenden oder nicht • LDAP-Server-Port (normalerweise 389 für LDAP und 636 für sicheres LDAP)

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

BlueXP Klassifizierung auf dem lokalen Linux-Host installieren

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





Installation mit einem Host für typische Konfigurationen

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

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

Was Sie benötigen

- Vergewissern Sie sich, dass Ihr Linux-System die erfüllt Host-Anforderungen erfüllt.
- Überprüfen Sie, ob Sie die beiden erforderlichen Softwarepakete (Docker Engine oder Podman und Python 3) installiert haben.

- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.
- Vergewissern Sie sich, dass die erforderliche Offline-Umgebung erfüllt ist Berechtigungen und Konnektivität.

Schritte

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

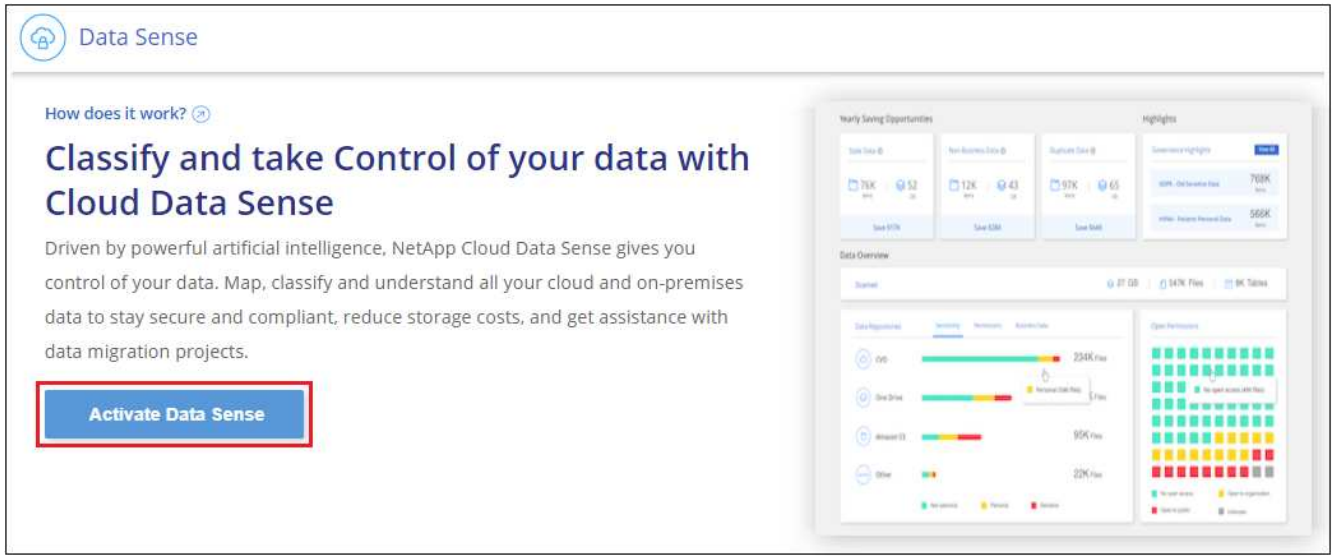
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

