Datenklassifizierung bereitstellen

NetApp Data Classification

NetApp
January 26, 2026

Inhalt

Datenklassifizierung bereitstellen

Welche NetApp Data Classification Bereitstellung sollten Sie verwenden?

Sie können NetApp Data Classification auf verschiedene Arten bereitstellen. Erfahren Sie, welche Methode Ihren Anforderungen entspricht.

Die Datenklassifizierung kann auf folgende Arten bereitgestellt werden:

- "Bereitstellung in der Cloud mithilfe der Konsole" . Die Konsole stellt die Datenklassifizierungsinstanz im selben Cloud-Anbieternetzwerk bereit wie der Konsolenagent.
- "Installation auf einem Linux-Host mit Internetzugang" . Installieren Sie Data Classification auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud, der über Internetzugang verfügt. Diese Art der Installation kann eine gute Option sein, wenn Sie lokale ONTAP -Systeme lieber mit einer Datenklassifizierungsinstanz scannen möchten, die sich ebenfalls vor Ort befindet. Dies ist jedoch keine Voraussetzung.
- "Installation auf einem Linux-Host an einem lokalen Standort ohne Internetzugang", auch als *privater Modus* bekannt. Dieser Installationstyp, der ein Installationsskript verwendet, hat keine Verbindung zur SaaS-Ebene der Konsole.

> Der private BlueXP Modus (alte BlueXP -Schnittstelle) wird normalerweise in lokalen Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, darunter AWS Secret Cloud, AWS Top Secret Cloud und Azure IL6. NetApp unterstützt diese Umgebungen weiterhin mit der alten BlueXP Schnittstelle. Die Dokumentation zum privaten Modus in der alten BlueXP Schnittstelle finden Sie unter"PDF-Dokumentation für den privaten Modus von BlueXP" .

Sowohl die Installation auf einem Linux-Host mit Internetzugang als auch die lokale Installation auf einem Linux-Host ohne Internetzugang verwenden ein Installationsskript. Das Skript prüft zunächst, ob das System und die Umgebung die Voraussetzungen erfüllen. Wenn die Voraussetzungen erfüllt sind, beginnt die Installation. Wenn Sie die Voraussetzungen unabhängig von der Ausführung der Data Classification-Installation überprüfen möchten, können Sie ein separates Softwarepaket herunterladen, das nur die Voraussetzungen testet.

Weitere Informationen finden Sie unter "Überprüfen Sie, ob Ihr Linux-Host für die Installation der Datenklassifizierung bereit ist." .

Stellen Sie NetApp Data Classification mithilfe der NetApp Console in der Cloud bereit

Sie können NetApp Data Classification mit der NetApp Console in der Cloud bereitstellen. Die Konsole stellt die Datenklassifizierungsinstanz im selben Cloud-Anbieternetzwerk bereit wie der Konsolenagent.

Beachten Sie, dass Sie auch"Installieren Sie Data Classification auf einem Linux-Host mit Internetzugang" . Diese Art der Installation kann eine gute Option sein, wenn Sie es vorziehen, lokale ONTAP -Systeme mit einer Datenklassifizierungsinstanz zu scannen, die sich ebenfalls vor Ort befindet – dies ist jedoch keine Voraussetzung. Die Software funktioniert unabhängig von der gewählten Installationsmethode auf genau

dieselbe Weise.

Schnellstart

Beginnen Sie schnell, indem Sie diese Schritte befolgen, oder scrollen Sie nach unten zu den restlichen Abschnitten, um alle Einzelheiten zu erfahren.

Erstellen eines Konsolenagenten

Wenn Sie noch keinen Konsolenagenten haben, erstellen Sie einen. Sehen"Erstellen eines Konsolenagenten in AWS" ,"Erstellen eines Konsolenagenten in Azure" , oder"Erstellen eines Konsolenagenten in GCP" Die

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

Voraussetzungen

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllt. Dazu gehören ausgehender Internetzugang für die Instanz, Konnektivität zwischen dem Console-Agent und Data Classification über Port 443 und mehr. Vollständige Liste anzeigen.

Datenklassifizierung bereitstellen

Starten Sie den Installationsassistenten, um die Data Classification-Instanz in der Cloud bereitzustellen.

Erstellen eines Konsolenagenten

Wenn Sie noch keinen Konsolenagenten haben, erstellen Sie einen Konsolenagenten bei Ihrem Cloud-Anbieter. Sehen "Erstellen eines Konsolenagenten in AWS" oder "Erstellen eines Konsolenagenten in Azure" , oder "Erstellen eines Konsolenagenten in GCP" Die In den meisten Fällen werden Sie wahrscheinlich einen Konsolenagenten eingerichtet haben, bevor Sie versuchen, die Datenklassifizierung zu aktivieren, da die meisten "Für Konsolenfunktionen ist ein Konsolenagent erforderlich" Es gibt jedoch Fälle, in denen Sie jetzt einen einrichten müssen.

Es gibt einige Szenarien, in denen Sie einen Konsolenagenten verwenden müssen, der bei einem bestimmten Cloud-Anbieter bereitgestellt wird:

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS oder Amazon FSx für ONTAP -Buckets verwenden Sie einen Konsolenagenten in AWS.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konsolenagenten in Azure.
  - Für Azure NetApp Files muss es in derselben Region bereitgestellt werden wie die Volumes, die Sie scannen möchten.
- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP verwenden Sie einen Konsolenagenten in GCP.

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

Beachten Sie, dass Sie auch "Installieren Sie den Konsolen-Agenten vor Ort" auf einem Linux-Host in Ihrem

Netzwerk oder in der Cloud. Einige Benutzer, die die Datenklassifizierung vor Ort installieren möchten, entscheiden sich möglicherweise auch für die Installation des Konsolenagenten vor Ort.

Es kann Situationen geben, in denen Sie verwenden müssen "mehrere Konsolenagenten" Die

> Die Datenklassifizierung setzt keine Begrenzung für die Menge der Daten, die gescannt werden kann. Jeder Konsolenagent unterstützt das Scannen und Anzeigen von 500 TiB Daten. Um mehr als 500 TiB Daten zu scannen,"einen anderen Konsolenagenten installieren" Dann"eine weitere Data Classification-Instanz bereitstellen" . + Die Konsolen-Benutzeroberfläche zeigt Daten von einem einzelnen Connector an. Tipps zum Anzeigen von Daten von mehreren Konsolenagenten finden Sie unter"Arbeiten mit mehreren Konsolenagenten" .

Unterstützung der Regierung in der Region

Die Datenklassifizierung wird unterstützt, wenn der Konsolenagent in einer Regierungsregion (AWS GovCloud, Azure Gov oder Azure DoD) bereitgestellt wird. Bei einer Bereitstellung auf diese Weise unterliegt die Datenklassifizierung den folgenden Einschränkungen:

"Erfahren Sie mehr über die Bereitstellung des Console-Agenten in einer Regierungsregion".

Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie die Datenklassifizierung in der Cloud bereitstellen. Wenn Sie die Datenklassifizierung in der Cloud bereitstellen, befindet sie sich im selben Subnetz wie der Konsolenagent.

Ausgehenden Internetzugriff von der Datenklassifizierung aus aktivieren

Für die Datenklassifizierung ist ein ausgehender Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxyserver für den Internetzugang verwendet, stellen Sie sicher, dass die Datenklassifizierungsinstanz über ausgehenden Internetzugang verfügt, um die folgenden Endpunkte zu kontaktieren. Der Proxy muss intransparent sein. Transparente Proxys werden derzeit nicht unterstützt.

Sehen Sie sich die entsprechende Tabelle unten an, je nachdem, ob Sie die Datenklassifizierung in AWS, Azure oder GCP bereitstellen.

