Erste Schritte

NetApp Data Classification

NetApp
February 06, 2026

Inhalt

Erste Schritte

Erfahren Sie mehr über die NetApp Data Classification

NetApp Data Classification ist ein Data-Governance-Service für die NetApp Console , der Ihre unternehmenseigenen Datenquellen vor Ort und in der Cloud scannt, um Daten zuzuordnen und zu klassifizieren und private Informationen zu identifizieren. Dies kann dazu beitragen, Ihr Sicherheits- und Compliance-Risiko zu verringern, die Speicherkosten zu senken und Ihre Datenmigrationsprojekte zu unterstützen.

Ab Version 1.31 ist die Datenklassifizierung als Kernfunktion in der NetApp Console verfügbar. Es fallen keine zusätzlichen Kosten an. Es ist keine Klassifizierungslizenz oder kein Abonnement erforderlich. + Wenn Sie die Vorgängerversion 1.30 oder früher verwendet haben, ist diese Version verfügbar, bis Ihr Abonnement abläuft.

NetApp Console

Auf die Datenklassifizierung kann über die NetApp Console zugegriffen werden.

Die NetApp Console ermöglicht eine zentrale Verwaltung von NetApp -Speicher- und Datendiensten in lokalen und Cloud-Umgebungen auf Unternehmensebene. Die Konsole ist für den Zugriff auf und die Nutzung der NetApp -Datendienste erforderlich. Als Verwaltungsschnittstelle ermöglicht es Ihnen, viele Speicherressourcen über eine Schnittstelle zu verwalten. Konsolenadministratoren können den Zugriff auf Speicher und Dienste für alle Systeme innerhalb des Unternehmens steuern.

Sie benötigen weder eine Lizenz noch ein Abonnement, um die NetApp Console zu verwenden. Es fallen nur dann Kosten an, wenn Sie Konsolenagenten in Ihrer Cloud bereitstellen müssen, um die Konnektivität zu Ihren Speichersystemen oder NetApp -Datendiensten sicherzustellen. Einige NetApp -Datendienste, auf die über die Konsole zugegriffen werden kann, sind jedoch lizenz- oder abonnementbasiert.

Erfahren Sie mehr über die"NetApp Console" .

Features

Bei der Datenklassifizierung werden künstliche Intelligenz (KI), natürliche Sprachverarbeitung (NLP) und maschinelles Lernen (ML) verwendet, um die gescannten Inhalte zu verstehen, Entitäten zu extrahieren und die Inhalte entsprechend zu kategorisieren. Dadurch kann die Datenklassifizierung die folgenden Funktionsbereiche bereitstellen.

"Erfahren Sie mehr über Anwendungsfälle für die Datenklassifizierung" .

Einhaltung der Vorschriften

Die Datenklassifizierung bietet mehrere Tools, die Sie bei Ihren Compliance-Bemühungen unterstützen können. Sie können die Datenklassifizierung für Folgendes verwenden:

- Identifizieren Sie personenbezogene Daten (PII).
- Identifizieren Sie ein breites Spektrum sensibler personenbezogener Daten gemäß den Datenschutzbestimmungen DSGVO, CCPA, PCI und HIPAA.
- Beantworten Sie Anfragen zum Zugriff auf personenbezogene Daten (DSAR) basierend auf Name oder E-Mail-Adresse.

Stärkung der Sicherheit

Durch die Datenklassifizierung können Daten identifiziert werden, bei denen das Risiko besteht, dass für kriminelle Zwecke auf sie zugegriffen wird. Sie können die Datenklassifizierung für Folgendes verwenden:

- Identifizieren Sie alle Dateien und Verzeichnisse (Freigaben und Ordner) mit offenen Berechtigungen, die Ihrer gesamten Organisation oder der Öffentlichkeit zugänglich sind.
- Identifizieren Sie vertrauliche Daten, die sich außerhalb des ursprünglichen, dedizierten Speicherorts befinden.
- Halten Sie die Richtlinien zur Datenaufbewahrung ein.
- Verwenden Sie *Richtlinien*, um neue Sicherheitsprobleme automatisch zu erkennen, damit das Sicherheitspersonal sofort Maßnahmen ergreifen kann.

Optimieren Sie die Speichernutzung

Die Datenklassifizierung bietet Tools, die Ihnen bei der Reduzierung der Gesamtbetriebskosten (TCO) Ihres Speichers helfen können. Sie können die Datenklassifizierung für Folgendes verwenden:

- Steigern Sie die Speichereffizienz, indem Sie doppelte oder nicht geschäftsbezogene Daten identifizieren.
- Sparen Sie Speicherkosten, indem Sie inaktive Daten identifizieren, die Sie in einen kostengünstigeren Objektspeicher verschieben können. "Erfahren Sie mehr über das Tiering von Cloud Volumes ONTAP -Systemen" . "Erfahren Sie mehr über das Tiering von On-Premises ONTAP -Systemen" .

Unterstützte Systeme und Datenquellen

Die Datenklassifizierung kann strukturierte und unstrukturierte Daten aus den folgenden Systemtypen und Datenquellen scannen und analysieren:

Systeme

- Amazon FSx for NetApp ONTAP -Verwaltung
- Azure NetApp Files
- Cloud Volumes ONTAP (bereitgestellt in AWS, Azure oder GCP)
- On-Premises- ONTAP -Cluster
- StorageGRID
- Google Cloud NetApp Volumes

Datenquellen

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

Die Datenklassifizierung unterstützt die NFS-Versionen 3.x, 4.0 und 4.1 sowie die CIFS-Versionen 1.x, 2.0, 2.1 und 3.0.

Kosten

Die Nutzung der Datenklassifizierung ist kostenlos. Es ist keine Klassifizierungslizenz oder kostenpflichtiges Abonnement erforderlich.

Infrastrukturkosten

- Für die Installation der Datenklassifizierung in der Cloud ist die Bereitstellung einer Cloud-Instanz erforderlich, wofür vom Cloud-Anbieter, bei dem die Instanz bereitgestellt wird, Gebühren anfallen. Sehen der Instanztyp, der für jeden Cloud-Anbieter bereitgestellt wird . Wenn Sie Data Classification auf einem lokalen System installieren, fallen keine Kosten an.
- Für die Datenklassifizierung müssen Sie einen Konsolenagenten bereitgestellt haben. In vielen Fällen verfügen Sie aufgrund anderer Speicher und Dienste, die Sie in der Konsole verwenden, bereits über einen Konsolenagenten. Für die Konsolen-Agentinstanz fallen Gebühren seitens des Cloud-Anbieters an, bei dem sie bereitgestellt wird. Siehe die "Typ der Instanz, die für jeden Cloud-Anbieter bereitgestellt wird" . Wenn Sie den Konsolenagenten auf einem lokalen System installieren, fallen keine Kosten an.

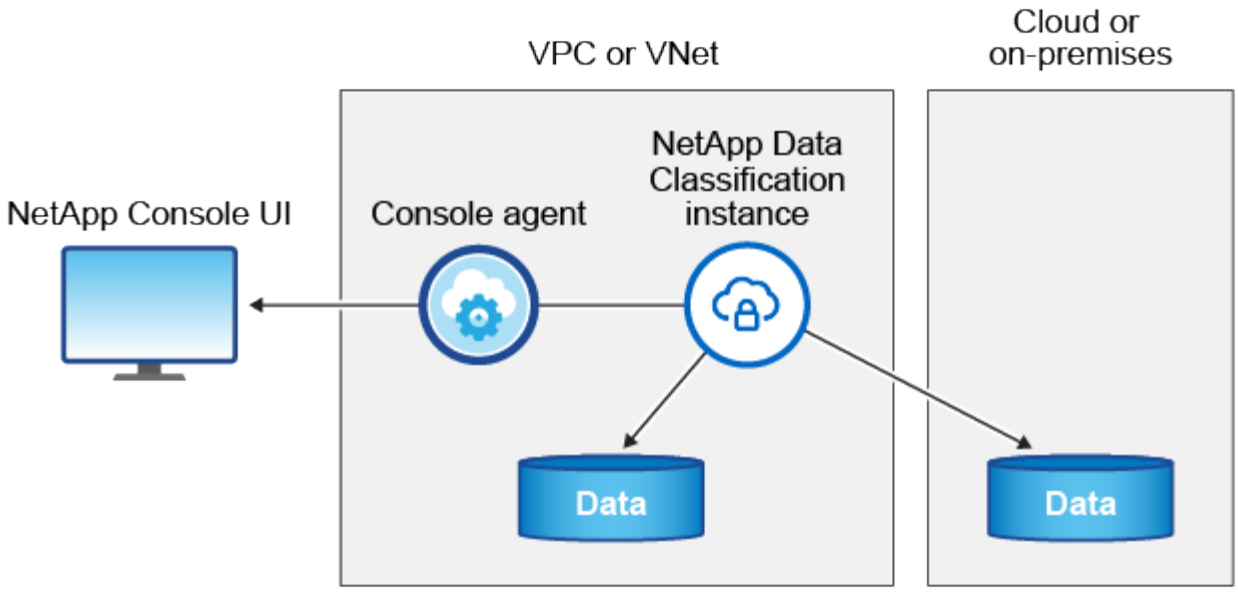
Kosten für die Datenübertragung

Die Kosten für die Datenübertragung hängen von Ihrer Konfiguration ab. Wenn sich die Datenklassifizierungsinstanz und die Datenquelle in derselben Verfügbarkeitszone und Region befinden, fallen keine Datenübertragungskosten an. Wenn sich die Datenquelle, beispielsweise ein Cloud Volumes ONTAP -System, jedoch in einer anderen Availability Zone oder Region befindet, werden Ihnen von Ihrem Cloud-Anbieter die Kosten für die Datenübertragung in Rechnung gestellt. Weitere Einzelheiten finden Sie unter diesen Links:

- "AWS: Preise für Amazon Elastic Compute Cloud (Amazon EC2)"
- "Microsoft Azure: Details zu den Bandbreitenpreisen"
- "Google Cloud: Preise für Storage Transfer Service"

Die Datenklassifizierungsinstanz

Wenn Sie die Datenklassifizierung in der Cloud bereitstellen, stellt die Konsole die Instanz im selben Subnetz wie der Konsolenagent bereit. "Erfahren Sie mehr über den Konsolenagenten."



Beachten Sie Folgendes zur Standardinstanz:

- In AWS läuft die Datenklassifizierung auf einem "m6i.4xlarge-Instanz" mit einer 500 GiB GP2-Festplatte. Das Betriebssystem-Image ist Amazon Linux 2. Bei der Bereitstellung in AWS können Sie eine kleinere Instanzgröße wählen, wenn Sie eine kleine Datenmenge scannen.
- In Azure läuft die Datenklassifizierung auf einem"Standard_D16s_v3 VM" mit einer 500-GiB-Festplatte. Das Betriebssystem-Image ist Ubuntu 22.04.
- In GCP läuft die Datenklassifizierung auf einem"n2-standard-16 VM" mit einer persistenten 500-GiB-Standardfestplatte. Das Betriebssystem-Image ist Ubuntu 22.04.
- In Regionen, in denen die Standardinstanz nicht verfügbar ist, wird die Datenklassifizierung auf einer alternativen Instanz ausgeführt. "Alternative Instance-Typen anzeigen" .
- Die Instanz trägt den Namen *CloudCompliance* und ist mit einem generierten Hash (UUID) verknüpft. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Pro Konsolenagent wird nur eine Datenklassifizierungsinstanz bereitgestellt.

Sie können die Datenklassifizierung auch auf einem Linux-Host in Ihren Räumlichkeiten oder auf einem Host bei Ihrem bevorzugten Cloud-Anbieter bereitstellen. Die Software funktioniert unabhängig von der gewählten Installationsmethode auf genau dieselbe Weise. Upgrades der Datenklassifizierungssoftware werden automatisiert, solange die Instanz über einen Internetzugang verfügt.

Die Instanz sollte ständig ausgeführt werden, da die Datenklassifizierung die Daten kontinuierlich scannt.

Auf verschiedenen Instanztypen bereitstellen

Überprüfen Sie die folgenden Spezifikationen für Instanztypen:

Systemgröße	Technische Daten	Einschränkungen
Extragroß	32 CPUs, 128 GB RAM, 1 TiB SSD	Kann bis zu 500 Millionen Dateien scannen.
Groß (Standard)	16 CPUs, 64 GB RAM, 500 GiB SSD	Kann bis zu 250 Millionen Dateien scannen.

Wenn Sie bei der Bereitstellung der Datenklassifizierung in Azure oder GCP Unterstützung benötigen und einen kleineren Instanztyp verwenden möchten, senden Sie eine E-Mail an ng-contact-data-sense@netapp.com.

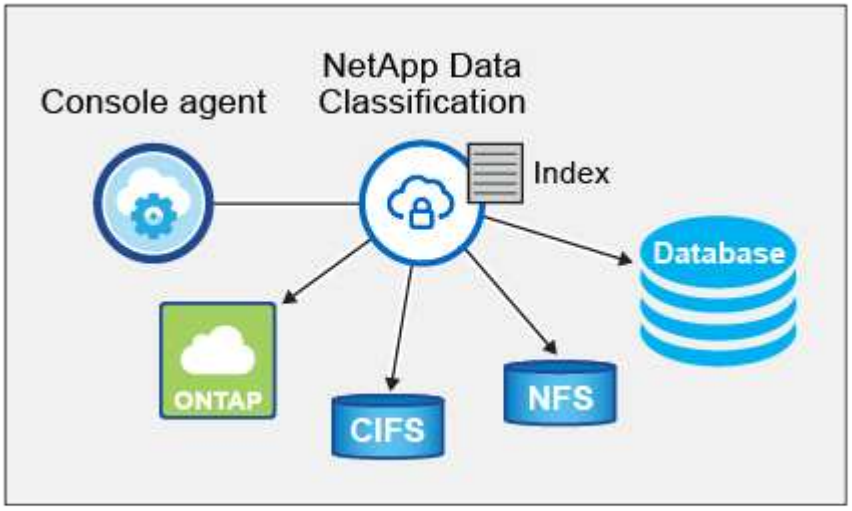
Funktionsweise des Datenklassifizierungsscans

Im Großen und Ganzen funktioniert das Scannen der Datenklassifizierung folgendermaßen:

1. Sie stellen eine Instanz der Datenklassifizierung in der Konsole bereit.
2. Sie aktivieren die Zuordnung auf hoher Ebene (sogenannte *Mapping only*-Scans) oder die Tiefenscans (sogenannte *Map & Classify*-Scans) für eine oder mehrere Datenquellen.
3. Bei der Datenklassifizierung werden Daten mithilfe eines KI-Lernprozesses gescannt.
4. Sie verwenden die bereitgestellten Dashboards und Berichtstools, um Ihre Compliance- und Governance-Bemühungen zu unterstützen.

Nachdem Sie die Datenklassifizierung aktiviert und die zu scannenden Repositories ausgewählt haben (das sind die Volumes, Datenbankschemata oder andere Benutzerdaten), beginnt das Programm sofort mit dem Scannen der Daten, um persönliche und vertrauliche Daten zu identifizieren. In den meisten Fällen sollten Sie sich auf das Scannen von Live-Produktionsdaten konzentrieren, anstatt auf Backups, Spiegel oder DR-Sites. Anschließend ordnet die Datenklassifizierung Ihre Organisationsdaten zu, kategorisiert jede Datei und identifiziert und extrahiert Entitäten und vordefinierte Muster in den Daten. Das Ergebnis des Scans ist ein Index mit persönlichen Informationen, sensiblen persönlichen Informationen, Datenkategorien und Dateitypen.

Data Classification stellt wie jeder andere Client eine Verbindung zu den Daten her, indem es NFS- und CIFS-Volumes einbindet. Auf NFS-Volumes wird automatisch schreibgeschützt zugegriffen, während Sie zum Scannen von CIFS-Volumes Active Directory-Anmeldeinformationen angeben müssen.



Nach dem ersten Scan scannt die Datenklassifizierung Ihre Daten kontinuierlich im Round-Robin-Verfahren, um inkrementelle Änderungen zu erkennen. Aus diesem Grund ist es wichtig, die Instanz am Laufen zu halten.

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

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" .

Was ist der Unterschied zwischen Mapping- und Klassifizierungsscans?

