Dokumentation der BlueXP Klassifizierung

BlueXP classification

NetApp
April 03, 2024

Inhalt

Dokumentation der BlueXP Klassifizierung

Versionshinweise

Neuerungen bei der BlueXP Klassifizierung

Informieren Sie sich über die Neuerungen bei der BlueXP Klassifizierung (Cloud Data Sense).

April 2024 (Version 1.30)

Unterstützung für die Klassifizierung von RHEL v8.8 und v9.3 BlueXP hinzugefügt

Diese Version bietet Unterstützung für Red hat Enterprise Linux v8.8 und v9.3 zusätzlich zu zuvor unterstützten 9.x, für die Podman anstelle der Docker Engine erforderlich ist. Dies gilt für jede manuelle On-Premises-Installation der BlueXP Klassifizierung.

Für die folgenden Betriebssysteme ist die Verwendung der Podman Container-Engine erforderlich. Sie erfordern die BlueXP-Klassifikation Version 1.30 oder höher: Red hat Enterprise Linux Version 8.8, 9.0, 9.1, 9.2 und 9.3.

Weitere Informationen zu "Übersicht über Implementierungen zur BlueXP Klassifizierung".

Option zum Aktivieren der Sammlung des Überwachungsprotokolls entfernt

Die Option zum Aktivieren der Überwachungsprotokollsammlung wurde deaktiviert.

Scangeschwindigkeit verbessert

Die Scanleistung auf sekundären Scannerknoten wurde verbessert. Sie können weitere Scannerknoten hinzufügen, wenn Sie zusätzliche Verarbeitungsleistung für Ihre Scans benötigen. Weitere Informationen finden Sie unter "Installieren Sie die BlueXP Klassifizierung auf einem Host mit Internetzugang".

Automatische Upgrades

Wenn Sie die BlueXP Klassifizierung auf einem System mit Internetzugang implementiert haben, wird das System automatisch aktualisiert. Zuvor erfolgte das Upgrade nach einer bestimmten Zeit seit der letzten Benutzeraktivität. Mit dieser Version wird die BlueXP Klassifizierung automatisch aktualisiert, wenn die lokale Zeit zwischen 1:00 und 5:00 UHR MORGENS liegt. Wenn die lokale Zeit außerhalb dieser Stunden liegt, erfolgt die Aktualisierung nach einem bestimmten Zeitraum seit der letzten Benutzeraktivität. Weitere Informationen finden Sie unter "Installation auf einem Linux-Host mit Internetzugang".

Wenn Sie die BlueXP Klassifizierung ohne Internetzugang implementiert haben, müssen Sie ein Upgrade manuell vornehmen. Weitere Informationen finden Sie unter "BlueXP Klassifizierung auf einem Linux-Host ohne Internetzugang installieren".

4. März 2024 (Version 1.29)

Jetzt können Sie Scandaten ausschließen, die sich in bestimmten Datenquellen-Verzeichnissen befinden

Wenn die BlueXP Klassifizierung Scandaten in bestimmten Quellverzeichnissen ausschließen soll, können Sie diese Verzeichnisnamen zu einer Konfigurationsdatei hinzufügen, die durch die BlueXP Klassifizierung verarbeitet wird. Mit dieser Funktion können Sie verhindern, dass Verzeichnisse gescannt werden, die unnötig

sind oder zu falsch positiven Ergebnissen von persönlichen Daten führen würden.

"Weitere Informationen .".

Unterstützung für extra große Instanzen ist jetzt qualifiziert

Wenn Sie mehr als 250 Millionen Dateien durch eine BlueXP Klassifizierung scannen möchten, können Sie eine besonders große Instanz in Ihrer Cloud-Implementierung oder vor-Ort-Installation verwenden. Dieser Systemtyp kann bis zu 500 Millionen Dateien scannen.

"Weitere Informationen .".

10. Januar 2024 (Version 1.27)

Die Ergebnisse der Untersuchungsseite zeigen jetzt zusätzlich zur Gesamtanzahl der Elemente die Gesamtgröße an

Die gefilterten Ergebnisse auf der Untersuchungsseite zeigen nun zusätzlich zur Gesamtanzahl der Dateien die Gesamtgröße der Elemente an. Dies kann beim Verschieben von Dateien, beim Löschen von Dateien und vielem mehr helfen.

Zusätzliche Gruppen-IDs als „für Organisation offen“ konfigurieren

Nun können Sie Gruppen-IDs in NFS so konfigurieren, dass sie direkt aus der BlueXP-Klassifizierung als „Open to Organization“ betrachtet werden, wenn die Gruppe ursprünglich nicht mit dieser Berechtigung festgelegt wurde. Alle Dateien und Ordner, denen diese Gruppen-IDs angehängt sind, werden auf der Seite „Untersuchungsdetails“ als „für Organisation offen“ angezeigt. Informieren Sie sich darüber "Zusätzliche Gruppen-IDs als „für Organisation offen“ hinzufügen".

14. Dezember 2023 (Version 1.26.6)

Diese Version enthält einige kleinere Verbesserungen.

Das Release hat auch vorübergehend die folgenden Optionen entfernt:

- Die Option zum Aktivieren der Überwachungsprotokollsammlung wurde deaktiviert. Siehe "Überwachen und managen Sie Dateizugriffsereignisse".
- Bei der Untersuchung der Verzeichnisse steht die Möglichkeit zur Berechnung der Anzahl der personenbezogenen Daten (PII) nach Verzeichnissen nicht zur Verfügung. Siehe "Untersuchen Sie die in Ihrem Unternehmen gespeicherten Daten".
- Die Option zur Integration von Daten mit AIP-Labels (Azure Information Protection) wurde deaktiviert. Siehe "Private Daten organisieren".

6. November 2023 (Version 1.26.3)

Die folgenden Probleme wurden in dieser Version behoben

- Es wurde eine Inkonsistenz bei der Darstellung der Anzahl der vom System gescannten Dateien in Dashboards behoben.
- Verbesserte das Scanverhalten durch die Handhabung und Berichterstattung von Dateien und Verzeichnissen mit Sonderzeichen im Namen und Metadaten.

4. Oktober 2023 (Version 1.26)

Unterstützung lokaler Installationen von BlueXP Klassifizierungen auf RHEL Version 9

Red hat Enterprise Linux Versionen 8 und 9 unterstützen nicht die Docker Engine, die für die Installation der BlueXP Klassifikation erforderlich war. Wir unterstützen jetzt die Installation der BlueXP Klassifizierung auf RHEL 9.0, 9.1 und 9.2 mit Podman Version 4 oder höher als Container-Infrastruktur. Wenn in Ihrer Umgebung die neuesten Versionen von RHEL erforderlich sind, können Sie Podman jetzt auch die BlueXP-Klassifizierung (Version 1.26 oder höher) installieren.

Derzeit werden bei Verwendung von RHEL 9.x. keine Dark-Site-Installationen oder verteilte Scanumgebungen (mit Master- und Remote-Scanner-Nodes) unterstützt

5. September 2023 (Version 1.25)

Kleine und mittlere Bereitstellungen sind vorübergehend nicht verfügbar

Wenn Sie eine Instanz der BlueXP Klassifizierung in AWS implementieren, ist die Option **Deploy > Configuration** und die Auswahl einer kleinen oder mittelgroßen Instanz derzeit nicht verfügbar. Sie können die Instanz weiterhin mit der Größe der großen Instanz bereitstellen, indem Sie **Deploy > Deploy** auswählen.

Verwenden Sie Tags auf bis zu 100,000 Elemente auf der Seite Untersuchungsergebnisse

In der Vergangenheit konnten Sie auf der Seite Untersuchungsergebnisse (20 Elemente) jeweils nur Tags auf eine Seite anwenden. Jetzt können Sie **alle** Elemente auf den Seiten Untersuchungsergebnisse auswählen und Tags auf alle Elemente anwenden - bis zu 100,000 Elemente gleichzeitig. "Erfahren Sie, wie".

Identifizieren Sie duplizierte Dateien mit einer Mindestdateigröße von 1 MB

Mit der BlueXP Klassifizierung werden duplizierte Dateien nur bei Dateien identifiziert, die 50 MB oder mehr betragen. Nun können duplizierte Dateien, die mit 1 MB beginnen, identifiziert werden. Sie können die Filter der Untersuchungsseite „Dateigröße“ zusammen mit „Duplikate“ verwenden, um zu sehen, welche Dateien einer bestimmten Größe in Ihrer Umgebung dupliziert werden.

17. Juli 2023 (Version 1.24)

Zwei neue Arten deutscher personenbezogener Daten werden durch die BlueXP Klassifizierung identifiziert

Mit der BlueXP Klassifizierung können Dateien identifiziert und kategorisiert werden, die die folgenden Datentypen enthalten:

- Personalausweisnummer
- Sozialversicherungsnummer

"Hier können Sie alle Arten von personenbezogenen Daten einsehen, die durch die BlueXP Klassifizierung in Ihren Daten identifiziert werden können".

Die BlueXP Klassifizierung wird im eingeschränkten und privaten Modus vollständig unterstützt

Die BlueXP Klassifizierung wird jetzt vollständig auf Websites ohne Internetzugang (privater Modus) und mit eingeschränktem Outbound-Internetzugang (eingeschränkter Modus) unterstützt. "Weitere Informationen zu den BlueXP Implementierungsmodi für den Connector".

Fähigkeit zum überspringen von Versionen beim Upgrade einer Installation von BlueXP Klassifizierung im Private-Modus

Sie können jetzt ein Upgrade auf eine neuere Version der BlueXP Klassifizierung durchführen, auch wenn diese nicht sequenziell ist. Das heißt, die aktuelle Einschränkung für das Upgrade der BlueXP Klassifizierung um jeweils eine Version ist nicht mehr erforderlich. Diese Funktion ist ab Version 1.24 relevant.

Die BlueXP Klassifizierungs-API ist jetzt verfügbar

Mithilfe der BlueXP Klassifizierungs-API können Sie Aktionen durchführen, Abfragen erstellen und Informationen zu den zu scannenden Daten exportieren. Die interaktive Dokumentation ist über Swagger verfügbar. Die Dokumentation ist in mehrere Kategorien unterteilt, darunter Untersuchung, Compliance, Governance und Konfiguration. Jede Kategorie dient als Verweis auf die Registerkarten in der BlueXP Klassifizierungs-UI.

"Erfahren Sie mehr über die BlueXP Klassifizierungs-APIs".

6. Juni 2023 (Version 1.23)

Japanisch wird jetzt bei der Suche nach Datenfachnamen unterstützt

Japanische Namen können jetzt bei der Suche nach dem Namen eines Studienteilnehmers als Antwort auf einen Antrag auf Zugang zu einem Datengegenstand (Data Subject Access Request, DSAR) eingegeben werden. Sie können eine erzeugen "Bericht für Anforderung von Datenfachzugriff" Mit den daraus resultierenden Informationen. Sie können auch japanische Namen in das eingeben "Filter „Betroffene“ auf der Seite „Datenuntersuchung“" Um Dateien zu identifizieren, die den Namen des Studienteilnehmers enthalten.

Ubuntu ist jetzt eine unterstützte Linux-Distribution, auf der Sie BlueXP Klassifizierung installieren können

Ubuntu 22.04 wurde als unterstütztes Betriebssystem für die BlueXP Klassifizierung qualifiziert. Sie können die BlueXP-Klassifizierung auf einem Ubuntu Linux-Host in Ihrem Netzwerk oder auf einem Linux-Host in der Cloud installieren, wenn Sie Version 1.23 des Installers verwenden. "Erfahren Sie, wie Sie die BlueXP Klassifizierung auf einem Host installieren, auf dem Ubuntu installiert ist".

Red hat Enterprise Linux 8.6 und 8.7 werden bei neuen BlueXP Klassifizierungssysteminstallationen nicht mehr unterstützt

Diese Versionen werden bei neuen Bereitstellungen nicht unterstützt, da Red hat Docker nicht mehr unterstützt, was eine Voraussetzung ist. Wenn Sie eine vorhandene BlueXP Klassifizierungsmaschine unter RHEL 8.6 oder 8.7 verwenden, unterstützt NetApp Ihre Konfiguration weiterhin.

Die BlueXP Klassifizierung kann als FPolicy Collector konfiguriert werden, um FPolicy Ereignisse von ONTAP Systemen zu empfangen

Sie können Audit-Protokolle für den Dateizugriff in Ihrem BlueXP Klassifizierungssystem für Dateizugriffsereignisse auf Volumes in Ihren Arbeitsumgebungen erfassen. Die BlueXP Klassifizierung kann die folgenden Arten von FPolicy Ereignissen und die Benutzer erfassen, die die Aktionen an Ihren Dateien durchgeführt haben: Erstellen, Lesen, Schreiben, Löschen, Umbenennen, Eigentümer/Berechtigungen ändern und SACL/DACL ändern. "Hier erfahren Sie, wie Sie Dateizugriffsereignisse überwachen und verwalten".

Data Sense BYOL-Lizenzen werden nun in Dark Sites unterstützt

Sie können jetzt Ihre Data Sense BYOL-Lizenz in das Digital Wallet von BlueXP auf einer Dark Site hochladen, sodass Sie bei einer geringen Lizenzierungsbeschränkung benachrichtigt werden. "Hier erfahren Sie, wie Sie

Ihre Data Sense BYOL-Lizenz erwerben und hochladen".

3. April 2023 (Version 1.22)

Neuer Data Discovery Assessment Report

Der Data Discovery Assessment Report bietet eine allgemeine Analyse Ihrer gescannten Umgebung, um die Ergebnisse des Systems hervorzuheben und Problembereiche und mögliche Schritte zur Problembehebung aufzuzeigen. Ziel dieses Berichts ist es, ein Bewusstsein für Bedenken im Zusammenhang mit der Data Governance, Schwachstellen bei der Datensicherheit und Lücken in der Daten-Compliance in Ihrem Datensatz zu schaffen. "Erfahren Sie, wie Sie den Data Discovery Assessment Report erstellen und verwenden".

Möglichkeit zur Implementierung der BlueXP Klassifizierung auf kleineren Instanzen in der Cloud

Bei der Implementierung der BlueXP Klassifizierung aus einem BlueXP Connector in einer AWS-Umgebung können Sie nun zwischen zwei kleineren Instanztypen wählen als bei der Standardinstanz. Wenn Sie eine kleine Umgebung scannen, können Sie hier Cloud-Kosten sparen. Allerdings gibt es einige Einschränkungen bei der Verwendung der kleineren Instanz. "Anzeigen der verfügbaren Instanztypen und Einschränkungen".

Eigenständiges Skript steht jetzt zur Verfügung, um Ihr Linux-System vor der Installation der BlueXP Klassifizierung zu qualifizieren

Wenn Sie unabhängig von der Ausführung der BlueXP Klassifizierungssysteminstallation überprüfen möchten, ob Ihr Linux-System alle Voraussetzungen erfüllt, steht Ihnen ein separates Skript zur Verfügung, das nur die Voraussetzungen testet. "Erfahren Sie, wie Sie überprüfen können, ob Ihr Linux-Host bereit ist, die BlueXP Klassifizierung zu installieren".

7. März 2023 (Version 1.21)

Neue Funktionen, mit denen Sie Ihre eigenen benutzerdefinierten Kategorien von der BlueXP Klassifizierungs-UI hinzufügen können

Mit der BlueXP Klassifizierung können Sie jetzt Ihre eigenen benutzerdefinierten Kategorien hinzufügen, sodass die Dateien nach der BlueXP Klassifizierung ermittelt werden, die zu diesen Kategorien passen. Die BlueXP Klassifizierung hat viele "Vordefinierte Kategorien"Diese Funktion ermöglicht es Ihnen, benutzerdefinierte Kategorien hinzuzufügen, um zu ermitteln, wo Informationen, die für Ihre Organisation einzigartig sind, in Ihren Daten gefunden werden.

"Weitere Informationen .".

Sie können jetzt benutzerdefinierte Schlüsselwörter aus der BlueXP Klassifizierungs-UI hinzufügen

Mit der BlueXP Klassifizierung konnten benutzerdefinierte Schlüsselwörter hinzugefügt werden, die durch die BlueXP Klassifizierung bei zukünftigen Scans ab und an identifiziert werden. Sie mussten sich jedoch beim BlueXP Klassifizierungs-Linux-Host anmelden und eine Befehlszeilenschnittstelle verwenden, um die Schlüsselwörter hinzuzufügen. In dieser Version können benutzerdefinierte Schlüsselwörter in der BlueXP Klassifizierungs-UI hinzugefügt werden. Dies macht es sehr einfach, diese Schlüsselwörter hinzuzufügen und zu bearbeiten.

"Weitere Informationen zum Hinzufügen benutzerdefinierter Schlüsselwörter finden Sie in der BlueXP Klassifizierungs-UI".

Möglichkeit zur BlueXP Klassifizierung nicht von Dateien, wenn die „Uhrzeit des letzten Zugriffs“ geändert wird

Wenn die BlueXP Klassifizierung keine ausreichenden „Schreib“-Berechtigungen besitzt, scannt das System standardmäßig keine Dateien in Ihren Volumes, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen jedoch egal ist, ob die letzte Zugriffszeit in Ihren Dateien auf die ursprüngliche Uhrzeit zurückgesetzt wird, können Sie dieses Verhalten auf der Konfigurationsseite außer Kraft setzen, damit die BlueXP Klassifizierung die Volumes unabhängig von den Berechtigungen scannt.

In Verbindung mit dieser Funktion steht nun ein neuer Filter namens „Scan Analysis Event“ zur Verfügung, mit dem Sie die Dateien anzeigen können, die nicht klassifiziert wurden, weil die BlueXP Klassifizierung den Zeitpunkt des letzten Zugriffs nicht rückgängig machen konnte, oder die Dateien, die klassifiziert wurden, obwohl die BlueXP Klassifizierung beim letzten Zugriff nicht rückgängig gemacht wurde.

"Erfahren Sie mehr über den „Zeitstempel des letzten Zugriffs“ und die Berechtigungen, die die BlueXP Klassifizierung erfordert".

Drei neue Arten von personenbezogenen Daten werden durch die BlueXP Klassifizierung identifiziert

Mit der BlueXP Klassifizierung können Dateien identifiziert und kategorisiert werden, die die folgenden Datentypen enthalten:

- Botswana Identity Card (Omang)-Nummer
- Botswana Passnummer
- Personalausweis für die nationale Registrierung in Singapur (NRIC)

"Hier können Sie alle Arten von personenbezogenen Daten einsehen, die durch die BlueXP Klassifizierung in Ihren Daten identifiziert werden können".

Aktualisierte Funktionalität für Verzeichnisse

- Die Option „leichter CSV-Bericht“ für Datenuntersuchungsberichte enthält jetzt Informationen aus Verzeichnissen.
- Der Zeitfilter „Letzter Zugriff“ zeigt jetzt die zuletzt verwendete Zeit für Dateien und Verzeichnisse an.

Installationsverbesserungen führen zu

- Der BlueXP Klassifizierungs-Installer für Standorte ohne Internetzugang (Dark Sites) führt jetzt eine Vorabprüfung durch, um sicherzustellen, dass Ihre System- und Netzwerkanforderungen für eine erfolgreiche Installation bestehen.
- Die Protokolldateien der Installationsaudits werden jetzt gespeichert und in geschrieben `/ops/netapp/install_logs`.

5. Februar 2023 (Version 1.20)

Möglichkeit, Policy-basierte Benachrichtigungs-E-Mails an jede beliebige E-Mail-Adresse zu senden

In früheren Versionen der BlueXP Klassifizierung können Sie E-Mail-Benachrichtigungen an die BlueXP Benutzer Ihres Kontos senden, wenn bestimmte kritische Richtlinien Ergebnisse liefern. Mit dieser Funktion erhalten Sie Benachrichtigungen zum Schutz Ihrer Daten, wenn Sie nicht online sind. Jetzt können Sie auch E-Mail-Benachrichtigungen von Policies an andere Benutzer senden - bis zu 20 E-Mail-Adressen - die nicht in Ihrem BlueXP-Konto sind.

"Erfahren Sie mehr über das Senden von E-Mail-Benachrichtigungen basierend auf Policy-Ergebnissen".

Sie können jetzt persönliche Muster über die BlueXP Klassifizierungs-UI hinzufügen

Mit der BlueXP Klassifizierung konnten individuelle „persönliche Daten“ hinzugefügt werden, die durch die BlueXP Klassifizierung in künftigen Scans schon seit einiger Zeit erkannt werden. Sie mussten sich jedoch beim BlueXP Klassifizierungs-Linux-Host anmelden und eine Befehlszeile verwenden, um die benutzerdefinierten Muster hinzuzufügen. In dieser Version besteht die Möglichkeit, persönliche Muster mit einem regex hinzuzufügen, indem sie die BlueXP Klassifizierungs-UI verwenden. Damit ist es sehr einfach, diese benutzerdefinierten Muster hinzuzufügen und zu bearbeiten.

"Weitere Informationen zum Hinzufügen benutzerdefinierter Muster erhalten Sie über die BlueXP Klassifizierungs-UI".

Möglichkeit zum Verschieben von 15 Millionen Dateien mithilfe der BlueXP Klassifizierung

In der Vergangenheit können Sie durch die BlueXP Klassifizierung maximal 100,000 Quelldateien auf eine beliebige NFS-Freigabe verschieben. Sie können jetzt bis zu 15 Millionen Dateien gleichzeitig verschieben. "Weitere Informationen zum Verschieben von Quelldateien mithilfe der BlueXP Klassifizierung".

Fähigkeit, die Anzahl der Benutzer zu sehen, die Zugriff auf SharePoint Online-Dateien haben

Der Filter "Anzahl der Benutzer mit Zugriff" unterstützt nun Dateien, die in SharePoint Online-Repositorys gespeichert sind. In der Vergangenheit wurden nur Dateien auf CIFS Shares unterstützt. Beachten Sie, dass SharePoint-Gruppen, die nicht auf Active Directory basieren, derzeit nicht in diesen Filter gezählt werden.

Der Aktionsstatus wurde um einen neuen Status „Teilerfolg“ erweitert

Der neue Status „Teilsuccess“ zeigt an, dass eine BlueXP-Klassifizierungsaktion abgeschlossen ist und einige Elemente fehlgeschlagen sind und einige Elemente erfolgreich waren, z. B. wenn Sie 100 Dateien verschieben oder löschen. Außerdem wurde der Status „Fertig“ in „Erfolg“ umbenannt. In der Vergangenheit können im Status „Fertig“ Aktionen aufgeführt werden, die erfolgreich waren und die fehlgeschlagen sind. Der Status „Erfolg“ bedeutet nun, dass alle Aktionen erfolgreich auf allen Elementen durchgeführt wurden. "Lesen Sie, wie Sie das Fenster „Aktionsstatus“ anzeigen".

9. Januar 2023 (Version 1.19)

Möglichkeit, ein Diagramm von Dateien anzuzeigen, die sensible Daten enthalten und die übermäßig permissiv sind

Das Governance Dashboard hat einen neuen Bereich mit „*sensitiven Daten“ und „Wide Permissions*“ hinzugefügt, der eine Heatmap mit Dateien enthält, die vertrauliche Daten (einschließlich sensibler und sensibler personenbezogener Daten) enthalten und die zu permissiv sind. So erkennen Sie, wo Sie möglicherweise Risiken mit sensiblen Daten haben. "Weitere Informationen .".

Auf der Seite „Datenuntersuchung“ stehen drei neue Filter zur Verfügung

Es stehen neue Filter zur Verfügung, um die Ergebnisse zu verfeinern, die auf der Seite „Datenuntersuchung“ angezeigt werden:

- Der Filter „Anzahl der Benutzer mit Zugriff“ zeigt an, welche Dateien und Ordner für eine bestimmte Anzahl von Benutzern geöffnet sind. Sie können einen Zahlenbereich auswählen, um die Ergebnisse zu verfeinern, z. B. um zu sehen, auf welche Dateien 51-100 Benutzer zugreifen können.

- Mit den Filtern „erstellte Zeit“, „entdeckte Zeit“, „Zuletzt geändert“ und „Letzter Zugriff“ können Sie jetzt einen benutzerdefinierten Datumsbereich erstellen, anstatt nur einen vordefinierten Zeitraum von Tagen auszuwählen. Sie können beispielsweise nach Dateien mit einer "Erstellungszeit" "älter als 6 Monate" oder mit einem "Letzter geändert" Datum innerhalb der "letzten 10 Tage" suchen.
- Mit dem Filter „Dateipfad“ können Sie nun Pfade festlegen, die Sie aus den gefilterten Abfrageergebnissen ausschließen möchten. Wenn Sie Pfade zum ein- und Ausschließen bestimmter Daten eingeben, findet die BlueXP Klassifizierung zuerst alle Dateien in den eingeschlossenen Pfaden, dann entfernt sie Dateien aus ausgeschlossenen Pfaden und zeigt dann die Ergebnisse an.

"Sehen Sie sich die Liste aller Filter an, mit denen Sie Ihre Daten untersuchen können".

Durch die BlueXP Klassifizierung kann die japanische individuelle Nummer identifiziert werden

Durch die BlueXP Klassifizierung können Dateien identifiziert und kategorisiert werden, die die japanische individuelle Nummer (auch „Meine Nummer“) enthalten. Dazu gehört sowohl die persönliche als auch die Firmennummer. "Hier können Sie alle Arten von personenbezogenen Daten einsehen, die durch die BlueXP Klassifizierung in Ihren Daten identifiziert werden können".

Bekannte Einschränkungen

Bekannte Einschränkungen identifizieren Funktionen, die von dieser Version des Produkts nicht unterstützt werden oder nicht korrekt mit ihr zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

Die BlueXP Klassifizierungs-Version hat Optionen vorübergehend entfernt

Die Veröffentlichung von Dezember 2023 (Version 1.26.6) hat die folgenden Optionen vorübergehend entfernt:

- Die Option zum Aktivieren der Überwachungsprotokollsammlung wurde deaktiviert.
- Bei der Untersuchung der Verzeichnisse steht die Möglichkeit zur Berechnung der Anzahl der personenbezogenen Daten (PII) nach Verzeichnissen nicht zur Verfügung.
- Die Option zur Integration von Daten mit AIP-Labels (Azure Information Protection) wurde deaktiviert.