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

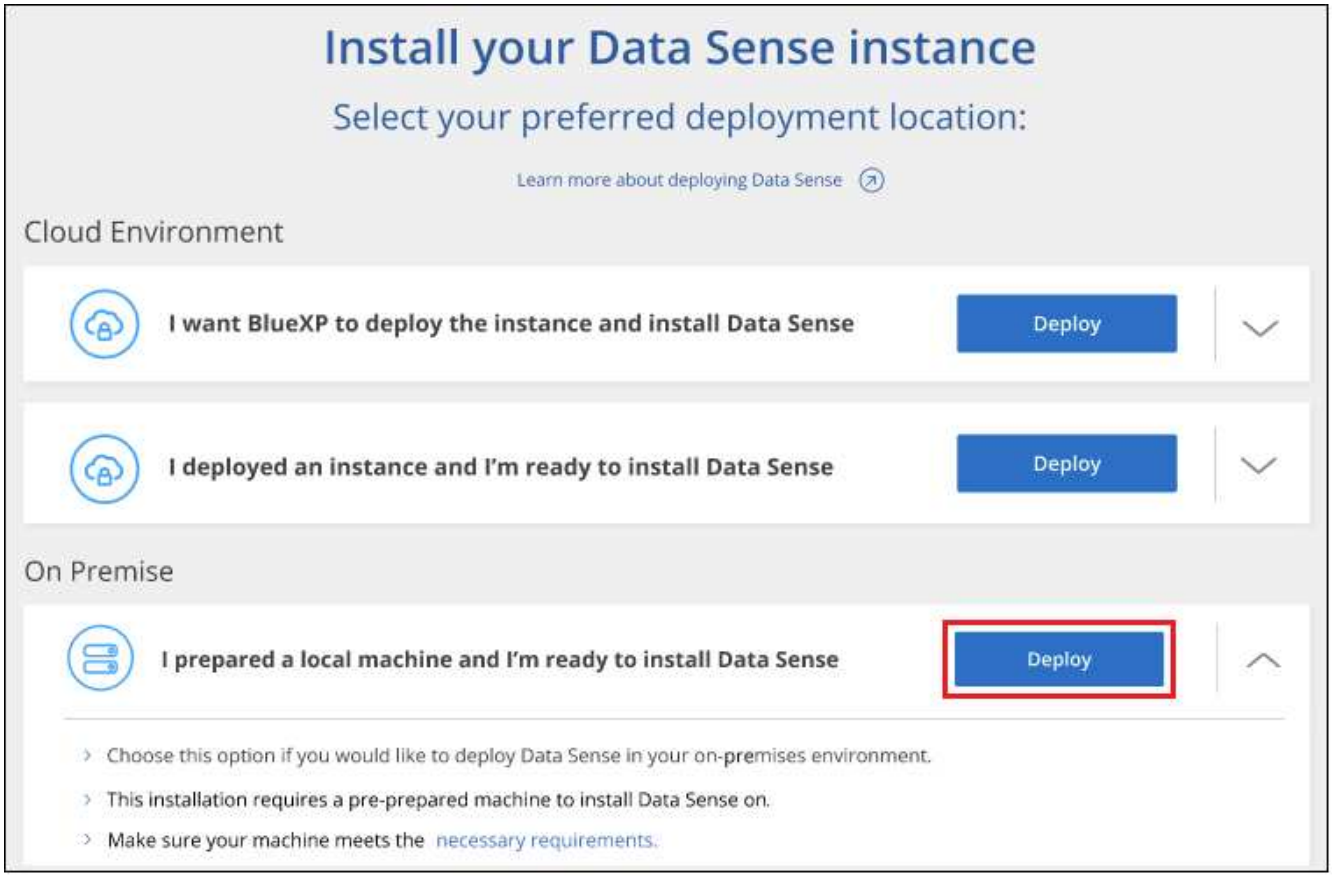
4. Entpacken Sie die Installationsdatei auf dem Host-Rechner, z. B.:

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

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



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



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

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

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

Variablenwerte:

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

Ergebnis

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

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

Nächste Schritte

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

Upgrade der BlueXP Klassifizierungssoftware

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

Bevor Sie beginnen

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

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

Schritte

1. Laden Sie die BlueXP Klassifizierungssoftware auf einem internetkonfigurierten System von der herunter "NetApp Support Website". Die ausgewählte Datei heißt **DataSense-offline-Bundle-<Version>.tar.gz**.
2. Kopieren Sie das Software-Bundle auf den Linux-Host, auf dem die BlueXP Klassifizierung am Dark Site installiert ist.
3. Entpacken Sie das Software-Bundle auf dem Host-Rechner, zum Beispiel:

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

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

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

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

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

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

```
start_darksite_upgrade.sh
```

Ergebnis

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

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

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

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

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

Erste Schritte

Sie führen die folgenden Aufgaben aus.

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

Einen Konnektor erstellen

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

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

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

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

Host-Anforderungen prüfen

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

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

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

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

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

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

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

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

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

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

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

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

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

Wenn Sie planen, zusätzliche BlueXP Klassifizierungs-Hosts als Scanner-Nodes (in einem verteilten Modell) zu verwenden, fügen Sie derzeit diese Regeln Ihrem Primärsystem hinzu:

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

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

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

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

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

Endpunkte	Zweck
https://api.bluexp.netapp.com	Kommunikation mit dem BlueXP Service, einschl. NetApp Accounts
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der BlueXP-Website zur zentralen Benutzerauthentifizierung.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste, Vorlagen und die Möglichkeit, Protokolle und Metriken zu senden.
https://support.compliance.api.bluexp.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://github.com/docker https://download.docker.com	Enthält die erforderlichen Pakete für die Installation von Dockern.

Endpunkte	Zweck
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Enthält die erforderlichen Pakete für die CentOS-Installation.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Enthält die erforderlichen Pakete für die Ubuntu-Installation.

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

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

Führen Sie das Skript für die Klassifizierungsvoraussetzungen von BlueXP aus

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

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

Was Sie benötigen

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

Schritte

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

3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

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

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

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

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

Ergebnis

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

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

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