Sie können in der Datenklassifizierung zwei Arten von Scans durchführen:

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

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

Informationen, die durch die Datenklassifizierung kategorisiert werden

Die Datenklassifizierung sammelt, indiziert und ordnet die folgenden Daten Kategorien zu:

- **Standardmetadaten** zu Dateien: Dateityp, Größe, Erstellungs- und Änderungsdatum usw.
- **Personenbezogene Daten**: Persönlich identifizierbare Informationen (PII) wie E-Mail-Adressen, Identifikationsnummern oder Kreditkartennummern, die durch die Datenklassifizierung anhand bestimmter Wörter, Zeichenfolgen und Muster in den Dateien identifiziert werden. "Erfahren Sie mehr über personenbezogene Daten" .
- **Sensible personenbezogene Daten**: Besondere Arten sensibler personenbezogener Daten (SPII), wie Gesundheitsdaten, ethnische Herkunft oder politische Meinungen, wie in der Datenschutz-Grundverordnung (DSGVO) und anderen Datenschutzbestimmungen definiert. "Erfahren Sie mehr über sensible personenbezogene Daten" .
- **Kategorien**: Die Datenklassifizierung nimmt die gescannten Daten und unterteilt sie in verschiedene Kategorien. Kategorien sind Themen, die auf einer KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Mehr über Kategorien erfahren".
- **Namensentitätserkennung**: Die Datenklassifizierung verwendet KI, um die natürlichen Namen von Personen aus Dokumenten zu extrahieren. "Erfahren Sie mehr über die Beantwortung von Auskunftsersuchen betroffener Personen" .

Netzwerkübersicht

Data Classification stellt einen einzelnen Server oder Cluster bereit, wo immer Sie möchten: in der Cloud oder vor Ort. Die Server stellen über Standardprotokolle eine Verbindung zu den Datenquellen her und indizieren die Ergebnisse in einem Elasticsearch-Cluster, der ebenfalls auf denselben Servern bereitgestellt wird. Dies ermöglicht die Unterstützung von Multi-Cloud-, Cross-Cloud-, Private-Cloud- und On-Premises-Umgebungen.

Die Konsole stellt die Datenklassifizierungsinstanz mit einer Sicherheitsgruppe bereit, die eingehende HTTP-Verbindungen vom Konsolenagenten ermöglicht.

Wenn Sie die Konsole im SaaS-Modus verwenden, wird die Verbindung zur Konsole über HTTPS bereitgestellt und die privaten Daten, die zwischen Ihrem Browser und der Datenklassifizierungsinstanz gesendet werden, werden mit einer End-to-End-Verschlüsselung unter Verwendung von TLS 1.2 gesichert, was bedeutet, dass NetApp und Dritte sie nicht lesen können.

Die Outbound-Regeln sind völlig offen. Für die Installation und Aktualisierung der Datenklassifizierungssoftware sowie zum Senden von Nutzungsmetriken ist ein Internetzugang erforderlich.

Wenn Sie strenge Netzwerkanforderungen haben,"Erfahren Sie mehr über die Endpunkte, die die Datenklassifizierung kontaktiert" .

Zugriff auf die NetApp Data Classification

Sie können über die NetApp Console auf die NetApp Data Classification zugreifen.

Um sich bei der Konsole anzumelden, können Sie Ihre Anmeldeinformationen für die NetApp Support-Site verwenden oder sich mit Ihrer E-Mail-Adresse und einem Kennwort für die NetApp Console anmelden. "Erfahren Sie mehr über die Anmeldung bei der Konsole" .

Für bestimmte Aufgaben sind bestimmte Konsolenbenutzerrollen erforderlich. "Erfahren Sie mehr über die Konsolenzugriffsrollen für alle Dienste" .

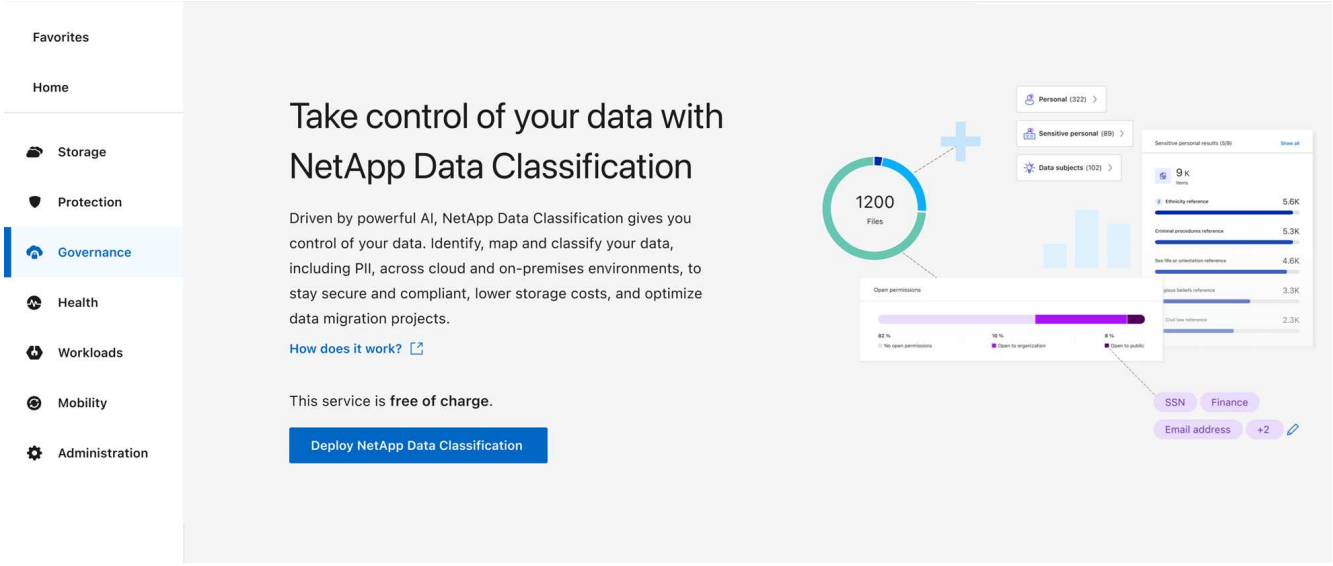
Bevor Sie beginnen

- "Sie sollten einen Konsolenagenten hinzufügen."
- "Finden Sie heraus, welcher Bereitstellungsstil für die Datenklassifizierung zu Ihrer Arbeitslast passt."

Schritte

1. Navigieren Sie in einem Webbrowser zu"Konsole" .
2. Melden Sie sich bei der Konsole an.
3. Wählen Sie auf der Hauptseite der NetApp Console*Governance* > **Datenklassifizierung**.
4. Wenn Sie zum ersten Mal auf die Datenklassifizierung zugreifen, wird die Zielseite angezeigt.

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



Andernfalls wird das Dashboard zur Datenklassifizierung angezeigt.

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

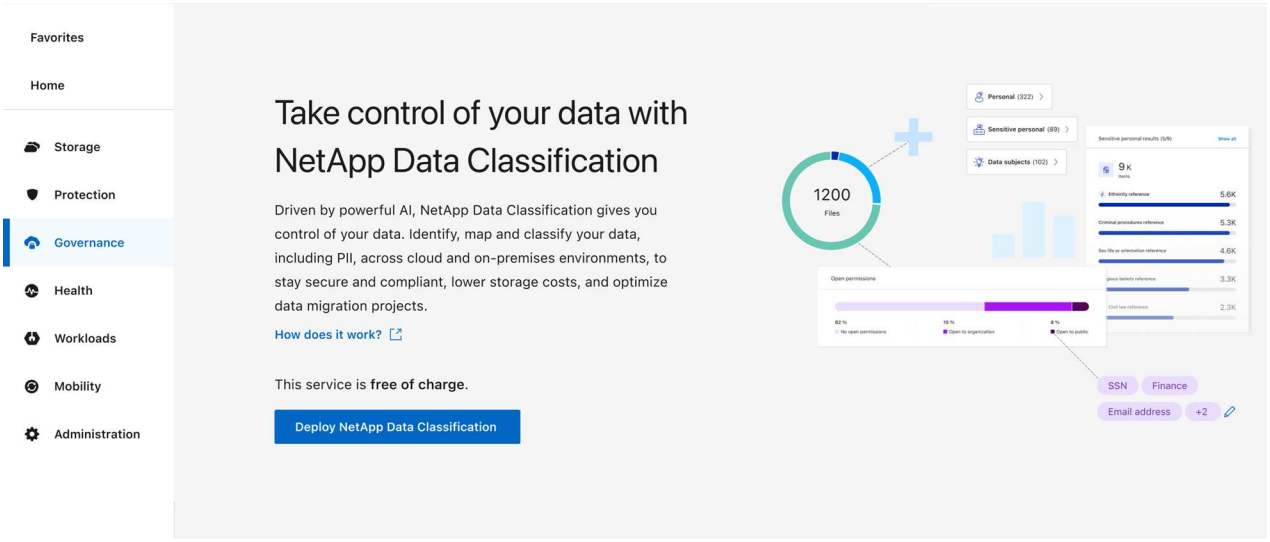
Befolgen Sie diese Schritte, um eine Instanz von Data Classification in der Cloud bereitzustellen. Der Konsolenagent stellt die Instanz in der Cloud bereit und installiert dann die Datenklassifizierungssoftware auf dieser Instanz.

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**.

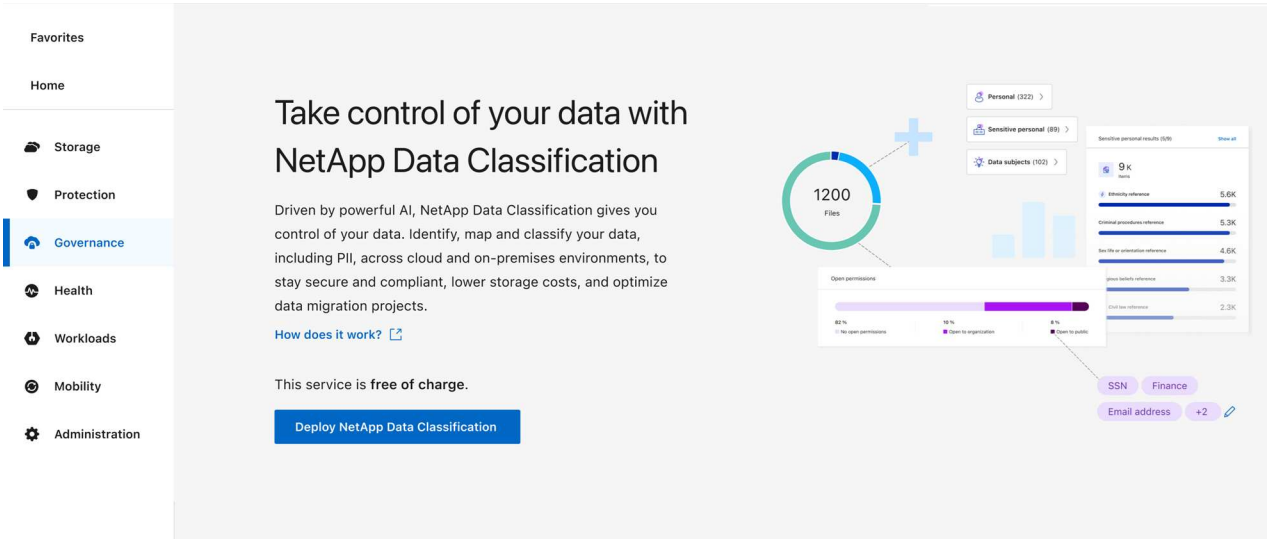


2. Wählen Sie auf der Seite „Installation“ die Option „Bereitstellen > Bereitstellen“ aus, um die Instanzgröße „Groß“ zu verwenden und den Cloud-Bereitstellungsassistenten zu starten.
3. Der Assistent zeigt den Fortschritt an, während er die Bereitstellungsschritte durchläuft. Wenn Eingaben erforderlich 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**.



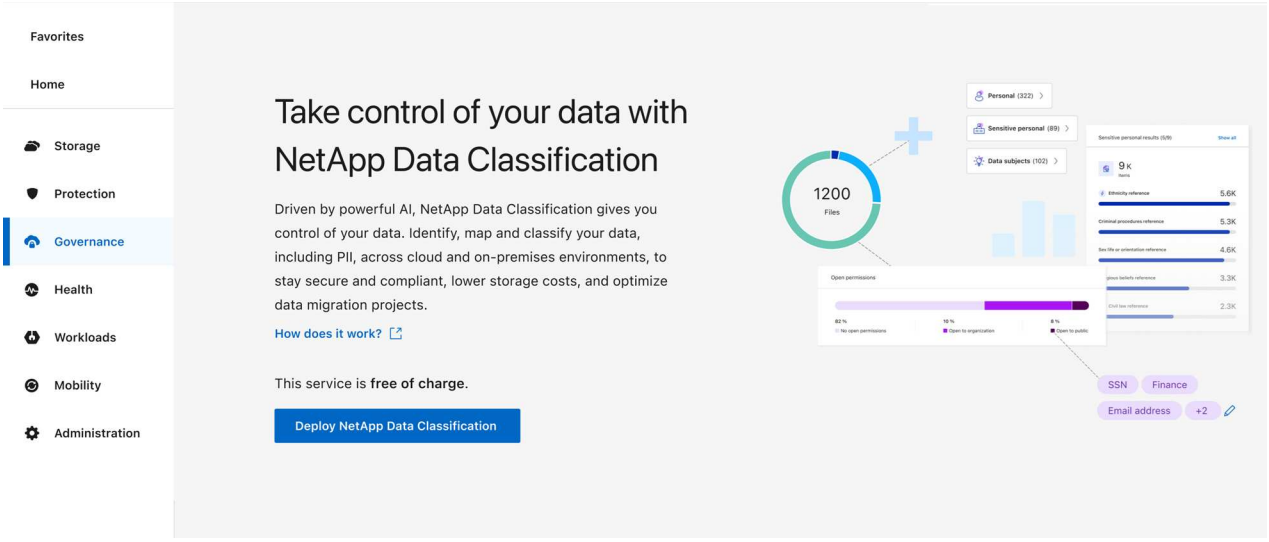
2. Wählen Sie **Bereitstellen**, um den Cloud-Bereitstellungsassistenten zu starten.

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

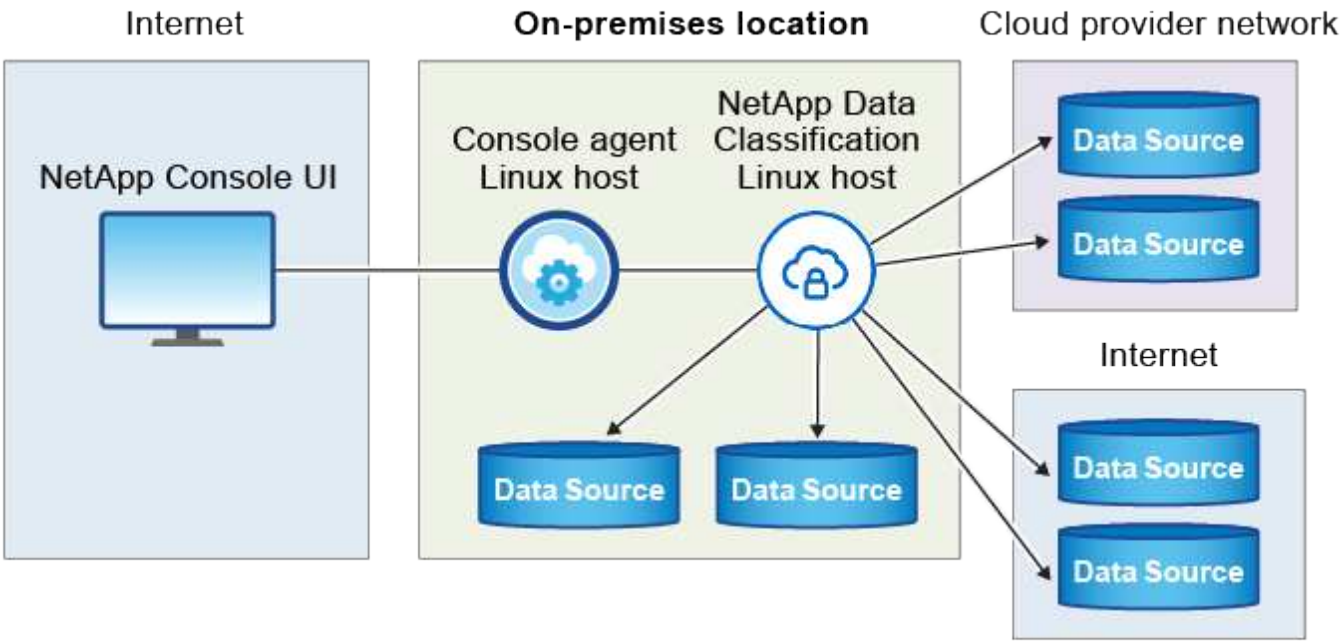
Um NetApp Data Classification auf einem Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud mit Internetzugang bereitzustellen, müssen Sie den Linux-Host manuell in Ihrem Netzwerk oder in der Cloud bereitstellen.