Erforderliche Endpunkte für AWS

Endpunkte	Zweck
https://api.console.netapp.com	Kommunikation mit dem Konsolendienst, der NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-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 Prüfdatensätzen.
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	Ermöglicht der Datenklassifizierung den Zugriff auf und das Herunterladen von Manifesten und Vorlagen sowie das Senden von Protokollen und Metriken.

Erforderliche Endpunkte für Azure

Endpunkte	Zweck
https://api.console.netapp.com	Kommunikation mit dem Konsolendienst, der NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-Website zur zentralen Benutzerauthentifizierung.
https://support.compliance.api.console.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 ermöglicht das Senden von Protokollen und Metriken.
https://support.compliance.api.console.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Prüfdatensätzen.

Erforderliche Endpunkte für GCP

Endpunkte	Zweck
https://api.console.netapp.com	Kommunikation mit dem Konsolendienst, der NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-Website zur zentralen Benutzerauthentifizierung.

Endpunkte	Zweck
https://support.compliance.api.console.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 ermöglicht das Senden von Protokollen und Metriken.
https://support.compliance.api.console.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Prüfdatensätzen.

Stellen Sie sicher, dass die Datenklassifizierung über die erforderlichen Berechtigungen verfügt

Stellen Sie sicher, dass Data Classification über die Berechtigung zum Bereitstellen von Ressourcen und Erstellen von Sicherheitsgruppen für die Data Classification-Instanz verfügt.

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

Stellen Sie sicher, dass der Konsolenagent auf die Datenklassifizierung zugreifen kann.

Stellen Sie die Konnektivität zwischen dem Konsolenagenten und der Datenklassifizierungsinstanz sicher. Die Sicherheitsgruppe für den Konsolenagenten muss eingehenden und ausgehenden Datenverkehr über Port 443 zur und von der Datenklassifizierungsinstanz zulassen. Diese Verbindung ermöglicht die Bereitstellung der Datenklassifizierungsinstanz und ermöglicht Ihnen die Anzeige von Informationen auf den Registerkarten „Compliance“ und „Governance“. Die Datenklassifizierung wird in Regierungsregionen in AWS und Azure unterstützt.

Für AWS- und AWS GovCloud-Bereitstellungen sind zusätzliche Sicherheitsgruppenregeln für eingehenden und ausgehenden Datenverkehr erforderlich. Sehen "Regeln für den Konsolenagenten in AWS" für Details.

Für Azure- und Azure Government-Bereitstellungen sind zusätzliche Sicherheitsgruppenregeln für eingehenden und ausgehenden Datenverkehr erforderlich. Sehen "Regeln für den Konsolen-Agent in Azure" für Details.

Stellen Sie sicher, dass die Datenklassifizierung weiterhin ausgeführt werden kann

Die Instanz zur Datenklassifizierung muss eingeschaltet bleiben, um Ihre Daten kontinuierlich zu scannen.

Sicherstellen der Webbrowser-Konnektivität zur Datenklassifizierung

Stellen Sie nach der Aktivierung der Datenklassifizierung sicher, dass Benutzer von einem Host aus auf die Konsolenschnittstelle zugreifen, der über eine Verbindung zur Datenklassifizierungsinstanz verfügt.

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

Überprüfen Sie Ihre vCPU-Grenzen

Stellen Sie sicher, dass das vCPU-Limit Ihres Cloud-Anbieters die Bereitstellung einer Instanz mit der erforderlichen Anzahl von Kernen zulässt. Sie müssen das vCPU-Limit für die entsprechende Instanzfamilie in der Region überprüfen, in der die Konsole ausgeführt wird. "Sehen Sie sich die erforderlichen

Instanztypen an" .

Weitere Einzelheiten zu vCPU-Grenzwerten finden Sie unter den folgenden Links:

- "AWS-Dokumentation: Amazon EC2-Servicekontingente"
- "Azure-Dokumentation: vCPU-Kontingente virtueller Computer"
- "Google Cloud-Dokumentation: Ressourcenkontingente"

Datenklassifizierung in der Cloud bereitstellen

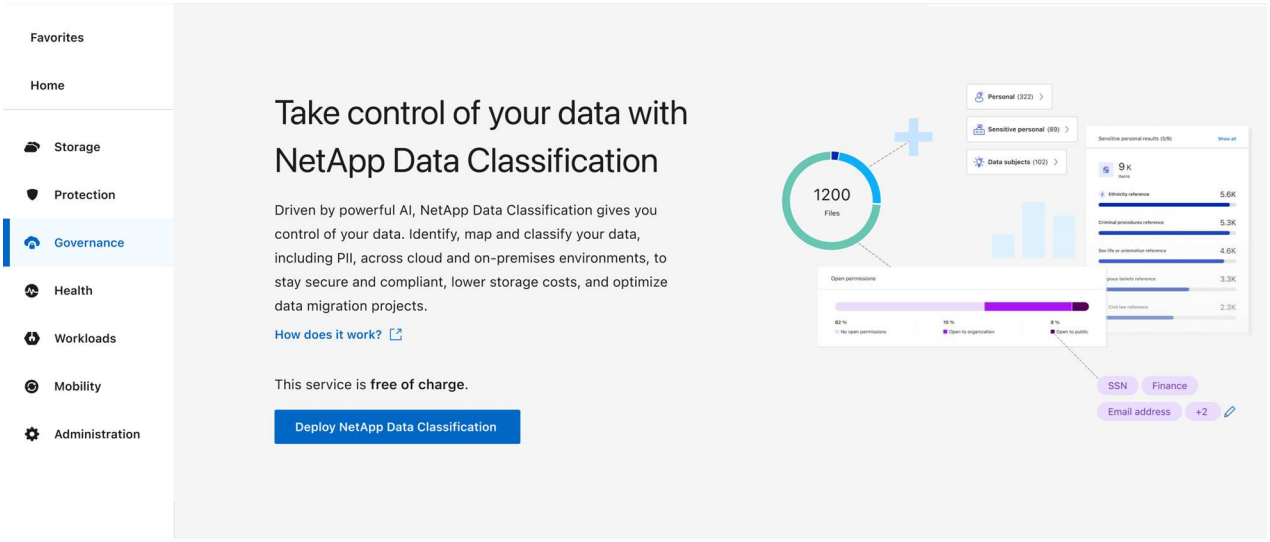
Befolgen Sie diese Schritte, um eine Instanz von Data Classification in der Cloud bereitzustellen. Der Konsolenagent stellt die Instanz in der Cloud bereit und installiert dann die Datenklassifizierungssoftware auf dieser Instanz.

In Regionen, in denen der Standardinstanztyp nicht verfügbar ist, läuft die Datenklassifizierung auf einem"alternativer Instanztyp" .

Bereitstellung in AWS

Schritte

1. Wählen Sie auf der Hauptseite der Datenklassifizierung die Option **Klassifizierung vor Ort oder in der Cloud bereitstellen**.