Einschränkungen beim Scannen der BlueXP Klassifizierung

Die BlueXP Klassifizierung scannt nur eine Freigabe unter einem Volume

Wenn Sie mehrere File Shares unter einem einzelnen Volume haben, scannt die BlueXP Klassifizierung die Freigabe mit der höchsten Hierarchie. Wenn Sie beispielsweise Freigaben wie die folgenden haben:

- /A
- /A/B
- /C
- /D/E

Anschließend werden die Daten in /A gescannt. Die Daten in /C und /D werden nicht gescannt.

Behelfslösung

Es gibt eine Problemumgehung, um sicherzustellen, dass Sie Daten von allen Freigaben in Ihrem Volume scannen. Führen Sie hierzu folgende Schritte aus:

1. Fügen Sie in der Arbeitsumgebung das zu scannende Volumen hinzu.
2. Nachdem die BlueXP Klassifizierung das Scannen des Volumes abgeschlossen hat, öffnen Sie die Seite „*Data Investigation*“ und erstellen Sie einen Filter, um zu sehen, welche Freigabe gescannt wird:

   Sie filtern die Daten nach „Name der Arbeitsumgebung“ und „Verzeichnistyp = Freigabe“, um zu sehen, welche Freigabe gescannt wird.

3. Rufen Sie die vollständige Liste der Freigaben auf, die im Volume vorhanden sind, damit Sie sehen können, welche Freigaben nicht gescannt werden.
4. "Fügen Sie die restlichen Freigaben einer Freigabengruppe hinzu".

   Sie müssen alle Freigaben einzeln hinzufügen, zum Beispiel:

   ```
   /C
   /D
   ```

5. Führen Sie diese Schritte für jedes Volume in der Arbeitsumgebung aus, die über mehrere Shares verfügt.

Los geht’s

Mehr zur BlueXP Klassifizierung

Die BlueXP Klassifizierung (Cloud Data Sense) ist ein Daten-Governance-Service für BlueXP. Er scannt Ihre lokalen und Cloud-Datenquellen Ihres Unternehmens, um Daten zuzuordnen und zu klassifizieren sowie private Informationen zu identifizieren. Auf diese Weise reduzieren Sie Sicherheits- und Compliance-Risiken, senken die Storage-Kosten und unterstützen Ihre Datenmigrationsprojekte.

Funktionen

Die BlueXP Klassifizierung verwendet künstliche Intelligenz (KI), Natural Language Processing (NLP) und Machine Learning (ML), um den gescannten Inhalt zu verstehen. Anhand dessen werden Entitäten extrahiert und die Inhalte entsprechend kategorisiert. Dadurch kann die BlueXP Klassifizierung folgende Funktionsbereiche bieten.

"Weitere Informationen zu Anwendungsfällen für die BlueXP Klassifizierung".

Einhaltung von Compliance-Vorschriften

Die BlueXP Klassifizierung bietet verschiedene Tools, die Sie bei Ihren Compliance-Bemühungen unterstützen können. Die BlueXP Klassifizierung ermöglicht Ihnen:

- Ermitteln von personenbezogenen Daten
- Vielzahl sensibler personenbezogener Daten gemäß den Datenschutzvorschriften des DSGVO, CCPA, PCI und HIPAA ermitteln.
- Reagieren Sie auf Data Subject Access Requests (DSAR) basierend auf Name oder E-Mail-Adresse.
- Ermitteln Sie, ob eindeutige IDs Ihrer Datenbanken in Dateien in anderen Repositorys gefunden werden. Erstellen Sie also Ihre eigene Liste mit „persönlichen Daten“, die in BlueXP Klassifizierungs-Scans identifiziert werden.
- Bestimmte Benutzer per E-Mail benachrichtigen, wenn Dateien bestimmte PII enthalten (Sie definieren diese Kriterien mit "Richtlinien") So können Sie über einen Aktionsplan entscheiden.

Erhöhte Sicherheit

Mit der BlueXP Klassifizierung können Daten identifiziert werden, die potenziell gefährdet sind, aus strafrechtlichen Gründen auf sie zugegriffen zu werden. Die BlueXP Klassifizierung ermöglicht Ihnen:

- Ermitteln Sie alle Dateien und Verzeichnisse (Shares und Ordner) mit offenen Berechtigungen, die Ihrem gesamten Unternehmen oder der Öffentlichkeit zugänglich sind.
- Identifizieren Sie sensible Daten, die sich außerhalb des ursprünglichen dedizierten Standorts befinden.
- Einhaltung von Richtlinien zur Datenaufbewahrung.
- Verwenden Sie *Policies*, um das Sicherheitspersonal automatisch über neue Sicherheitsprobleme zu informieren, damit sie sofort reagieren können.
- Fügen Sie benutzerdefinierte Tags zu Dateien hinzu (z. B. „muss verschoben werden“) und weisen Sie einen BlueXP-Benutzer zu, damit diese Person Updates für die Dateien besitzen kann.

- Anzeigen und ändern Sie "Azure Information Protection (AIP)-Etiketten" In Ihren Dateien.

Optimieren Sie die Storage-Auslastung

Die BlueXP Klassifizierung bietet Tools, die Sie bei Ihren Storage-Gesamtbetriebskosten (TCO) unterstützen. Die BlueXP Klassifizierung ermöglicht Ihnen:

- Erhöhte Storage-Effizienz durch Identifizierung doppelter oder nicht geschäftlicher Daten Mit diesen Informationen können Sie entscheiden, ob Sie bestimmte Dateien verschieben oder löschen möchten.
- Löschen Sie Dateien, die unsicher oder zu riskant erscheinen, um in Ihrem Speichersystem zu belassen, oder die Sie als Duplikat identifiziert haben. Mit *Policies* können Dateien, die bestimmten Kriterien entsprechen, automatisch gelöscht werden.
- Sparen Sie Storage-Kosten, indem Sie inaktive Daten ermitteln, die auf kostengünstigeren Objektspeicher verschoben werden können. "Weitere Informationen zum Tiering von Cloud Volumes ONTAP Systemen". "Weitere Informationen zum Tiering von lokalen ONTAP Systemen".

Beschleunigte Datenmigration

Mit der BlueXP Klassifizierung können Sie Ihre On-Premises-Daten scannen, bevor sie in die Public oder Private Cloud migrieren. Die BlueXP Klassifizierung ermöglicht Ihnen:

- Zeigen Sie die Größe der Daten an und ob die Daten vertrauliche Informationen enthalten, bevor Sie sie verschieben.
- Filtern Sie die Quelldaten (basierend auf über 25 Kriterientypen), damit Sie nur die erforderlichen Dateien in das Ziel verschieben können - unnötige Daten werden nicht verschoben.
- Automatisches und unterbrechungsfreies Verschieben, Kopieren oder Synchronisieren nur der erforderlichen Daten in das Cloud-Repository

Unterstützte Datenquellen

Die BlueXP Klassifizierung kann strukturierte und unstrukturierte Daten aus folgenden Datenquellen scannen und analysieren:

NetApp:

- Cloud Volumes ONTAP (implementiert in AWS, Azure oder GCP)
- On-Premises ONTAP Cluster
- StorageGRID
- Azure NetApp Dateien
- Amazon FSX für ONTAP
- Cloud Volumes Service für Google Cloud
- Kein NetApp:*
- Dell EMC Isilon
- Pure Storage
- Nutanix
- Alle anderen Storage-Anbieter

Wolke:

- Amazon S3
- Google Cloud Storage
- OneDrive
- SharePoint Online
- SharePoint On-Premises (SharePoint Server)
- Google Drive

Datenbanken:

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

Die BlueXP Klassifizierung unterstützt NFS-Versionen 3.x und CIFS-Versionen 1.x, 2.0, 2.1 und 3.0.

Kosten

- Die Kosten der BlueXP Klassifizierung hängen von der Datenmenge ab, die Sie scannen. Die ersten 1 TB an Daten, die die BlueXP Klassifizierung in einem BlueXP Workspace scannt, sind 30 Tage lang kostenlos. Dies umfasst alle Daten aus allen Arbeitsumgebungen und Datenquellen. Um mit dem Scannen von Daten nach diesem Zeitpunkt fortzufahren, müssen Sie auf AWS, Azure oder GCP Marketplace oder eine BYOL-Lizenz von NetApp abonnieren. Siehe "Preisgestaltung" Entsprechende Details.

  "Informieren Sie sich über die Lizenzierung der BlueXP Klassifizierung".

- Für die Installation der BlueXP Klassifizierung in der Cloud ist die Implementierung einer Cloud-Instanz erforderlich. Dies führt zu Gebühren beim Cloud-Provider, wo die Klassifizierung implementiert wird. Siehe Der für jeden Cloud-Provider implementierte Instanztyp. Die Installation der BlueXP Klassifizierung auf einem lokalen System kostet Sie nichts.
- Für die Klassifizierung von BlueXP müssen Sie einen BlueXP Connector implementiert haben. In vielen Fällen haben Sie bereits einen Connector, weil Sie andere Speicher und Dienste in BlueXP verwenden. Die Connector-Instanz verursacht Gebühren bei dem Cloud-Provider, wo sie implementiert wird. Siehe "Für jeden Cloud-Provider implementierte Instanztyp". Bei der Installation des Connectors in einem On-Premises-System entstehen keine Kosten.

Datentransferkosten

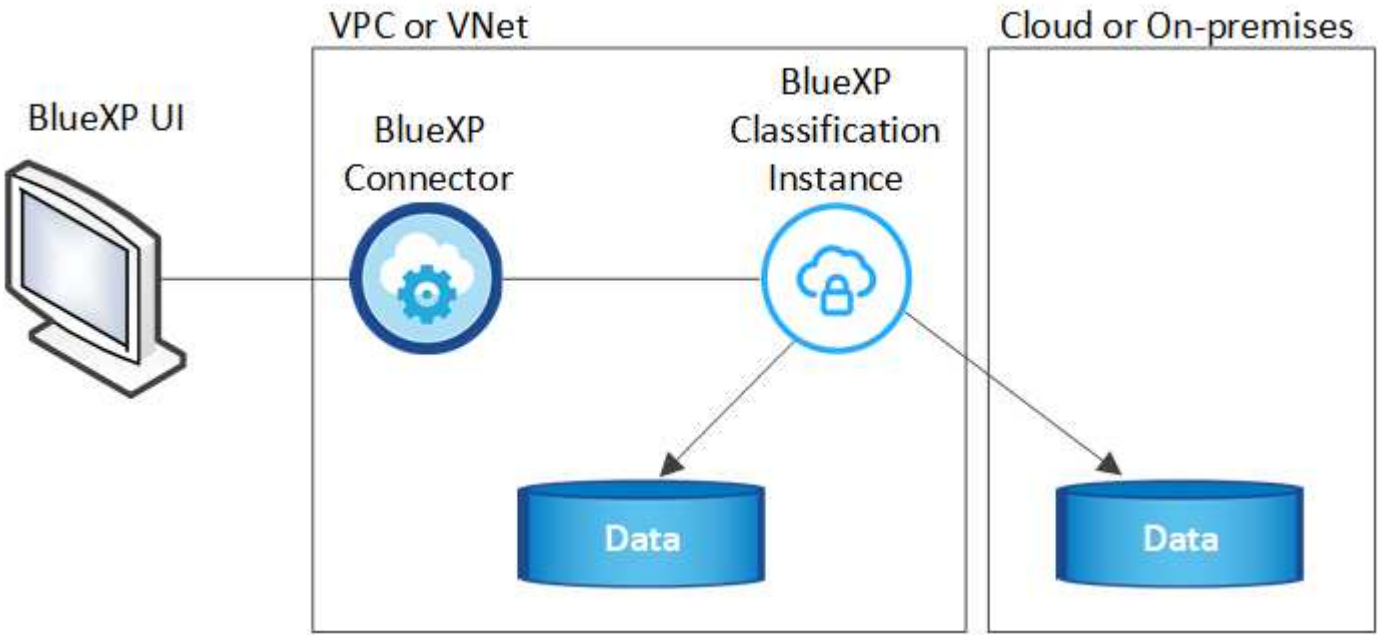
Die Datentransferkosten hängen von Ihrer Einrichtung ab. Wenn sich die BlueXP Klassifizierungs-Instanz und Datenquelle in derselben Verfügbarkeitszone und -Region befinden, entstehen keine Kosten für Datentransfers. Wenn sich die Datenquelle, beispielsweise ein Cloud Volumes ONTAP-System oder S3-Bucket, jedoch in einer *verschiedenen* Verfügbarkeitszone oder -Region befindet, wird Ihr Cloud-Provider für Datentransferkosten berechnet. Weitere Informationen finden Sie unter diesen Links:

- "AWS: Amazon EC2-Preisgestaltung"

- "Microsoft Azure: Preisangaben Für Die Bandbreite"
- "Google Cloud: Preis für Storage Transfer Service"

Die BlueXP Klassifizierungsinstanz

Wenn Sie die BlueXP Klassifizierung in der Cloud implementieren, stellt BlueXP die Instanz im selben Subnetz bereit, in dem sich der Connector befindet. "Erfahren Sie mehr über Steckverbinder."



Beachten Sie Folgendes über die Standardinstanz:

- In AWS wird die BlueXP Klassifizierung auf einer ausgeführt "M6i.4xlarge-Instanz" Mit einer GP2-Festplatte mit 500 gib. Das Betriebssystem-Image ist Amazon Linux 2. Bei der Implementierung in AWS können Sie eine kleinere Instanzgröße wählen, wenn Sie eine kleine Datenmenge scannen.
- In Azure wird die BlueXP Klassifizierung auf einer ausgeführt "Standard_D16s_v3 VM" Auf einer Festplatte mit 500 gib. Das Betriebssystem-Image ist CentOS 7.9.
- In GCP wird die BlueXP Klassifizierung auf einer ausgeführt "n2-Standard-16-VM" Mit einer persistenten Festplatte mit 500 gib Standard. Das Betriebssystem-Image ist CentOS 7.9.
- In Regionen, in denen die Standardinstanz nicht verfügbar ist, wird die BlueXP Klassifizierung auf einer alternativen Instanz ausgeführt. "Sehen Sie sich die alternativen Instanztypen an".
- Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Pro Connector wird nur eine BlueXP Klassifizierungsinstanz implementiert.

Sie können die BlueXP Klassifizierung auch auf einem Linux-Host vor Ort oder auf einem Host in Ihrem bevorzugten Cloud-Provider implementieren. Die Software funktioniert unabhängig von der gewählten Installationsmethode genau auf die gleiche Weise. Upgrades der BlueXP Klassifizierungs-Software werden automatisiert, solange die Instanz einen Internetzugang hat.

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

Verwenden eines kleineren Instanztyps

Sie können die BlueXP Klassifizierung auf einem System mit weniger CPUs und weniger RAM implementieren. Bei der Nutzung dieser weniger leistungsstarken Systeme bestehen jedoch einige Einschränkungen.

Systemgröße	Spezifikationen	Einschränkungen
Extra Groß	32 CPUs, 128 GB RAM, 1 tib SSD	Kann bis zu 500 Millionen Dateien scannen.
Groß (Standard)	16 CPUs, 64 GB RAM, 500 gib SSD	Kann bis zu 250 Millionen Dateien scannen.
Mittel	8 CPUs, 32 GB RAM, 200 gib SSD	Langsamer Scan und kann nur bis zu 1 Million Dateien scannen.
Klein	8 CPUs, 16 GB RAM, 100 gib SSD	Die gleichen Einschränkungen wie „Mittel“ und die Möglichkeit, sich zu identifizieren "Namen der Betroffenen" Innerhalb von Dateien ist deaktiviert.

Bei der Implementierung der BlueXP Klassifizierung in der Cloud auf AWS können Sie sich für eine große/mittlere/kleine Instanz entscheiden. Wenn Sie die BlueXP Klassifizierung in Azure oder GCP implementieren, senden Sie eine E-Mail an ng-contact-data-sense@netapp.com, um Unterstützung zu erhalten, wenn Sie eines dieser alternativen Systeme verwenden möchten. Wir müssen mit Ihnen zusammenarbeiten, um diese anderen Cloud-Konfigurationen zu implementieren.

Bei der Implementierung der BlueXP Klassifizierung vor Ort müssen Sie einfach einen Linux-Host mit den alternativen Spezifikationen verwenden. Sie müssen sich nicht an NetApp wenden, um Unterstützung zu erhalten.

Funktionsweise der BlueXP Klassifizierung

Die allgemeine BlueXP Klassifizierung funktioniert wie folgt:

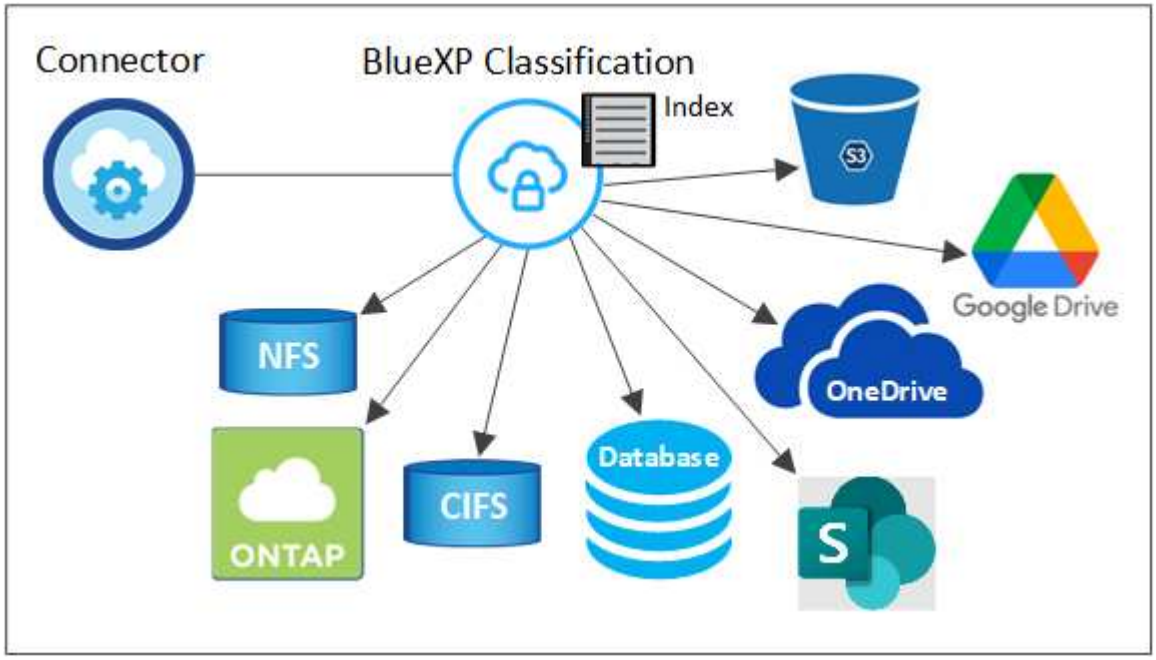
1. Sie implementieren eine Instanz der BlueXP Klassifizierung in BlueXP.
2. Sie ermöglichen ein hohes Mapping oder tiefes Scannen auf einer oder mehreren Datenquellen.
3. Bei der BlueXP Klassifizierung werden die Daten mithilfe eines KI-Lernprozesses gescannt.
4. Sie nutzen die bereitgestellten Dashboards und Berichterstellungs-Tools, um Ihre Compliance- und Governance-Bemühungen zu unterstützen.

Funktionsweise von Scans

Nachdem die BlueXP Klassifizierung aktiviert und die Repositorys ausgewählt wurden, die gescannt werden sollen (dies sind die Volumes, Buckets, Datenbankschemata oder OneDrive- oder SharePoint Benutzerdaten), beginnt der Scan sofort mit dem Scannen der Daten zur Identifizierung persönlicher und sensibler Daten. Sie sollten sich in den meisten Fällen auf die Scans von Live-Produktionsdaten konzentrieren und nicht auf Backups, Spiegelungen oder DR-Standorte. Die BlueXP Klassifizierung ordnet anschließend Ihre Unternehmensdaten zu, kategorisiert jede Datei und identifiziert und extrahiert Entitäten und vordefinierte Muster in den Daten. Das Ergebnis des Scans ist ein Index von persönlichen Daten, sensiblen persönlichen Daten, Datenkategorien und Dateitypen.

Wie bei jedem anderen Client lässt sich die BlueXP Klassifizierung mit den Daten verbinden, indem NFS- und CIFS-Volumes gemountet werden. NFS Volumes werden automatisch als schreibgeschützt abgerufen und

müssen zur Überprüfung von CIFS Volumes Active Directory Anmeldeinformationen bereitstellen.



Nach dem ersten Scan scannt die BlueXP Klassifizierung Ihre Daten fortlaufend und nach Round Robin-Verfahren, um inkrementelle Änderungen zu erkennen (aus diesem Grund ist es wichtig, die Instanz weiterhin auszuführen).

Sie können Scans auf Volume-Ebene, auf Bucket-Ebene, auf Datenbankschemaebene, auf OneDrive-Benutzerebene und auf SharePoint-Standortebene aktivieren und deaktivieren.

Was ist der Unterschied zwischen Mapping und Classification Scans

Die BlueXP Klassifizierung ermöglicht Ihnen die Durchführung eines allgemeinen „Mapping“-Scans für ausgewählte Datenquellen. Das Mapping bietet nur einen Überblick über Ihre Daten auf hoher Ebene, während die Klassifizierung ein tiefes Scannen Ihrer Daten ermöglicht. Das Mapping kann auf Ihren Datenquellen sehr schnell durchgeführt werden, da es nicht auf Dateien zugegriffen wird, um die darin enthaltenen Daten zu sehen.

Viele Benutzer mögen diese Funktionalität, weil sie ihre Daten schnell scannen möchten, um die Datenquellen zu identifizieren, die mehr Forschungsarbeiten benötigen. Sie können dann Scans nur auf die erforderlichen Datenquellen oder Volumes klassifizieren.

In der folgenden Tabelle sind einige Unterschiede aufgeführt:

Merkmal	Klassifizierung	Zuordnung
Scangeschgeschwindigkeit	Langsam	Schnell
Liste der Dateitypen und der genutzten Kapazität	Ja.	Ja.
Anzahl der Dateien und genutzte Kapazität	Ja.	Ja.
Alter und Größe der Dateien	Ja.	Ja.
Fähigkeit, ein auszuführen "Datenzuordnungsbericht"	Ja.	Ja.
Datenuntersuchung, um Dateidetails anzuzeigen	Ja.	Nein

Merkmal	Klassifizierung	Zuordnung
Suche nach Namen in Dateien	Ja.	Nein
Erstellen "Richtlinien" Die benutzerdefinierte Suchergebnisse liefern	Ja.	Nein
Kategorisieren Sie Daten mit AIP-Etiketten und Status-Tags	Ja.	Nein
Quelldateien kopieren, löschen und verschieben	Ja.	Nein
Möglichkeit zur Ausführung anderer Berichte	Ja.	Nein

Wie schnell scannt die BlueXP Klassifizierung Daten

Die Scan-Geschwindigkeit wird durch Netzwerklatenz, Festplattenlatenz, Netzwerkbandbreite, Umgebungsgröße und Dateiverteilungsgrößen beeinflusst.

- Bei der Durchführung von Mapping-Scans kann die BlueXP Klassifizierung zwischen 100-150 TIBS Daten pro Tag und Scanner-Node scannen.
- Bei der Durchführung von Classification Scans können mit der BlueXP Klassifizierung Daten pro Tag und Scanner-Node zwischen 15-40 TB gescannt werden.

"Erfahren Sie mehr über die Implementierung mehrerer Scanner-Knoten zum Scannen Ihrer Daten".

Informationen, die die BlueXP Klassifizierung indexiert

Die BlueXP Klassifizierung erfasst, indiziert und weist Ihren Daten (Dateien) Kategorien zu. Die Daten, die die BlueXP Klassifizierung indiziert, umfassen die folgenden:

Standard-Metadaten

Die BlueXP Klassifizierung erfasst Standardmetadaten zu Dateien: Die Art der Datei, ihre Größe, das Erstellungsdatum und die Änderungsdaten usw.

Persönliche Daten

Personenbezogene Informationen wie E-Mail-Adressen, Identifikationsnummern oder Kreditkartennummern. "Weitere Informationen zu personenbezogenen Daten".

Sensible persönliche Daten

Besondere Arten sensibler Daten, wie etwa Gesundheitsdaten, ethnische Herkunft oder politische Ansichten, wie in der DSGVO und anderen Datenschutzvorschriften definiert "Erfahren Sie mehr über sensible persönliche Daten".

Kategorien

Die BlueXP Klassifizierung unterteilt die gescannten Daten in unterschiedliche Kategorien. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Weitere Informationen zu Kategorien".

Typen

Die BlueXP Klassifizierung unterteilt die gescannten Daten nach Dateityp. "Erfahren Sie mehr über Types".

Name der Entität Anerkennung

Die BlueXP Klassifizierung verwendet KI, um Namen natürlicher Personen aus Dokumenten zu extrahieren. "Informieren Sie sich über die Reaktion auf Zugriffsanfragen von Betroffenen".

Netzwerkübersicht

BlueXP implementiert die BlueXP Klassifizierungsinstanz mit einer Sicherheitsgruppe, die eingehende HTTP-Verbindungen von der Connector-Instanz ermöglicht.

Wenn Sie BlueXP im SaaS-Modus verwenden, wird die Verbindung zu BlueXP über HTTPS hergestellt. Die privaten Daten, die zwischen Ihrem Browser und der BlueXP Klassifizierungsinstanz gesendet werden, sind durch End-to-End-Verschlüsselung mit TLS 1.2 geschützt. Dies bedeutet, dass NetApp und Drittanbieter die Daten nicht lesen können.