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

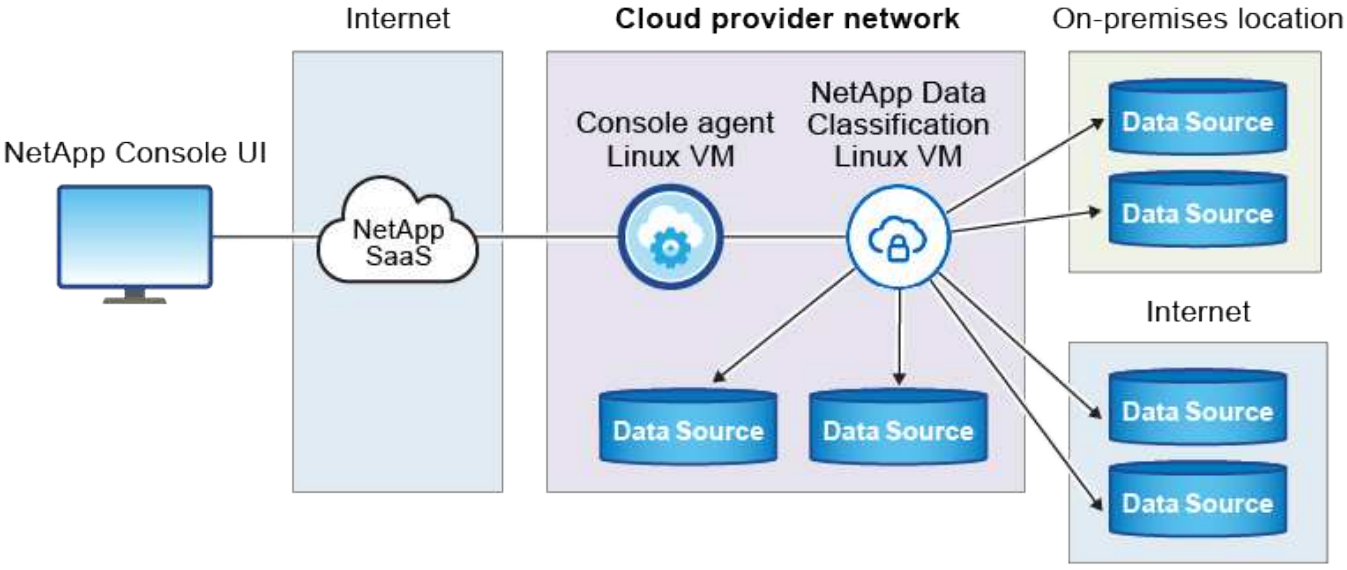
Voraussetzung. Die Software funktioniert unabhängig von der gewählten Installationsmethode gleich.

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

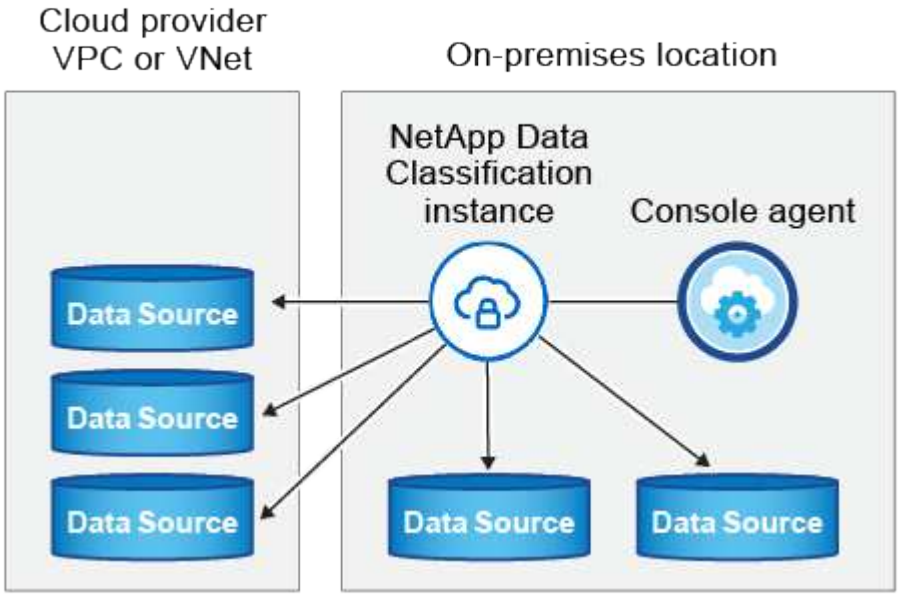
Sie müssen sicherstellen, dass alle erforderlichen Ports für die Kommunikation zwischen dem Konsolenagenten, der Datenklassifizierung, Active Directory und Ihren Datenquellen geöffnet sind.

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

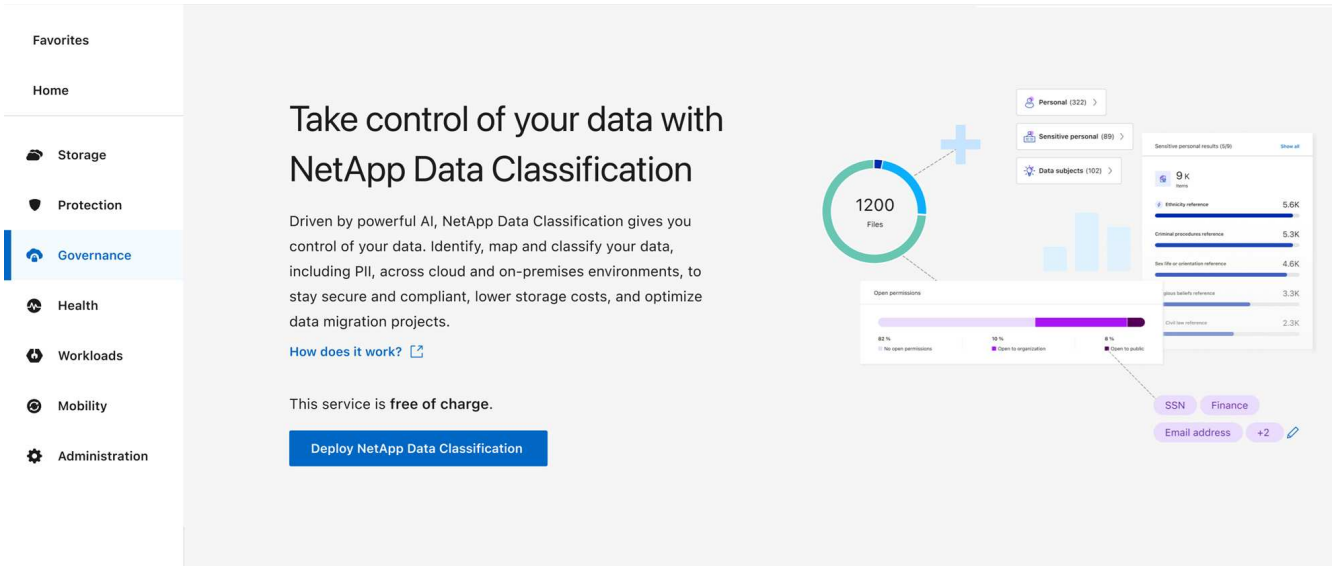
- Überprüfen Sie, ob Ihr Linux-System dieHostanforderungen .
- Stellen Sie sicher, dass auf dem System die beiden erforderlichen Softwarepakete installiert sind (Docker Engine oder Podman und Python 3).
- Stellen Sie sicher, dass Sie über Root-Rechte auf dem Linux-System verfügen.
- Wenn Sie einen Proxy 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.

Aktivieren Sie das Scannen Ihrer Datenquellen

Scannen Sie Datenquellen mit NetApp Data Classification

NetApp Data Classification scannt die Daten in den von Ihnen ausgewählten Repositories (Volumes, Datenbankschemata oder andere Benutzerdaten), um persönliche und vertrauliche Daten zu identifizieren. Die Datenklassifizierung ordnet dann Ihre Organisationsdaten zu, kategorisiert jede Datei und identifiziert vordefinierte Muster in den Daten. Das Ergebnis des Scans ist ein Index mit persönlichen Informationen, sensiblen persönlichen Informationen, Datenkategorien und Dateitypen.

Nach dem ersten Scan scannt die Datenklassifizierung Ihre Daten kontinuierlich im Round-Robin-Verfahren, um inkrementelle Änderungen zu erkennen. Aus diesem Grund ist es wichtig, die Instanz am Laufen zu halten.

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

Was ist der Unterschied zwischen Mapping- und Klassifizierungsscans?

Sie können in der Datenklassifizierung zwei Arten von Scans durchführen:

- **Nur-Mapping-Scans** bieten nur einen allgemeinen Überblick über Ihre Daten und werden für ausgewählte Datenquellen durchgeführt. Scans, die nur eine Zuordnung vornehmen, benötigen weniger Zeit als Scans, die eine Zuordnung und Klassifizierung vornehmen, da sie nicht auf Dateien zugreifen, um die darin enthaltenen Daten anzuzeigen. Möglicherweise möchten Sie dies zunächst tun, um Forschungsbereiche zu identifizieren und dann einen Map & Classify-Scan für diese Bereiche durchzuführen.
- **Map & Classify-Scans** ermöglichen ein gründliches Scannen Ihrer Daten.

Die folgende Tabelle zeigt einige der Unterschiede:

Funktion	Scans zuordnen und klassifizieren	Nur-Mapping-Scans
Scangeschwindigkeit	Langsam	Schnell
Preise	Frei	Frei
Kapazität	Begrenzt auf 500 TiB*	Begrenzt auf 500 TiB*
Liste der Dateitypen und der verwendeten Kapazität	Ja	Ja
Anzahl der Dateien und genutzte Kapazität	Ja	Ja
Alter und Größe der Dateien	Ja	Ja
Fähigkeit zur Ausführung eines"Datenzuordnungsbericht"	Ja	Ja
Seite „Datenuntersuchung“ zum Anzeigen von Dateidetails	Ja	Nein
Suchen nach Namen in Dateien	Ja	Nein
Erstellen"gespeicherte Abfragen" die benutzerdefinierte Suchergebnisse bereitstellen	Ja	Nein
Möglichkeit, andere Berichte auszuführen	Ja	Nein
Möglichkeit, Metadaten aus Dateien anzuzeigen**	Nein	Ja

* Die Datenklassifizierung setzt keine Begrenzung für die Datenmenge, 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" .

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

- System
- Systemtyp
- Speicherrepository
- Dateityp
- Genutzte Kapazität
- Anzahl der Dateien
- Dateigröße
- Dateierstellung
- Letzter Dateizugriff
- Datei zuletzt geändert
- Uhrzeit der Dateierkennung
- Berechtigungsextraktion

Unterschiede im Governance-Dashboard:

Funktion	Kartieren und klassifizieren	Karte
Veraltete Daten	Ja	Ja
Nicht-geschäftliche Daten	Ja	Ja
Duplizierte Dateien	Ja	Ja
Vordefinierte gespeicherte Abfragen	Ja	Nein
Standardmäßig gespeicherte Abfragen	Ja	Ja
DDA-Bericht	Ja	Ja
Mapping-Bericht	Ja	Ja
Erkennung der Empfindlichkeitsstufe	Ja	Nein
Sensible Daten mit umfassenden Berechtigungen	Ja	Nein
Berechtigungen öffnen	Ja	Ja
Alter der Daten	Ja	Ja
Datenmenge	Ja	Ja
Kategorien	Ja	Nein
Dateitypen	Ja	Ja

Unterschiede im Compliance-Dashboard:

Funktion	Kartieren und klassifizieren	Karte
Persönliche Informationen	Ja	Nein
Sensible persönliche Informationen	Ja	Nein
Bericht zur Bewertung des Datenschutzrisikos	Ja	Nein
HIPAA-Bericht	Ja	Nein
PCI DSS-Bericht	Ja	Nein

Unterschiede bei den Untersuchungsfiltern:

Funktion	Kartieren und klassifizieren	Karte
Gespeicherte Abfragen	Ja	Ja
Systemtyp	Ja	Ja
System	Ja	Ja
Speicherrepository	Ja	Ja
Dateityp	Ja	Ja
Dateigröße	Ja	Ja
Erstellungszeit	Ja	Ja
Entdeckte Zeit	Ja	Ja
Zuletzt geändert	Ja	Ja
Letzter Zugriff	Ja	Ja
Berechtigungen öffnen	Ja	Ja
Dateiverzeichnispfad	Ja	Ja
Kategorie	Ja	Nein
Empfindlichkeitsstufe	Ja	Nein
Anzahl der Kennungen	Ja	Nein
personenbezogene Daten	Ja	Nein
Sensible personenbezogene Daten	Ja	Nein
Betroffene Person	Ja	Nein
Duplikate	Ja	Ja
Klassifizierungsstatus	Ja	Der Status ist immer „Eingeschränkte Einblicke“
Scan-Analyseereignis	Ja	Ja
Datei-Hash	Ja	Ja
Anzahl der Benutzer mit Zugriff	Ja	Ja
Benutzer-/Gruppenberechtigungen	Ja	Ja
Dateieigentümer	Ja	Ja
Verzeichnistyp	Ja	Ja

Amazon FSx nach ONTAP -Volumes mit NetApp Data Classification scannen

Führen Sie einige Schritte aus, um Amazon FSx mit NetApp Data Classification nach ONTAP -Volumes zu scannen.

Bevor Sie beginnen

- Sie benötigen einen aktiven Konsolenagenten in AWS, um die Datenklassifizierung bereitzustellen und zu verwalten.
- Die Sicherheitsgruppe, die Sie beim Erstellen des Systems ausgewählt haben, muss Datenverkehr von der Data Classification-Instanz zulassen. Sie können die zugehörige Sicherheitsgruppe mithilfe der mit dem FSx for ONTAP Dateisystem verbundenen ENI finden und mithilfe der AWS Management Console bearbeiten.

  "AWS-Sicherheitsgruppen für Linux-Instanzen"

  "AWS-Sicherheitsgruppen für Windows-Instances"

  "Elastische AWS-Netzwerkschnittstellen (ENI)"

- Stellen Sie sicher, dass die folgenden Ports für die Data Classification-Instanz geöffnet sind:
  - Für NFS – Ports 111 und 2049.
  - Für CIFS – Ports 139 und 445.

Bereitstellen der Datenklassifizierungsinstanz

"Datenklassifizierung bereitstellen"wenn noch keine Instanz bereitgestellt ist.

Sie sollten die Datenklassifizierung im selben AWS-Netzwerk bereitstellen wie den Konsolenagenten für AWS und die FSx-Volumes, die Sie scannen möchten.

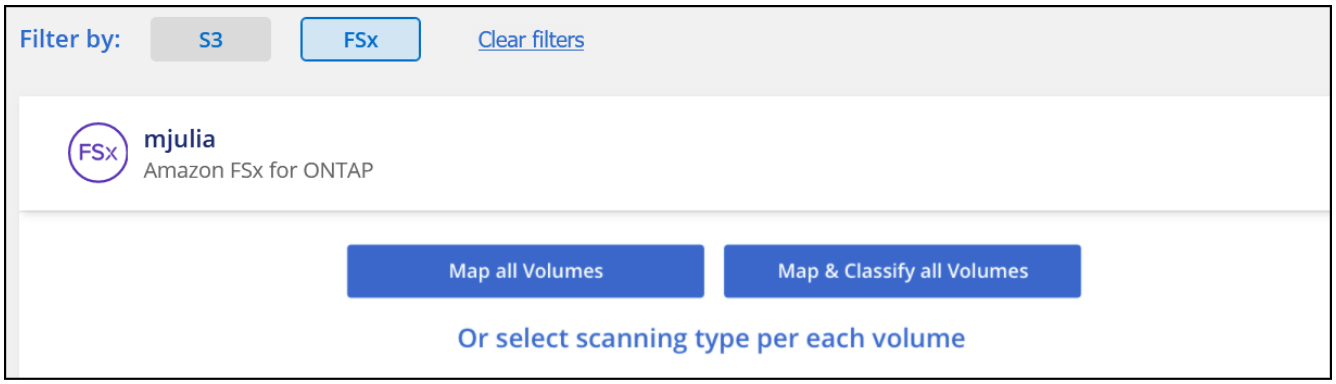
Hinweis: Die Bereitstellung der Datenklassifizierung an einem lokalen Standort wird beim Scannen von FSx-Volumes derzeit nicht unterstützt.