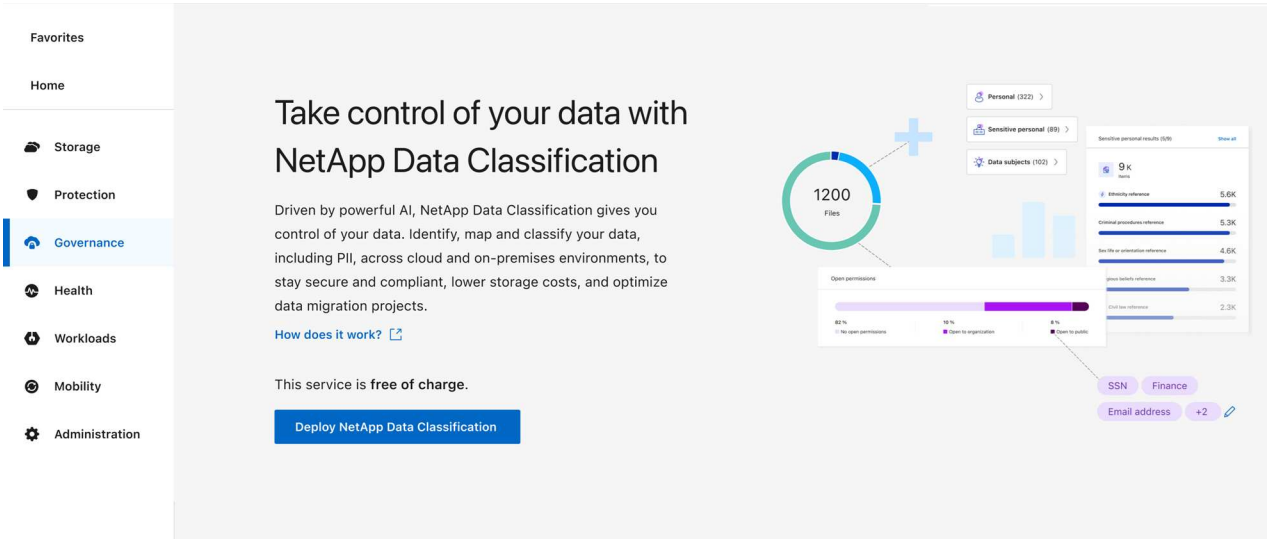


2. Wählen Sie auf der Seite „Installation“ die Option „Bereitstellen > Bereitstellen“ aus, um die Instanzgröße „Groß“ zu verwenden und den Cloud-Bereitstellungsassistenten zu starten.
3. Der Assistent zeigt den Fortschritt an, während er die Bereitstellungsschritte durchläuft. Wenn Eingaben erforderlich sind oder Probleme auftreten, werden Sie dazu aufgefordert.
4. Wenn die Instanz bereitgestellt und die Datenklassifizierung installiert ist, wählen Sie **Weiter zur Konfiguration**, um zur Seite *Konfiguration* zu gelangen.

Bereitstellen in Azure

Schritte

1. Wählen Sie auf der Hauptseite der Datenklassifizierung die Option **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



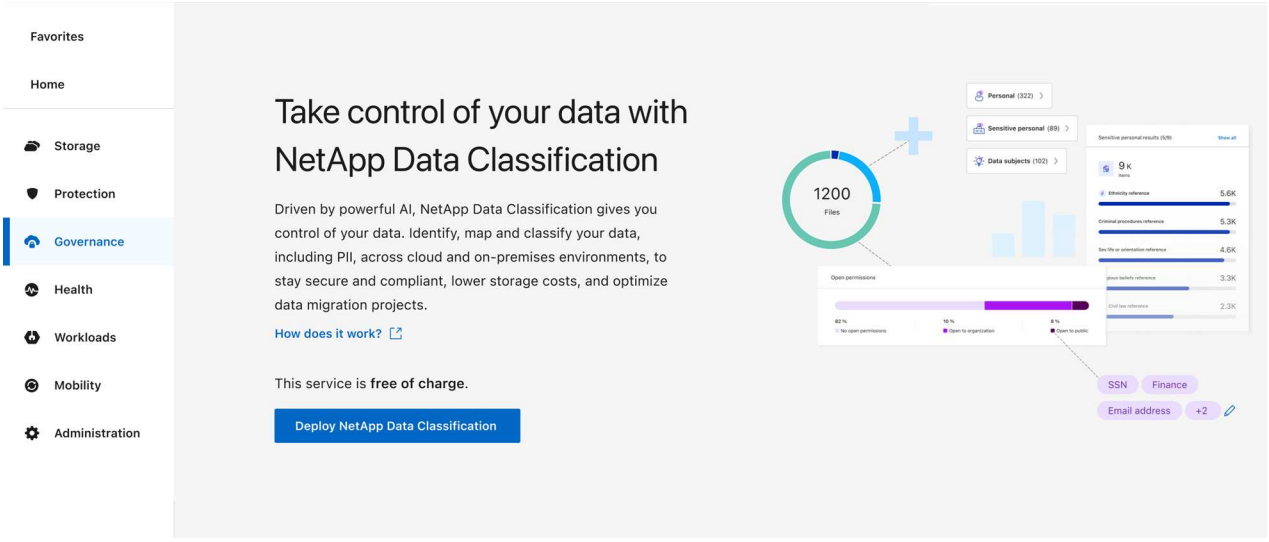
2. Wählen Sie **Bereitstellen**, um den Cloud-Bereitstellungsassistenten zu starten.

3. Der Assistent zeigt den Fortschritt an, während er die Bereitstellungsschritte durchläuft. Wenn Probleme auftreten, wird es angehalten und zur Eingabe aufgefordert.
4. Wenn die Instanz bereitgestellt und die Datenklassifizierung installiert ist, wählen Sie **Weiter zur Konfiguration**, um zur Seite *Konfiguration* zu gelangen.

Bereitstellung in Google Cloud

Schritte

1. Wählen Sie auf der Hauptseite der Datenklassifizierung **Governance > Klassifizierung** aus.
2. Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



3. Wählen Sie **Bereitstellen**, um den Cloud-Bereitstellungsassistenten zu starten.
4. Der Assistent zeigt den Fortschritt an, während er die Bereitstellungsschritte durchläuft. Wenn Probleme auftreten, wird es angehalten und zur Eingabe aufgefordert.
5. Wenn die Instanz bereitgestellt und die Datenklassifizierung installiert ist, wählen Sie **Weiter zur Konfiguration**, um zur Seite *Konfiguration* zu gelangen.

Ergebnis

Die Konsole stellt die Datenklassifizierungsinstanz bei Ihrem Cloud-Anbieter bereit.

Upgrades des Konsolenagenten und der Datenklassifizierungssoftware erfolgen automatisiert, solange die Instanzen über eine Internetverbindung verfügen.

Was kommt als Nächstes

Auf der Konfigurationsseite können Sie die Datenquellen auswählen, die Sie scannen möchten.

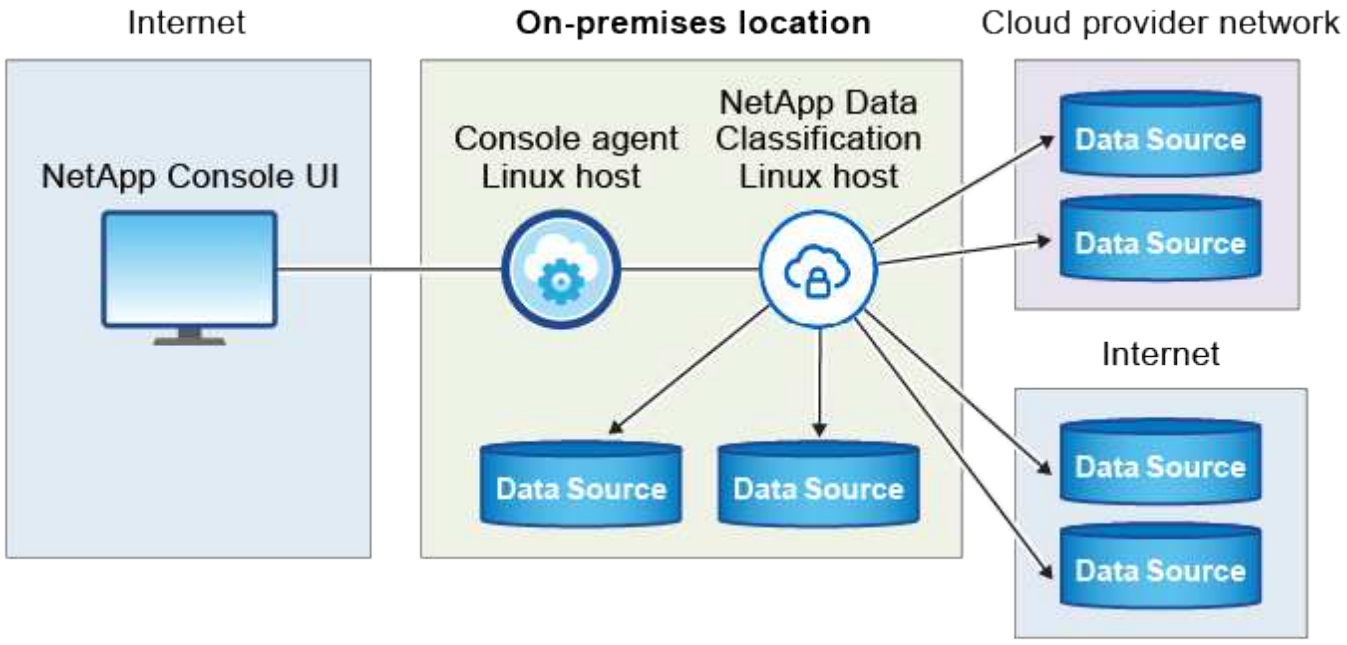
Installieren Sie NetApp Data Classification auf einem Host mit Internetzugang