Ausgehende Regeln sind vollständig geöffnet. Zum Installieren und Aktualisieren der BlueXP Klassifizierungssoftware und zum Senden von Nutzungsmetriken ist ein Internetzugriff erforderlich.

Wenn Sie strenge Netzwerkanforderungen erfüllen, "Erfahren Sie mehr über die Endpunkte, auf die BlueXP Klassifizierungen setzt".

Zugriff des Benutzers auf Compliance-Informationen

Die Rolle, die jedem Benutzer zugewiesen wurde, bietet unterschiedliche Funktionen in BlueXP und innerhalb der BlueXP Klassifizierung:

- Ein **Account Admin** kann Compliance-Einstellungen verwalten und Compliance-Informationen für alle Arbeitsumgebungen anzeigen.
- Ein **Workspace Admin** kann Compliance-Einstellungen verwalten und Compliance-Informationen nur für Systeme anzeigen, auf die sie Zugriff haben. Wenn ein Workspace-Administrator nicht auf eine Arbeitsumgebung in BlueXP zugreifen kann, werden keine Compliance-Informationen für die Arbeitsumgebung auf der Registerkarte BlueXP Klassifizierung angezeigt.
- Benutzer mit der Rolle **Compliance Viewer** können Compliance-Informationen nur anzeigen und Berichte für Systeme erstellen, auf die sie zugreifen können. Diese Benutzer können das Scannen von Volumes, Buckets oder Datenbankschemata nicht aktivieren/deaktivieren. Diese Benutzer können Dateien auch nicht kopieren, verschieben oder löschen.

"Erfahren Sie mehr über BlueXP-Rollen" Und wie "Benutzer mit bestimmten Rollen hinzufügen".

Implementieren Sie die BlueXP Klassifizierung

Welche BlueXP Klassifizierungs-Implementierung sollten Sie verwenden?

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

Die BlueXP Klassifizierung kann wie folgt implementiert werden:

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

Modus. Diese Art der Installation, die ein Installationsskript verwendet, ist gut für Ihre sicheren Seiten.

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

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

Implementieren Sie die BlueXP Klassifizierung in der Cloud mit BlueXP

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

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

Schnellstart

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

1 Einen Konnektor erstellen

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

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

2 Voraussetzungen prüfen

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

3 Implementieren Sie die BlueXP Klassifizierung

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

4 Abonnieren Sie den BlueXP Klassifizierungsservice

Die ersten 1 TB an Daten, die die BlueXP Klassifizierung in BlueXP scannt, sind 30 Tage lang kostenlos. Um

die Daten nach diesem Zeitpunkt weiterhin zu scannen, ist ein BlueXP Abonnement über Ihren Cloud-Provider Marketplace oder eine BYOL-Lizenz von NetApp erforderlich.

Einen Konnektor erstellen

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

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

- Zum Scannen von Daten in Cloud Volumes ONTAP in AWS, Amazon FSX für ONTAP oder in AWS S3-Buckets verwenden Sie einen Connector in AWS.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Connector in Azure.
  - Bei Azure NetApp Files muss sie in demselben Bereich bereitgestellt werden wie die Volumes, die Sie scannen möchten.
- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP wird ein Connector in GCP verwendet.

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

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

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

Unterstützung für Regierungsregionen

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

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

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

Voraussetzungen prüfen

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

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

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

kontaktieren. Der Proxy muss nicht transparent sein - wir unterstützen derzeit keine transparenten Proxys.

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

Erforderliche Endpunkte für AWS

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

Erforderliche Endpunkte für Azure

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

Erforderliche Endpunkte für GCP

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

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

Stellen Sie sicher, dass BlueXP über die erforderlichen Berechtigungen verfügt

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

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

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

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

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

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

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

Webbrowser-Konnektivität zur BlueXP Klassifizierung sicherstellen

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

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

Überprüfen Sie Ihre vCPU-Limits

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

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

- "AWS Dokumentation: Amazon EC2 Service Quotas"

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

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

Implementieren Sie die BlueXP Klassifizierung in der Cloud

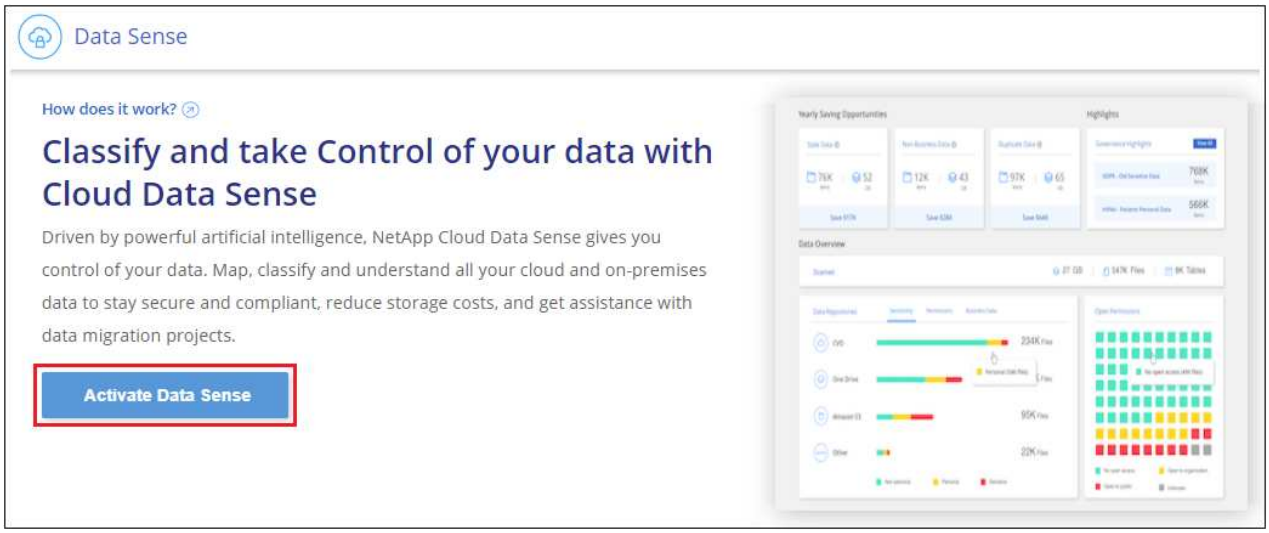
Führen Sie diese Schritte aus, um eine Instanz der BlueXP Klassifizierung in der Cloud zu implementieren. Der Connector implementiert die Instanz in der Cloud und installiert dann die BlueXP Klassifizierungssoftware auf dieser Instanz.

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

Implementieren in AWS

Schritte

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



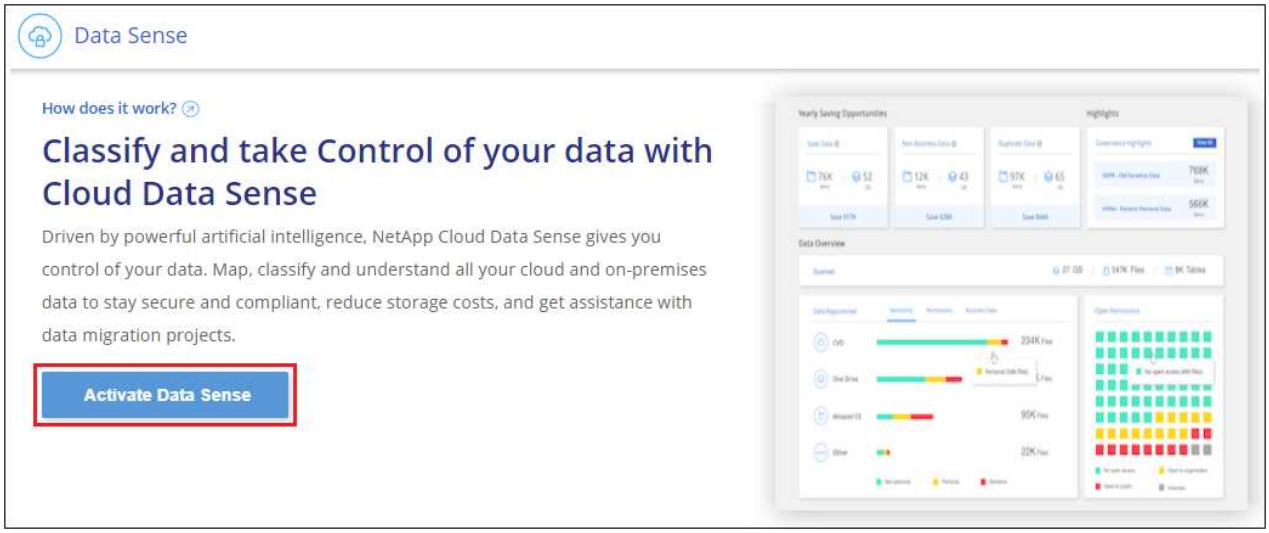
2. Klicken Sie Auf **Datensense Aktivieren**.
3. Klicken Sie auf der Seite *Installation* auf **Deploy > Deploy**, um die „große“ Instanzgröße zu verwenden und den Cloud-Bereitstellungsassistenten zu starten.
4. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Es wird angehalten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

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

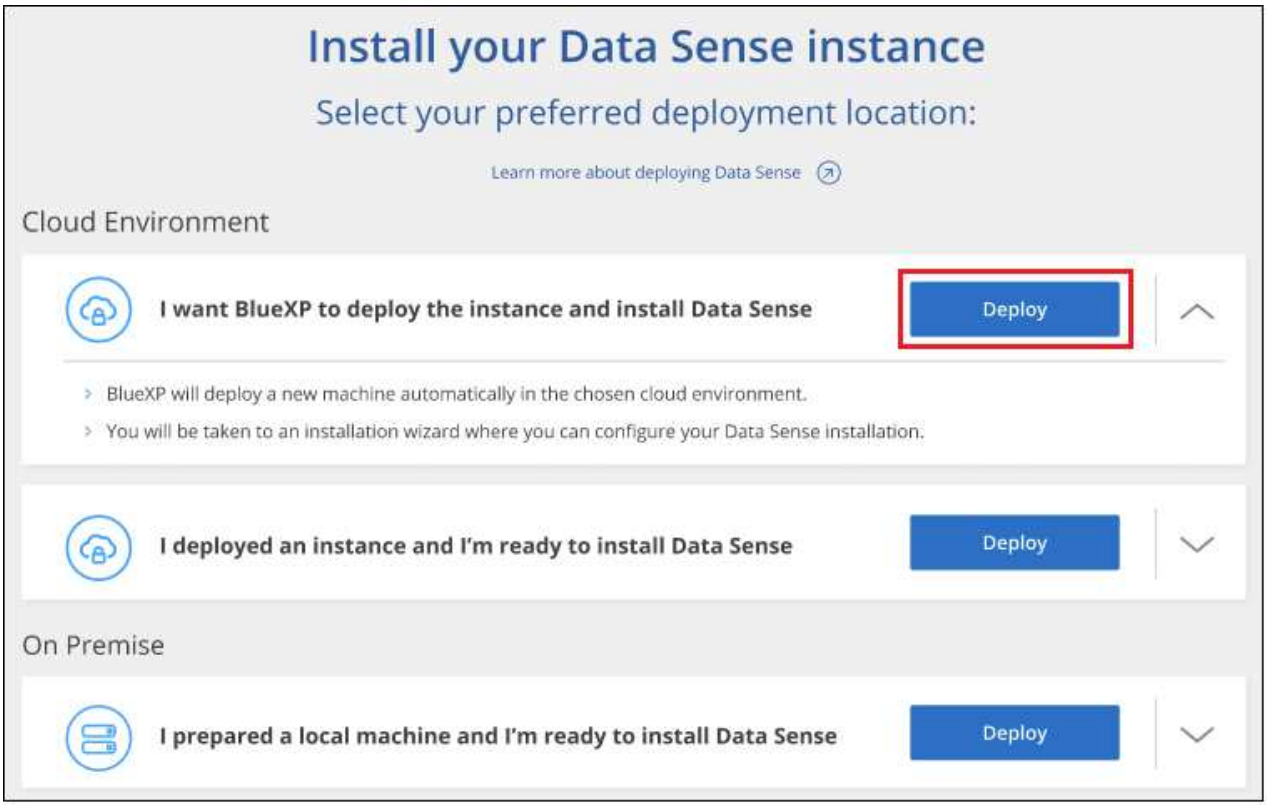
Implementieren in Azure

Schritte

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



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



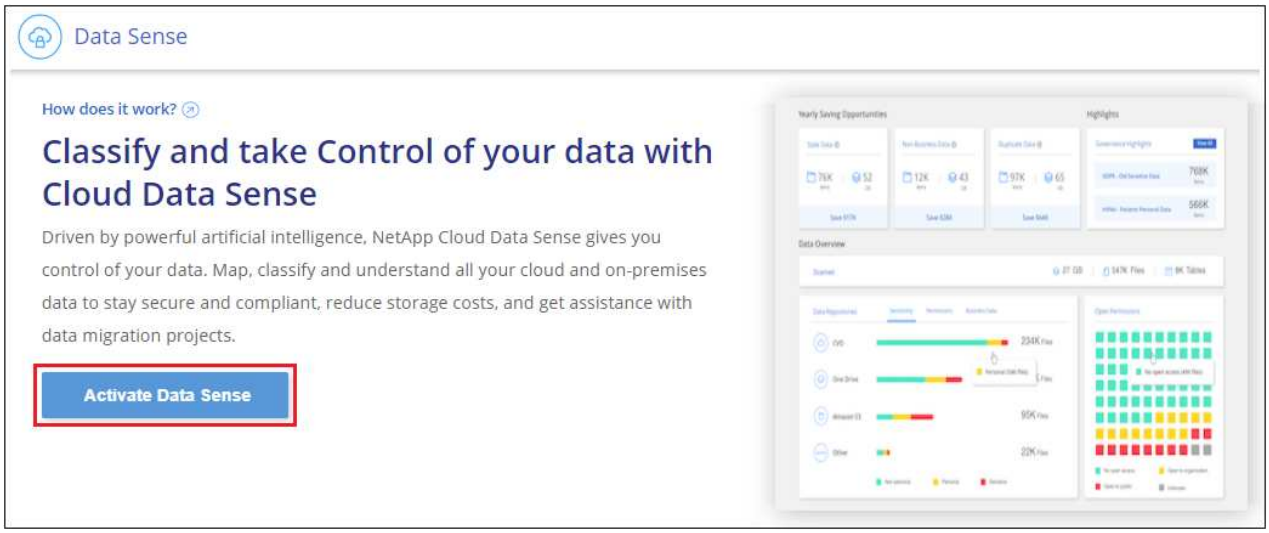
4. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Es wird angehalten und zur Eingabe aufgefordert, wenn Probleme auftreten.

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

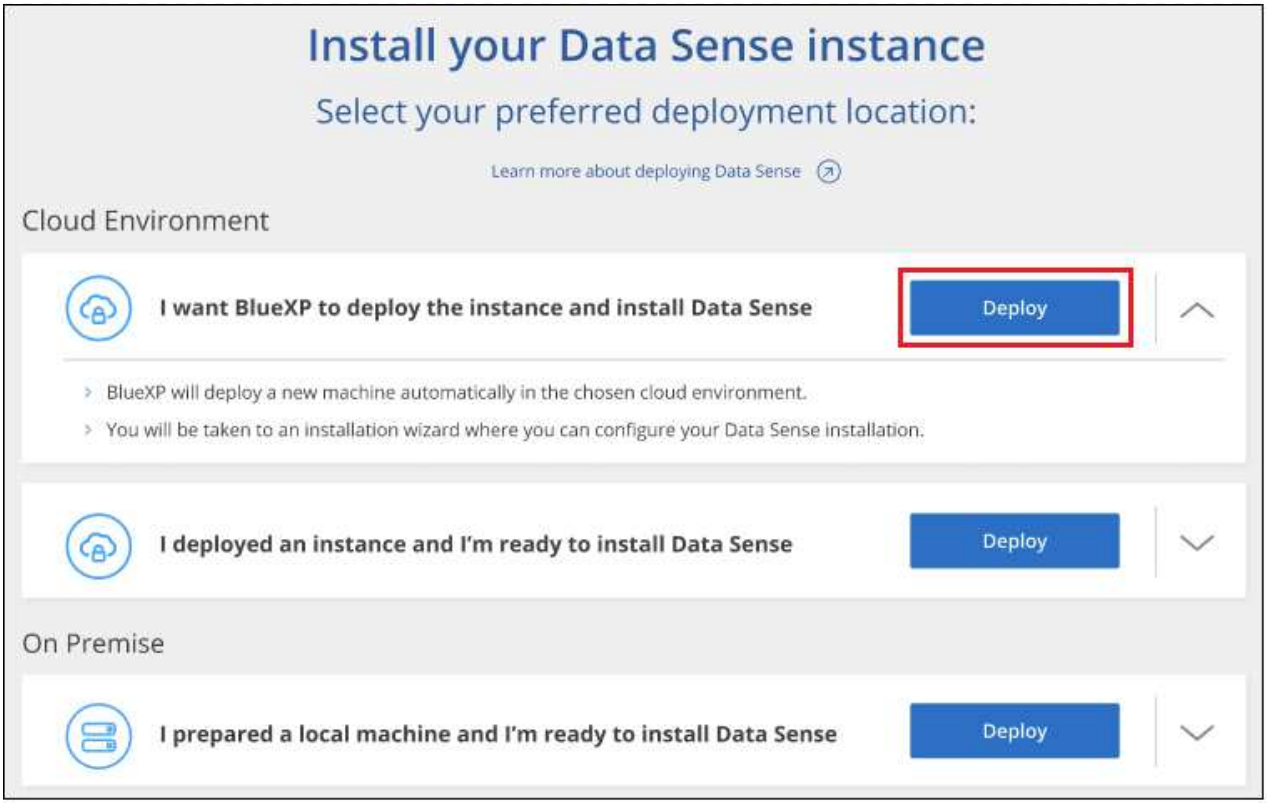
Implementieren in Google Cloud

Schritte

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



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



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

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

Ergebnis

BlueXP implementiert die BlueXP Klassifizierungsinstanz in Ihrem Cloud-Provider.

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

Nächste Schritte

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

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

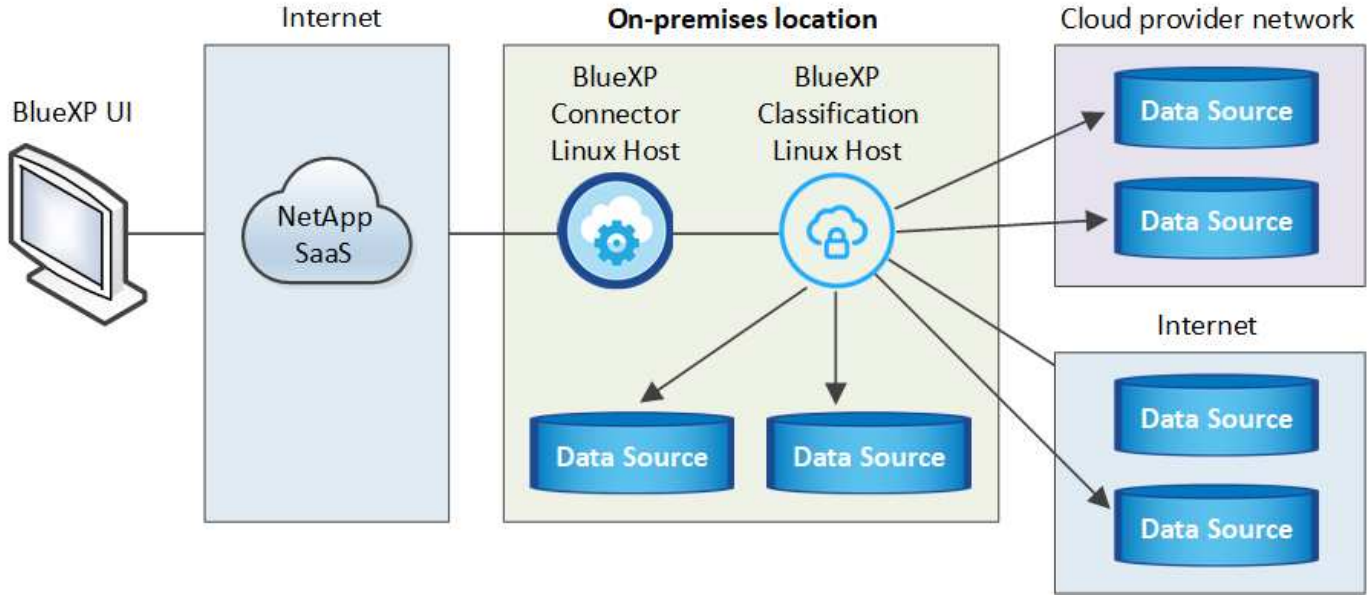
Installieren Sie die BlueXP Klassifizierung auf einem Host mit Internetzugang

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

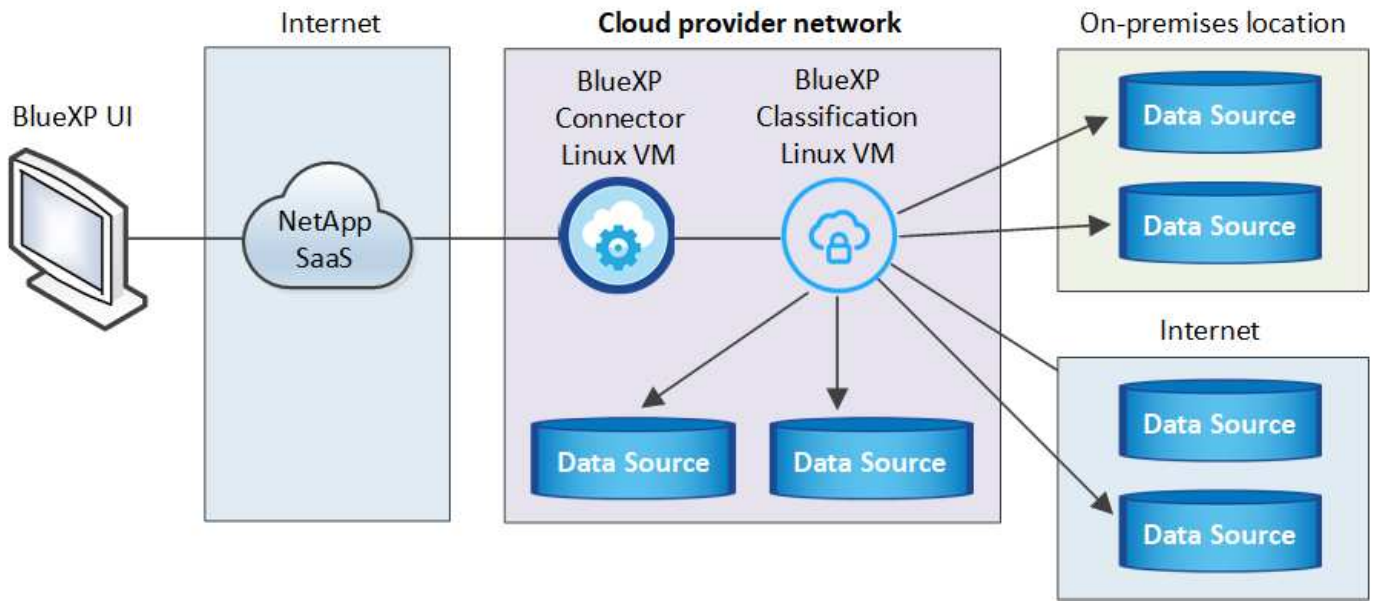
Die On-Premises-Installation ist möglicherweise eine gute Option, wenn Sie On-Premises-ONTAP Systeme mit einer BlueXP Klassifizierungsinstanz scannen möchten, die sich auch vor Ort befindet – dies ist jedoch keine Anforderung. Die Software funktioniert unabhängig von der gewählten Installationsmethode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

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

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



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



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

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

Schnellstart

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

1 Einen Konnektor erstellen

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

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

2 Voraussetzungen prüfen

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

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

3 Laden Sie die BlueXP Klassifizierung herunter und implementieren Sie sie

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

befolgen Sie die Anweisungen zur Implementierung der BlueXP Klassifizierungsinstanz.

4 Abonnieren Sie den BlueXP Klassifizierungsservice

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

Einen Konnektor erstellen

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

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

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

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

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

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

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

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

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

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

Bereiten Sie das Linux-Hostsystem vor

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

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

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

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

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

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

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

- **Betriebssystem**:

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

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

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

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

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

    - Podman Version 4 oder höher. Um Podman zu installieren, aktualisieren Sie die Systempakete (`sudo yum update -y`), und installieren Sie dann Podman (`sudo yum install netavark -y`).
- Python Version 3.6 oder höher. "Installationsanweisungen anzeigen".