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

Aktivieren Sie die Datenklassifizierung in Ihren Systemen

Sie können die Datenklassifizierung für FSx für ONTAP -Volumes aktivieren.

1. In der NetApp Console: **Governance > Klassifizierung**.
2. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.



3. Wählen Sie aus, wie Sie die Volumes in jedem System scannen möchten. "Erfahren Sie mehr über Mapping- und Klassifizierungsscans":

- Um alle Volumes zuzuordnen, wählen Sie **Alle Volumes zuordnen**.
- Um alle Volumes zuzuordnen und zu klassifizieren, wählen Sie **Alle Volumes zuordnen und klassifizieren**.
- Um das Scannen für jedes Volume anzupassen, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus** und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

4. Wählen Sie im Bestätigungsdialogfeld **Genehmigen** aus, damit die Datenklassifizierung mit dem Scannen Ihrer Datenträger beginnt.

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse stehen im Compliance-Dashboard zur Verfügung, sobald die Datenklassifizierung die ersten Scans abgeschlossen hat. Die dafür benötigte Zeit hängt von der Datenmenge ab und kann einige Minuten oder Stunden betragen. Sie können den Fortschritt des ersten Scans verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die **Systemkonfiguration** auswählen. Verfolgen Sie den Fortschritt jedes Scans in der Fortschrittsleiste. Sie können mit der Maus über die Fortschrittsleiste fahren, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen.

- Wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, scannt das System die Dateien in Ihren Volumes standardmäßig nicht, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus**. Auf der resultierenden Seite können Sie eine Einstellung aktivieren, sodass die Datenklassifizierung die Volumes unabhängig von den Berechtigungen scannt.
- Die Datenklassifizierung scannt nur eine Dateifreigabe unter einem Volume. Wenn Ihre Volumes mehrere Freigaben enthalten, müssen Sie diese anderen Freigaben separat als Freigabegruppe scannen. "Weitere Einzelheiten zu dieser Datenklassifizierungsbeschränkung" .

Überprüfen Sie, ob die Datenklassifizierung Zugriff auf die Volumes hat.

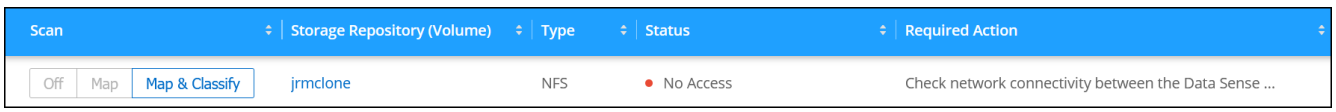
Stellen Sie sicher, dass die Datenklassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien überprüfen.

Sie müssen Data Classification CIFS-Anmeldeinformationen bereitstellen, damit es auf CIFS-Volumes zugreifen kann.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite **Details anzeigen** aus, um den Status zu überprüfen und etwaige Fehler zu beheben.

   Das folgende Bild zeigt beispielsweise ein Volume, das Data Classification aufgrund von Netzwerkverbindungsproblemen zwischen der Data Classification-Instanz und dem Volume nicht scannen kann.



3. Stellen Sie sicher, dass zwischen der Data Classification-Instanz und jedem Netzwerk, das Volumes für

FSx for ONTAP enthält, eine Netzwerkverbindung besteht.

> Bei FSx for ONTAP kann die Datenklassifizierung Volumes nur in derselben Region wie die Konsole scannen.

4. Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Classification-Instanz enthalten, damit diese auf die Daten auf jedem Volume zugreifen kann.
5. Wenn Sie CIFS verwenden, stellen Sie der Datenklassifizierung Active Directory-Anmeldeinformationen zur Verfügung, damit CIFS-Volumes gescannt werden können.

   a. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.

   b. Wählen Sie für jedes System **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Data Classification für den Zugriff auf CIFS-Volumes auf dem System benötigt.

      Die Anmeldeinformationen können schreibgeschützt sein, durch die Angabe von Administratoranmeldeinformationen wird jedoch sichergestellt, dass die Datenklassifizierung alle Daten lesen kann, für die erweiterte Berechtigungen erforderlich sind. Die Anmeldeinformationen werden auf der Data Classification-Instanz gespeichert.

      Wenn Sie sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Datenklassifizierungsscans unverändert bleiben, wird empfohlen, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

Nachdem Sie die Anmeldeinformationen eingegeben haben, sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.

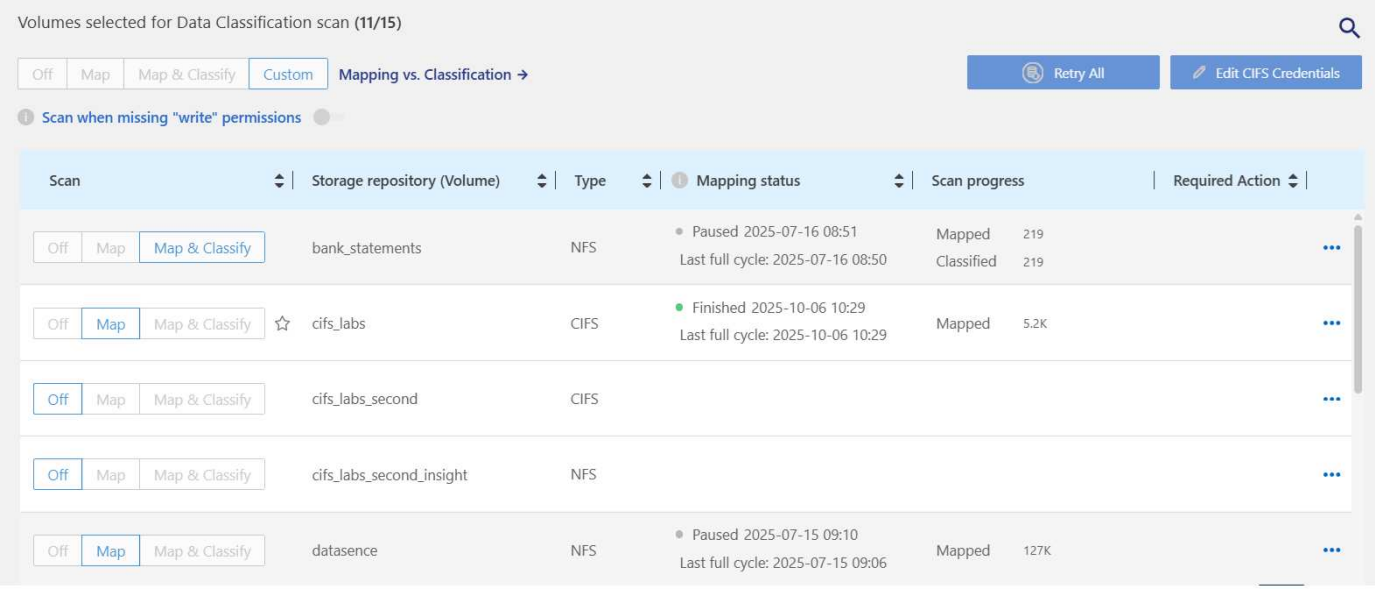
Aktivieren und Deaktivieren von Scans auf Volumes

Sie können Scans auf jedem System jederzeit von der Konfigurationsseite aus starten oder stoppen. Sie können Scans auch von reinen Mapping-Scans auf Mapping- und Klassifizierungs-Scans umstellen und umgekehrt. Es wird empfohlen, alle Volumes in einem System zu scannen.

> Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und klassifizieren** ausgewählt haben. Wenn Sie im Überschriftenbereich die Option **Benutzerdefiniert** oder **Aus** einstellen, müssen Sie die Zuordnung und/oder das vollständige Scannen für jedes neue Volume aktivieren, das Sie dem System hinzufügen.

Der Schalter oben auf der Seite für **Scannen bei fehlenden Schreibberechtigungen** ist standardmäßig deaktiviert. Dies bedeutet, dass das System die Dateien nicht scannt, wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter auf EIN und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Mehr erfahren".

Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und Klassifizieren** festgelegt haben. Wenn die Einstellung für alle Volumes **Benutzerdefiniert** oder **Aus** ist, müssen Sie das Scannen für jedes neue Volume, das Sie hinzufügen, manuell aktivieren.



Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie ein System und dann **Konfiguration**.
3. Um Scans für alle Volumes zu aktivieren oder zu deaktivieren, wählen Sie in der Überschrift über allen Volumes **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus**.

   Um Scans für einzelne Volumes zu aktivieren oder zu deaktivieren, suchen Sie die Volumes in der Liste und wählen Sie dann neben dem Volumenamen **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus** aus.

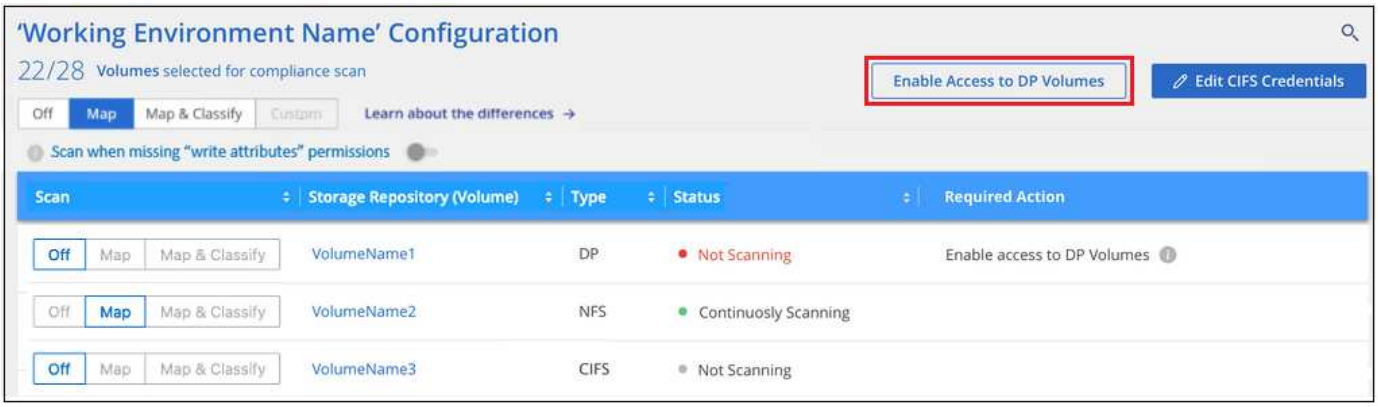
Ergebnis

Wenn Sie das Scannen aktivieren, beginnt die Datenklassifizierung mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse werden im Compliance-Dashboard angezeigt, sobald die Datenklassifizierung mit dem Scan beginnt. Die Dauer des Scans hängt von der Datenmenge ab und kann zwischen Minuten und Stunden liegen.

Scannen von Datenschutzvolumes

Standardmäßig werden Datenschutzvolumes (DP) nicht gescannt, da sie nicht extern verfügbar sind und die Datenklassifizierung nicht auf sie zugreifen kann. Dies sind die Zielvolumes für SnapMirror -Vorgänge von einem FSx für ONTAP Dateisystem.

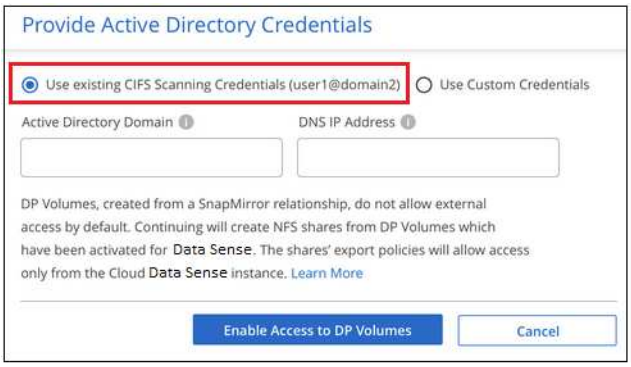
Zunächst werden diese Volumes in der Volumeliste als *Typ* **DP** mit dem *Status* **Nicht scannen** und der *Erforderlichen Aktion* **Zugriff auf DP-Volumes aktivieren** identifiziert.

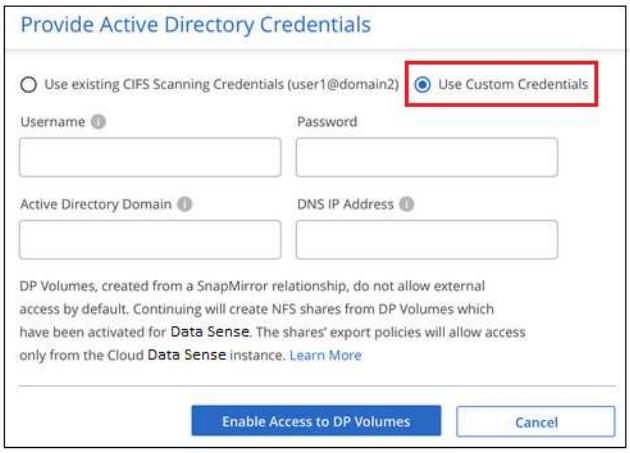


Schritte

Wenn Sie diese Datenschutzvolumes scannen möchten:

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie oben auf der Seite **Zugriff auf DP-Volumes aktivieren** aus.
3. Überprüfen Sie die Bestätigungsnachricht und wählen Sie erneut **Zugriff auf DP-Volumes aktivieren**.
   - Volumes, die ursprünglich als NFS-Volumes im Quell-FSx für ONTAP -Dateisystem erstellt wurden, sind aktiviert.
   - Für Volumes, die ursprünglich als CIFS-Volumes im Quelldateisystem FSx for ONTAP erstellt wurden, müssen Sie CIFS-Anmeldeinformationen eingeben, um diese DP-Volumes zu scannen. Wenn Sie bereits Active Directory-Anmeldeinformationen eingegeben haben, damit Data Classification CIFS-Volumes scannen kann, können Sie diese Anmeldeinformationen verwenden oder einen anderen Satz von Administratoranmeldeinformationen angeben.





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

Ergebnis

Nach der Aktivierung erstellt die Datenklassifizierung eine NFS-Freigabe aus jedem DP-Volume, das zum Scannen aktiviert wurde. Die Freigabeexportrichtlinien erlauben nur den Zugriff von der Datenklassifizierungsinstanz.

Wenn Sie beim ersten Aktivieren des Zugriffs auf DP-Volumes keine CIFS-Datensicherungsvolumes hatten und später welche hinzufügen, wird oben auf der Konfigurationsseite die Schaltfläche **Zugriff auf CIFS DP aktivieren** angezeigt. Wählen Sie diese Schaltfläche und fügen Sie CIFS-Anmeldeinformationen hinzu, um den Zugriff auf diese CIFS-DP-Volumes zu ermöglichen.

Active Directory-Anmeldeinformationen werden nur in der Speicher-VM des ersten CIFS-DP-Volumes registriert, daher werden alle DP-Volumes auf dieser SVM gescannt. Bei Volumes, die sich auf anderen SVMs befinden, sind die Active Directory-Anmeldeinformationen nicht registriert, sodass diese DP-Volumes nicht gescannt werden.

Scannen von Azure NetApp Files Volumes mit NetApp Data Classification

Führen Sie einige Schritte aus, um mit der NetApp Data Classification für Azure NetApp Files zu beginnen.

Ermitteln Sie das Azure NetApp Files -System, das Sie scannen möchten.

Wenn das Azure NetApp Files -System, das Sie scannen möchten, nicht bereits als System in der NetApp Console vorhanden ist,"fügen Sie es auf der Seite „Systeme“ hinzu" .

Bereitstellen der Datenklassifizierungsinstanz

"Datenklassifizierung bereitstellen"wenn noch keine Instanz bereitgestellt ist.

Die Datenklassifizierung muss beim Scannen von Azure NetApp Files Volumes in der Cloud bereitgestellt werden und zwar in derselben Region wie die Volumes, die Sie scannen möchten.

Hinweis: Die Bereitstellung der Datenklassifizierung an einem lokalen Standort wird beim Scannen von Azure NetApp Files -Volumes derzeit nicht unterstützt.

Aktivieren Sie die Datenklassifizierung in Ihren Systemen

Sie können die Datenklassifizierung auf Ihren Azure NetApp Files Volumes aktivieren.

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.

2. Wählen Sie aus, wie Sie die Volumes in jedem System scannen möchten. "Erfahren Sie mehr über Mapping- und Klassifizierungsscans":
   - Um alle Volumes zuzuordnen, wählen Sie **Alle Volumes zuordnen**.
   - Um alle Volumes zuzuordnen und zu klassifizieren, wählen Sie **Alle Volumes zuordnen und klassifizieren**.
   - Um das Scannen für jedes Volume anzupassen, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus** und wählen Sie dann die Volumes aus, die Sie zuordnen oder zuordnen und klassifizieren möchten.