Um NetApp Data Classification auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud mit Internetzugang bereitzustellen, müssen Sie den Linux-Host manuell in Ihrem Netzwerk oder in der Cloud bereitstellen.

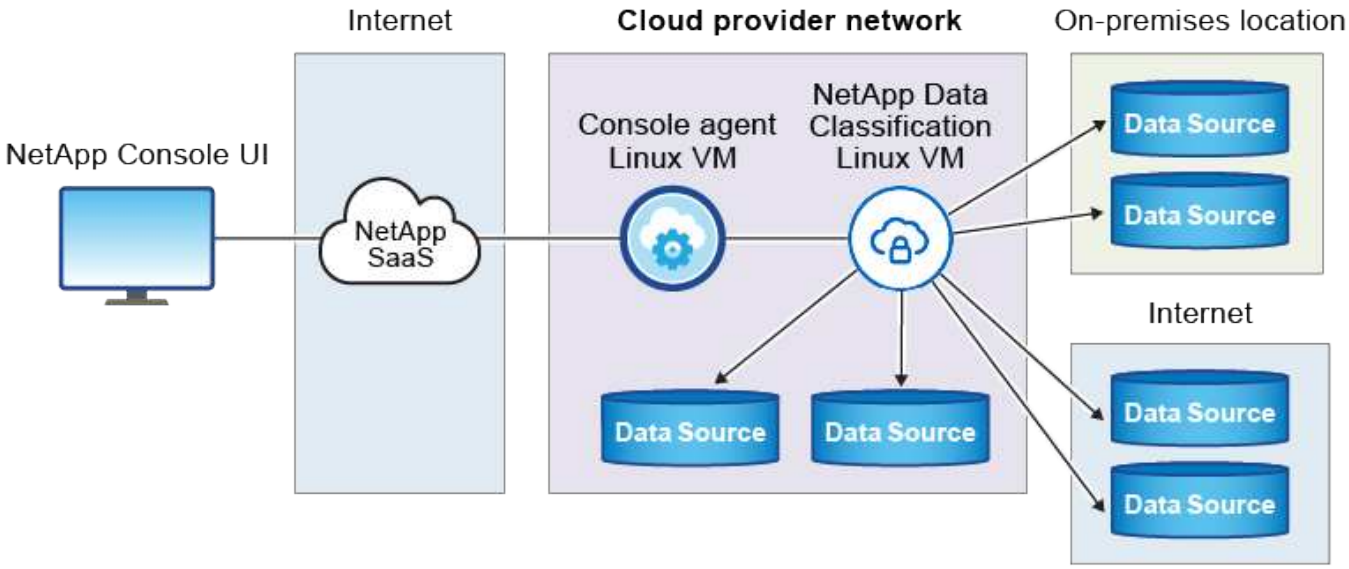
Die lokale Installation ist eine gute Option, wenn Sie lokale ONTAP -Systeme lieber mit einer Datenklassifizierungsinstanz scannen möchten, die sich ebenfalls vor Ort befindet. Dies ist keine Voraussetzung. Die Software funktioniert unabhängig von der gewählten Installationsmethode gleich.

Das Installationsskript für die Datenklassifizierung prüft zunächst, ob das System und die Umgebung die erforderlichen Voraussetzungen erfüllen. Wenn alle Voraussetzungen erfüllt sind, beginnt die Installation. Wenn Sie die Voraussetzungen unabhängig von der Ausführung der Data Classification-Installation überprüfen möchten, können Sie ein separates Softwarepaket herunterladen, das nur die Voraussetzungen testet. "Erfahren Sie, wie Sie überprüfen können, ob Ihr Linux-Host für die Installation der Datenklassifizierung bereit ist." .

Die typische Installation auf einem Linux-Host *in Ihren Räumlichkeiten* verfügt über die folgenden Komponenten und Verbindungen.



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



Schnellstart

Beginnen Sie schnell, indem Sie diese Schritte befolgen, oder scrollen Sie nach unten zu den restlichen Abschnitten, um alle Einzelheiten zu erfahren.

1 Erstellen eines Konsolenagenten

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

Sie können auch einen Konsolenagenten bei Ihrem Cloud-Anbieter erstellen. Sehen "Erstellen eines Konsolenagenten in AWS" , "Erstellen eines Konsolenagenten in Azure" , oder "Erstellen eines Konsolenagenten in GCP" .

2 Überprüfen der Voraussetzungen

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllt. Dazu gehören der ausgehende Internetzugriff für die Instanz, die Konnektivität zwischen dem Konsolenagenten und der Datenklassifizierung über Port 443 und mehr. Vollständige Liste anzeigen .

Sie benötigen außerdem ein Linux-System, das diefolgende Anforderungen .

3 Herunterladen und Bereitstellen der Datenklassifizierung

Laden Sie die Cloud Data Classification-Software von der NetApp -Support-Site herunter und kopieren Sie die Installationsdatei auf den Linux-Host, den Sie verwenden möchten. Starten Sie dann den Installationsassistenten und folgen Sie den Anweisungen zum Bereitstellen der Data Classification-Instanz.

Erstellen eines Konsolenagenten

Bevor Sie Data Classification installieren und verwenden können, ist ein Konsolenagent erforderlich. In den meisten Fällen haben Sie wahrscheinlich einen Konsolenagenten eingerichtet, bevor Sie versuchen, die Datenklassifizierung zu aktivieren, da die meisten "Für Konsolenfunktionen ist ein Konsolenagent erforderlich" , aber es gibt Fälle, in denen Sie jetzt eines einrichten müssen.

Informationen zum Erstellen eines solchen in der Umgebung Ihres Cloud-Anbieters finden Sie unter "Erstellen eines Konsolenagenten in AWS" , "Erstellen eines Konsolenagenten in Azure" , oder "Erstellen eines Konsolenagenten in GCP" .

Es gibt einige Szenarien, in denen Sie einen Konsolenagenten verwenden müssen, der bei einem bestimmten Cloud-Anbieter bereitgestellt wird:

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

  Für Azure NetApp Files muss es in derselben Region bereitgestellt werden wie die Volumes, die Sie scannen möchten.

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

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

Beachten Sie, dass Sie auch "Stellen Sie den Konsolenagenten vor Ort bereit" auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud. Einige Benutzer, die Data Classification vor Ort installieren möchten, entscheiden sich möglicherweise auch für die Installation des Konsolenagenten vor Ort.

Sie benötigen die IP-Adresse oder den Hostnamen des Konsolenagentensystems, wenn Sie die Datenklassifizierung installieren. Sie verfügen über diese Informationen, wenn Sie den Konsolenagenten in Ihren Räumlichkeiten installiert haben. Wenn der Konsolenagent in der Cloud bereitgestellt wird, finden Sie diese Informationen in der Konsole: Wählen Sie das Hilfesymbol, dann **Support** und dann **Konsolenagent**.