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

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

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

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

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

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

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

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

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

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

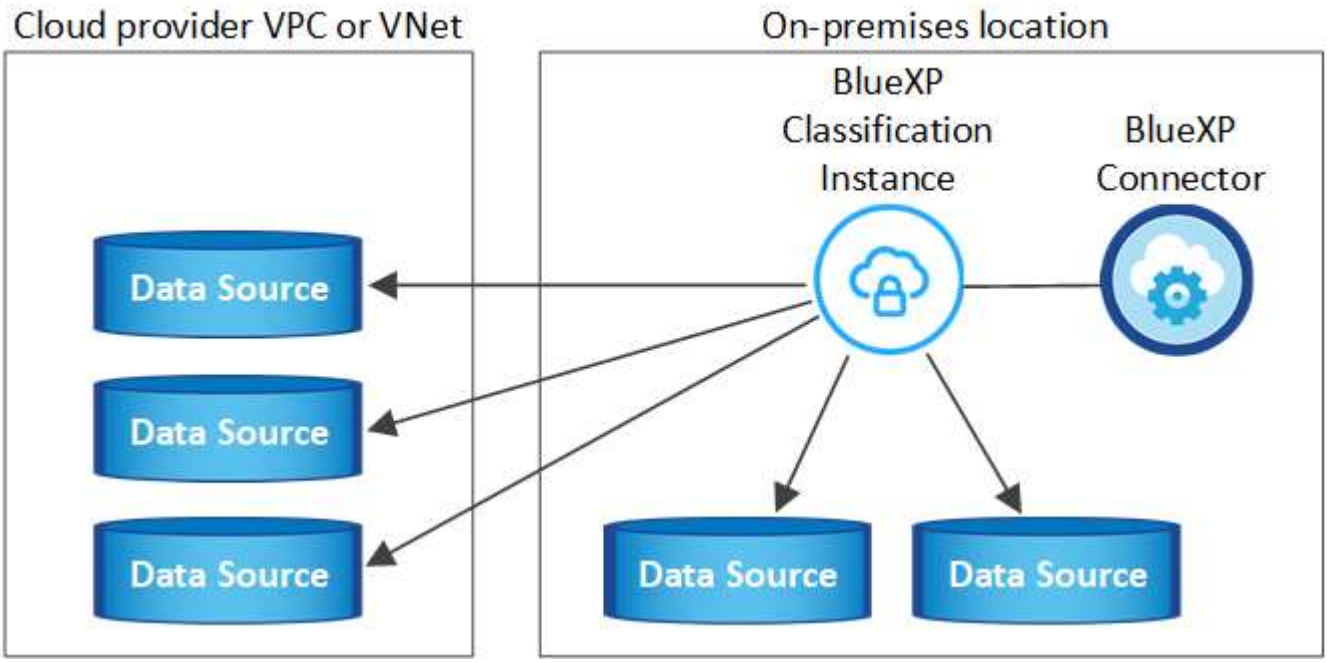
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 443 (TCP) und 80	Die Firewall- oder Routing-Regeln für den Connector müssen ein- und ausgehenden Datenverkehr über Port 443 zur und von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass Port 8080 geöffnet ist, damit Sie den Installationsfortschritt in BlueXP sehen können.
Connector <> ONTAP-Cluster (NAS)	443 (TCP)	BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen: • Der Connector-Host muss ausgehenden HTTPS-Zugriff über Port 443 ermöglichen. Wenn sich der Connector in der Cloud befindet, ist die gesamte ausgehende Kommunikation durch vordefinierte Firewall- oder Routingregeln zulässig. • Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen. Die standardmäßige "mgmt"-Firewall-Richtlinie ermöglicht eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert haben oder wenn Sie eine eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff über den Connector-Host aktivieren.
BlueXP Klassifizierung <> ONTAP Cluster	• Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS - 139 (TCP\UDP) und 445 (TCP\UDP)	Für die BlueXP Klassifizierung benötigen Sie eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder Ihrem lokalen ONTAP System. Firewalls oder Routingregeln für Cloud Volumes ONTAP müssen eingehende Verbindungen von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind: • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.

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

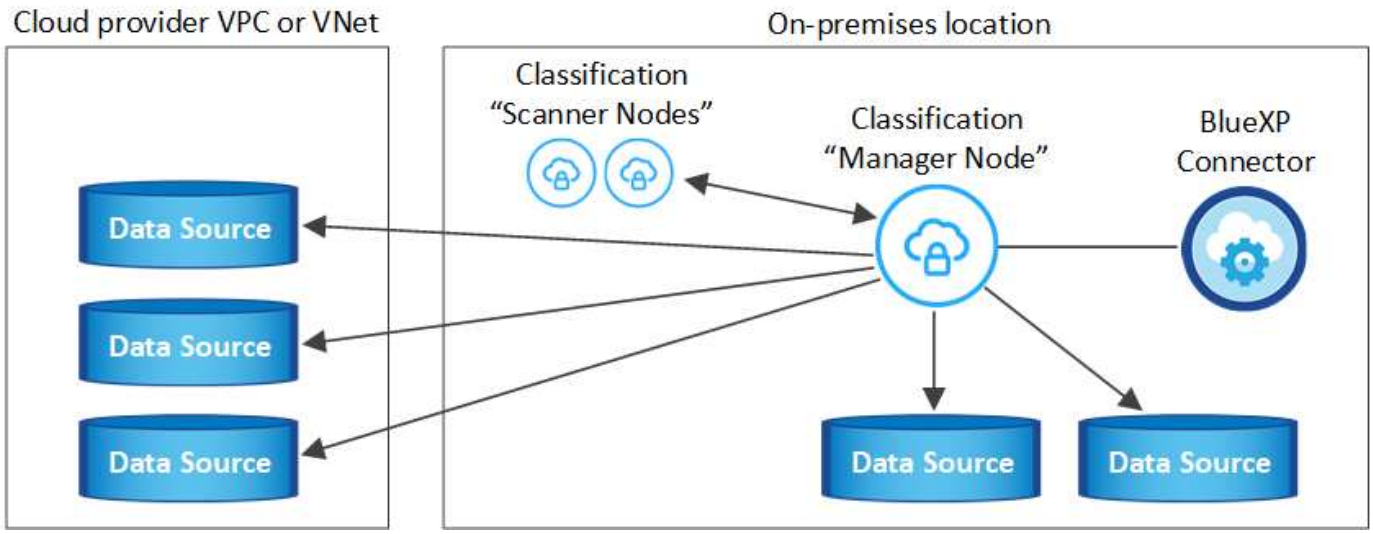
Wenn Sie mehrere BlueXP Klassifizierungs-Hosts nutzen, um eine zusätzliche Rechenleistung zum Scannen Ihrer Datenquellen zu bieten, müssen Sie zusätzliche Ports/Protokolle aktivieren. "Siehe zusätzliche Anschlussanforderungen".

BlueXP Klassifizierung auf dem Linux-Host installieren

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



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



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

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

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

Installation mit einem Host für typische Konfigurationen

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

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

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

Was Sie benötigen

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

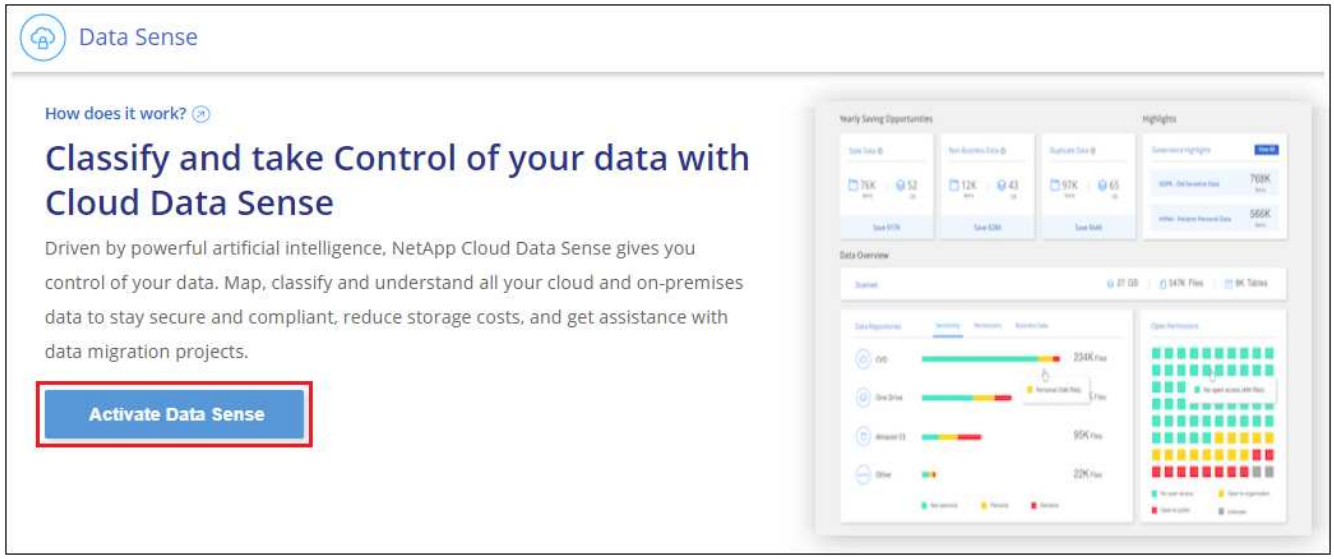
- Vergewissern Sie sich, dass die erforderliche Offline-Umgebung erfüllt ist Berechtigungen und Konnektivität.

Schritte

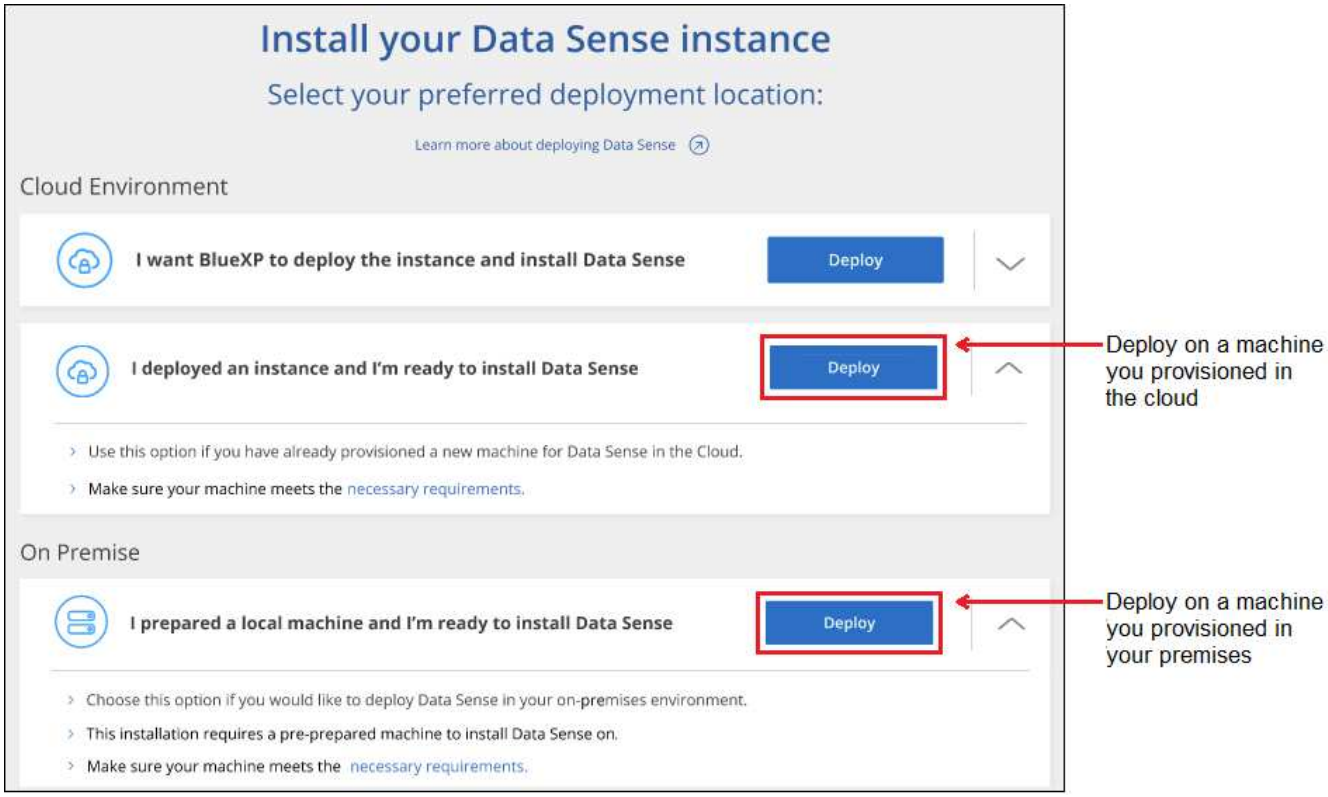
1. Laden Sie die BlueXP Klassifizierungssoftware von herunter "NetApp Support Website". Die ausgewählte Datei heißt **DATASENSE-INSTALLER-<Version>.tar.gz**.
2. Kopieren Sie die Installationsdatei auf den Linux-Host, den Sie verwenden möchten (mit `scp` Oder eine andere Methode).
3. Entpacken Sie die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

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

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



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



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

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

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

Variablenwerte:

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

Ergebnis

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

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

Nächste Schritte

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

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

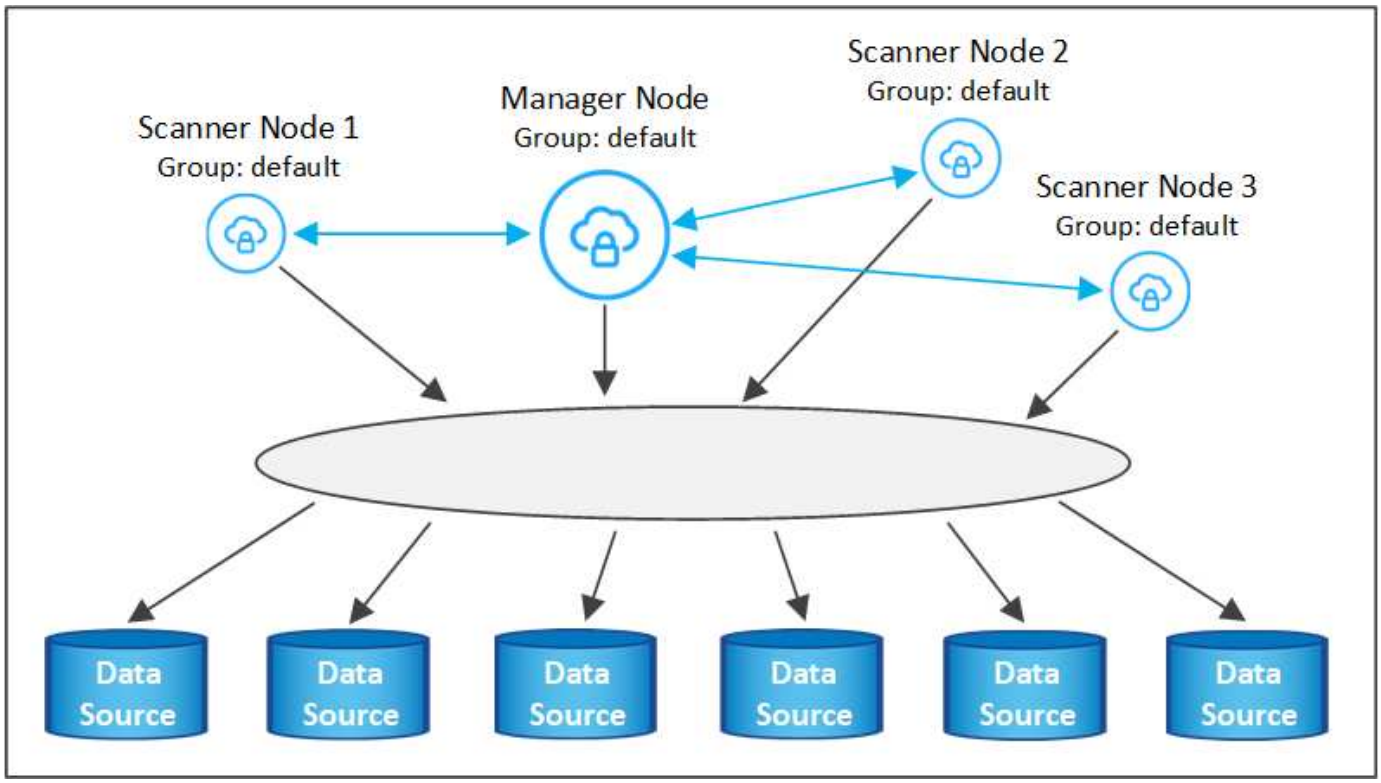
Fügen Sie Scannerknoten zu einer vorhandenen Implementierung hinzu

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

Es gibt zwei Möglichkeiten, weitere Scanner-Knoten hinzuzufügen:

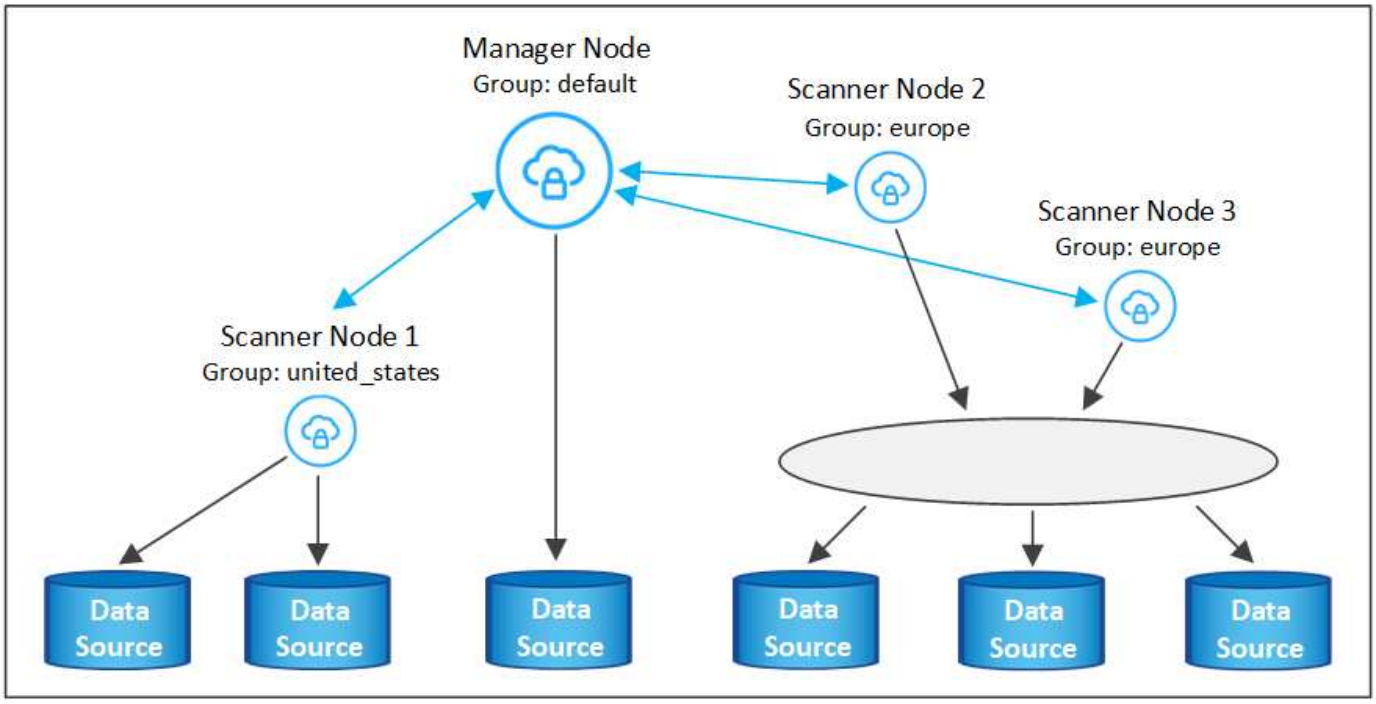
- Fügen Sie einen Knoten hinzu, um das Scannen aller Datenquellen zu unterstützen
- Fügen Sie einen Knoten hinzu, um das Scannen einer bestimmten Datenquelle oder einer bestimmten Gruppe von Datenquellen zu unterstützen (typischerweise basierend auf dem Speicherort).

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



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

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



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

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

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

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

Was Sie benötigen

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

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

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

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

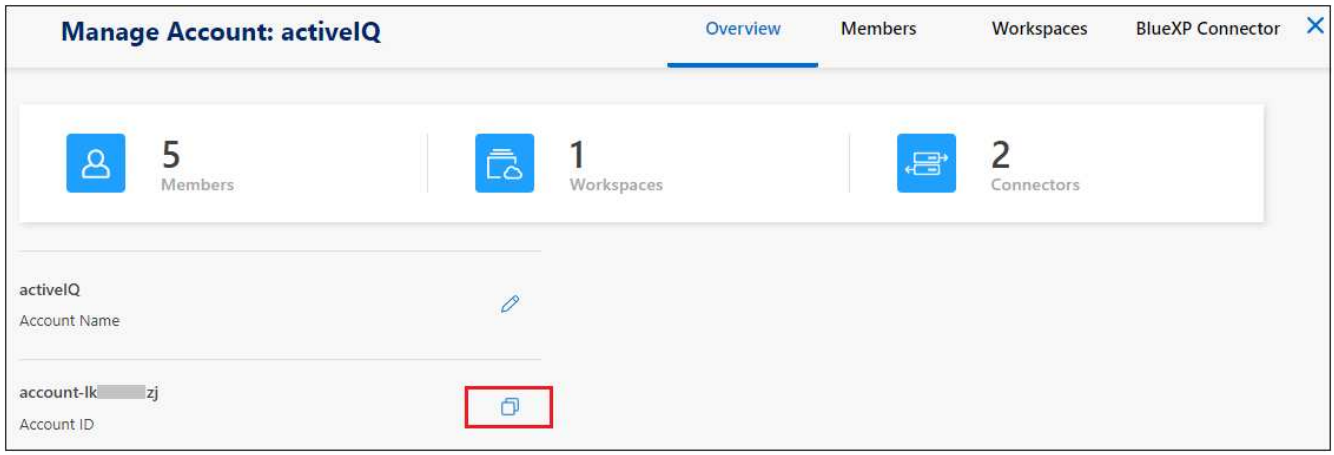
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp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

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

Erforderliche Schritte

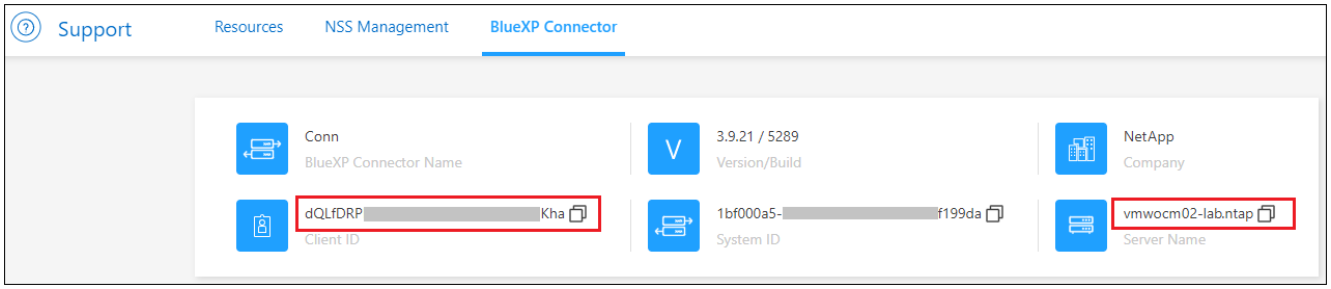
Führen Sie diese Schritte aus, um die NetApp Account ID, die Connector Client ID, den Connector Server-Namen und das Token für den Benutzerzugriff zu erhalten, die erforderlich sind, um Scanner-Nodes hinzuzufügen.

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

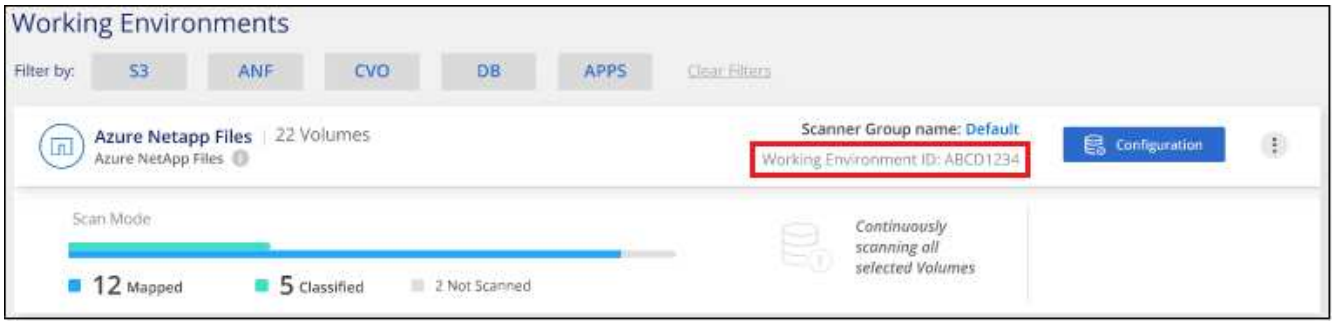


2. Kopieren Sie die *Konto-ID*.

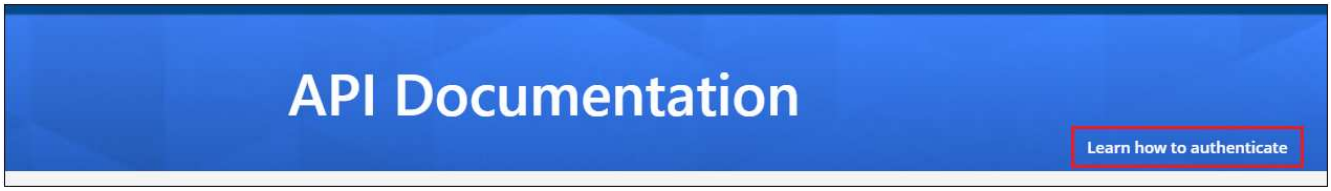
3. Klicken Sie in der Menüleiste von BlueXP auf **Hilfe > Support > BlueXP Connector**.



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



6. Wechseln Sie zum "API Documentation Developer Hub" Und klicken Sie auf **Erfahren Sie, wie Sie sich authentifizieren**.



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

Schritte

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

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

   Variablenwerte:

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

- *Cm_Host* = IP-Adresse oder Hostname des Steckverbindersystems
- *ds_Manager_ip* = Private IP-Adresse des Node-Systems BlueXP Classification Manager
- *Node_Private_ip* = IP-Adressen der BlueXP Klassifizierungsscanner Node-Systeme (mehrere Scanner-Node-IPs werden durch ein Komma getrennt)
- *User_Token* = JWT-Benutzer-Zugriffstoken

2. Bevor das Skript add_Scanner_Node abgeschlossen wird, wird in einem Dialogfeld der Installationsbefehl angezeigt, der für die Scanner-Knoten benötigt wird. Kopieren Sie den Befehl (z. B.: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`) Und in einer Textdatei speichern.
3. Auf * jedem Scanner-Knoten-Host:
   a. Kopieren Sie die Data Sense Installer-Datei (**DATASENSE-INSTALLER-<Version>.tar.gz**) auf den Host-Rechner (mit `scp` Oder eine andere Methode).
   b. Entpacken Sie die Installationsdatei.
   c. Fügen Sie den Befehl ein, den Sie in Schritt 2 kopiert haben, und führen Sie ihn aus.
   d. Wenn Sie einen Scannerknoten zu einer "Scannergruppe" hinzufügen möchten, fügen Sie dem Befehl den Parameter **-r <Scanner_Group_Name>** hinzu. Andernfalls wird der Scannerknoten zur Gruppe „Standard“ hinzugefügt.