     SehenAktivieren oder Deaktivieren von Scans auf Volumes für Details.

3. Wählen Sie im Bestätigungsdialogfeld **Genehmigen** aus.

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse sind im Compliance-Dashboard verfügbar, sobald die Datenklassifizierung die ersten Scans abgeschlossen hat. Die dafür benötigte Zeit hängt von der Datenmenge ab und kann einige Minuten oder Stunden betragen. Sie können den Fortschritt des ersten Scans verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die **Systemkonfiguration** auswählen. Die Datenklassifizierung zeigt für jeden Scan einen Fortschrittsbalken an. Sie können mit der Maus über den Fortschrittsbalken fahren, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen.

- Wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, scannt das System die Dateien in Ihren Volumes standardmäßig nicht, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus**. Auf der resultierenden Seite können Sie eine Einstellung aktivieren, sodass die Datenklassifizierung die Volumes unabhängig von den Berechtigungen scannt.
- Die Datenklassifizierung scannt nur eine Dateifreigabe unter einem Volume. Wenn Ihre Volumes mehrere Freigaben enthalten, müssen Sie diese anderen Freigaben separat als Freigabegruppe scannen. "Erfahren Sie mehr über diese Einschränkung der Datenklassifizierung" .

Überprüfen Sie, ob die Datenklassifizierung Zugriff auf die Volumes hat.

Stellen Sie sicher, dass die Datenklassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien überprüfen. Sie müssen Data Classification CIFS-Anmeldeinformationen bereitstellen, damit es auf CIFS-Volumes zugreifen kann.

Bei Azure NetApp Files kann die Datenklassifizierung nur Volumes in derselben Region wie die Konsole scannen.

Checklist

- Stellen Sie sicher, dass zwischen der Data Classification-Instanz und jedem Netzwerk, das Volumes für Azure NetApp Files enthält, eine Netzwerkverbindung besteht.
- Stellen Sie sicher, dass die folgenden Ports für die Data Classification-Instanz geöffnet sind:
  - Für NFS – Ports 111 und 2049.
  - Für CIFS – Ports 139 und 445.
- Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Classification-Instanz enthalten, damit diese auf die Daten auf jedem Volume zugreifen kann.

Schritte

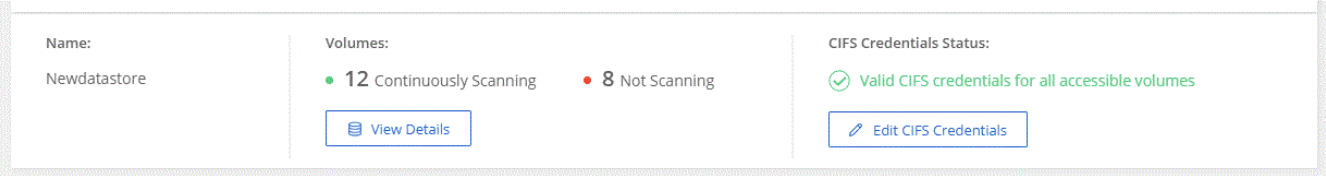
1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.

   a. Wenn Sie CIFS (SMB) verwenden, stellen Sie sicher, dass die Active Directory-Anmeldeinformationen korrekt sind. Wählen Sie für jedes System **CIFS-Anmeldeinformationen bearbeiten** und geben Sie dann den Benutzernamen und das Kennwort ein, die Data Classification für den Zugriff auf CIFS-Volumes auf dem System benötigt.

      Die Anmeldeinformationen können schreibgeschützt sein. Durch die Angabe von Administratoranmeldeinformationen wird sichergestellt, dass die Datenklassifizierung alle Daten lesen kann, für die erweiterte Berechtigungen erforderlich sind. Die Anmeldeinformationen werden auf der Data Classification-Instanz gespeichert.

Wenn Sie sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Datenklassifizierungsscans unverändert bleiben, wird empfohlen, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

Nachdem Sie die Anmeldeinformationen eingegeben haben, sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.



2. Wählen Sie auf der Konfigurationsseite **Details anzeigen** aus, um den Status für jedes CIFS- und NFS-Volume zu überprüfen. Korrigieren Sie gegebenenfalls alle Fehler, beispielsweise Probleme mit der Netzwerkverbindung.

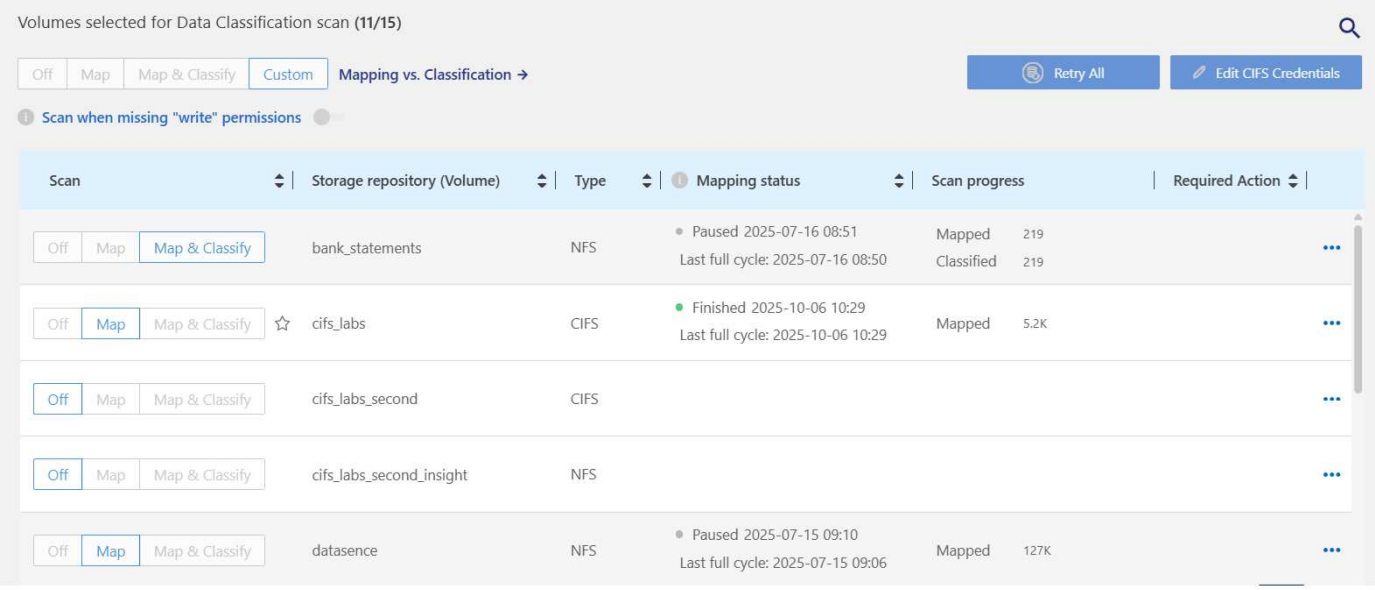
Aktivieren oder Deaktivieren von Scans auf Volumes

Sie können Scans auf jedem System jederzeit von der Konfigurationsseite aus starten oder stoppen. Sie können Scans auch von reinen Mapping-Scans auf Mapping- und Klassifizierungs-Scans umstellen und umgekehrt. Es wird empfohlen, alle Volumes in einem System zu scannen.

Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und klassifizieren** ausgewählt haben. Wenn Sie im Überschriftenbereich die Option **Benutzerdefiniert** oder **Aus** einstellen, müssen Sie die Zuordnung und/oder das vollständige Scannen für jedes neue Volume aktivieren, das Sie dem System hinzufügen.

Der Schalter oben auf der Seite für **Scannen bei fehlenden Schreibberechtigungen** ist standardmäßig deaktiviert. Dies bedeutet, dass das System die Dateien nicht scannt, wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter auf EIN und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Mehr erfahren".

Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und Klassifizieren** festgelegt haben. Wenn die Einstellung für alle Volumes **Benutzerdefiniert** oder **Aus** ist, müssen Sie das Scannen für jedes neue Volume, das Sie hinzufügen, manuell aktivieren.



Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie ein System und dann **Konfiguration**.
3. Um Scans für alle Volumes zu aktivieren oder zu deaktivieren, wählen Sie in der Überschrift über allen Volumes **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus**.

   Um Scans für einzelne Volumes zu aktivieren oder zu deaktivieren, suchen Sie die Volumes in der Liste und wählen Sie dann neben dem Volumenamen **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus** aus.

Ergebnis

Wenn Sie das Scannen aktivieren, beginnt die Datenklassifizierung mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse werden im Compliance-Dashboard angezeigt, sobald die Datenklassifizierung mit dem Scan beginnt. Die Dauer des Scans hängt von der Datenmenge ab und kann zwischen Minuten und Stunden liegen.

Scannen Sie Cloud Volumes ONTAP und lokale ONTAP Volumes mit NetApp Data Classification

Führen Sie einige Schritte aus, um mit dem Scannen Ihrer Cloud Volumes ONTAP und lokalen ONTAP Volumes mithilfe der NetApp Data Classification zu beginnen.

Voraussetzungen

Stellen Sie vor dem Aktivieren der Datenklassifizierung sicher, dass Sie über eine unterstützte Konfiguration verfügen.

- Wenn Sie Cloud Volumes ONTAP und lokale ONTAP -Systeme scannen, die über das Internet zugänglich sind, können Sie"Datenklassifizierung in der Cloud bereitstellen" oder"an einem lokalen Standort mit Internetzugang" .
- Wenn Sie lokale ONTAP -Systeme scannen, die an einem Dark Site ohne Internetzugang installiert wurden, müssen Sie"Stellen Sie die Datenklassifizierung am selben lokalen Standort bereit, der keinen Internetzugang hat" . Dazu muss der Konsolenagent am selben lokalen Standort bereitgestellt werden.

Überprüfen Sie, ob die Datenklassifizierung Zugriff auf die Volumes hat.

Stellen Sie sicher, dass die Datenklassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien überprüfen. Sie müssen Data Classification CIFS-Anmeldeinformationen bereitstellen, damit es auf CIFS-Volumes zugreifen kann.

Checklist

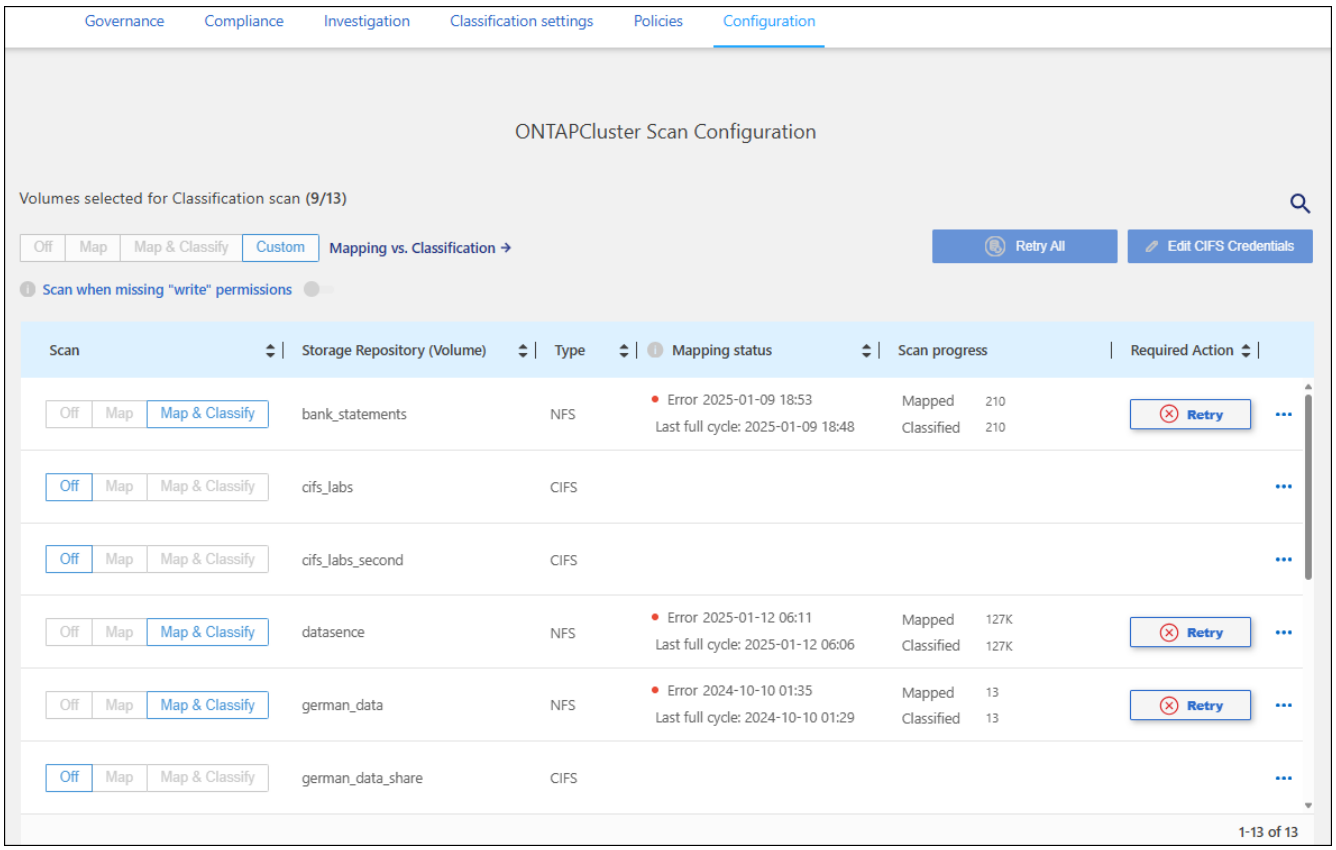
- Stellen Sie sicher, dass zwischen der Data Classification-Instanz und jedem Netzwerk, das Volumes für Cloud Volumes ONTAP oder lokale ONTAP Cluster enthält, eine Netzwerkverbindung besteht.
- Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr von der Data Classification-Instanz zulässt.

  Sie können die Sicherheitsgruppe entweder für den Datenverkehr von der IP-Adresse der Data Classification-Instanz öffnen oder Sie können die Sicherheitsgruppe für den gesamten Datenverkehr innerhalb des virtuellen Netzwerks öffnen.

- Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Classification-Instanz enthalten, damit diese auf die Daten auf jedem Volume zugreifen kann.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.



2. Wenn Sie CIFS verwenden, stellen Sie der Datenklassifizierung Active Directory-Anmeldeinformationen zur Verfügung, damit CIFS-Volumes gescannt werden können. Wählen Sie für jedes System **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Data Classification für den Zugriff auf CIFS-Volumes auf dem System benötigt.

   Die Anmeldeinformationen können schreibgeschützt sein, durch die Angabe von Administratoranmeldeinformationen wird jedoch sichergestellt, dass die Datenklassifizierung alle Daten

lesen kann, für die erweiterte Berechtigungen erforderlich sind. Die Anmeldeinformationen werden auf der Data Classification-Instanz gespeichert.

Wenn Sie sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Datenklassifizierungsscans unverändert bleiben, wird empfohlen, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

Wenn Sie die Anmeldeinformationen korrekt eingegeben haben, bestätigt eine Meldung, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.

3. Wählen Sie auf der Konfigurationsseite **Konfiguration** aus, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und etwaige Fehler zu beheben.