Vorbereiten des Linux-Hostsystems

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

Stellen Sie sicher, dass die Datenklassifizierung weiterhin ausgeführt werden kann. Die Datenklassifizierungsmaschine muss eingeschaltet bleiben, um Ihre Daten kontinuierlich zu scannen.

- Die Datenklassifizierung muss auf einem dedizierten Host erfolgen. Der Host darf nicht mit anderen Anwendungen oder Drittanbietersoftware wie z. B. Antivirenprogrammen geteilt werden.
- Wählen Sie die Größe, die zu dem Datensatz passt, den Sie mit der Datenklassifizierung scannen möchten.

Systemgröße	CPU	RAM (Auslagerungsspeicher muss deaktiviert sein)	Scheibe
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 • **Für Podman, 30 GB auf /var/tmp**
Groß	16 CPUs	64 GB RAM	• 500 GiB SSD auf / oder 100 GiB verfügbar auf /opt • 400 GiB verfügbar auf /var/lib/docker oder für Podman /var/lib/containers • 5 GiB auf /tmp • **Für Podman, 30 GB auf /var/tmp**

- Wenn Sie für Ihre Data Classification-Installation eine Compute-Instanz in der Cloud bereitstellen, wird empfohlen, ein System zu verwenden, das die oben genannten Systemanforderungen für „Groß“ erfüllt:

- **Amazon Elastic Compute Cloud (Amazon EC2)-Instanztyp**: „m6i.4xlarge“. "Weitere AWS-Instanztypen anzeigen" .
- **Azure-VM-Größe**: „Standard_D16s_v3“. "Weitere Azure-Instanztypen anzeigen" .
- **GCP-Maschinentyp**: „n2-standard-16“. "Weitere GCP-Instanztypen anzeigen" .

- **UNIX-Ordnerberechtigungen**: Die folgenden UNIX-Mindestberechtigungen sind erforderlich:

Ordner	Mindestberechtigungen
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Betriebssystem**:
  - Die folgenden Betriebssysteme erfordern die Verwendung der Docker-Container-Engine:
    - Red Hat Enterprise Linux Version 7.8 und 7.9
    - Ubuntu 22.04 (erfordert Data Classification Version 1.23 oder höher)
    - Ubuntu 24.04 (erfordert Data Classification Version 1.23 oder höher)
  - Die folgenden Betriebssysteme erfordern die Verwendung der Podman-Container-Engine und erfordern Data Classification Version 1.30 oder höher:
    - Red Hat Enterprise Linux Version 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 und 9.6.
  - Advanced Vector Extensions (AVX2) müssen auf dem Hostsystem aktiviert sein.
- **Red Hat Subscription Management**: Der Host muss bei Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositories zugreifen, um erforderliche Software von Drittanbietern zu aktualisieren.
- **Zusätzliche Software**: Sie müssen die folgende Software auf dem Host installieren, bevor Sie Data Classification installieren:
  - Je nach verwendetem Betriebssystem müssen Sie eine der Container-Engines installieren:
    - Docker Engine Version 19.3.1 oder höher. "Installationsanweisungen anzeigen" .
    - Podman Version 4 oder höher. Um Podman zu installieren, geben Sie ein(`sudo yum install podman netavark -y`).
- Python Version 3.6 oder höher. "Installationsanweisungen anzeigen" .
  - **NTP-Überlegungen**: NetApp empfiehlt, das Datenklassifizierungssystem für die Verwendung eines Network Time Protocol (NTP)-Dienstes zu konfigurieren. Die Zeit muss zwischen dem Datenklassifizierungssystem und dem Konsolenagentsystem synchronisiert werden.
- **Firewalld-Überlegungen**: Wenn Sie planen, `firewalld` , wir empfehlen, dass Sie es vor der Installation der Datenklassifizierung aktivieren. Führen Sie die folgenden Befehle aus, um zu konfigurieren `firewalld` damit es mit der Datenklassifizierung 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 zusätzliche Datenklassifizierungshosts als Scannerknoten verwenden möchten, fügen Sie Ihrem primären System jetzt diese Regeln 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 Data Classification-Hostsystems kann nach der Installation nicht mehr geändert werden.

Ausgehenden Internetzugriff von der Datenklassifizierung aus aktivieren

Für die Datenklassifizierung ist ein ausgehender Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxyserver für den Internetzugang verwendet, stellen Sie sicher, dass die Datenklassifizierungsinstanz über ausgehenden Internetzugang verfügt, um die folgenden Endpunkte zu kontaktieren.

Endpunkte	Zweck
https://api.console.netapp.com	Kommunikation mit der Konsole, die NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-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 ermöglicht das Senden von Protokollen und Metriken.
https://support.compliance.api.bluexp.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Prüfdatensätzen.
https://github.com/docker https://download.docker.com	Stellt erforderliche Pakete für die Docker-Installation bereit.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Stellt erforderliche Pakete für die Ubuntu-Installation bereit.

Stellen Sie sicher, dass alle erforderlichen Ports aktiviert sind

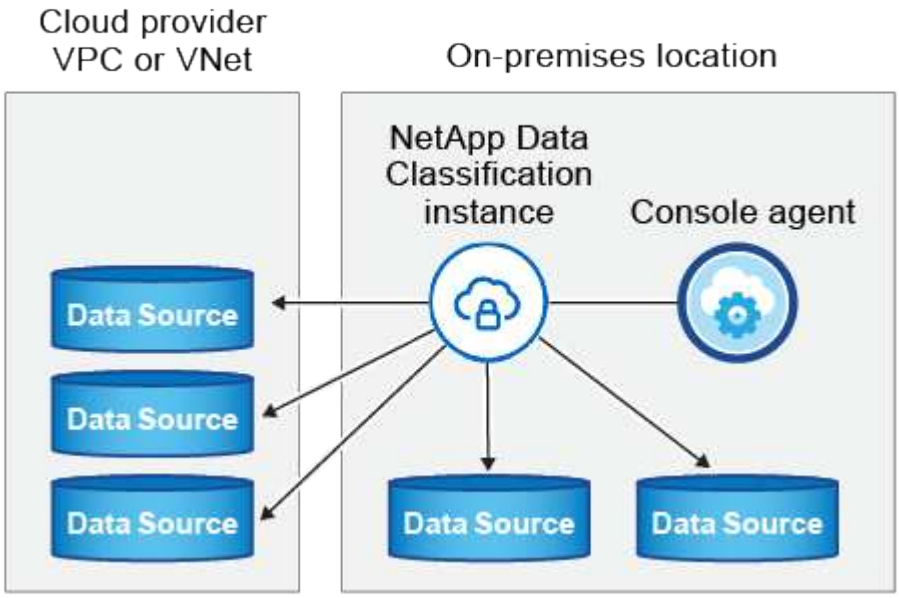
Sie müssen sicherstellen, dass alle erforderlichen Ports für die Kommunikation zwischen dem Konsolenagenten, der Datenklassifizierung, Active Directory und Ihren Datenquellen geöffnet sind.