      Wenn die Installation auf allen Scanner-Knoten abgeschlossen ist und sie mit dem Manager-Knoten verbunden wurden, wird das Skript „add_Scanner_Node.sh“ ebenfalls beendet. Die Installation dauert 10 bis 20 Minuten.
4. Wenn Sie Scannerknoten zu einer Scannergruppe hinzugefügt haben, kehren Sie zum Manager-Knoten zurück und führen Sie die folgenden beiden Aufgaben aus:
   a. Öffnen Sie die Datei „/opt/netapp/config/Custom_Configuration/working_environment_to_Scanner_Group_config.yml“ und geben Sie die Zuordnung ein, für welche Scannergruppen bestimmte Arbeitsumgebungen scannen sollen. Sie benötigen die *Working Environment ID* für jede Datenquelle. Die folgenden Einträge fügen beispielsweise 2 Arbeitsumgebungen zur Scanner-Gruppe „europa“ und 2 zur Scannergruppe „united_States“ hinzu:

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

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

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

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

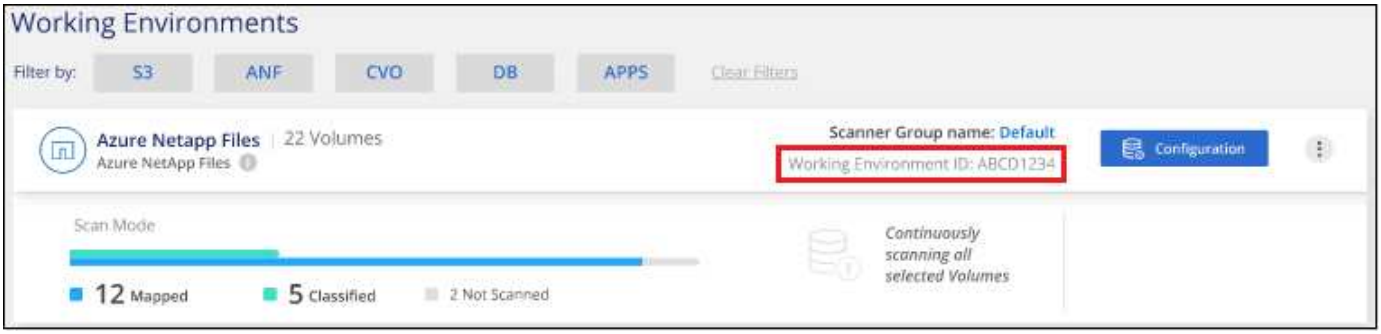
Ergebnis

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

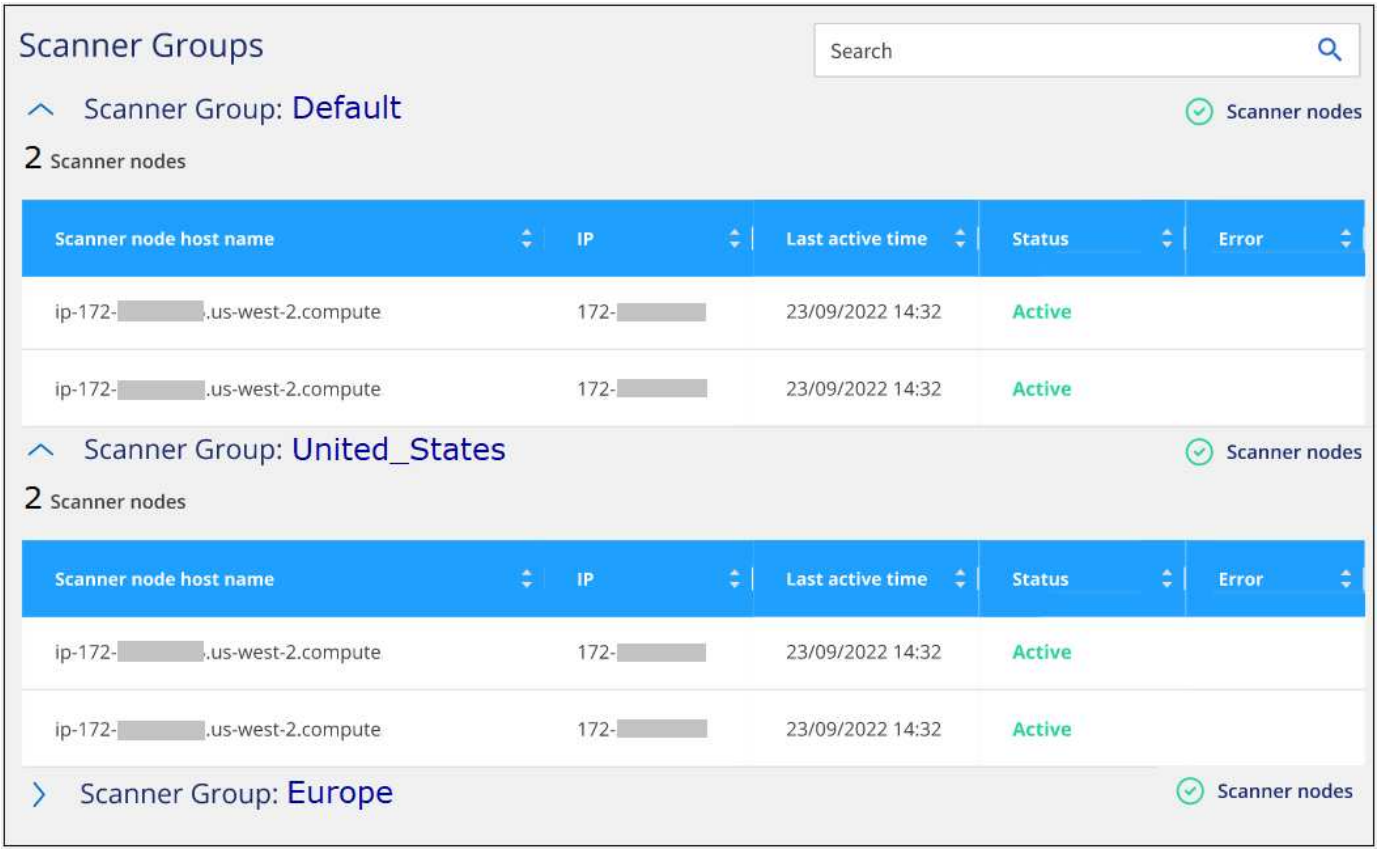
Nächste Schritte

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

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



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



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

Installation mit mehreren Hosts für große Konfigurationen

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

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

Was Sie benötigen

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

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

Schritte

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

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

   Mit diesem Befehl werden beispielsweise 3 Scannerknoten hinzugefügt:
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy
   ```

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

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

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

Ergebnis

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

Nächste Schritte

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

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

BlueXP Klassifizierung auf einem Linux-Host ohne Internetzugang installieren

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

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

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

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

Unterstützte Datenquellen

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

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

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

Einschränkungen

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

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

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

Schnellstart

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

1 Installieren Sie den BlueXP-Anschluss

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

2 Voraussetzungen für die BlueXP Klassifizierung prüfen

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

3 Laden Sie die BlueXP Klassifizierung herunter und implementieren Sie sie

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

4 Abonnieren Sie den BlueXP Klassifizierungsservice

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

Installieren Sie den BlueXP-Anschluss

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

Bereiten Sie das Linux-Hostsystem vor

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

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

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

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

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

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

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

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

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

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

    - Podman Version 4 oder höher. Um Podman zu installieren, aktualisieren Sie die Systempakete (`sudo yum update -y`), und installieren Sie dann Podman (`sudo yum install netavark -y`).
- Python Version 3.6 oder höher. "Installationsanweisungen anzeigen".

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

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

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

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

Voraussetzungen für die Klassifizierung von BlueXP und BlueXP prüfen

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

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

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

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

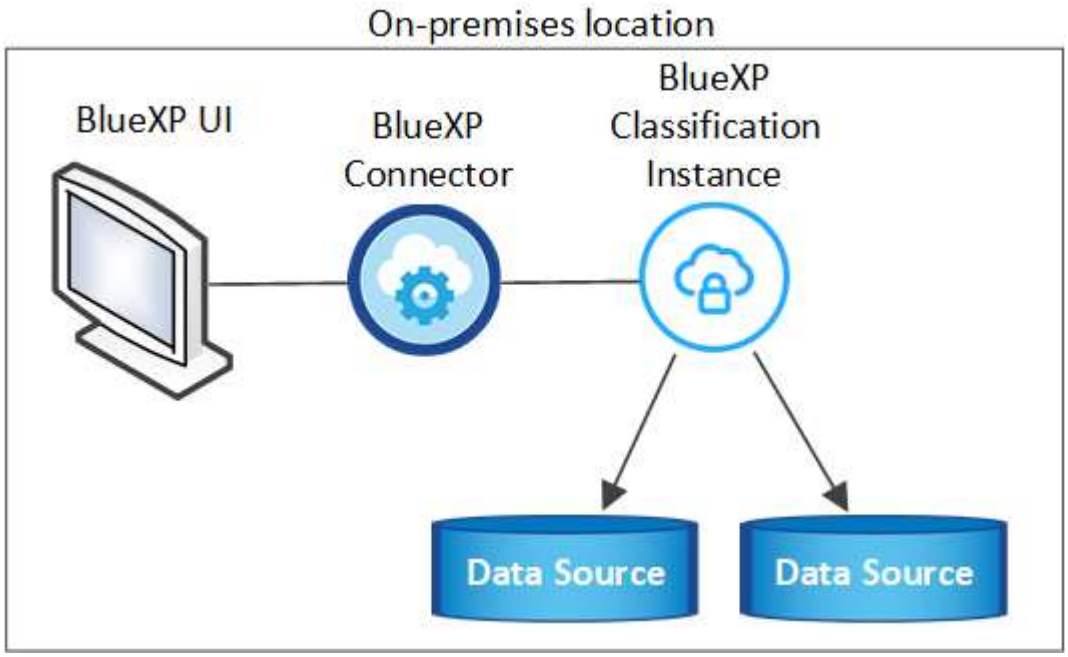
Verbindungstyp	Ports	Beschreibung
Connector <> BlueXP Klassifizierung	8080 (TCP), 6000 (TCP), 443 (TCP) UND 80	Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über die Ports 6000 und 443 zur und von der BlueXP Klassifizierungsinstanz zulassen. • Port 6000 ist erforderlich, damit die BYOL-Lizenz für die BlueXP Klassifizierung an einem Dark Site funktioniert. • Port 8080 sollte offen sein, damit Sie den Installationsfortschritt in BlueXP sehen können.
Connector <> ONTAP-Cluster (NAS)	443 (TCP)	BlueXP erkennt ONTAP-Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen: • Der Connector-Host muss ausgehenden HTTPS-Zugriff über Port 443 ermöglichen. Wenn sich der Connector in der Cloud befindet, ist die gesamte ausgehende Kommunikation durch die vordefinierte Sicherheitsgruppe zulässig. • Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen. Die standardmäßige "mgmt"-Firewall-Richtlinie ermöglicht eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert haben oder wenn Sie eine eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff über den Connector-Host aktivieren.
BlueXP Klassifizierung <> ONTAP Cluster	• Für NFS – 111 (TCP\UDP) und 2049 (TCP\UDP) • Für CIFS - 139 (TCP\UDP) und 445 (TCP\UDP)	Für die BlueXP Klassifizierung benötigen Sie eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder Ihrem lokalen ONTAP System. Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen von der BlueXP Klassifizierungsinstanz ermöglichen. Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind: • Für NFS - 111 und 2049 • Für CIFS - 139 und 445 NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.

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

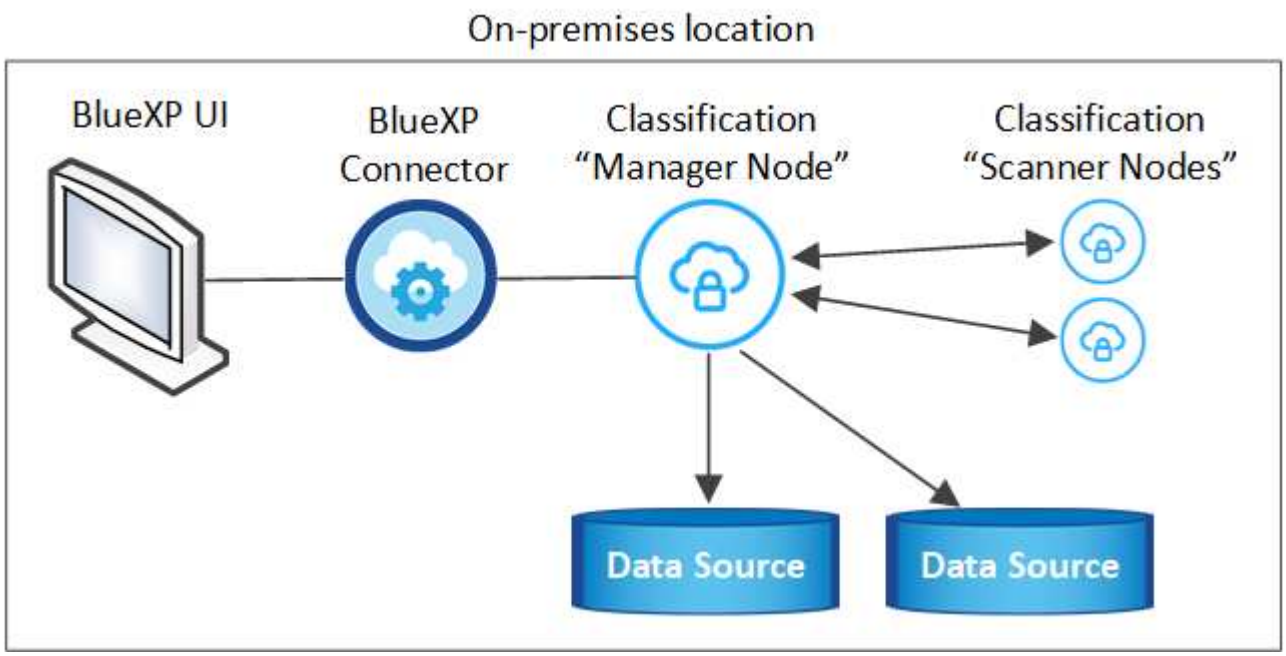
Wenn Sie mehrere BlueXP Klassifizierungs-Hosts nutzen, um eine zusätzliche Rechenleistung zum Scannen Ihrer Datenquellen zu bieten, müssen Sie zusätzliche Ports/Protokolle aktivieren. "Siehe zusätzliche Anschlussanforderungen".

BlueXP Klassifizierung auf dem lokalen Linux-Host installieren

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



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



Installation mit einem Host für typische Konfigurationen

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

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

Was Sie benötigen

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

Schritte

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

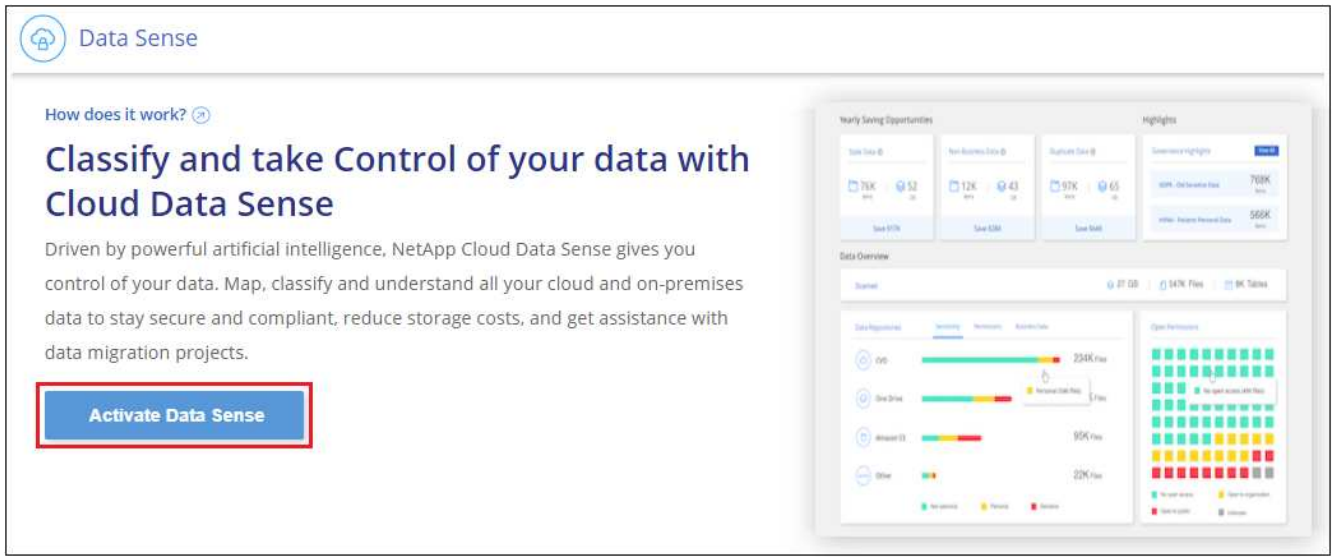
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

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

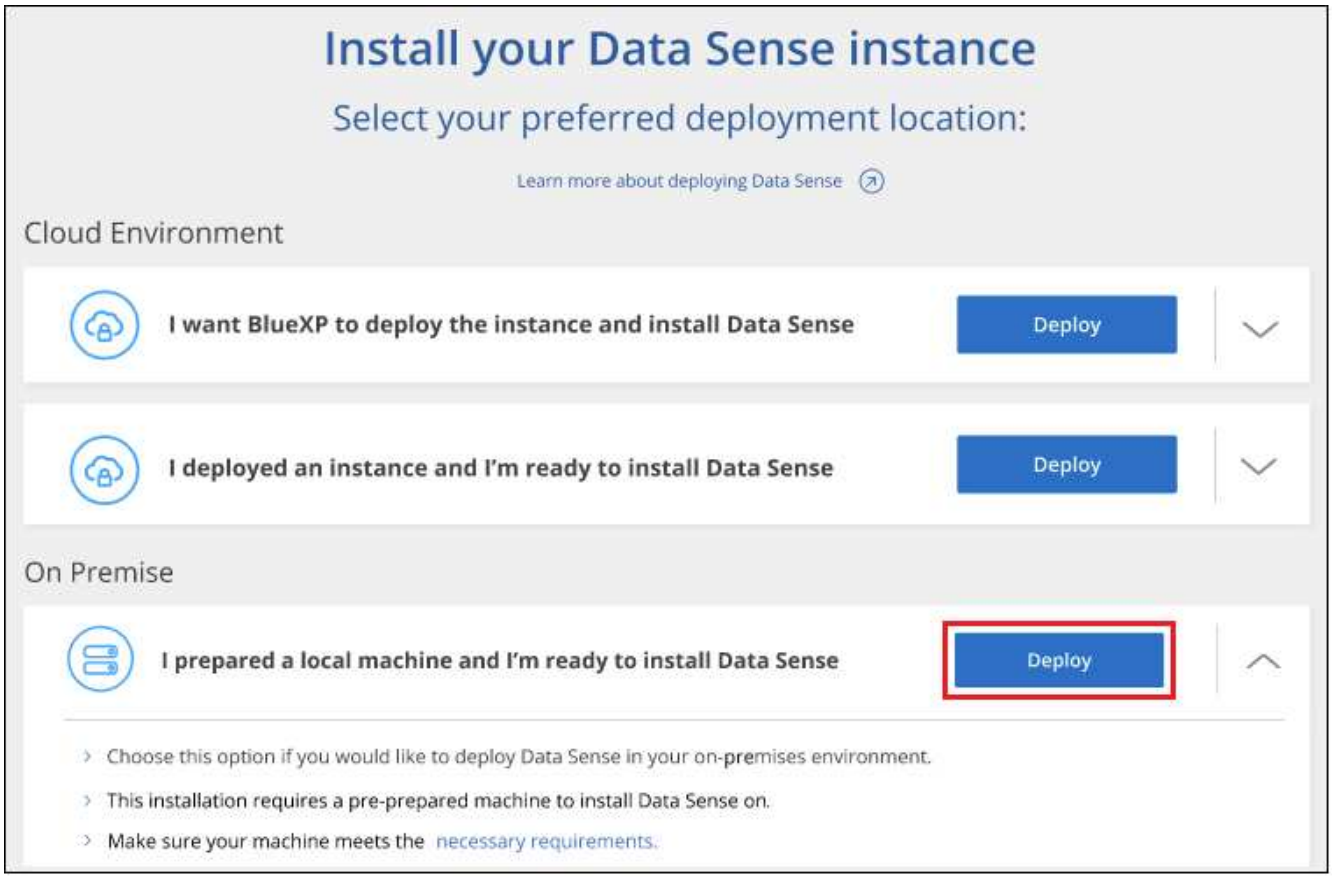
4. Entpacken Sie die Installationsdatei auf dem Host-Rechner, z. B.:

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

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



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



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

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

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

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

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

   Variablenwerte:

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

Ergebnis

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

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

Nächste Schritte

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

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

Installation mit mehreren Hosts für große Konfigurationen

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

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

Was Sie benötigen

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

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

Schritte

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

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

   Mit diesem Befehl werden beispielsweise 3 Scannerknoten hinzugefügt:
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no
   -proxy --darksite
   ```

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

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

Ergebnis

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

Nächste Schritte

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

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

Upgrade der BlueXP Klassifizierungssoftware

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

Bevor Sie beginnen

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

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

Schritte

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

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

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

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

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

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

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

```
start_darksite_upgrade.sh
```

Ergebnis

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

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

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

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

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

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

Erste Schritte

Sie führen die folgenden Aufgaben aus.

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

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

Einen Konnektor erstellen

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

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

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

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

Host-Anforderungen prüfen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ermöglichen Sie Outbound-Internetzugriff aus der BlueXP Klassifizierung

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

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

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

Vergewissern Sie sich, dass alle erforderlichen Ports aktiviert sind

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

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

Führen Sie das Skript für die Klassifizierungsvoraussetzungen von BlueXP aus

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

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

Was Sie benötigen

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

Schritte

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

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

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

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

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

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

Ergebnis

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

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

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

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

Aktivieren Sie das Scannen Ihrer Datenquellen

Erste Schritte mit der BlueXP Klassifizierung für Cloud Volumes ONTAP und lokale ONTAP

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

Schnellstart

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

1 Ermitteln Sie die Datenquellen, die Sie scannen möchten

Bevor Sie Volumes scannen können, müssen Sie die Systeme als Arbeitsumgebung in BlueXP hinzufügen:

- Bei Cloud Volumes ONTAP-Systemen sollten diese Arbeitsumgebungen bereits in BlueXP zur Verfügung stehen
- Für On-Premises-ONTAP-Systeme bietet die "BlueXP muss die ONTAP Cluster ermitteln"

2 Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

3 Aktivieren Sie die BlueXP Klassifizierung und wählen Sie die zu scannenden Volumes aus

Wählen Sie die Registerkarte **Configuration** und aktivieren Sie Compliance-Scans nach Volumes in bestimmten Arbeitsumgebungen.

4 Zugriff auf Volumes sicherstellen

Nachdem die BlueXP Klassifizierung aktiviert ist, vergewissern Sie sich jetzt, dass sie auf alle Volumes zugreifen kann.

- Die BlueXP Klassifizierungsinstanz benötigt eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz oder zu jedem lokalen ONTAP System.
- Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen von der BlueXP Klassifizierungsinstanz ermöglichen.
- Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind:
  - Für NFS - die Ports 111 und 2049.
  - Für CIFS - Ports 139 und 445.

- NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.
- Die BlueXP Klassifizierung erfordert Active Directory Zugangsdaten, um CIFS-Volumes zu scannen.

  Klicken Sie auf **Compliance** > **Konfiguration** > **CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an.

5 Verwalten Sie die Volumes, die Sie scannen möchten

Wählen Sie die Volumes aus, die Sie scannen möchten, oder deaktivieren Sie sie. Die BlueXP Klassifizierung startet bzw. stoppt die Suche.

Ermitteln der Datenquellen, die gescannt werden sollen

Wenn sich die zu scannenden Datenquellen nicht bereits in Ihrer BlueXP-Umgebung befinden, können Sie diese zu diesem Zeitpunkt zur Leinwand hinzufügen.

Ihre Cloud Volumes ONTAP-Systeme sollten bereits auf dem Canvas in BlueXP verfügbar sein. Bei ONTAP Systemen vor Ort ist ein muss erforderlich "BlueXP ermittelt diese Cluster".

Implementieren der BlueXP Klassifizierungsinstanz

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

Wenn Sie Cloud Volumes ONTAP und lokale ONTAP Systeme scannen, die über das Internet zugänglich sind, können Sie diese ausführen "Implementieren Sie die BlueXP Klassifizierung in der Cloud" Oder "In einer Anlage mit Internetzugang".