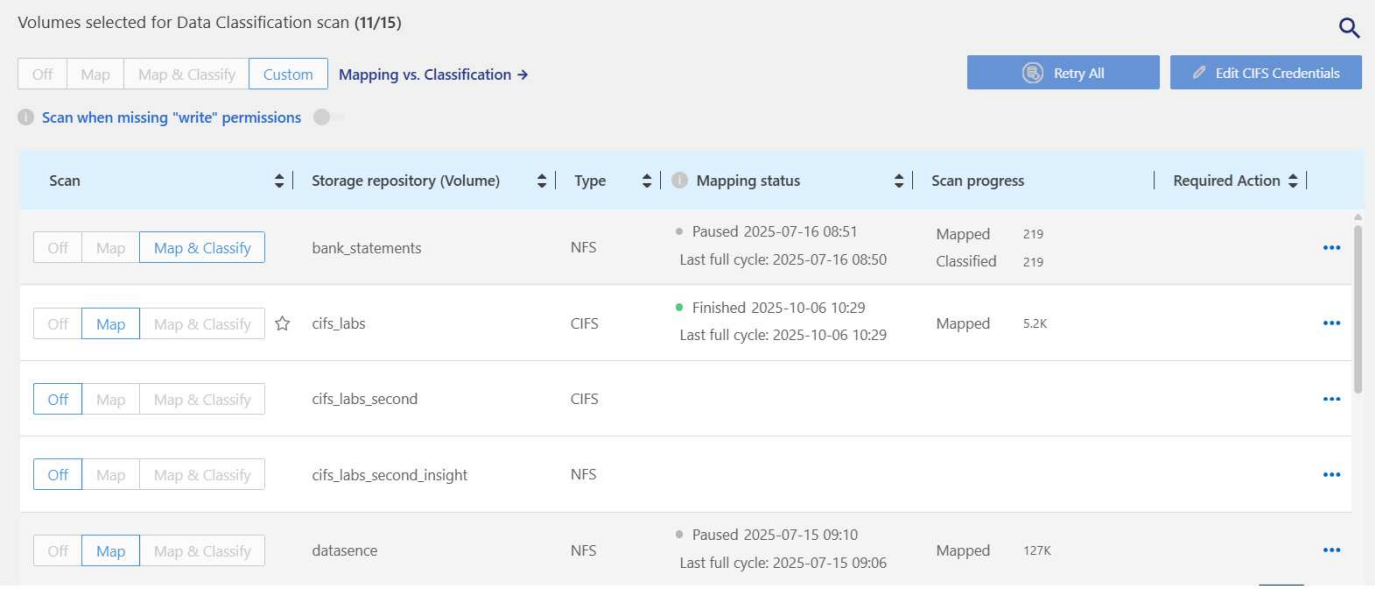
Aktivieren oder Deaktivieren von Scans auf Volumes

Sie können Scans auf jedem System jederzeit von der Konfigurationsseite aus starten oder stoppen. Sie können Scans auch von reinen Mapping-Scans auf Mapping- und Klassifizierungs-Scans umstellen und umgekehrt. Es wird empfohlen, alle Volumes in einem System zu scannen.

> Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und klassifizieren** ausgewählt haben. Wenn Sie im Überschriftenbereich die Option **Benutzerdefiniert** oder **Aus** einstellen, müssen Sie die Zuordnung und/oder das vollständige Scannen für jedes neue Volume aktivieren, das Sie dem System hinzufügen.

Der Schalter oben auf der Seite für **Scannen bei fehlenden Schreibberechtigungen** ist standardmäßig deaktiviert. Dies bedeutet, dass das System die Dateien nicht scannt, wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter auf EIN und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Mehr erfahren".

> Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und Klassifizieren** festgelegt haben. Wenn die Einstellung für alle Volumes **Benutzerdefiniert** oder **Aus** ist, müssen Sie das Scannen für jedes neue Volume, das Sie hinzufügen, manuell aktivieren.



Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie ein System und dann **Konfiguration**.
3. Um Scans für alle Volumes zu aktivieren oder zu deaktivieren, wählen Sie in der Überschrift über allen Volumes **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus**.

   Um Scans für einzelne Volumes zu aktivieren oder zu deaktivieren, suchen Sie die Volumes in der Liste und wählen Sie dann neben dem Volumenamen **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus** aus.

Ergebnis

Wenn Sie das Scannen aktivieren, beginnt die Datenklassifizierung mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse werden im Compliance-Dashboard angezeigt, sobald die Datenklassifizierung mit dem Scan beginnt. Die Dauer des Scans hängt von der Datenmenge ab und kann zwischen Minuten und Stunden liegen.

Die Datenklassifizierung scannt nur eine Dateifreigabe unter einem Volume. Wenn Ihre Volumes mehrere Freigaben enthalten, müssen Sie diese anderen Freigaben separat als Freigabegruppe scannen. "Weitere Einzelheiten zu dieser Datenklassifizierungsbeschränkung" .

Scannen Sie Datenbankschemata mit NetApp Data Classification

Führen Sie einige Schritte aus, um mit dem Scannen Ihrer Datenbankschemata mit NetApp Data Classification zu beginnen.

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie die Datenklassifizierung aktivieren.

Unterstützte Datenbanken

Die Datenklassifizierung kann Schemata aus den folgenden Datenbanken scannen:

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

Die Funktion zum Sammeln von Statistiken **muss** in der Datenbank aktiviert sein.

Datenbankanforderungen

Jede Datenbank mit Verbindung zur Datenklassifizierungsinstanz kann gescannt werden, unabhängig davon, wo sie gehostet wird. Um eine Verbindung zur Datenbank herzustellen, benötigen Sie lediglich die folgenden Informationen:

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

  Bei der Auswahl eines Benutzernamens und Kennworts ist es wichtig, dass Sie einen Benutzernamen und ein Kennwort auswählen, der über vollständige Leseberechtigungen für alle Schemata und Tabellen verfügt, die Sie scannen möchten. Wir empfehlen Ihnen, einen dedizierten Benutzer für das Datenklassifizierungssystem mit allen erforderlichen Berechtigungen zu erstellen.

Für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

Bereitstellen der Datenklassifizierungsinstanz

Stellen Sie die Datenklassifizierung bereit, wenn noch keine Instanz bereitgestellt ist.

Wenn Sie Datenbankschemata scannen, die über das Internet zugänglich sind, können Sie"Datenklassifizierung in der Cloud bereitstellen" oder"Stellen Sie die Datenklassifizierung an einem lokalen Standort mit Internetzugang bereit" .

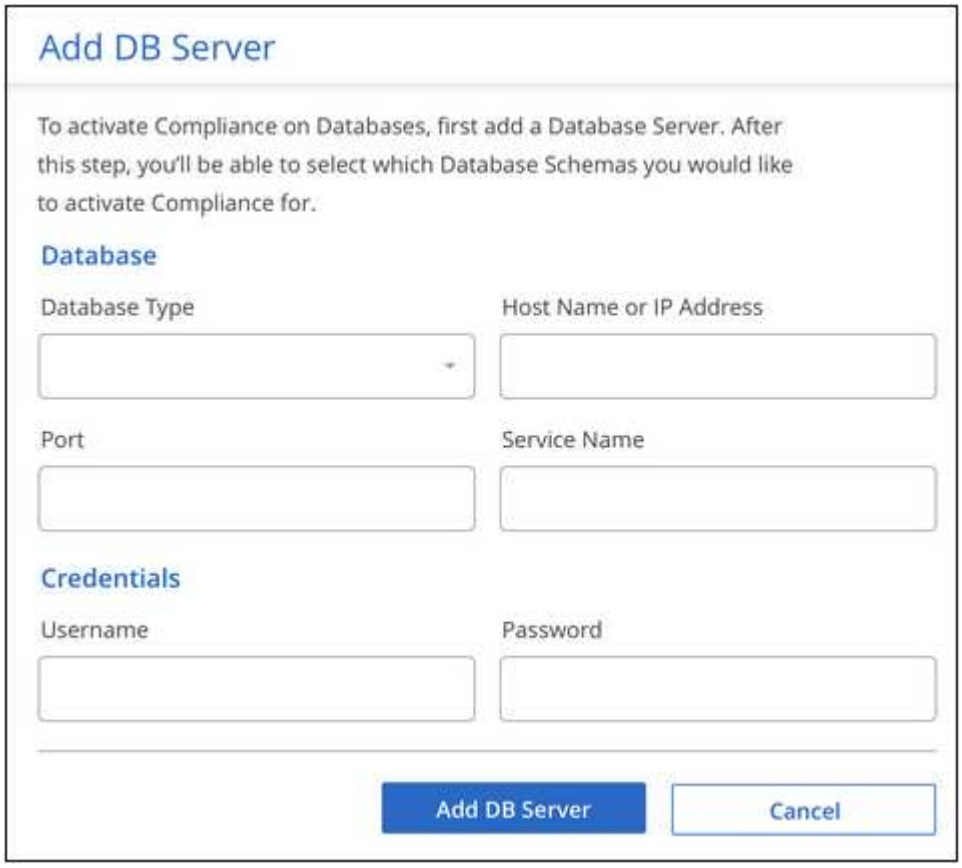
Wenn Sie Datenbankschemata scannen, die in einer Dark Site ohne Internetzugang installiert wurden, müssen Sie"Stellen Sie die Datenklassifizierung am selben lokalen Standort bereit, der keinen Internetzugang hat" . Dies erfordert auch, dass der Konsolenagent am selben lokalen Standort bereitgestellt wird.

Hinzufügen des Datenbankservers

Fügen Sie den Datenbankserver hinzu, auf dem sich die Schemas befinden.

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite **System hinzufügen** > **Datenbankserver hinzufügen**.
3. Geben Sie die erforderlichen Informationen zur Identifizierung des Datenbankservers ein.

a. Wählen Sie den Datenbanktyp aus.
b. Geben Sie den Port und den Hostnamen oder die IP-Adresse ein, um eine Verbindung zur Datenbank herzustellen.
c. Geben Sie für Oracle-Datenbanken den Dienstnamen ein.
d. Geben Sie die Anmeldeinformationen ein, damit Data Classification auf den Server zugreifen kann.
e. Wählen Sie **DB-Server hinzufügen**.



Die Datenbank wird der Liste der Systeme hinzugefügt.

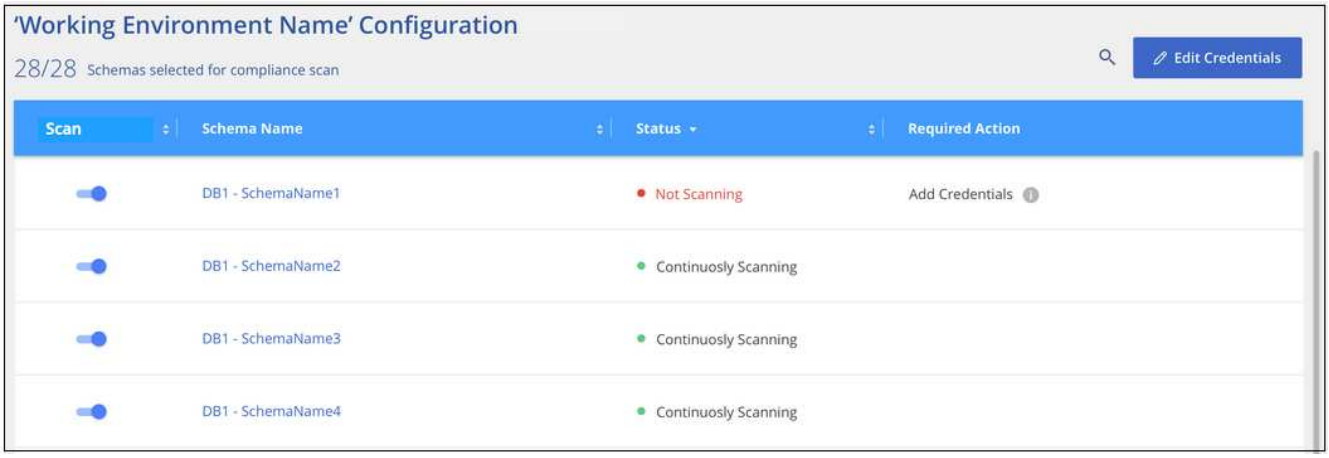
Aktivieren und Deaktivieren von Scans für Datenbankschemata

Sie können den vollständigen Scan Ihrer Schemata jederzeit stoppen oder starten.

Es gibt keine Option zum Auswählen von Nur-Mapping-Scans für Datenbankschemata.

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

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



Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen aktivierten Datenbankschemata. Sie können den Fortschritt des ersten Scans verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die **Systemkonfiguration** auswählen. Der Fortschritt jedes Scans wird als Fortschrittsbalken angezeigt. Sie können auch mit der Maus über den Fortschrittsbalken fahren, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen. Wenn Fehler vorliegen, werden diese zusammen mit den erforderlichen Maßnahmen zur Behebung des Fehlers in der Spalte „Status“ angezeigt.

Die Datenklassifizierung scannt Ihre Datenbanken einmal pro Tag; Datenbanken werden nicht kontinuierlich gescannt wie andere Datenquellen.

Google Cloud NetApp Volumes mit NetApp Data Classification scannen

NetApp Data Classification unterstützt Google Cloud NetApp Volumes als System. Erfahren Sie, wie Sie Ihr Google Cloud NetApp Volumes -System scannen.

Ermitteln Sie das Google Cloud NetApp Volumes -System, das Sie scannen möchten

Wenn das Google Cloud NetApp Volumes -System, das Sie scannen möchten, nicht bereits als System in der NetApp Console vorhanden ist,"fügen Sie es der Seite „Systeme“ hinzu" .

Bereitstellen der Datenklassifizierungsinstanz

"Datenklassifizierung bereitstellen"wenn noch keine Instanz bereitgestellt ist.

Beim Scannen von Google Cloud NetApp Volumes muss die Datenklassifizierung in der Cloud bereitgestellt werden, und zwar in derselben Region wie die Volumes, die Sie scannen möchten.

Hinweis: Die Bereitstellung der Datenklassifizierung an einem lokalen Standort wird beim Scannen von Google Cloud NetApp Volumes derzeit nicht unterstützt.

Aktivieren Sie die Datenklassifizierung in Ihren Systemen

Sie können die Datenklassifizierung auf Ihrem Google Cloud NetApp Volumes -System aktivieren.

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie aus, wie Sie die Volumes in jedem System scannen möchten. "Erfahren Sie mehr über Mapping- und Klassifizierungsscans":
   - Um alle Volumes zuzuordnen, wählen Sie **Alle Volumes zuordnen**.
   - Um alle Volumes zuzuordnen und zu klassifizieren, wählen Sie **Alle Volumes zuordnen und klassifizieren**.
   - Um das Scannen für jedes Volume anzupassen, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus** und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

     SehenAktivieren und Deaktivieren von Scans auf Volumes für Details.
3. Wählen Sie im Bestätigungsdialogfeld **Genehmigen** aus.

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse sind im Compliance-Dashboard verfügbar, sobald die Datenklassifizierung die ersten Scans abgeschlossen hat. Die dafür benötigte Zeit hängt von der Datenmenge ab: einige Minuten bis einige Stunden. Sie können den Fortschritt des ersten Scans im Abschnitt **Systemkonfiguration** des Menüs **Konfiguration** verfolgen. Die Datenklassifizierung zeigt für jeden Scan einen Fortschrittsbalken an. Sie können auch mit der Maus über den Fortschrittsbalken fahren, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen.

- Wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, scannt das System die Dateien in Ihren Volumes standardmäßig nicht, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, wählen Sie **Oder wählen Sie den Scantyp für jedes Volume aus**. Auf der resultierenden Seite können Sie eine Einstellung aktivieren, sodass die Datenklassifizierung die Volumes unabhängig von den Berechtigungen scannt.
- Die Datenklassifizierung scannt nur eine Dateifreigabe unter einem Volume. Wenn Ihre Volumes mehrere Freigaben enthalten, müssen Sie diese anderen Freigaben separat als Freigabegruppe scannen. "Erfahren Sie mehr über diese Einschränkung der Datenklassifizierung".

Überprüfen Sie, ob die Datenklassifizierung Zugriff auf die Volumes hat.

Stellen Sie sicher, dass die Datenklassifizierung auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien überprüfen. Für CIFS-Volumes müssen Sie die Datenklassifizierung mit CIFS-Anmeldeinformationen bereitstellen.

Bei Google Cloud NetApp Volumes kann die Datenklassifizierung nur Volumes in derselben Region wie die Konsole scannen.

Checklist

- Stellen Sie sicher, dass zwischen der Data Classification-Instanz und jedem Netzwerk, das Volumes für Google Cloud NetApp Volumes enthält, eine Netzwerkverbindung besteht.
- Stellen Sie sicher, dass die folgenden Ports für die Data Classification-Instanz geöffnet sind:
  - Für NFS – Ports 111 und 2049.
  - Für CIFS – Ports 139 und 445.
- Stellen Sie sicher, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Data Classification-Instanz enthalten, damit diese auf die Daten auf jedem Volume zugreifen kann.

Schritte

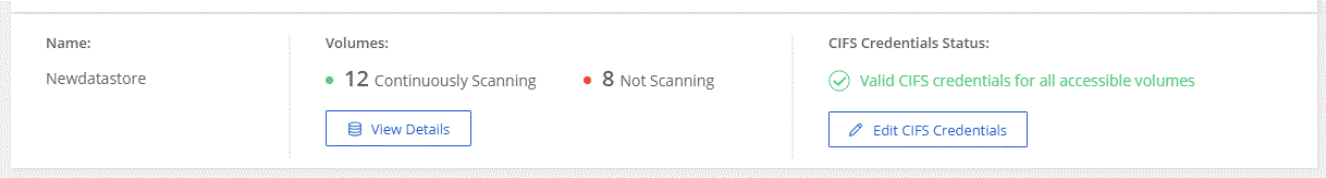
1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.

   a. Wenn Sie CIFS (SMB) verwenden, stellen Sie sicher, dass die Active Directory-Anmeldeinformationen korrekt sind. Wählen Sie für jedes System **CIFS-Anmeldeinformationen bearbeiten** und geben Sie dann den Benutzernamen und das Kennwort ein, die Data Classification für den Zugriff auf CIFS-Volumes auf dem System benötigt.