Verbindungstyp	Häfen	Beschreibung
Konsolenagent <> Datenklassifizierung	8080 (TCP), 443 (TCP) und 80. 9000	Die Firewall- oder Routing-Regeln für den Konsolen-Agenten müssen eingehenden und ausgehenden Datenverkehr über Port 443 zur und von der Datenklassifizierungsinstanz zulassen. Stellen Sie sicher, dass Port 8080 geöffnet ist, damit Sie den Installationsfortschritt in der Konsole sehen können. Wenn auf dem Linux-Host eine Firewall verwendet wird, wird Port 9000 für interne Prozesse innerhalb eines Ubuntu-Servers benötigt.
Konsolenagent <> ONTAP -Cluster (NAS)	443 (TCP)	Die Konsole erkennt ONTAP Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen: • Der Konsolen-Agent-Host muss ausgehenden HTTPS-Zugriff über Port 443 zulassen. Wenn sich der Konsolenagent in der Cloud befindet, wird die gesamte ausgehende Kommunikation durch die vordefinierten Firewall- oder Routing-Regeln zugelassen. • Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen. Die standardmäßige Firewall-Richtlinie „mgmt“ erlaubt eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert oder Ihre eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff vom Konsolen-Agent-Host aus aktivieren.
Datenklassifizierung <> ONTAP -Cluster	• Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS – 139 (TCP\UDP) und 445 (TCP\UDP)	Für die Datenklassifizierung ist eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder On-Premise ONTAP System erforderlich. Firewalls oder Routing-Regeln für Cloud Volumes ONTAP müssen eingehende Verbindungen von der Data Classification-Instanz zulassen. Stellen Sie sicher, dass diese Ports für die Data Classification-Instanz geöffnet sind: • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 NFS-Volume-Exportrichtlinien müssen den Zugriff von der Datenklassifizierungsinstanz aus zulassen.

Verbindungstyp	Häfen	Beschreibung
Datenklassifizierung <> Active Directory	389 (TCP und UDP), 636 (TCP), 3268 (TCP) und 3269 (TCP)	Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben. Darüber hinaus benötigt die Datenklassifizierung Active Directory-Anmeldeinformationen, um CIFS-Volumes zu scannen. Sie benötigen die Informationen für das Active Directory: • DNS-Server-IP-Adresse oder mehrere IP-Adressen • Benutzername und Passwort für den Server • Domänenname (Active Directory-Name) • Ob Sie sicheres LDAP (LDAPS) verwenden oder nicht • LDAP-Server-Port (normalerweise 389 für LDAP und 636 für sicheres LDAP)

Installieren Sie Data Classification auf dem Linux-Host

Bei typischen Konfigurationen installieren Sie die Software auf einem einzelnen Hostsystem. Sehen Sie sich diese Schritte hier an .



SehenVorbereiten des Linux-Hostsystems UndVoraussetzungen überprüfen für die vollständige Liste der Anforderungen, bevor Sie die Datenklassifizierung bereitstellen.

Upgrades der Datenklassifizierungssoftware erfolgen automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Data Classification kann derzeit keine S3-Buckets, Azure NetApp Files oder FSx für ONTAP scannen, wenn die Software vor Ort installiert ist. In diesen Fällen müssen Sie einen separaten Konsolenagenten und eine Instanz der Datenklassifizierung in der Cloud bereitstellen und "zwischen Anschlüssen wechseln" für Ihre verschiedenen Datenquellen.

Single-Host-Installation für typische Konfigurationen

Überprüfen Sie die Anforderungen und befolgen Sie diese Schritte, wenn Sie die Datenklassifizierungssoftware auf einem einzelnen lokalen Host installieren.

"Sehen Sie sich dieses Video an"um zu sehen, wie die Datenklassifizierung installiert wird.

Beachten Sie, dass bei der Installation von Data Classification alle Installationsaktivitäten protokolliert werden. Wenn während der Installation Probleme auftreten, können Sie den Inhalt des Installationsüberwachungsprotokolls anzeigen. Es ist geschrieben an `/opt/netapp/install_logs/` .

Bevor Sie beginnen

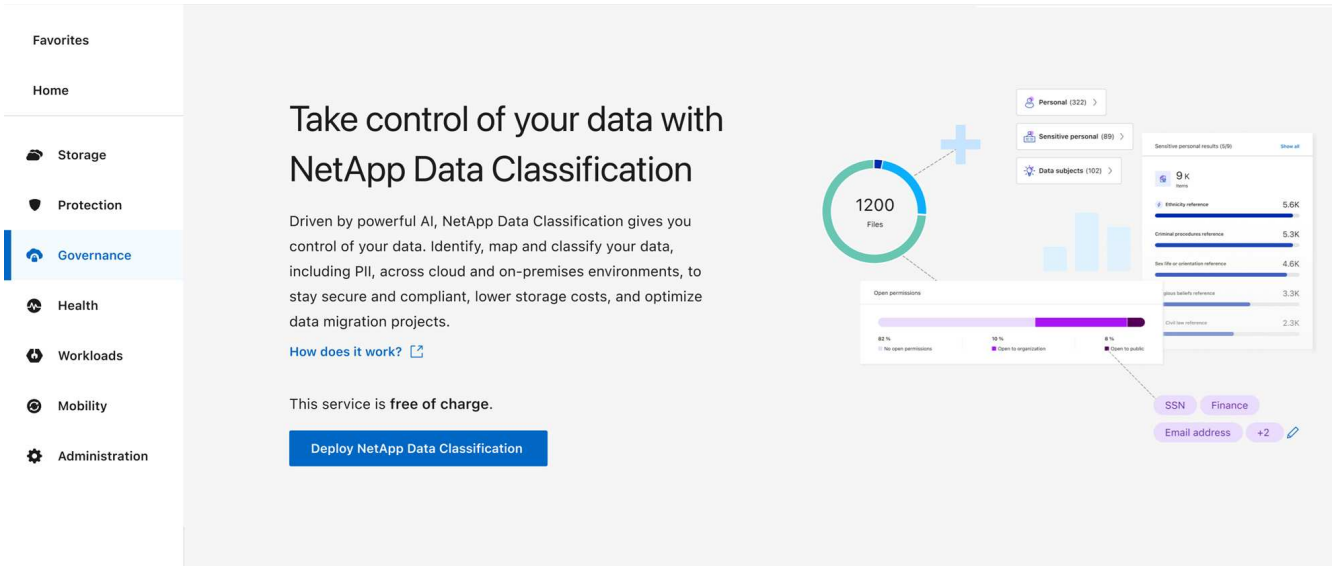
- Überprüfen Sie, ob Ihr Linux-System dieHostanforderungen .
- Stellen Sie sicher, dass auf dem System die beiden erforderlichen Softwarepakete installiert sind (Docker Engine oder Podman und Python 3).
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.
- Wenn Sie einen Proxy für den Internetzugang verwenden:
  - Sie benötigen die Proxyserver-Informationen (IP-Adresse oder Hostname, Verbindungsport, Verbindungsschema: https oder http, Benutzername und Passwort).
  - Wenn der Proxy eine TLS-Abfangfunktion ausführt, müssen Sie den Pfad auf dem Data Classification Linux-System kennen, in dem die TLS-CA-Zertifikate gespeichert sind.
  - Der Proxy muss intransparent sein. Die Datenklassifizierung unterstützt derzeit keine transparenten Proxys.
  - Der Benutzer muss ein lokaler Benutzer sein. Domänenbenutzer werden nicht unterstützt.
- Überprüfen Sie, ob Ihre Offline-Umgebung die erforderlichenBerechtigungen und Konnektivität .

Schritte

1. Laden Sie die Datenklassifizierungssoftware von der "NetApp Support Site" . Die Datei, die Sie auswählen sollten, 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, zum Beispiel:

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

4. Wählen Sie in der Konsole **Governance > Klassifizierung** aus.
5. Wählen Sie **Klassifizierung vor Ort oder in der Cloud bereitstellen**.



6. Je nachdem, ob Sie Data Classification auf einer Instanz installieren, die Sie in der Cloud vorbereitet haben, oder auf einer Instanz, die Sie bei Ihnen vor Ort vorbereitet haben, wählen Sie die entsprechende Option **Bereitstellen** aus, um die Installation von Data Classification zu starten.
7. Das Dialogfeld „Datenklassifizierung vor Ort bereitstellen“ wird angezeigt. Kopieren Sie den bereitgestellten Befehl (zum Beispiel: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`) und fügen Sie es in eine Textdatei ein, damit Sie es später verwenden können. Wählen Sie dann **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 angeben.