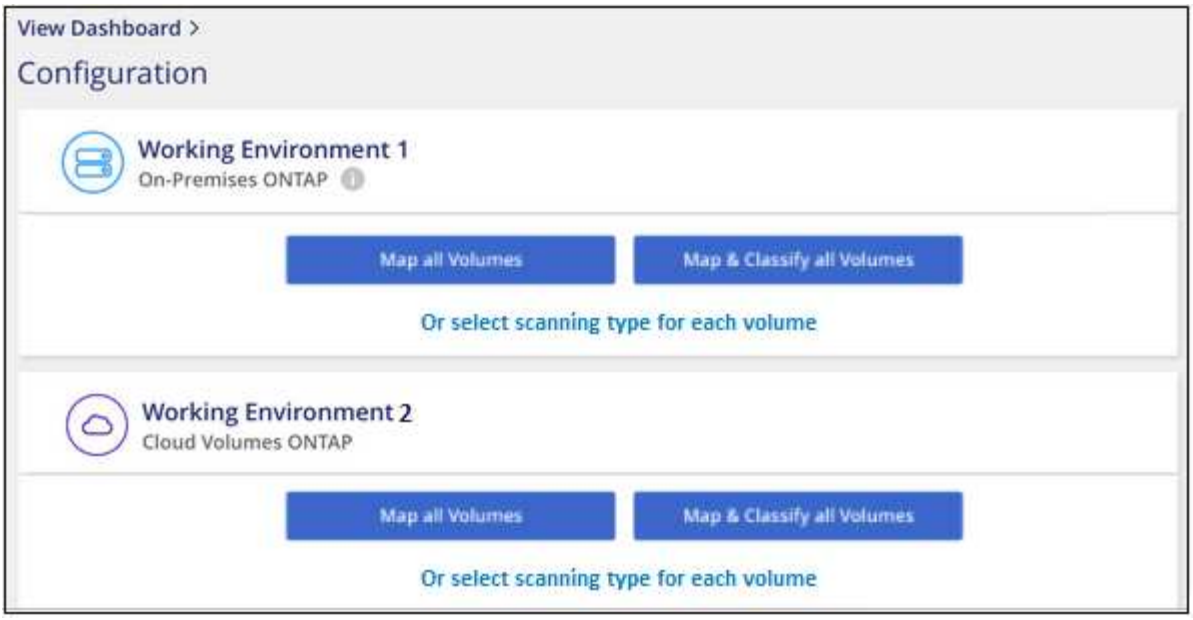
Wenn Sie lokale ONTAP-Systeme scannen, die in einer dunklen Site installiert wurden und über keinen Internetzugang verfügen, müssen Sie sie überprüfen "Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

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

Ermöglichen der BlueXP Klassifizierung in Ihren Arbeitsumgebungen

Sie können die BlueXP Klassifizierung auf Cloud Volumes ONTAP Systemen auf jedem unterstützten Cloud-Provider oder auf lokalen ONTAP Clustern aktivieren.

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.



2. Wählen Sie aus, wie die Volumes in den einzelnen Arbeitsumgebungen gescannt werden sollen. "Hier erfahren Sie mehr über Mapping und Klassifizierungsmessungen":
   - Um alle Volumes zuzuordnen, klicken Sie auf **Alle Volumes zuordnen**.
   - Um alle Bände zu ordnen und zu klassifizieren, klicken Sie auf **Karte & alle Bände klassifizieren**.
   - Um den Scan für jedes Volume anzupassen, klicken Sie auf **oder wählen Sie für jedes Volume** den Scantyp aus, und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

     Siehe Aktivieren und Deaktivieren von Compliance-Scans auf Volumes Entsprechende Details.
3. Klicken Sie im Bestätigungsdialogfeld auf **approve**, damit die BlueXP Klassifizierung mit dem Scannen Ihrer Volumes beginnt.

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen in der Arbeitsumgebung ausgewählten Volumes. Sobald die ersten Scans durch die BlueXP-Klassifizierung abgeschlossen sind, werden die Ergebnisse im Compliance-Dashboard verfügbar sein. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.

- Wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, scannt das System standardmäßig nicht die Dateien in Ihren Volumes, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, klicken Sie auf **oder wählen Sie den Scantyp für jedes Volume** aus. Die resultierende Seite verfügt über eine Einstellung, die Sie aktivieren können, sodass die BlueXP Klassifizierung die Volumes unabhängig von ihren Berechtigungen scannt.
- Die BlueXP Klassifizierung scannt nur eine Datei-Freigabe unter einem Volume. Wenn Sie mehrere Freigaben in Ihren Volumes haben, müssen Sie diese anderen Freigaben separat als Gruppe „Freigaben“ scannen. "Weitere Informationen zu dieser BlueXP Klassifizierungsbeschränkung".

Überprüfung, ob die BlueXP Klassifizierung Zugriff auf Volumes hat

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

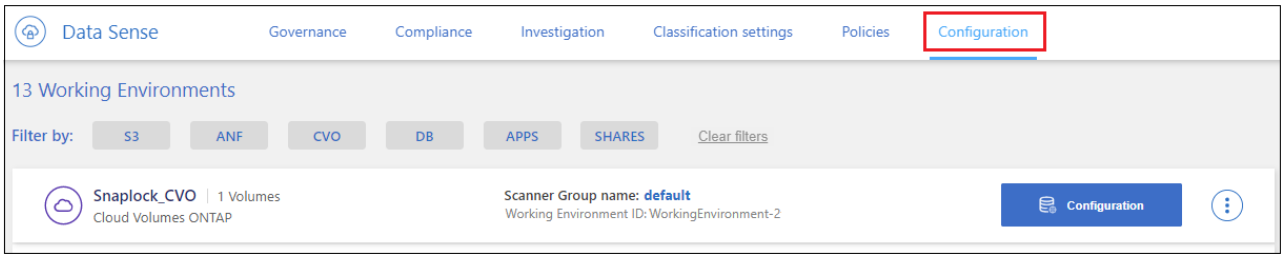
Schritte

1. Stellen Sie sicher, dass eine Netzwerkverbindung zwischen der BlueXP Klassifizierungsinstanz und jedem Netzwerk, das Volumes für Cloud Volumes ONTAP- oder lokale ONTAP-Cluster umfasst, besteht.
2. Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr von der BlueXP Klassifizierungsinstanz zulässt.

   Sie können die Sicherheitsgruppe für Datenverkehr von der IP-Adresse der BlueXP Klassifizierungsinstanz öffnen oder Sie können die Sicherheitsgruppe für den gesamten Datenverkehr innerhalb des virtuellen Netzwerks öffnen.

3. Stellen Sie sicher, dass die folgenden Ports für die BlueXP Klassifizierungsinstanz offen sind:
   - Für NFS - die Ports 111 und 2049.
   - Für CIFS - Ports 139 und 445.
4. Vergewissern Sie sich, dass die Richtlinien für den Export von NFS Volumes die IP-Adresse der BlueXP Klassifizierungsinstanz enthalten, damit sie auf die Daten auf jedem Volume zugreifen können.
5. Wenn Sie CIFS verwenden, bieten Sie BlueXP Klassifizierung mit Active Directory Anmeldeinformationen, um CIFS Volumes zu scannen.

   a. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.

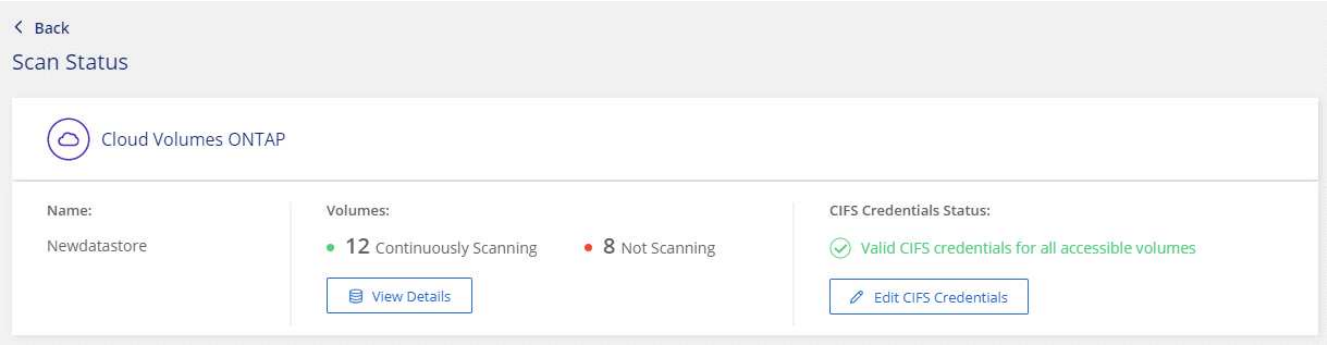
   

   b. Klicken Sie für jede Arbeitsumgebung auf **Edit CIFS Credentials** und geben Sie den Benutzernamen und das Passwort ein, die die BlueXP Klassifizierung für den Zugriff auf CIFS Volumes auf dem System benötigt.

   Die Zugangsdaten können schreibgeschützt sein, aber durch die Angabe von Administratorberechtigungen wird sichergestellt, dass die BlueXP Klassifizierung alle Daten lesen kann, die erhöhte Berechtigungen erfordern. Die Zugangsdaten werden in der BlueXP Klassifizierungsinstanz gespeichert.

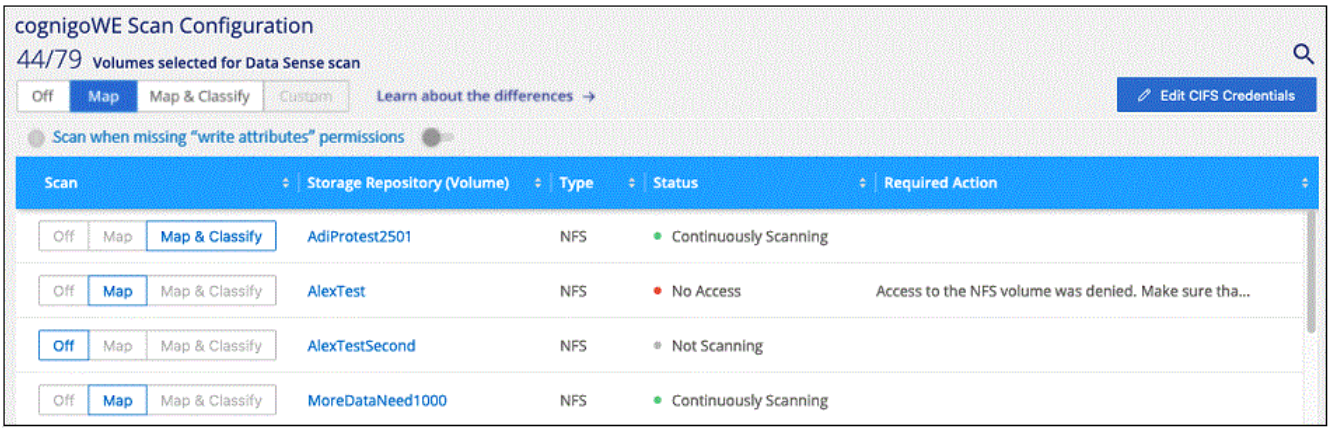
   Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

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



6. Klicken Sie auf der Seite *Configuration* auf **Details anzeigen**, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und eventuelle Fehler zu beheben.

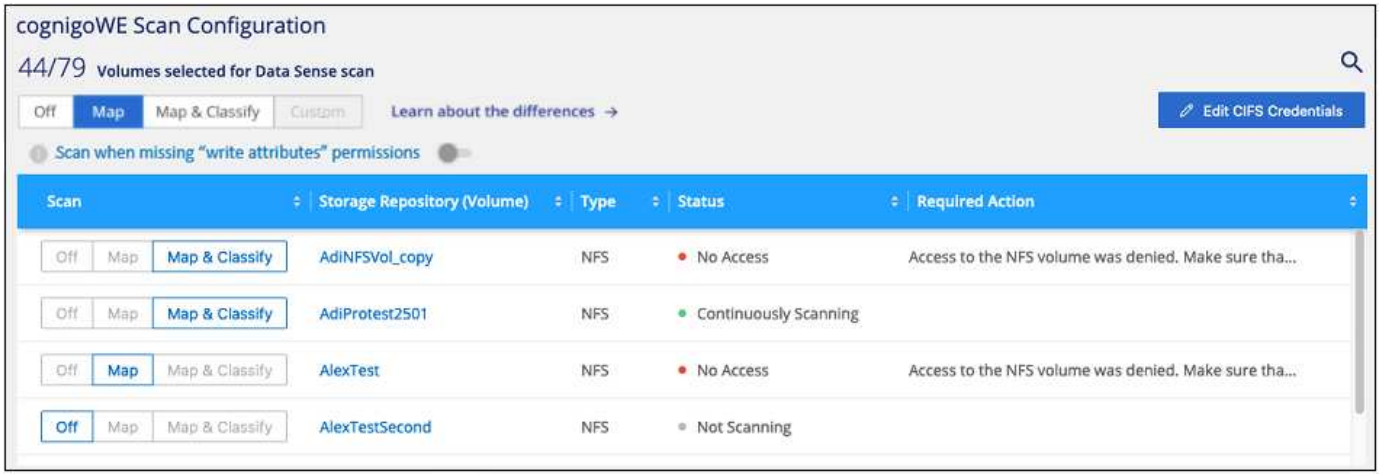
   Das folgende Bild zeigt beispielsweise vier Volumes. Eine davon kann aufgrund von Netzwerkverbindungsproblemen zwischen der BlueXP Klassifizierungsinstanz und dem Volume nicht mit der BlueXP Klassifizierung gescannt werden.



Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

Sie können jederzeit auf der Konfigurationsseite Scans oder Scans von nur-Zuordnungen oder Klassifizierungen in einer Arbeitsumgebung starten oder stoppen. Sie können auch von mappingonly Scans zu Mapping- und Klassifizierungsscans und umgekehrt wechseln. Wir empfehlen, alle Volumen zu scannen.

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Weitere Informationen .".



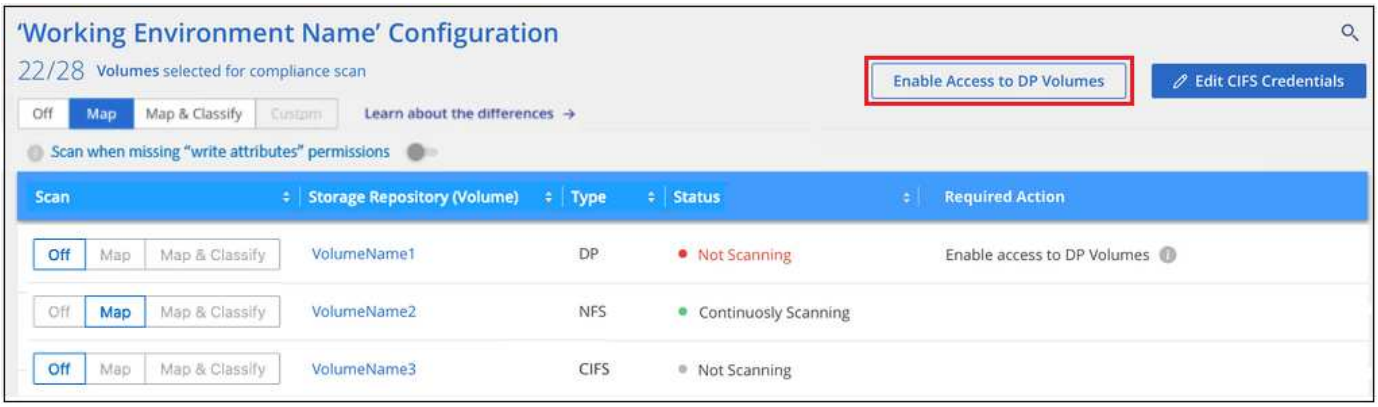
An:	Tun Sie dies:
Aktivieren von mappinggeschützten Scans auf einem Volume	Klicken Sie im Volumenbereich auf **Karte**
Aktivieren Sie das vollständige Scannen auf einem Volume	Klicken Sie im Volumenbereich auf **Karte & Klassieren**
Deaktivieren Sie das Scannen auf einem Volume	Klicken Sie im Volumenbereich auf **aus**
Aktivieren Sie ausschließlich mappingbare Scans auf allen Volumes	Klicken Sie im Steuerkursbereich auf **Karte**
Aktivieren Sie das vollständige Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf **Karte & Klassieren**
Deaktivieren Sie das Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf **aus**

Neue Volumen, die der Arbeitsumgebung hinzugefügt wurden, werden automatisch nur gescannt, wenn Sie die Einstellung **Karte** oder **Karte & Klassieren** im Steuerkursbereich festgelegt haben. Wenn Sie im Bereich Überschrift auf **Benutzerdefiniert** oder **aus** eingestellt sind, müssen Sie für jedes neue Volumen, das Sie in der Arbeitsumgebung hinzufügen, das Mapping und/oder das vollständige Scannen aktivieren.

Scannen von Datensicherungs-Volumes

Datensicherung-Volumes werden standardmäßig nicht gescannt, da sie nicht extern offengelegt werden und die BlueXP Klassifizierung kann nicht auf sie zugreifen. Es handelt sich dabei um Ziel-Volumes für SnapMirror Vorgänge von einem ONTAP System vor Ort oder von einem Cloud Volumes ONTAP System aus.

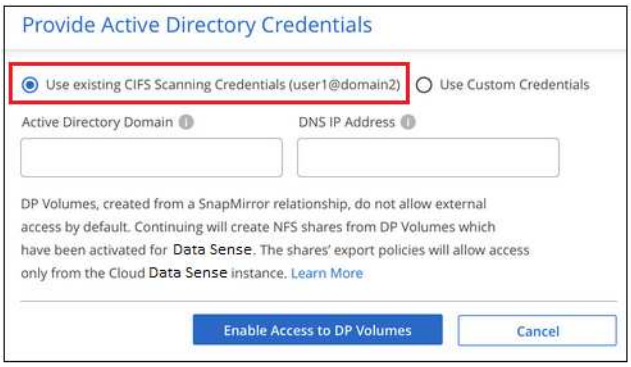
Zunächst erkennt die Volume-Liste diese Volumes als *Type* **DP** mit dem *Status* **Not Scanning** und der *required Action* **Enable Access to DP Volumes**.

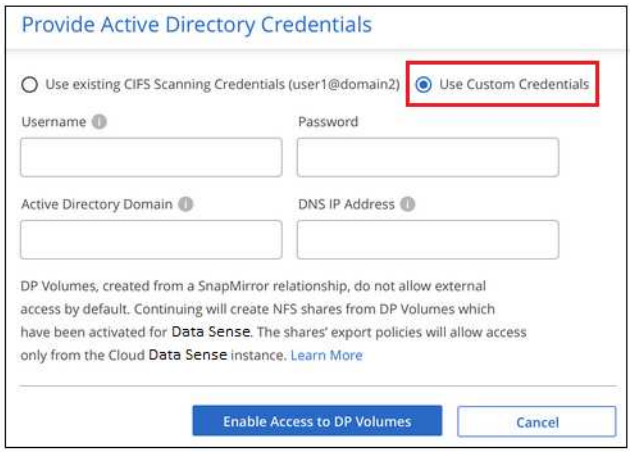


Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

1. Klicken Sie oben auf der Seite auf **Zugriff auf DP-Volumes aktivieren**.
2. Überprüfen Sie die Bestätigungsmeldung und klicken Sie erneut auf **Zugriff auf DP-Volumes**.
   - Volumes, die anfangs als NFS Volumes im ONTAP Quellsystem erstellt wurden, sind aktiviert.
   - Für Volumes, die ursprünglich als CIFS Volumes im Quell-ONTAP System erstellt wurden, müssen Sie die CIFS-Anmeldeinformationen eingeben, um diese DP-Volumes zu scannen. Wenn Sie bereits Active Directory-Anmeldedaten eingegeben haben, sodass die BlueXP Klassifizierung CIFS-Volumes scannen kann, können Sie diese Anmeldedaten verwenden oder einen anderen Satz von Admin-Anmeldedaten angeben.





3. Aktivieren Sie jedes zu scannenden DP-Volume Auf die gleiche Weise haben Sie andere Volumes aktiviert.

Ergebnis

Nach Aktivierung erstellt die BlueXP Klassifizierung von jedem DP-Volume, das zum Scannen aktiviert wurde, eine NFS-Freigabe. Die Richtlinien für den Export von Freigaben sind nur für den Zugriff aus der BlueXP Klassifizierungsinstanz zulässig.

Hinweis: Wenn Sie beim ersten Aktivieren des Zugriffs auf DP-Volumes keine CIFS-Datenschutzvolumes hatten und später noch etwas hinzufügen, erscheint oben auf der Konfigurationsseite die Schaltfläche **Zugriff auf CIFS DP aktivieren**. Klicken Sie auf diese Schaltfläche, und fügen Sie CIFS-Anmeldeinformationen hinzu, um den Zugriff auf diese CIFS-DP-Volumes zu ermöglichen.

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

Erste Schritte mit der BlueXP Klassifizierung für Azure NetApp Files

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

Schnellstart

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

1 Entdecken Sie die Azure NetApp Files-Systeme, die Sie scannen möchten

Vor dem Scannen von Azure NetApp Files-Volumes "BlueXP muss eingerichtet sein, um die Konfiguration zu ermitteln".

2 Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung in BlueXP" Falls noch keine Instanz implementiert wurde.

3 Aktivieren Sie die BlueXP Klassifizierung und wählen Sie die zu scannenden Volumes aus

Klicken Sie auf **Compliance**, wählen Sie die Registerkarte **Konfiguration** und aktivieren Sie Compliance-Scans für Volumes in bestimmten Arbeitsumgebungen.

4 Zugriff auf Volumes sicherstellen

Nachdem die BlueXP Klassifizierung aktiviert ist, vergewissern Sie sich jetzt, dass sie auf alle Volumes zugreifen kann.

- Die BlueXP Klassifizierungsinstanz benötigt eine Netzwerkverbindung zu jedem Azure NetApp Files Subnetz.
- Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind:
  - Für NFS – die Ports 111 und 2049.
  - Für CIFS – die Ports 139 und 445.
- NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.
- Die BlueXP Klassifizierung erfordert Active Directory Zugangsdaten, um CIFS-Volumes zu scannen.

  Klicken Sie auf **Compliance** > **Konfiguration** > **CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an.

5 Verwalten Sie die Volumes, die Sie scannen möchten

Wählen Sie die Volumes aus, die Sie scannen möchten, oder deaktivieren Sie sie. Die BlueXP Klassifizierung startet bzw. stoppt die Suche.

Ermitteln des Azure NetApp Files-Systems, das Sie scannen möchten

Wenn sich das zu scannenden Azure NetApp Files-System nicht bereits in BlueXP als Arbeitsumgebung befindet, können Sie es zu diesem Zeitpunkt der Arbeitsfläche hinzufügen.

"Erfahren Sie, wie Sie das Azure NetApp Files-System in BlueXP entdecken".

Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

Die BlueXP Klassifizierung muss bei der Überprüfung von Azure NetApp Files Volumes in der Cloud bereitgestellt werden und muss in derselben Region wie die Volumes bereitgestellt werden, die Sie scannen möchten.

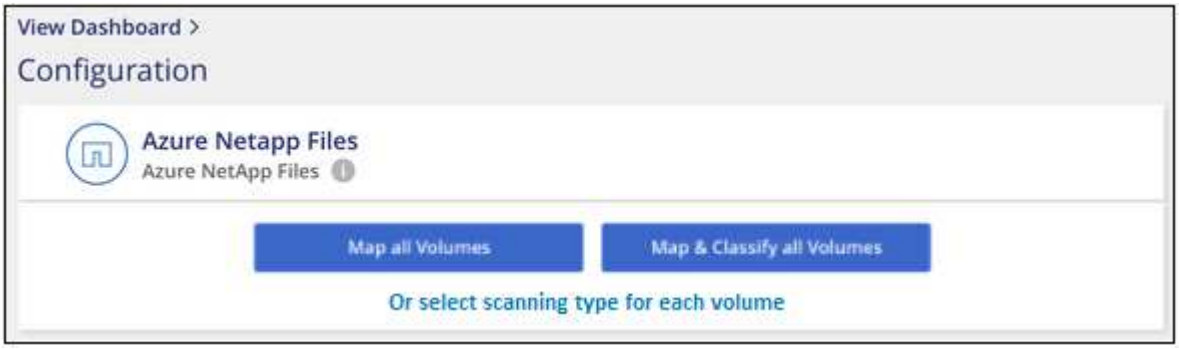
Hinweis: die Implementierung der BlueXP Klassifizierung an einem lokalen Standort wird derzeit beim Scannen von Azure NetApp Files Volumes nicht unterstützt.

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

Ermöglichen der BlueXP Klassifizierung in Ihren Arbeitsumgebungen

Die BlueXP Klassifizierung für Ihre Azure NetApp Files Volumes kann aktiviert werden.

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.



2. Wählen Sie aus, wie die Volumes in den einzelnen Arbeitsumgebungen gescannt werden sollen. "Hier erfahren Sie mehr über Mapping und Klassifizierungsmessungen":
   - Um alle Volumes zuzuordnen, klicken Sie auf **Alle Volumes zuordnen**.
   - Um alle Bände zu ordnen und zu klassifizieren, klicken Sie auf **Karte & alle Bände klassifizieren**.
   - Um den Scan für jedes Volume anzupassen, klicken Sie auf **oder wählen Sie für jedes Volume** den Scantyp aus, und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

     Siehe Aktivieren und Deaktivieren von Compliance-Scans auf Volumes Entsprechende Details.

3. Klicken Sie im Bestätigungsdialogfeld auf **approve**, damit die BlueXP Klassifizierung mit dem Scannen Ihrer Volumes beginnt.

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen in der Arbeitsumgebung ausgewählten Volumes. Sobald die ersten Scans durch die BlueXP-Klassifizierung abgeschlossen sind, werden die Ergebnisse im Compliance-Dashboard verfügbar sein. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.

- Wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, scannt das System standardmäßig nicht die Dateien in Ihren Volumes, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, klicken Sie auf **oder wählen Sie den Scantyp für jedes Volume** aus. Die resultierende Seite verfügt über eine Einstellung, die Sie aktivieren können, sodass die BlueXP Klassifizierung die Volumes unabhängig von ihren Berechtigungen scannt.
- Die BlueXP Klassifizierung scannt nur eine Datei-Freigabe unter einem Volume. Wenn Sie mehrere Freigaben in Ihren Volumes haben, müssen Sie diese anderen Freigaben separat als Gruppe „Freigaben“ scannen. "Weitere Informationen zu dieser BlueXP Klassifizierungsbeschränkung".