      Die Anmeldeinformationen können schreibgeschützt sein, durch die Angabe von Administratoranmeldeinformationen wird jedoch sichergestellt, dass die Datenklassifizierung alle Daten lesen kann, für die erweiterte Berechtigungen erforderlich sind. Die Anmeldeinformationen werden auf der Data Classification-Instanz gespeichert.

      Wenn Sie sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Datenklassifizierungsscans unverändert bleiben, wird empfohlen, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

      Nachdem Sie die Anmeldeinformationen eingegeben haben, sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.



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

Aktivieren und Deaktivieren von Scans auf Volumes

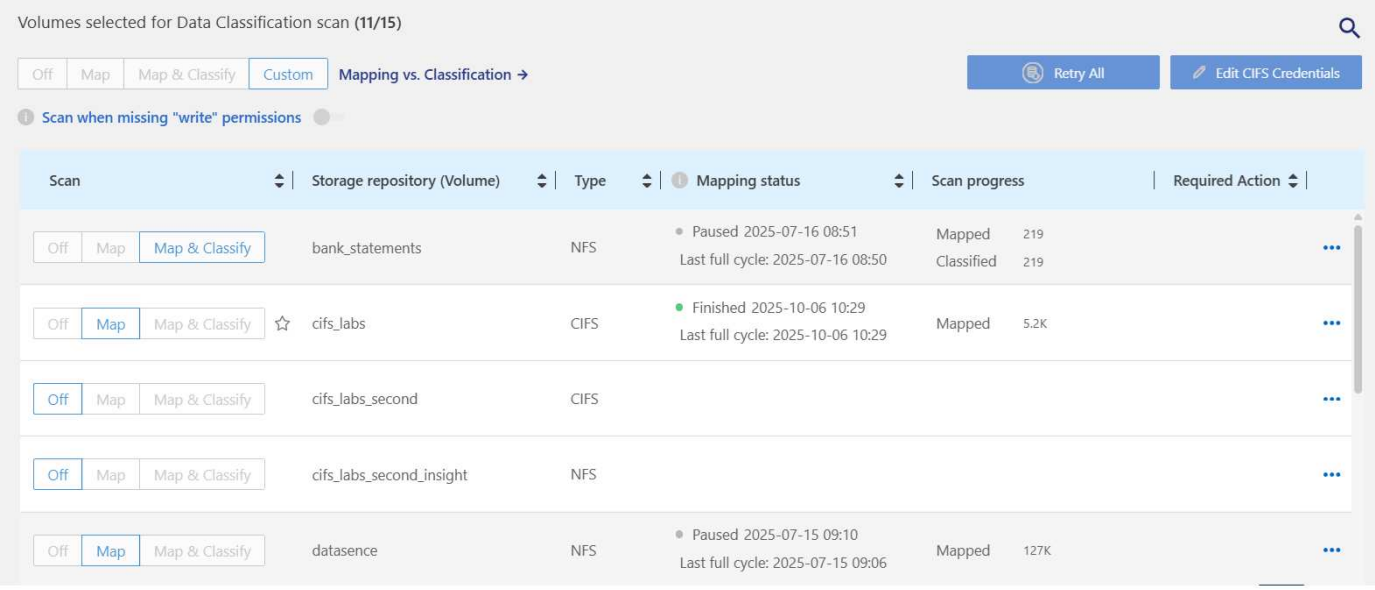
Sie können Scans auf jedem System jederzeit von der Konfigurationsseite aus starten oder stoppen. Sie können Scans auch von reinen Mapping-Scans auf Mapping- und Klassifizierungs-Scans umstellen und umgekehrt. Es wird empfohlen, alle Volumes in einem System zu scannen.

> Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und klassifizieren** ausgewählt haben. Wenn Sie im Überschriftenbereich die Option **Benutzerdefiniert** oder **Aus** einstellen, müssen Sie die Zuordnung und/oder das vollständige Scannen für jedes neue Volume aktivieren, das Sie dem System hinzufügen.

Der Schalter oben auf der Seite für **Scannen bei fehlenden Schreibberechtigungen** ist standardmäßig

deaktiviert. Dies bedeutet, dass das System die Dateien nicht scannt, wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter auf EIN und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Mehr erfahren".

Neue Datenträger, die dem System hinzugefügt werden, werden nur dann automatisch gescannt, wenn Sie im Überschriftenbereich die Einstellung **Zuordnen** oder **Zuordnen und Klassifizieren** festgelegt haben. Wenn die Einstellung für alle Volumes **Benutzerdefiniert** oder **Aus** ist, müssen Sie das Scannen für jedes neue Volume, das Sie hinzufügen, manuell aktivieren.



Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie ein System und dann **Konfiguration**.
3. Um Scans für alle Volumes zu aktivieren oder zu deaktivieren, wählen Sie in der Überschrift über allen Volumes **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus**.

   Um Scans für einzelne Volumes zu aktivieren oder zu deaktivieren, suchen Sie die Volumes in der Liste und wählen Sie dann neben dem Volumenamen **Zuordnen**, **Zuordnen und klassifizieren** oder **Aus** aus.

Ergebnis

Wenn Sie das Scannen aktivieren, beginnt die Datenklassifizierung mit dem Scannen der von Ihnen im System ausgewählten Volumes. Die Ergebnisse werden im Compliance-Dashboard angezeigt, sobald die Datenklassifizierung mit dem Scan beginnt. Die Dauer des Scans hängt von der Datenmenge ab und kann zwischen Minuten und Stunden liegen.

Scannen Sie Dateifreigaben mit NetApp Data Classification

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

Das Scannen von Daten aus Nicht- NetApp Dateifreigaben wird in der Kernversion der Datenklassifizierung nicht unterstützt.

Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie die Datenklassifizierung aktivieren.

- Die Freigaben können überall gehostet werden, auch in der Cloud oder vor Ort. CIFS-Freigaben von älteren NetApp 7-Mode-Speichersystemen können als Dateifreigaben gescannt werden.
  - Die Datenklassifizierung kann aus 7-Mode-Systemen weder Berechtigungen noch die „letzte Zugriffszeit“ extrahieren.
  - Aufgrund eines bekannten Problems zwischen einigen Linux-Versionen und CIFS-Freigaben auf 7-Mode-Systemen müssen Sie die Freigabe so konfigurieren, dass nur SMBv1 mit aktivierter NTLM-Authentifizierung verwendet wird.
- Zwischen der Data Classification-Instanz und den Freigaben muss eine Netzwerkverbindung bestehen.
- Sie können eine DFS-Freigabe (Distributed File System) als normale CIFS-Freigabe hinzufügen. Da die Datenklassifizierung nicht erkennt, dass die Freigabe auf mehreren Servern/Volumes basiert, die zu einer einzigen CIFS-Freigabe zusammengefasst sind, erhalten Sie möglicherweise Berechtigungs- oder Verbindungsfehler bezüglich der Freigabe, obwohl die Meldung tatsächlich nur für einen der Ordner/Freigaben gilt, der sich auf einem anderen Server/Volume befindet.
- Stellen Sie bei CIFS-Freigaben (SMB) sicher, dass Sie über Active Directory-Anmeldeinformationen verfügen, die Lesezugriff auf die Freigaben ermöglichen. Administratoranmeldeinformationen werden bevorzugt, wenn die Datenklassifizierung Daten scannen muss, für die erweiterte Berechtigungen erforderlich sind.

  Wenn Sie sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Datenklassifizierungsscans unverändert bleiben, wird empfohlen, dass der Benutzer über Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS verfügt. Konfigurieren Sie den Active Directory-Benutzer nach Möglichkeit als Teil einer übergeordneten Gruppe in der Organisation, die über Berechtigungen für alle Dateien verfügt.

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

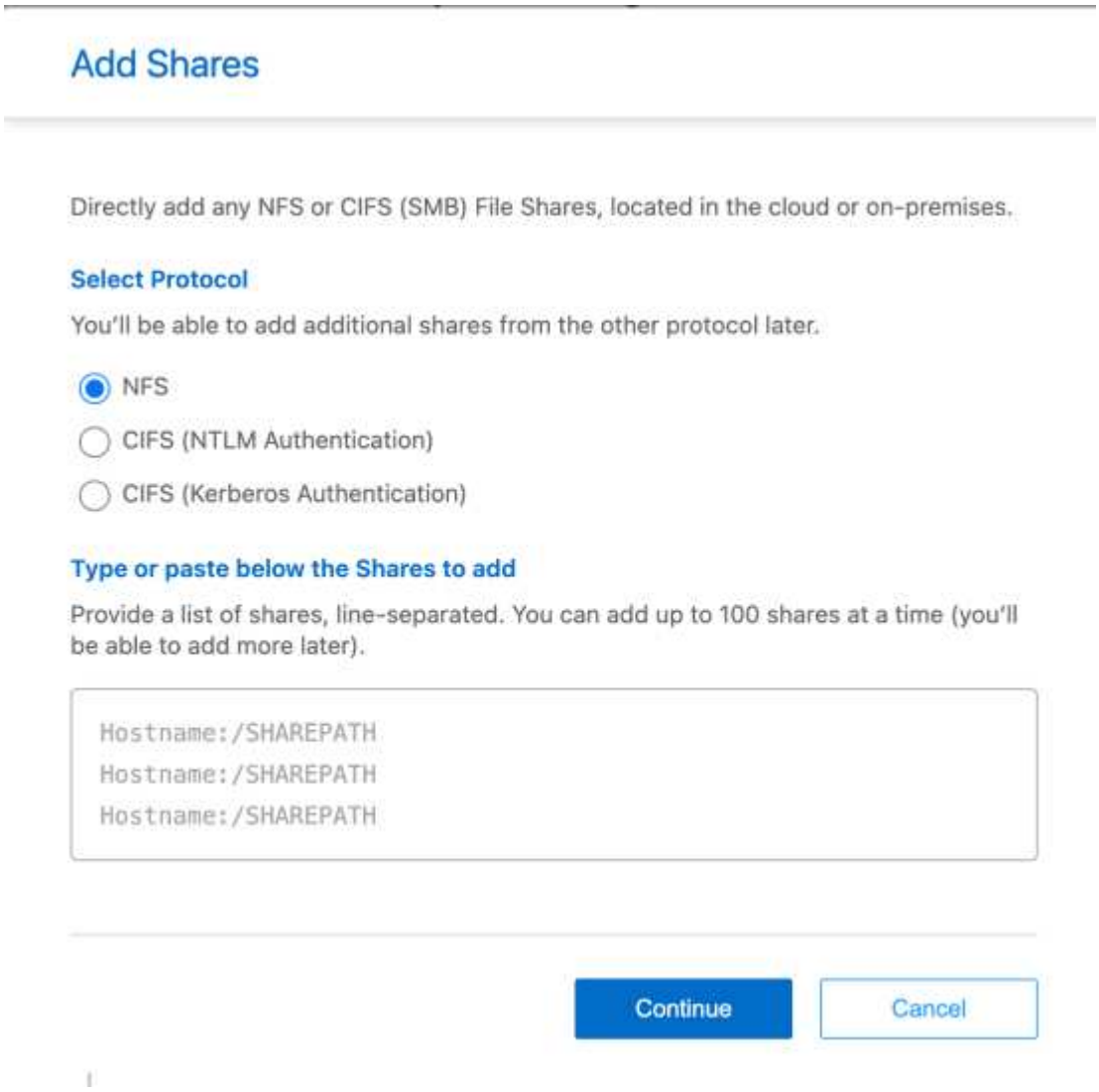
Erstellen einer Dateifreigabegruppe

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

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

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite **System hinzufügen** > **Dateifreigabegruppe hinzufügen**.
3. Geben Sie im Dialogfeld „Dateifreigabegruppe hinzufügen“ den Namen für die Freigabegruppe ein und wählen Sie dann **Weiter**.
4. Wählen Sie das Protokoll für die Dateifreigaben aus, die Sie hinzufügen.



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

5. Fügen Sie die Dateifreigaben hinzu, die Sie scannen möchten (eine Dateifreigabe pro Zeile). Wählen Sie dann **Weiter**.
6. Ein Bestätigungsdialogfeld zeigt die Anzahl der hinzugefügten Freigaben an.

   Wenn im Dialogfeld Freigaben aufgelistet sind, die nicht hinzugefügt werden konnten, erfassen Sie diese Informationen, damit Sie das Problem beheben können. Wenn das Problem eine Namenskonvention betrifft, können Sie die Freigabe mit einem korrigierten Namen erneut hinzufügen.

7. Konfigurieren Sie das Scannen auf dem Volume:
   - Um Nur-Mapping-Scans auf Dateifreigaben zu aktivieren, wählen Sie **Map**.
   - Um vollständige Scans von Dateifreigaben zu aktivieren, wählen Sie **Zuordnen und klassifizieren**.
   - Um das Scannen von Dateifreigaben zu deaktivieren, wählen Sie **Aus**.

> Der Schalter oben auf der Seite für **Scannen, wenn Berechtigungen zum Schreiben von Attributen fehlen** ist standardmäßig deaktiviert. Dies bedeutet, dass das System die Dateien nicht scannt, wenn Data Classification keine Schreibberechtigungen für Attribute in CIFS oder Schreibberechtigungen in NFS hat, da Data Classification die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. + Wenn Sie **Scannen bei fehlenden Berechtigungen zum Schreiben von Attributen** auf **Ein** stellen, setzt der Scan die letzte Zugriffszeit zurück und scannt alle Dateien unabhängig von den Berechtigungen. + Weitere Informationen zum Zeitstempel des letzten Zugriffs finden Sie unter"Aus Datenquellen in der Datenklassifizierung gesammelte Metadaten" .

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der Dateien in den von Ihnen hinzugefügten Dateifreigaben. Du kannstVerfolgen Sie den Scan-Fortschritt und sehen Sie sich die Ergebnisse des Scans im **Dashboard** an.

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

Bearbeiten einer Dateifreigabegruppe

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

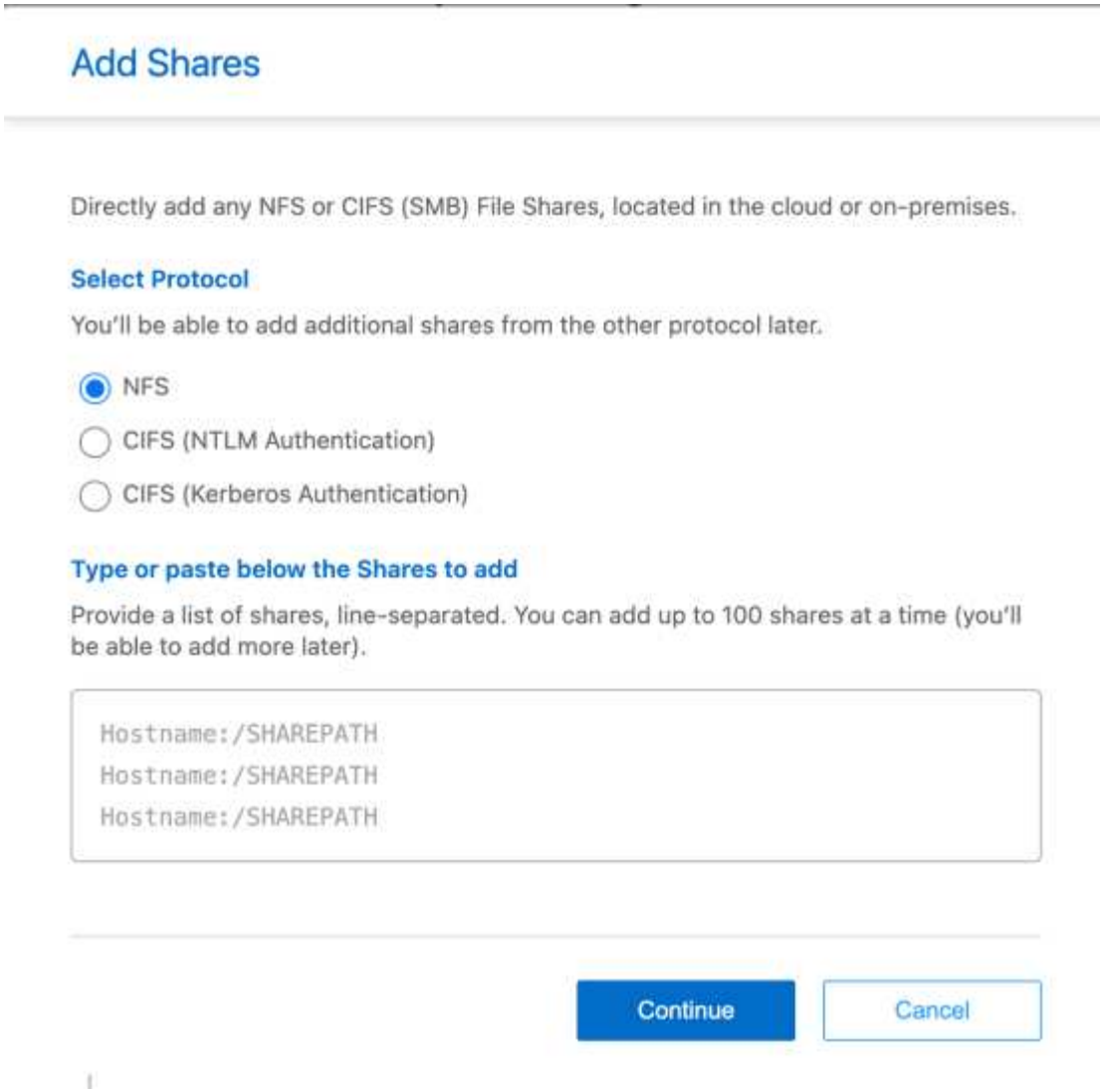
Bearbeiten Sie die CIFS-Protokollkonfiguration

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite die Dateifreigabegruppe aus, die Sie ändern möchten.
3. Wählen Sie **CIFS-Anmeldeinformationen bearbeiten**.