   Beachten Sie, dass das Installationsprogramm eine Vorprüfung durchführt, um sicherzustellen, dass Ihre System- und Netzwerkanforderungen für eine erfolgreiche Installation erfüllt sind. "Sehen Sie sich dieses Video an" um die Vorabprüfungsnachrichten 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 in 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 bei Ihnen vor Ort) durchführen, fügen Sie hinzu `--manual-cloud-install <cloud_provider>`. b. Geben Sie die IP-Adresse oder den Hostnamen des Data Classification-Hostcomputers ein, damit das Konsolenagentsystem darauf zugreifen kann. c. Geben Sie die IP-Adresse oder den Hostnamen des Hostcomputers des Konsolenagenten ein, damit das Datenklassifizierungssystem darauf zugreifen kann. d. Geben Sie die Proxy-Details wie aufgefordert ein. Wenn Ihr Konsolenagent bereits einen Proxy verwendet, müssen Sie diese Informationen hier nicht erneut eingeben, da die Datenklassifizierung automatisch den vom Konsolenagenten verwendeten Proxy verwendet.	Alternativ können Sie den gesamten Befehl im Voraus erstellen und dabei die erforderlichen Host- und Proxy-Parameter angeben: `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* = Client-ID des Konsolenagenten (fügen Sie der Client-ID das Suffix „clients“ hinzu, falls es nicht bereits vorhanden ist)
- *user_token* = JWT-Benutzerzugriffstoken
- *ds_host* = IP-Adresse oder Hostname des Data Classification Linux-Systems.
- *cm_host* = IP-Adresse oder Hostname des Konsolenagentensystems.
- *cloud_provider* = Geben Sie bei der Installation auf einer Cloud-Instanz je nach Cloud-Anbieter „AWS“, „Azure“ oder „Gcp“ ein.
- *proxy_host* = IP oder Hostname des Proxyservers, wenn sich der Host hinter einem Proxyserver befindet.
- *proxy_port* = Port für die Verbindung mit dem Proxyserver (Standard 80).
- *proxy_scheme* = Verbindungsschema: https oder http (Standard: http).
- *proxy_user* = Authentifizierter Benutzer zur Verbindung mit dem Proxyserver, wenn eine Basisauthentifizierung 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 Data Classification-Linux-System, der zusätzliche TLS-CA-

Zertifikatspakete enthält. Nur erforderlich, wenn der Proxy eine TLS-Abfangfunktion durchführt.

Ergebnis

Das Data Classification-Installationsprogramm installiert Pakete, registriert die Installation und installiert Data Classification. Die Installation kann 10 bis 20 Minuten dauern.

Wenn zwischen dem Hostcomputer und der Konsolen-Agentinstanz eine Verbindung über Port 8080 besteht, wird der Installationsfortschritt auf der Registerkarte „Datenklassifizierung“ in der Konsole angezeigt.

Was kommt als Nächstes

Auf der Konfigurationsseite können Sie die Datenquellen auswählen, die Sie scannen möchten.

Installieren Sie NetApp Data Classification auf einem Linux-Host ohne Internetzugang

Die Installation von NetApp Data Classification auf einem Linux-Host an einem lokalen Standort ohne Internetzugang wird als *privater Modus* bezeichnet. Bei dieser Art der Installation, bei der ein Installationsskript verwendet wird, besteht keine Verbindung zur SaaS-Schicht der NetApp Console .

> Der private BlueXP Modus (alte BlueXP -Schnittstelle) wird normalerweise in lokalen Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, darunter AWS Secret Cloud, AWS Top Secret Cloud und Azure IL6. NetApp unterstützt diese Umgebungen weiterhin mit der alten BlueXP Schnittstelle. Die Dokumentation zum privaten Modus in der alten BlueXP Schnittstelle finden Sie unter"PDF-Dokumentation für den privaten Modus von BlueXP" .

Überprüfen Sie, ob Ihr Linux-Host für die Installation von NetApp Data Classification bereit ist.

Bevor Sie NetApp Data Classification manuell auf einem Linux-Host installieren, führen Sie optional ein Skript auf dem Host aus, um zu überprüfen, ob alle Voraussetzungen für die Installation von Data Classification erfüllt 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 sein oder sich an einem Standort ohne Internetzugang befinden (ein „Dark Site“).

Das Installationsskript für die Datenklassifizierung enthält ein Testskript, um sicherzustellen, dass Ihre Umgebung die Anforderungen erfüllt. Sie können dieses Skript separat ausführen, um die Bereitschaft des Linux-Hosts vor dem Ausführen des Installationsskripts zu überprüfen.

Erste Schritte

Sie führen die folgenden Aufgaben aus.

- Installieren Sie optional einen Konsolenagenten, falls Sie noch keinen installiert haben. Sie können das Testskript ausführen, ohne dass ein Konsolenagent installiert ist. Das Skript prüft jedoch die Konnektivität zwischen dem Konsolenagenten und dem Hostcomputer der Datenklassifizierung. Daher wird empfohlen, dass Sie über einen Konsolenagenten verfügen.

- Bereiten Sie den Hostcomputer vor und überprüfen Sie, ob er alle Anforderungen erfüllt.
- Aktivieren Sie den ausgehenden Internetzugriff vom Data Classification-Hostcomputer.
- Stellen Sie sicher, dass alle erforderlichen Ports auf allen Systemen aktiviert sind.
- Laden Sie das Prerequisite-Testskript herunter und führen Sie es aus.

Erstellen eines Konsolenagenten

Bevor Sie Data Classification installieren und verwenden können, ist ein Konsolenagent erforderlich. Sie können das Skript „Voraussetzungen“ jedoch ohne einen Konsolenagenten ausführen.

Du kannst "Installieren Sie den Konsolen-Agenten vor Ort" auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud. Sie können die Datenklassifizierung auch lokal installieren, wenn der Konsolenagent lokal installiert ist.

Informationen zum Erstellen eines Console-Agenten in Ihrer Cloud-Provider-Umgebung finden Sie hier:

- "Erstellen eines Konsolenagenten in AWS"
- "Erstellen eines Konsolenagenten in Azure"
- "Erstellen eines Konsolenagenten in GCP"

Sie benötigen die IP-Adresse oder den Hostnamen des Konsolenagentensystems, wenn Sie das Skript „Voraussetzungen“ ausführen. Diese Informationen stehen Ihnen zur Verfügung, wenn Sie den Console-Agenten in Ihren Räumlichkeiten installiert haben. Wenn der Console-Agent in der Cloud bereitgestellt wird, finden Sie diese Informationen in der Console: Wählen Sie das Hilfesymbol und dann **Support**; wählen Sie im Abschnitt Agent und Audit **Zum Agenten**.

Überprüfen der Hostanforderungen

Die Software zur Datenklassifizierung muss auf einem Host ausgeführt werden, der bestimmte Anforderungen an das Betriebssystem, den Arbeitsspeicher und die Software erfüllt.

- Die Datenklassifizierung muss auf einem dedizierten Host erfolgen. Der Host darf nicht mit anderen Anwendungen oder Drittanbietersoftware wie z. B. Antivirenprogrammen geteilt werden.
- Wählen Sie die Größe, die zu dem Datensatz passt, den Sie mit der Datenklassifizierung scannen möchten.