Überprüfung, ob die BlueXP Klassifizierung Zugriff auf Volumes hat

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

Schritte

1. Stellen Sie sicher, dass eine Netzwerkverbindung zwischen der BlueXP Klassifizierungsinstanz und jedem Netzwerk, das Volumes für Azure NetApp Files umfasst, besteht.

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

2. Stellen Sie sicher, dass die folgenden Ports für die BlueXP Klassifizierungsinstanz offen sind:
   - Für NFS – die Ports 111 und 2049.
   - Für CIFS – die Ports 139 und 445.
3. Vergewissern Sie sich, dass die Richtlinien für den Export von NFS Volumes die IP-Adresse der BlueXP Klassifizierungsinstanz enthalten, damit sie auf die Daten auf jedem Volume zugreifen können.
4. Wenn Sie CIFS verwenden, bieten Sie BlueXP Klassifizierung mit Active Directory Anmeldeinformationen, um CIFS Volumes zu scannen.

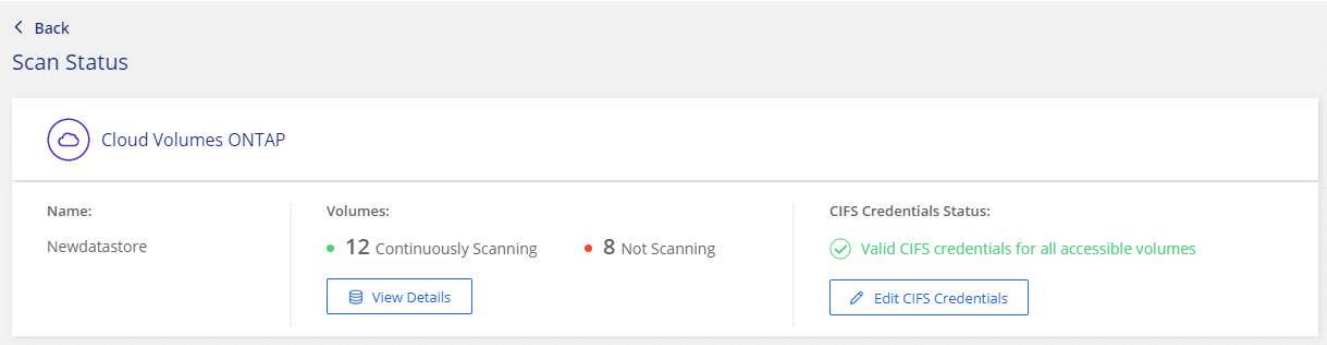
   a. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.

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

   Die Zugangsdaten können schreibgeschützt sein, aber durch die Angabe von Administratorberechtigungen wird sichergestellt, dass die BlueXP Klassifizierung alle Daten lesen kann, die erhöhte Berechtigungen erfordern. Die Zugangsdaten werden in der BlueXP Klassifizierungsinstanz gespeichert.

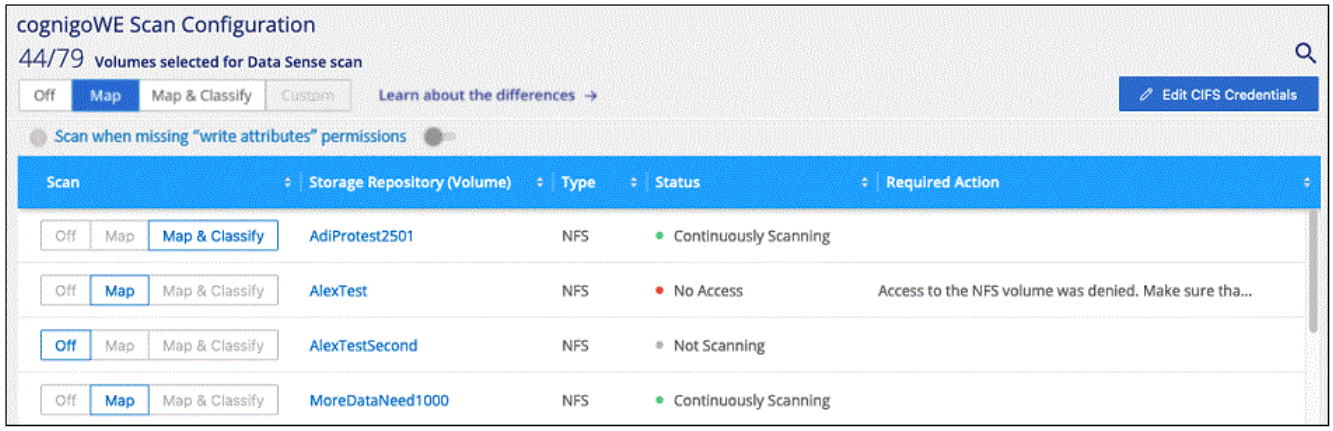
   Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

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



5. Klicken Sie auf der Seite *Configuration* auf **Details anzeigen**, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und eventuelle Fehler zu beheben.

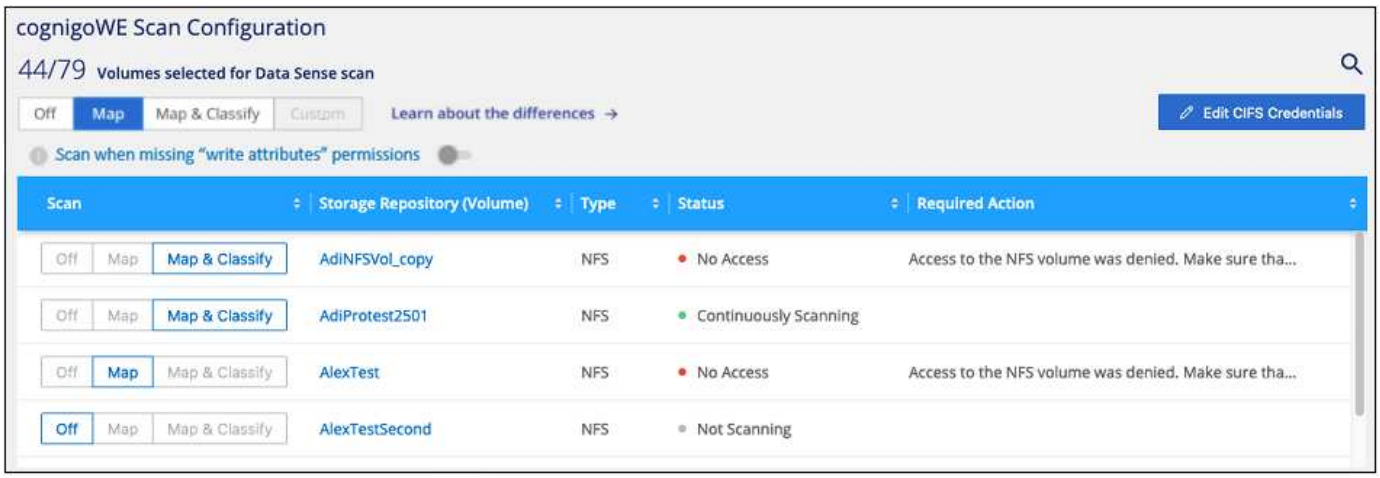
   Das folgende Bild zeigt beispielsweise vier Volumes. Eine davon kann aufgrund von Netzwerkverbindungsproblemen zwischen der BlueXP Klassifizierungsinstanz und dem Volume nicht mit der BlueXP Klassifizierung gescannt werden.



Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

Sie können jederzeit auf der Konfigurationsseite Scans oder Scans von nur-Zuordnungen oder Klassifizierungen in einer Arbeitsumgebung starten oder stoppen. Sie können auch von mappingonly Scans zu Mapping- und Klassifizierungsscans und umgekehrt wechseln. Wir empfehlen, alle Volumen zu scannen.

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung die „letzte Zugriffszeit" nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Weitere Informationen .".



An:	Tun Sie dies:
Aktivieren von mappinggeschützten Scans auf einem Volume	Klicken Sie im Volumenbereich auf **Karte**
Aktivieren Sie das vollständige Scannen auf einem Volume	Klicken Sie im Volumenbereich auf **Karte & Klassieren**
Deaktivieren Sie das Scannen auf einem Volume	Klicken Sie im Volumenbereich auf **aus**
Aktivieren Sie ausschließlich mappingbare Scans auf allen Volumes	Klicken Sie im Steuerkursbereich auf **Karte**

An:	Tun Sie dies:
Aktivieren Sie das vollständige Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf **Karte & Klassieren**
Deaktivieren Sie das Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf **aus**

> Neue Volumen, die der Arbeitsumgebung hinzugefügt wurden, werden automatisch nur gescannt, wenn Sie die Einstellung **Karte** oder **Karte & Klassieren** im Steuerkursbereich festgelegt haben. Wenn Sie im Bereich Überschrift auf **Benutzerdefiniert** oder **aus** eingestellt sind, müssen Sie für jedes neue Volumen, das Sie in der Arbeitsumgebung hinzufügen, das Mapping und/oder das vollständige Scannen aktivieren.

Erste Schritte mit der BlueXP Klassifizierung für Amazon FSX for ONTAP

Führen Sie ein paar Schritte durch, um zu beginnen, Amazon FSX für ONTAP Volumes mit BlueXP Klassifizierung zu scannen.

Bevor Sie beginnen

- Sie benötigen einen aktiven Connector in AWS für die Implementierung und das Management der BlueXP Klassifizierung.
- Die beim Erstellen der Arbeitsumgebung ausgewählte Sicherheitsgruppe muss Datenverkehr von der BlueXP Klassifizierungsinstanz zulassen. Sie können die zugehörige Sicherheitsgruppe mithilfe der ENI finden, die mit dem FSX für ONTAP-Dateisystem verbunden ist, und es mit der AWS-Verwaltungskonsole bearbeiten.

  "AWS Sicherheitsgruppen für Linux Instanzen"

  "AWS Sicherheitsgruppen für Windows Instanzen"

  "Elastische AWS Netzwerkschnittstellen (ENI)"

Schnellstart

Führen Sie die folgenden Schritte aus, oder scrollen Sie nach unten, um weitere Informationen zu erhalten.

1 Entdecken Sie die FSX für ONTAP-Dateisysteme, die Sie scannen möchten

Bevor Sie FSX für ONTAP Volumes scannen können, "Sie benötigen eine FSX-Arbeitsumgebung mit konfigurierten Volumes".

2 Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung in BlueXP" Falls noch keine Instanz implementiert wurde.

3 Aktivieren Sie die BlueXP Klassifizierung und wählen Sie die zu scannenden Volumes aus

Wählen Sie die Registerkarte **Configuration** und aktivieren Sie Compliance-Scans nach Volumes in bestimmten Arbeitsumgebungen.

4 Zugriff auf Volumes sicherstellen

Nachdem die BlueXP Klassifizierung aktiviert ist, vergewissern Sie sich jetzt, dass sie auf alle Volumes zugreifen kann.

- Die BlueXP Klassifizierungsinstanz benötigt eine Netzwerkverbindung zu jedem FSX for ONTAP Subnetz.
- Stellen Sie sicher, dass die folgenden Ports für die BlueXP Klassifizierungsinstanz offen sind:
  - Für NFS – die Ports 111 und 2049.
  - Für CIFS – die Ports 139 und 445.
- NFS-Volume-Exportrichtlinien müssen den Zugriff von der BlueXP Klassifizierungsinstanz ermöglichen.
- Die BlueXP Klassifizierung erfordert Active Directory Zugangsdaten, um CIFS-Volumes zu scannen. + Klicken Sie auf **Compliance** > **Konfiguration** > **CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an.

5 Verwalten Sie die Volumes, die Sie scannen möchten

Wählen Sie die Volumes aus, die Sie scannen möchten, oder deaktivieren Sie sie. Die BlueXP Klassifizierung startet bzw. stoppt ihre Suche.

Erkennung des FSX für ONTAP-Dateisystems, das Sie scannen möchten

Wenn das Dateisystem FSX für ONTAP, das Sie scannen möchten, nicht bereits in BlueXP als Arbeitsumgebung vorhanden ist, können Sie es zu diesem Zeitpunkt der Arbeitsfläche hinzufügen.

"Lesen Sie, wie Sie das Dateisystem FSX für ONTAP in BlueXP erkennen oder erstellen".

Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

Sie sollten die BlueXP Klassifizierung im selben AWS-Netzwerk implementieren wie der Connector für AWS und die FSX Volumes, die Sie scannen möchten.

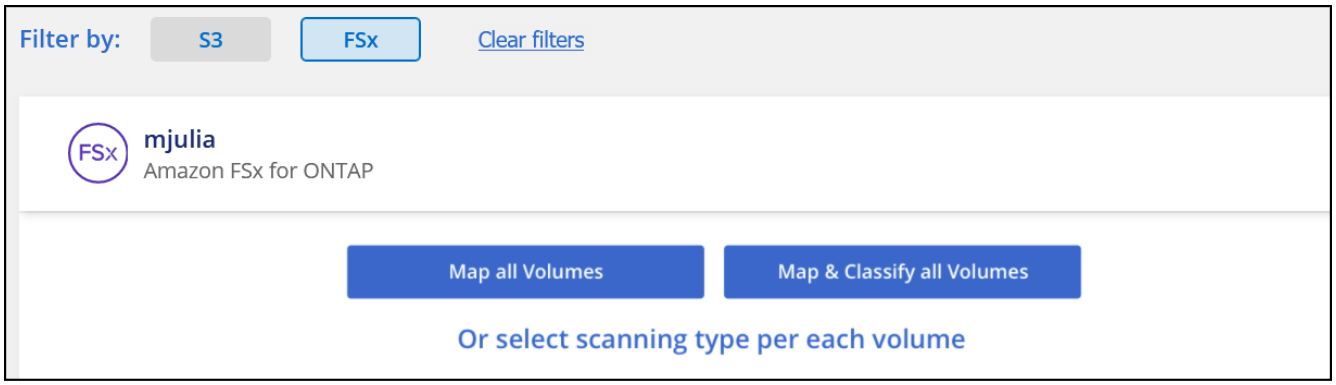
Hinweis: die Implementierung der BlueXP Klassifizierung an einem lokalen Standort wird derzeit beim Scannen von FSX Volumes nicht unterstützt.

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

Ermöglichen der BlueXP Klassifizierung in Ihren Arbeitsumgebungen

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

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.



2. Wählen Sie aus, wie die Volumes in den einzelnen Arbeitsumgebungen gescannt werden sollen. "Hier erfahren Sie mehr über Mapping und Klassifizierungsmessungen":
   - Um alle Volumes zuzuordnen, klicken Sie auf **Alle Volumes zuordnen**.
   - Um alle Bände zu ordnen und zu klassifizieren, klicken Sie auf **Karte & alle Bände klassifizieren**.
   - Um den Scan für jedes Volume anzupassen, klicken Sie auf **oder wählen Sie für jedes Volume** den Scantyp aus, und wählen Sie dann die Volumes aus, die Sie zuordnen und/oder klassifizieren möchten.

     Siehe Aktivieren und Deaktivieren von Compliance-Scans auf Volumes Entsprechende Details.
3. Klicken Sie im Bestätigungsdialogfeld auf **approve**, damit die BlueXP Klassifizierung mit dem Scannen Ihrer Volumes beginnt.

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen in der Arbeitsumgebung ausgewählten Volumes. Sobald die ersten Scans durch die BlueXP-Klassifizierung abgeschlossen sind, werden die Ergebnisse im Compliance-Dashboard verfügbar sein. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.

- Wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, scannt das System standardmäßig nicht die Dateien in Ihren Volumes, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, klicken Sie auf **oder wählen Sie den Scantyp für jedes Volume** aus. Die resultierende Seite verfügt über eine Einstellung, die Sie aktivieren können, sodass die BlueXP Klassifizierung die Volumes unabhängig von ihren Berechtigungen scannt.
- Die BlueXP Klassifizierung scannt nur eine Datei-Freigabe unter einem Volume. Wenn Sie mehrere Freigaben in Ihren Volumes haben, müssen Sie diese anderen Freigaben separat als Gruppe „Freigaben“ scannen. "Weitere Informationen zu dieser BlueXP Klassifizierungsbeschränkung".

Überprüfung, ob die BlueXP Klassifizierung Zugriff auf Volumes hat

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

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

Schritte

1. Klicken Sie auf der Seite *Configuration* auf **Details anzeigen**, um den Status zu überprüfen und Fehler zu

beheben.

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

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	No Access	Check network connectivity between the Data Sense ...

2. Stellen Sie sicher, dass zwischen der BlueXP Klassifizierungsinstanz und jedem Netzwerk, das Volumes für FSX für ONTAP umfasst, eine Netzwerkverbindung besteht.

   Bei FSX for ONTAP kann die BlueXP Klassifizierung Volumes nur in derselben Region wie BlueXP scannen.

3. Stellen Sie sicher, dass die folgenden Ports für die BlueXP Klassifizierungsinstanz offen sind.
   - Für NFS – die Ports 111 und 2049.
   - Für CIFS – die Ports 139 und 445.
4. Vergewissern Sie sich, dass die Richtlinien für den Export von NFS Volumes die IP-Adresse der BlueXP Klassifizierungsinstanz enthalten, damit sie auf die Daten auf jedem Volume zugreifen können.
5. Wenn Sie CIFS verwenden, bieten Sie BlueXP Klassifizierung mit Active Directory Anmeldeinformationen, um CIFS Volumes zu scannen.

   a. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Konfiguration**.

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

      Die Zugangsdaten können schreibgeschützt sein, aber durch die Angabe von Administratorberechtigungen wird sichergestellt, dass die BlueXP Klassifizierung alle Daten lesen kann, die erhöhte Berechtigungen erfordern. Die Zugangsdaten werden in der BlueXP Klassifizierungsinstanz gespeichert.

      Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

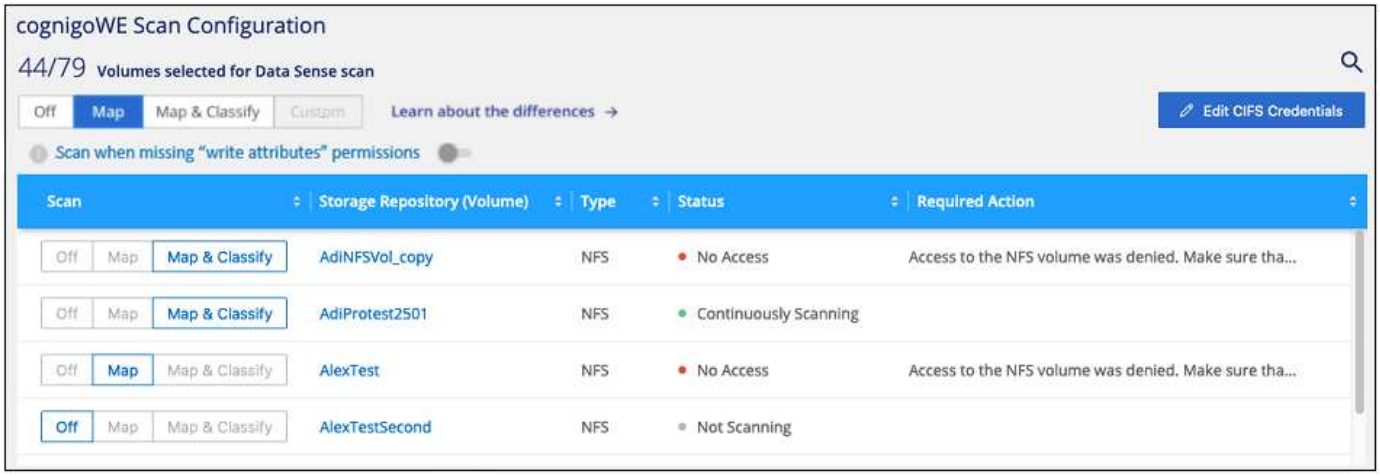
   Nach Eingabe der Anmeldedaten sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.

Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

Sie können jederzeit auf der Konfigurationsseite Scans oder Scans von nur-Zuordnungen oder Klassifizierungen in einer Arbeitsumgebung starten oder stoppen. Sie können auch von mappingonly Scans zu Mapping- und Klassifizierungsscans und umgekehrt wechseln. Wir empfehlen, alle Volumen zu scannen.

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-

Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Weitere Informationen .".



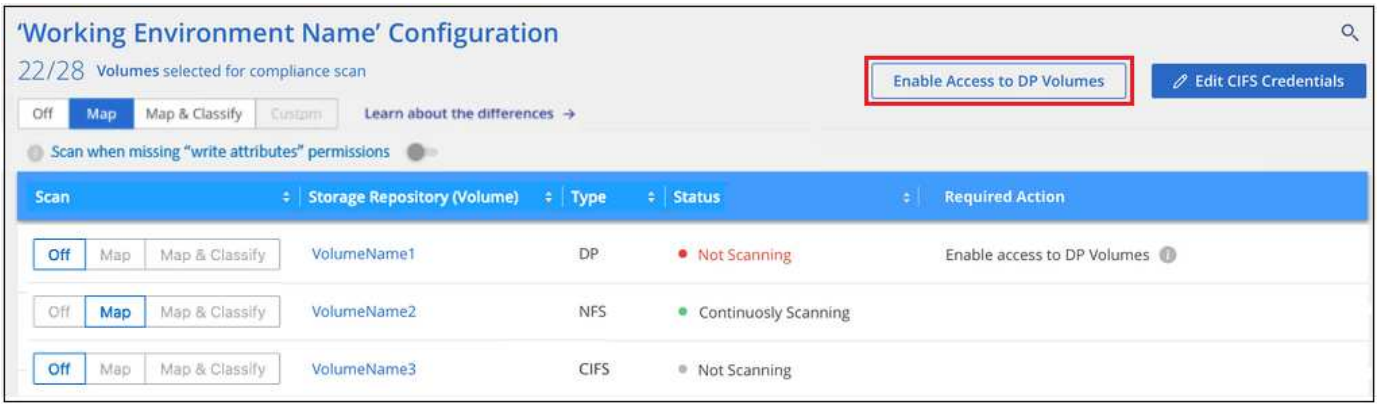
An:	Tun Sie dies:
Aktivieren von mappinggeschützten Scans auf einem Volume	Klicken Sie im Volumenbereich auf **Karte**
Aktivieren Sie das vollständige Scannen auf einem Volume	Klicken Sie im Volumenbereich auf **Karte & Klassieren**
Deaktivieren Sie das Scannen auf einem Volume	Klicken Sie im Volumenbereich auf **aus**
Aktivieren Sie ausschließlich mappingbare Scans auf allen Volumes	Klicken Sie im Steuerkursbereich auf **Karte**
Aktivieren Sie das vollständige Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf **Karte & Klassieren**
Deaktivieren Sie das Scannen auf allen Volumes	Klicken Sie im Bereich Überschrift auf **aus**

Neue Volumen, die der Arbeitsumgebung hinzugefügt wurden, werden automatisch nur gescannt, wenn Sie die Einstellung **Karte** oder **Karte & Klassieren** im Steuerkursbereich festgelegt haben. Wenn Sie im Bereich Überschrift auf **Benutzerdefiniert** oder **aus** eingestellt sind, müssen Sie für jedes neue Volumen, das Sie in der Arbeitsumgebung hinzufügen, das Mapping und/oder das vollständige Scannen aktivieren.

Scannen von Datensicherungs-Volumes

Datensicherung-Volumes werden standardmäßig nicht gescannt, da sie nicht extern offengelegt werden und die BlueXP Klassifizierung kann nicht auf sie zugreifen. Dies sind die Ziel-Volumes für SnapMirror Vorgänge von einem FSX für ONTAP Filesystem.

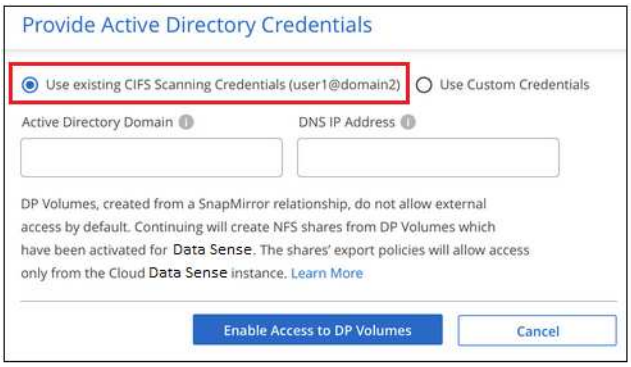
Zunächst erkennt die Volume-Liste diese Volumes als *Type* **DP** mit dem *Status* **Not Scanning** und der *required Action* **Enable Access to DP Volumes**.

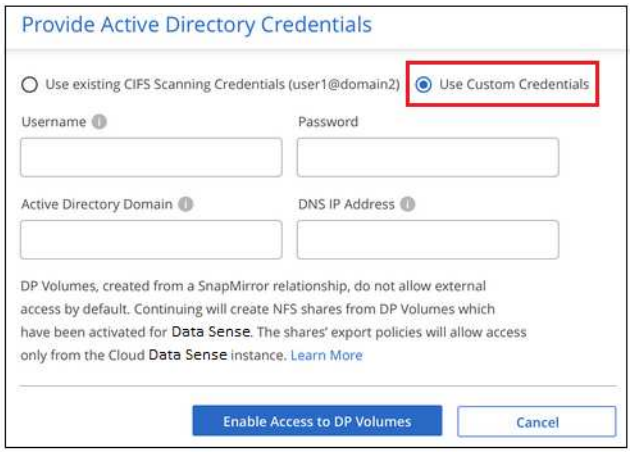


Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

1. Klicken Sie oben auf der Seite auf **Zugriff auf DP-Volumes aktivieren**.
2. Überprüfen Sie die Bestätigungsmeldung und klicken Sie erneut auf **Zugriff auf DP-Volumes**.
   - Volumes, die ursprünglich als NFS-Volumes im Quell-FSX für ONTAP erstellt wurden, sind aktiviert.
   - Für Volumes, die ursprünglich als CIFS Volumes im Quell-FSX für ONTAP erstellt wurden, müssen Sie CIFS-Anmeldeinformationen eingeben, um diese DP-Volumes zu scannen. Wenn Sie bereits Active Directory-Anmeldedaten eingegeben haben, sodass die BlueXP Klassifizierung CIFS-Volumes scannen kann, können Sie diese Anmeldedaten verwenden oder einen anderen Satz von Admin-Anmeldedaten angeben.