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

Dateifreigaben zu Scans hinzufügen

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite die Dateifreigabegruppe aus, die Sie ändern möchten.
3. Wählen Sie **+ Freigaben hinzufügen**.
4. Wählen Sie das Protokoll für die Dateifreigaben aus, die Sie hinzufügen.



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

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

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

Entfernen einer Dateifreigabe aus Scans

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie das System aus, von dem Sie Dateifreigaben entfernen möchten.
3. Wählen Sie **Konfiguration**.
4. Wählen Sie auf der Konfigurationsseite die Aktionen ••• für die Dateifreigabe, die Sie entfernen möchten.
5. Wählen Sie im Menü „Aktionen“ die Option „Freigabe entfernen“ aus.

Verfolgen Sie den Scan-Fortschritt

Sie können den Fortschritt des ersten Scans verfolgen.

1. Wählen Sie das Menü **Konfiguration**.
2. Wählen Sie die **Systemkonfiguration**.
3. Überprüfen Sie für das Speicherrepository die Spalte „Scan-Fortschritt“, um den Status anzuzeigen.

Scannen Sie StorageGRID -Daten mit NetApp Data Classification

Führen Sie einige Schritte aus, um mit dem Scannen von Daten in StorageGRID direkt mit NetApp Data Classification zu beginnen.

Überprüfen Sie die StorageGRID Anforderungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie die Datenklassifizierung aktivieren.

- Sie benötigen die Endpunkt-URL, um eine Verbindung mit dem Objektspeicherdienst herzustellen.
- Sie benötigen den Zugriffsschlüssel und den geheimen Schlüssel von StorageGRID , damit die Datenklassifizierung auf die Buckets zugreifen kann.

Bereitstellen der Datenklassifizierungsinstanz

Stellen Sie die Datenklassifizierung bereit, wenn noch keine Instanz bereitgestellt ist.

Wenn Sie Daten von StorageGRID scannen, die über das Internet zugänglich sind, können Sie"Datenklassifizierung in der Cloud bereitstellen" oder"Stellen Sie die Datenklassifizierung an einem lokalen Standort mit Internetzugang bereit" .

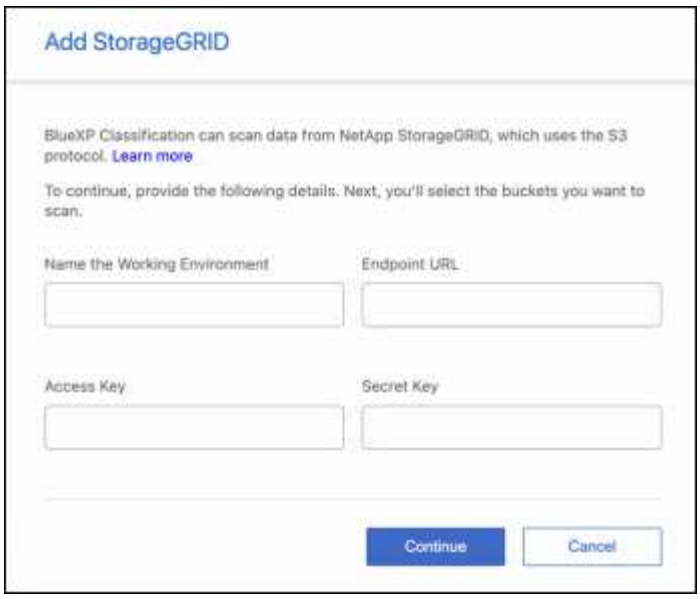
Wenn Sie Daten von StorageGRID scannen, das in einer Dark Site ohne Internetzugang installiert wurde, müssen Sie"Stellen Sie die Datenklassifizierung am selben lokalen Standort bereit, der keinen Internetzugang hat" . Dies erfordert auch, dass der Konsolenagent am selben lokalen Standort bereitgestellt wird.

Fügen Sie den StorageGRID -Dienst zur Datenklassifizierung hinzu

Fügen Sie den StorageGRID -Dienst hinzu.

Schritte

1. Wählen Sie im Menü „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie auf der Konfigurationsseite **System hinzufügen** > * StorageGRID hinzufügen*.
3. Geben Sie im Dialogfeld „StorageGRID -Dienst hinzufügen“ die Details für den StorageGRID -Dienst ein und wählen Sie **Weiter**.
   a. Geben Sie den Namen ein, den Sie für das System verwenden möchten. Dieser Name sollte den Namen des StorageGRID -Dienstes widerspiegeln, mit dem Sie eine Verbindung herstellen.
   b. Geben Sie die Endpunkt-URL ein, um auf den Objektspeicherdienst zuzugreifen.
   c. Geben Sie den Zugriffsschlüssel und den geheimen Schlüssel ein, damit die Datenklassifizierung auf die Buckets in StorageGRID zugreifen kann.



Ergebnis

StorageGRID wird zur Liste der Systeme hinzugefügt.

Aktivieren und Deaktivieren von Scans auf StorageGRID Buckets

Nachdem Sie die Datenklassifizierung auf StorageGRID aktiviert haben, besteht der nächste Schritt darin, die Buckets zu konfigurieren, die Sie scannen möchten. Die Datenklassifizierung erkennt diese Buckets und zeigt sie in dem von Ihnen erstellten System an.

Schritte

1. Suchen Sie auf der Konfigurationsseite das StorageGRID -System.
2. Wählen Sie auf der StorageGRID -Systemkachel **Konfiguration** aus.
3. Führen Sie einen der folgenden Schritte aus, um das Scannen zu aktivieren oder zu deaktivieren:
   - Um Nur-Mapping-Scans für einen Bucket zu aktivieren, wählen Sie **Map**.
   - Um vollständige Scans für einen Bucket zu aktivieren, wählen Sie **Zuordnen und klassifizieren**.
   - Um das Scannen eines Buckets zu deaktivieren, wählen Sie **Aus**.

Ergebnis

Die Datenklassifizierung beginnt mit dem Scannen der von Ihnen aktivierten Buckets. Sie können den Fortschritt des ersten Scans verfolgen, indem Sie zum Menü **Konfiguration** navigieren und dann die **Systemkonfiguration** auswählen. Der Fortschritt jedes Scans wird als Fortschrittsbalken angezeigt. Sie können auch mit der Maus über den Fortschrittsbalken fahren, um die Anzahl der gescannten Dateien im Verhältnis zur Gesamtzahl der Dateien im Volume anzuzeigen. Wenn Fehler vorliegen, werden diese zusammen mit der erforderlichen Aktion zur Behebung des Fehlers in der Spalte „Status“ angezeigt.

Integrieren Sie Ihr Active Directory mit NetApp Data Classification

Sie können ein globales Active Directory mit NetApp Data Classification integrieren, um die von Data Classification gemeldeten Ergebnisse zu Dateibesitzern und zu den Benutzern und Gruppen, die Zugriff auf Ihre Dateien haben, zu verbessern.

Wenn Sie bestimmte Datenquellen (unten aufgeführt) einrichten, müssen Sie Active Directory-Anmeldeinformationen eingeben, damit Data Classification CIFS-Volumes scannen kann. Diese Integration bietet der Datenklassifizierung Details zu Dateieigentümern und Berechtigungen für die in diesen Datenquellen gespeicherten Daten. Das für diese Datenquellen eingegebene Active Directory kann sich von den globalen Active Directory-Anmeldeinformationen unterscheiden, die Sie hier eingeben. Die Datenklassifizierung sucht in allen integrierten Active Directorys nach Benutzer- und Berechtigungsdetails.

Diese Integration bietet zusätzliche Informationen an den folgenden Stellen in der Datenklassifizierung:

- Sie können den "Dateibesitzer" verwenden"Filter" und sehen Sie sich die Ergebnisse in den Metadaten der Datei im Untersuchungsbereich an. Anstelle des Dateibesitzers, der die SID (Security IDentifier) enthält, wird der tatsächliche Benutzername eingetragen.

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

- Sie können sehen"vollständige Dateiberechtigungen" für jede Datei und jedes Verzeichnis, wenn Sie auf die Schaltfläche „Alle Berechtigungen anzeigen“ klicken.
- Im"Governance-Dashboard" , zeigt das Bedienfeld „Berechtigungen öffnen“ einen größeren Detaillierungsgrad zu Ihren Daten an.

Lokale Benutzer-SIDs und SIDs aus unbekannten Domänen werden nicht in den tatsächlichen Benutzernamen übersetzt.

Unterstützte Datenquellen

Eine Active Directory-Integration mit Datenklassifizierung kann Daten aus den folgenden Datenquellen identifizieren:

- On-Premises- ONTAP -Systeme
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSx für ONTAP

Stellen Sie eine Verbindung zu Ihrem Active Directory-Server her

Nachdem Sie die Datenklassifizierung bereitgestellt und das Scannen Ihrer Datenquellen aktiviert haben, können Sie die Datenklassifizierung in Ihr Active Directory integrieren. Auf Active Directory kann über eine DNS-Server-IP-Adresse oder eine LDAP-Server-IP-Adresse zugegriffen werden.

Die Active Directory-Anmeldeinformationen können schreibgeschützt sein, durch die Bereitstellung von Administratoranmeldeinformationen wird jedoch sichergestellt, dass die Datenklassifizierung alle Daten lesen kann, für die erweiterte Berechtigungen erforderlich sind. Die Anmeldeinformationen werden auf der Data Classification-Instanz gespeichert.

Wenn Sie bei CIFS-Volumes/Dateifreigaben sicherstellen möchten, dass die „letzten Zugriffszeiten“ Ihrer Dateien durch Klassifizierungsscans der Datenklassifizierung unverändert bleiben, muss der Benutzer über die Berechtigung „Attribute schreiben“ verfügen. Wenn möglich, empfehlen wir, den in Active Directory konfigurierten Benutzer zu einem Teil einer übergeordneten Gruppe in der Organisation zu machen, die über Berechtigungen für alle Dateien verfügt.

Anforderungen

- Sie müssen bereits ein Active Directory für die Benutzer in Ihrem Unternehmen eingerichtet haben.
- Sie benötigen die Informationen für das Active Directory:
  - DNS-Server-IP-Adresse oder mehrere IP-Adressen

    oder

  LDAP-Server-IP-Adresse oder mehrere IP-Adressen
  - Benutzername und Passwort für den Zugriff auf 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)
- Die folgenden Ports müssen für die ausgehende Kommunikation durch die Data Classification-Instanz geöffnet sein:

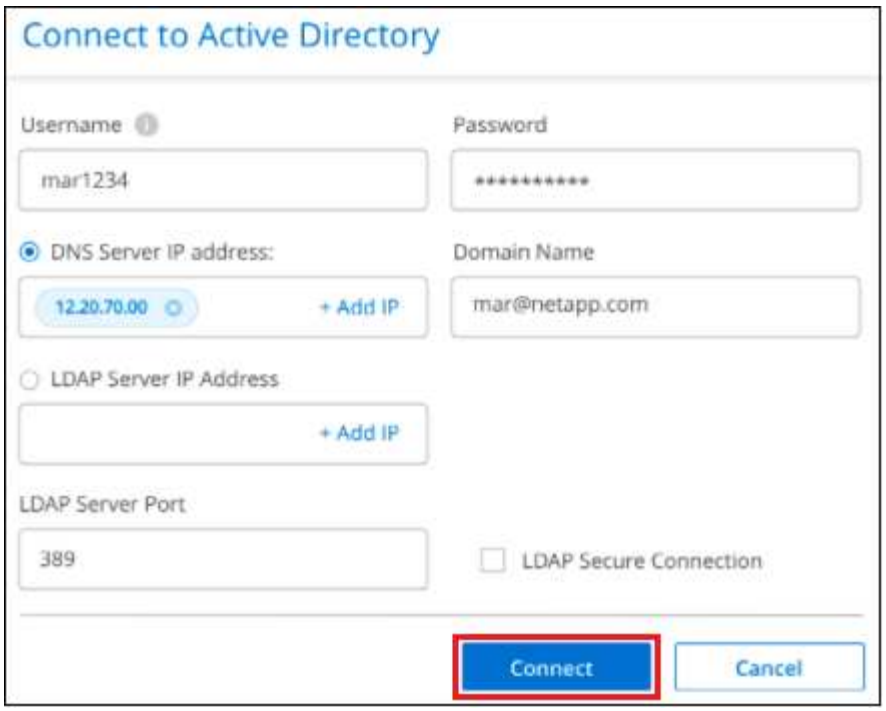
Protokoll	Hafen	Ziel	Zweck
TCP und UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP über SSL
TCP	3268	Active Directory	Globaler Katalog
TCP	3269	Active Directory	Globaler Katalog über SSL

Schritte

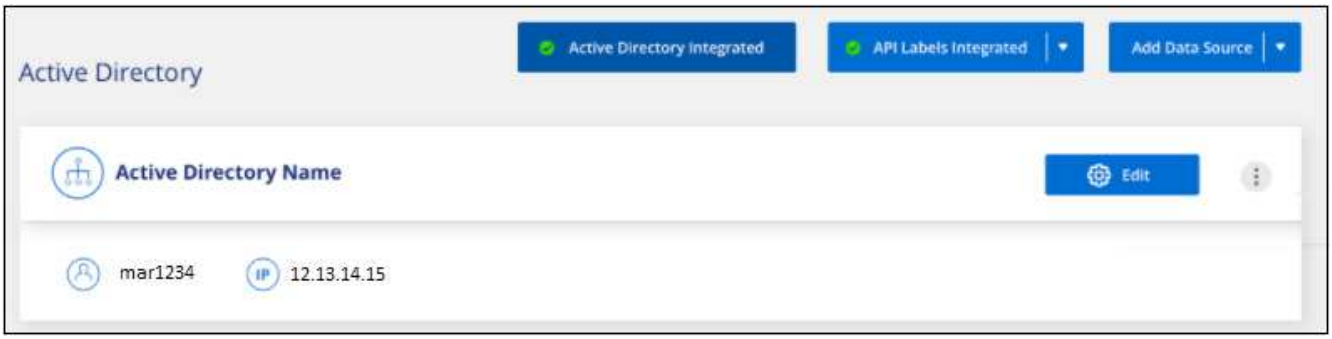
1. Klicken Sie auf der Seite „Datenklassifizierungskonfiguration“ auf **Active Directory hinzufügen**.

2. Geben Sie im Dialogfeld „Mit Active Directory verbinden“ die Active Directory-Details ein und klicken Sie auf **Verbinden**.

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



Die Datenklassifizierung wird in das Active Directory integriert und der Konfigurationsseite wird ein neuer Abschnitt hinzugefügt.



Verwalten Sie Ihre Active Directory-Integration

Wenn Sie Werte in Ihrer Active Directory-Integration ändern müssen, klicken Sie auf die Schaltfläche **Bearbeiten** und nehmen Sie die Änderungen vor.

Sie können die Integration auch löschen, indem Sie das Klicken Sie auf die Schaltfläche „Active Directory entfernen“ und dann auf „Active Directory entfernen“.