Systemgröße	CPU	RAM (Auslagerungsspeicher muss deaktiviert sein)	Scheibe
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 • **Für Podman, 30 GB auf /var/tmp**

Systemgröße	CPU	RAM (Auslagerungsspeicher muss deaktiviert sein)	Scheibe
Groß	16 CPUs	64 GB RAM	• 500 GiB SSD auf / oder 100 GiB verfügbar auf /opt • 400 GiB verfügbar auf /var/lib/docker oder für Podman /var/lib/containers • 5 GiB auf /tmp • **Für Podman, 30 GB auf /var/tmp**

- Wenn Sie für Ihre Data Classification-Installation eine Compute-Instanz in der Cloud bereitstellen, wird empfohlen, ein System zu verwenden, das die oben genannten Systemanforderungen für „Groß“ erfüllt:
  - **Amazon Elastic Compute Cloud (Amazon EC2)-Instanztyp**: „m6i.4xlarge“. "Weitere AWS-Instanztypen anzeigen" .
  - **Azure-VM-Größe**: „Standard_D16s_v3“. "Weitere Azure-Instanztypen anzeigen" .
  - **GCP-Maschinentyp**: „n2-standard-16“. "Weitere GCP-Instanztypen anzeigen" .
- **UNIX-Ordnerberechtigungen**: Die folgenden UNIX-Mindestberechtigungen sind erforderlich:

Ordner	Mindestberechtigungen
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Betriebssystem**:
  - Die folgenden Betriebssysteme erfordern die Verwendung der Docker-Container-Engine:
    - Red Hat Enterprise Linux Version 7.8 und 7.9
    - Ubuntu 22.04 (erfordert Data Classification Version 1.23 oder höher)
    - Ubuntu 24.04 (erfordert Data Classification Version 1.23 oder höher)
  - Die folgenden Betriebssysteme erfordern die Verwendung der Podman-Container-Engine und erfordern Data Classification Version 1.30 oder höher:
    - Red Hat Enterprise Linux Version 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 und 9.6.
  - Advanced Vector Extensions (AVX2) müssen auf dem Hostsystem aktiviert sein.
- **Red Hat Subscription Management**: Der Host muss bei Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Installation nicht auf Repositories zugreifen, um erforderliche Software von Drittanbietern zu aktualisieren.
- **Zusätzliche Software**: Sie müssen die folgende Software auf dem Host installieren, bevor Sie Data Classification installieren:
  - Je nach verwendetem Betriebssystem müssen Sie eine der Container-Engines installieren:

- Docker Engine Version 19.3.1 oder höher. "Installationsanweisungen anzeigen" .
- Podman Version 4 oder höher. Um Podman zu installieren, geben Sie ein(`sudo yum install podman netavark -y`).

- Python Version 3.6 oder höher. "Installationsanweisungen anzeigen" .
  - **NTP-Überlegungen**: NetApp empfiehlt, das Datenklassifizierungssystem für die Verwendung eines Network Time Protocol (NTP)-Dienstes zu konfigurieren. Die Zeit muss zwischen dem Datenklassifizierungssystem und dem Konsolenagentsystem synchronisiert werden.
- **Firewalld-Überlegungen**: Wenn Sie planen, `firewalld` , wir empfehlen, dass Sie es vor der Installation der Datenklassifizierung aktivieren. Führen Sie die folgenden Befehle aus, um zu konfigurieren `firewalld` damit es mit der Datenklassifizierung 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 Datenklassifizierungshosts als Scannerknoten (in einem verteilten Modell) zu verwenden, fügen Sie Ihrem primären System jetzt diese Regeln 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.

Ausgehenden Internetzugriff von der Datenklassifizierung aus aktivieren

Für die Datenklassifizierung ist ein ausgehender Internetzugang erforderlich. Wenn Ihr virtuelles oder physisches Netzwerk einen Proxyserver für den Internetzugang verwendet, stellen Sie sicher, dass die Datenklassifizierungsinstanz über ausgehenden 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.console.netapp.com	Kommunikation mit dem Konsolendienst, der NetApp -Konten umfasst.
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit der Konsolen-Website zur zentralen Benutzerauthentifizierung.

Endpunkte	Zweck
https://support.compliance.api.console.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 ermöglicht das Senden von Protokollen und Metriken.
https://support.compliance.api.console.netapp.com/	Ermöglicht NetApp das Streamen von Daten aus Prüfdatensätzen.
https://github.com/docker https://download.docker.com	Stellt erforderliche Pakete für die Docker-Installation bereit.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Stellt erforderliche Pakete für die Ubuntu-Installation bereit.

Stellen Sie sicher, dass alle erforderlichen Ports aktiviert sind

Sie müssen sicherstellen, dass alle erforderlichen Ports für die Kommunikation zwischen dem Konsolenagenten, der Datenklassifizierung, Active Directory und Ihren Datenquellen geöffnet sind.

Verbindungstyp	Häfen	Beschreibung
Konsolenagent <> Datenklassifizierung	8080 (TCP), 443 (TCP) und 80. 9000	Die Firewall- oder Routing-Regeln für den Konsolen-Agenten müssen eingehenden und ausgehenden Datenverkehr über Port 443 zur und von der Datenklassifizierungsinstanz zulassen. Stellen Sie sicher, dass Port 8080 geöffnet ist, damit Sie den Installationsfortschritt in der Konsole sehen können. Wenn auf dem Linux-Host eine Firewall verwendet wird, wird Port 9000 für interne Prozesse innerhalb eines Ubuntu-Servers benötigt.
Konsolenagent <> ONTAP -Cluster (NAS)	443 (TCP)	Die Konsole erkennt ONTAP Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, muss der Konsolen-Agent-Host ausgehenden HTTPS-Zugriff über Port 443 zulassen. Wenn sich der Konsolenagent in der Cloud befindet, wird die gesamte ausgehende Kommunikation durch die vordefinierten Firewall- oder Routing-Regeln zugelassen.

Ausführen des Voraussetzungenskripts für die Datenklassifizierung

Führen Sie die folgenden Schritte aus, um das Voraussetzungenskript für die Datenklassifizierung auszuführen.

"Sehen Sie sich dieses Video an"um zu sehen, wie Sie das Voraussetzungen-Skript ausführen und die Ergebnisse interpretieren.

Bevor Sie beginnen

- Überprüfen Sie, ob Ihr Linux-System dieHostanforderungen .

- Stellen Sie sicher, dass 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 „Data Classification Prerequisites“ von der "NetApp Support Site" . Die Datei, die Sie auswählen sollten, hat den Namen **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 des Data Classification-Hostcomputers auf.
   - Geben Sie die IP-Adresse oder den Hostnamen ein.
6. Das Skript fragt, ob Sie einen installierten Konsolenagenten haben.
   - Geben Sie **N** ein, wenn Sie keinen installierten Konsolenagenten haben.
   - Geben Sie **Y** ein, wenn Sie einen installierten Konsolenagenten haben. Geben Sie dann die IP-Adresse oder den Hostnamen des Konsolenagenten ein, damit das Testskript diese Konnektivität testen kann.
7. Das Skript führt verschiedene Tests auf dem System aus und zeigt im Verlauf die Ergebnisse an. Wenn es fertig ist, schreibt es ein Protokoll der Sitzung in eine Datei namens `prerequisites-test-<timestamp>.log` im Verzeichnis `/opt/netapp/install_logs` .

Ergebnis

Wenn alle erforderlichen Tests erfolgreich ausgeführt wurden, können Sie Data Classification auf dem Host installieren, wenn Sie bereit sind.

Wenn Probleme entdeckt wurden, werden sie zur Behebung als „Empfohlen“ oder „Erforderlich“ kategorisiert. Bei den empfohlenen Problemen handelt es sich in der Regel um Elemente, die die Ausführung der Scan- und Kategorisierungsaufgaben zur Datenklassifizierung verlangsamen würden. Diese Punkte müssen nicht korrigiert werden, Sie möchten sie aber möglicherweise dennoch ansprechen.

Wenn Sie „Erforderliche“ Probleme haben, sollten Sie diese beheben und das Voraussetzungen-Testskript erneut ausführen.