3. Aktivieren Sie jedes zu scannenden DP-Volume Auf die gleiche Weise haben Sie andere Volumes aktiviert.

Ergebnis

Nach Aktivierung erstellt die BlueXP Klassifizierung von jedem DP-Volume, das zum Scannen aktiviert wurde, eine NFS-Freigabe. Die Richtlinien für den Export von Freigaben sind nur für den Zugriff aus der BlueXP Klassifizierungsinstanz zulässig.

Hinweis: Wenn Sie beim ersten Aktivieren des Zugriffs auf DP-Volumes keine CIFS-Datenschutzvolumes hatten und später noch etwas hinzufügen, erscheint oben auf der Konfigurationsseite die Schaltfläche **Zugriff auf CIFS DP aktivieren**. Klicken Sie auf diese Schaltfläche, und fügen Sie CIFS-Anmeldeinformationen hinzu, um den Zugriff auf diese CIFS-DP-Volumes zu ermöglichen.

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

Erste Schritte mit der BlueXP Klassifizierung für Amazon S3

Die BlueXP Klassifizierung kann Ihre Amazon S3 Buckets scannen, um die persönlichen und sensiblen Daten im S3 Objekt-Storage zu identifizieren. Die BlueXP Klassifizierung kann beliebige Buckets im Konto scannen, unabhängig davon, ob sie für eine NetApp Lösung erstellt wurden.

Schnellstart

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

1. **S3-Anforderungen in Ihrer Cloud-Umgebung einrichten**

Stellen Sie sicher, dass Ihre Cloud-Umgebung die Anforderungen für die BlueXP Klassifizierung erfüllen kann. Bereiten Sie dazu eine IAM-Rolle vor und richten Sie die Konnektivität von der BlueXP Klassifizierung zu S3 ein. Eine vollständige Liste finden Sie hier.

2. **Implementieren der BlueXP Klassifizierungsinstanz**

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

3. **BlueXP-Klassifizierung in Ihrer S3-Arbeitsumgebung aktivieren**

Wählen Sie die Amazon S3-Arbeitsumgebung aus, klicken Sie auf **Aktivieren** und wählen Sie eine IAM-Rolle aus, die die erforderlichen Berechtigungen enthält.

4. **Wählen Sie die zu scannenden Buckets aus**

Wählen Sie die Buckets aus, die Sie scannen möchten. Die BlueXP Klassifizierung beginnt mit dem Scannen.

Überprüfen der S3-Voraussetzungen

Die folgenden Anforderungen gelten insbesondere für das Scannen von S3-Buckets.

Richten Sie eine IAM-Rolle für die BlueXP Klassifizierungsinstanz ein

Die BlueXP Klassifizierung erfordert Berechtigungen, um eine Verbindung zu den S3 Buckets in Ihrem Konto herzustellen und sie zu scannen. Richten Sie eine IAM-Rolle ein, die die unten aufgeführten Berechtigungen enthält. BlueXP fordert Sie zur Auswahl einer IAM-Rolle auf, wenn Sie die BlueXP-Klassifizierung in der Amazon S3 Arbeitsumgebung aktivieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:GetPolicyVersion",
              "iam:GetPolicy",
              "iam:ListAttachedRolePolicies"
          ],
          "Resource": [
              "arn:aws:iam::*:policy/*",
              "arn:aws:iam::*:role/*"
          ]
      }
  ]
}
```

Konnektivität von der BlueXP Klassifizierung bis zu Amazon S3

Die Klassifizierung von BlueXP erfordert eine Verbindung zu Amazon S3. Die beste Möglichkeit, eine solche Verbindung bereitzustellen, ist über einen VPC Endpunkt zum S3-Service. Anweisungen hierzu finden Sie unter "AWS Dokumentation: Erstellen eines Gateway-Endpunkts".

Wenn Sie den VPC-Endpunkt erstellen, müssen Sie die Region, die VPC und die Routetabelle auswählen, die der BlueXP Klassifizierungsinstanz entsprechen. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann die BlueXP Klassifizierung keine Verbindung zum S3-Service herstellen.

Informationen zu Problemen finden Sie unter "AWS Support Knowledge Center: Warum kann ich keine Verbindung zu einem S3-Bucket über einen Gateway-VPC-Endpunkt herstellen?"

Eine Alternative besteht darin, die Verbindung über ein NAT Gateway bereitzustellen.

> Sie können keinen Proxy verwenden, um über das Internet nach S3 zu gelangen.

Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung in BlueXP" Falls noch keine Instanz implementiert wurde.

Sie müssen die Instanz mithilfe eines in AWS bereitgestellten Connectors implementieren, damit BlueXP die S3-Buckets in diesem AWS-Konto automatisch erkennt und diese in einer Amazon S3-Arbeitsumgebung anzeigt.

Hinweis: die Implementierung der BlueXP Klassifizierung an einem lokalen Speicherort wird derzeit beim Scannen von S3-Buckets nicht unterstützt.

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

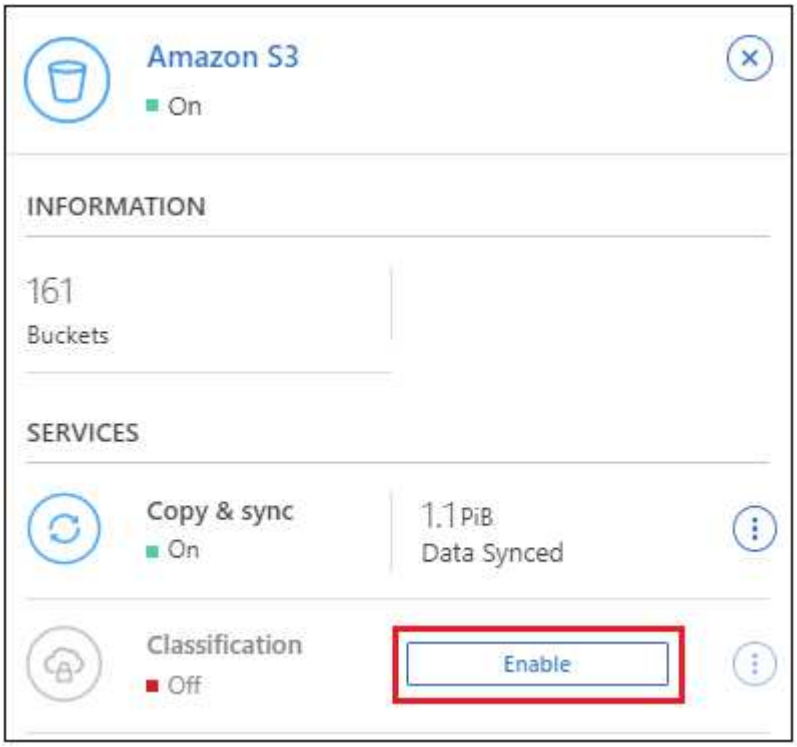
Aktivierung der BlueXP Klassifizierung in Ihrer S3-Arbeitsumgebung

Aktivieren Sie die BlueXP Klassifizierung für Amazon S3, nachdem Sie die Voraussetzungen überprüft haben.

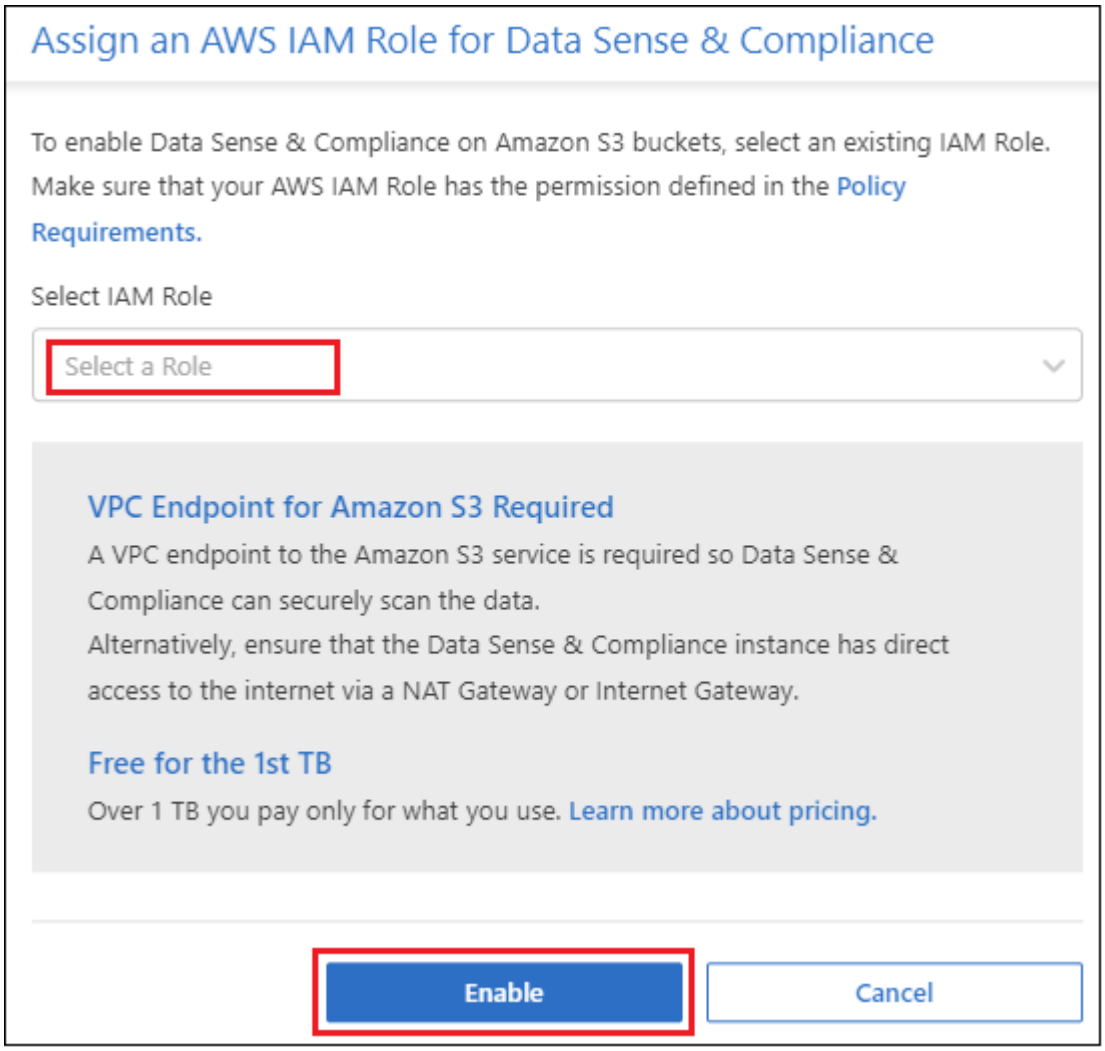
Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Speicherung > Leinwand**.
2. Wählen Sie die Amazon S3-Arbeitsumgebung aus.

3. Klicken Sie im Bereich Services rechts neben **Classification** auf **enable**.



4. Weisen Sie der BlueXP Klassifizierungsinstanz eine IAM-Rolle zu, wenn Sie dazu aufgefordert werden Die erforderlichen Berechtigungen.



5. Klicken Sie Auf **Aktivieren**.

> Sie können auch Compliance-Scans für eine Arbeitsumgebung über die Konfigurationsseite aktivieren, indem Sie auf die klicken ⋮ Und dann **BlueXP Klassifizierung aktivieren**.

Ergebnis

BlueXP weist der Instanz die IAM-Rolle zu.

Aktivieren und Deaktivieren von Compliance-Scans auf S3-Buckets

Nachdem BlueXP die BlueXP Klassifizierung für Amazon S3 aktiviert hat, müssen die zu scannenden Buckets konfiguriert werden.

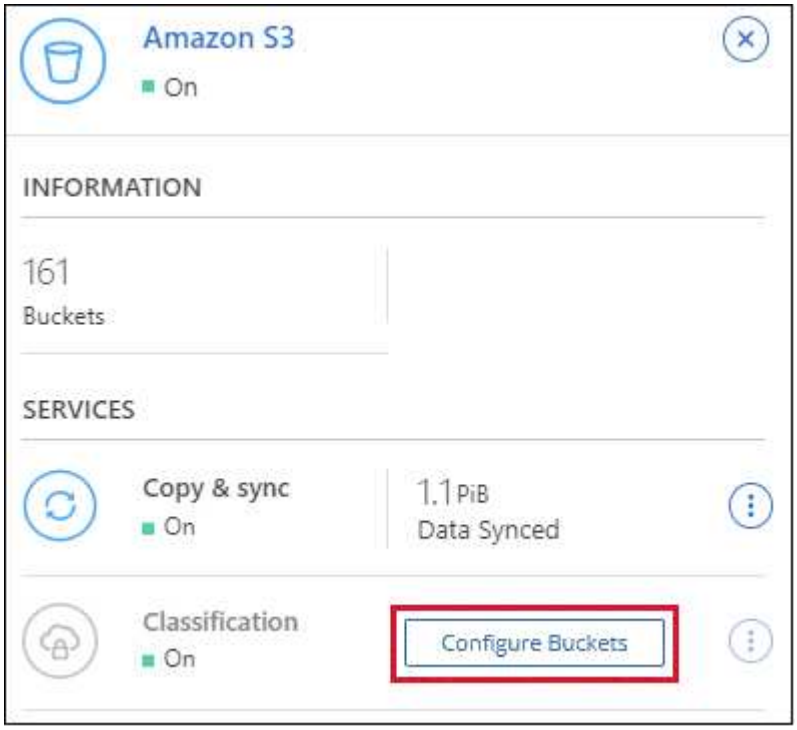
Wenn BlueXP im AWS Konto ausgeführt wird, das über die S3-Buckets verfügt, die Sie scannen möchten, erkennt es diese Buckets und zeigt sie in einer Amazon S3-Arbeitsumgebung an.

Die BlueXP Klassifizierung kann Sie ebenfalls Scannen von S3-Buckets, die in unterschiedlichen AWS Konten vorhanden sind.

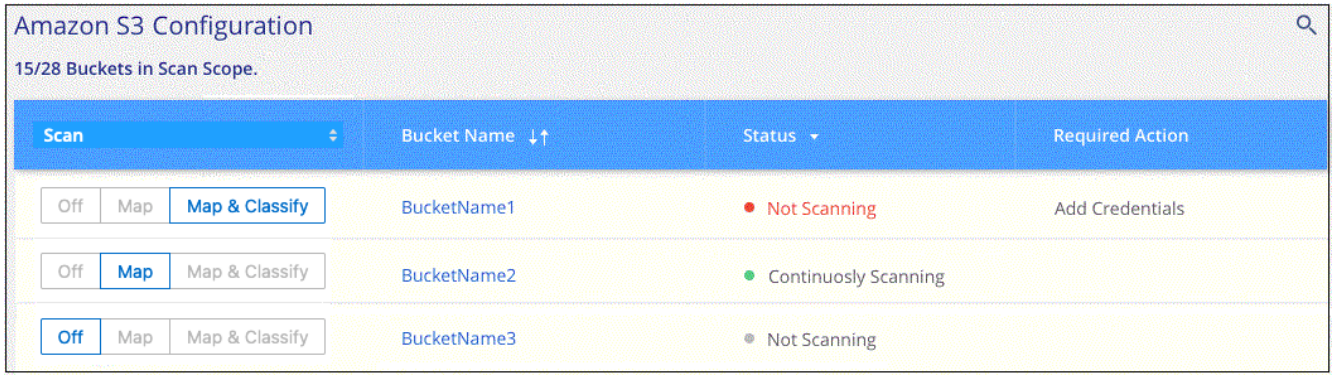
Schritte

1. Wählen Sie die Amazon S3-Arbeitsumgebung aus.

2. Klicken Sie im Bereich Dienste auf der rechten Seite auf **Buckets konfigurieren**.



3. Aktivieren Sie Scans, die nur mappen oder Scans zuordnen und klassifizieren, auf Ihren Buckets.



An:	Tun Sie dies:
Ermöglichen Sie Mapping-Only-Scans auf einem Bucket	Klicken Sie Auf **Karte**
Aktivieren vollständiger Scans auf einem Bucket	Klicken Sie Auf **Karte & Klassieren**
Deaktivieren des Scans auf einem Bucket	Klicken Sie Auf **Aus**

Ergebnis

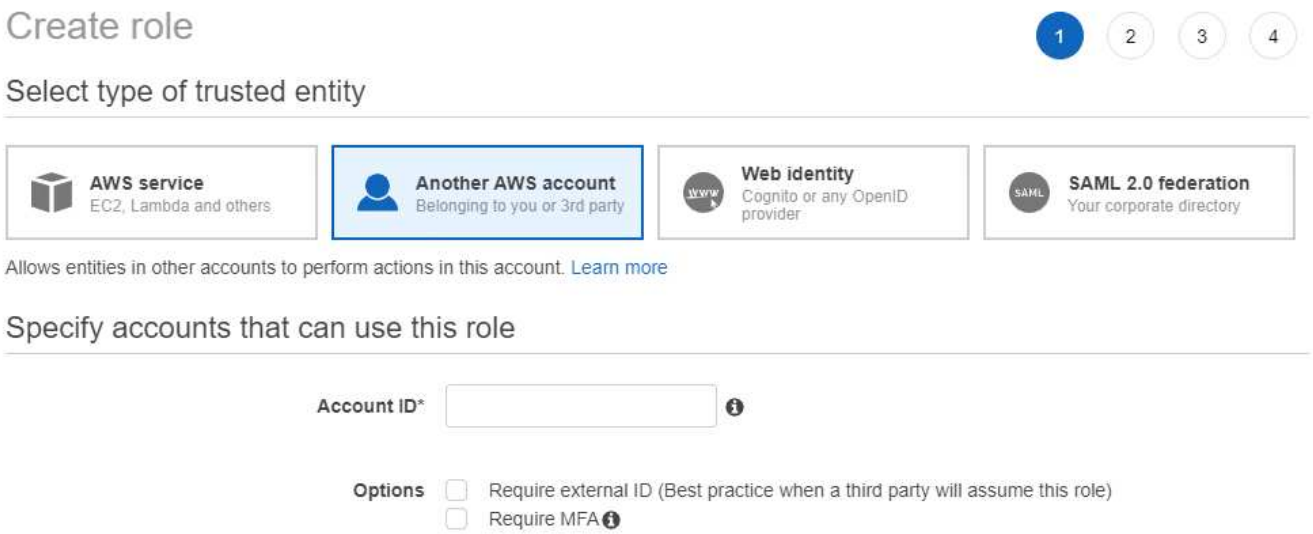
Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen aktivierten S3-Buckets. Wenn Fehler auftreten, werden sie neben der erforderlichen Aktion zur Behebung des Fehlers in der Spalte Status angezeigt.

Scannen von Buckets für weitere AWS Konten

Sie können S3-Buckets, die sich unter einem anderen AWS-Konto befinden, scannen, indem Sie eine Rolle von diesem Konto zuweisen, um auf die bestehende BlueXP Klassifizierungsinstanz zuzugreifen.

Schritte

1. Gehen Sie zum AWS Ziel-Konto, in dem Sie S3 Buckets scannen und eine IAM-Rolle erstellen möchten, indem Sie **ein weiteres AWS-Konto** auswählen.



Gehen Sie wie folgt vor:

- Geben Sie die ID des Kontos ein, unter dem sich die BlueXP Klassifizierungsinstanz befindet.
- Ändern Sie die maximale CLI/API-Sitzungsdauer* von 1 Stunde auf 12 Stunden und speichern Sie diese Änderung.
- Hängen Sie die BlueXP Klassifizierungs-IAM-Richtlinie an. Stellen Sie sicher, dass es über die erforderlichen Berechtigungen verfügt.

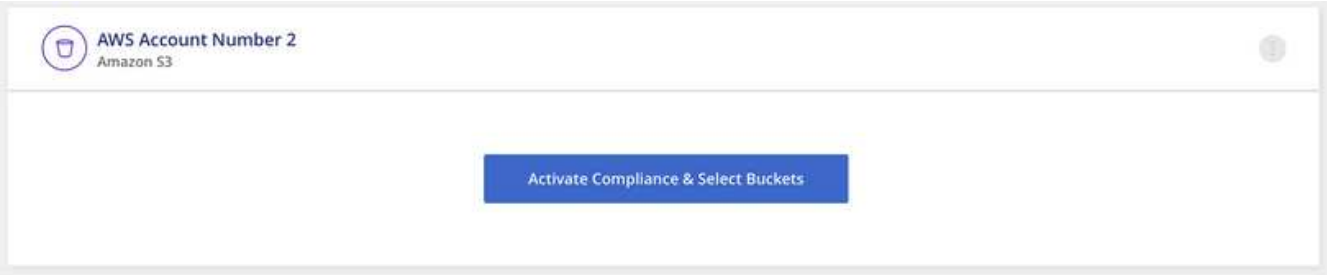
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Wechseln Sie zum AWS-Quellkonto, in dem sich die BlueXP Klassifizierungsinstanz befindet, und wählen Sie die mit der Instanz verbundene IAM-Rolle aus.
   a. Ändern Sie die maximale CLI/API-Sitzungsdauer* von 1 Stunde auf 12 Stunden und speichern Sie diese Änderung.
   b. Klicken Sie auf **Richtlinien anhängen** und dann auf **Richtlinien erstellen**.
   c. Erstellen Sie eine Richtlinie, die die Aktion „STS:AssumeRole“ enthält, und geben Sie den ARN der Rolle an, die Sie im Zielkonto erstellt haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

   Das BlueXP Profil für Klassifizierungsinstanzen hat jetzt Zugriff auf das zusätzliche AWS-Konto.

3. Gehen Sie auf die Seite **Amazon S3 Configuration** und das neue AWS-Konto wird angezeigt. Beachten Sie, dass es ein paar Minuten für die BlueXP Klassifizierung dauern kann, bis die Arbeitsumgebung des neuen Kunden synchronisiert und diese Informationen angezeigt werden.



4. Klicken Sie auf **BlueXP classification & Select Buckets** aktivieren und wählen Sie die Buckets aus, die Sie scannen möchten.

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der neuen S3-Buckets, die Sie aktiviert haben.

Datenbankschemas scannen

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

Beachten Sie, dass Sie nach der Datenbanküberprüfung eindeutige IDs hinzufügen können, die die BlueXP Klassifizierung in allen Datenquellen anhand bestimmter Spalten in Ihren Datenbanken identifiziert. Dies wird als *Data Fusion* -Funktion bezeichnet. "Erfahren Sie, wie Sie benutzerdefinierte Kennungen für persönliche Daten aus Ihren Datenbanken hinzufügen".

Schnellstart

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

1 Datenbankvoraussetzungen prüfen

Stellen Sie sicher, dass Ihre Datenbank unterstützt wird und dass Sie über die erforderlichen Informationen verfügen, um eine Verbindung zur Datenbank herzustellen.

2 Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

3 Fügen Sie den Datenbankserver hinzu

Fügen Sie den Datenbankserver hinzu, auf den Sie zugreifen möchten.

4 Wählen Sie die Schemas aus

Wählen Sie die Schemata aus, die Sie scannen möchten.

Voraussetzungen prüfen

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

Unterstützte Datenbanken

Die BlueXP Klassifizierung kann Schemata aus den folgenden Datenbanken scannen:

- Amazon Relational Database Service (Amazon RDS)
- MongoDB

- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

Die Statistik-Sammelfunktion *muss in der Datenbank aktiviert sein.

Datenbankanforderungen erfüllt

Jede Datenbank, die mit der BlueXP Klassifizierungsinstanz verbunden ist, kann unabhängig vom Hosting gescannt werden. Sie benötigen lediglich die folgenden Informationen, um eine Verbindung zur Datenbank herzustellen:

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

  Bei der Auswahl eines Benutzernamens und Passworts ist es wichtig, einen zu wählen, der über vollständige Leseberechtigungen für alle Schemas und Tabellen verfügt, die Sie scannen möchten. Wir empfehlen, einen dedizierten Benutzer für das BlueXP Klassifizierungssystem mit allen erforderlichen Berechtigungen zu erstellen.

Hinweis: für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

Implementieren der BlueXP Klassifizierungsinstanz

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

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

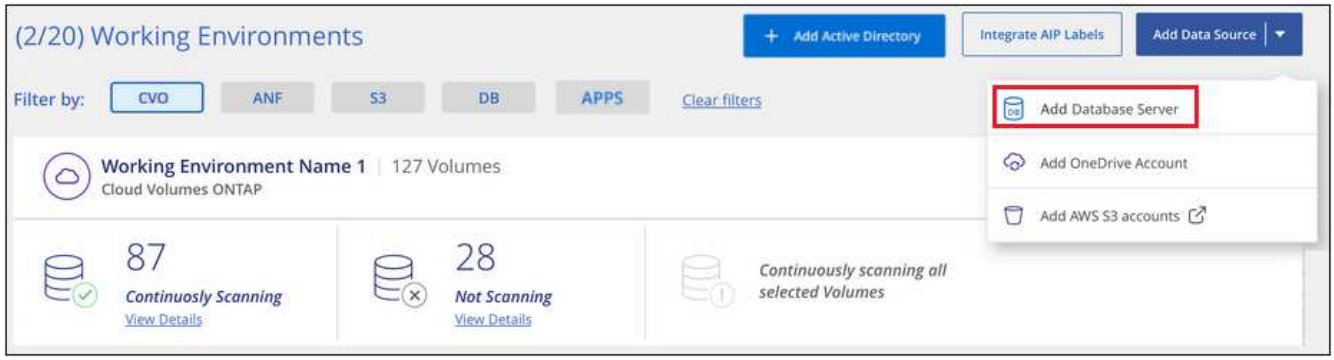
Wenn Sie Datenbankschemas scannen, die in einer dunklen Site installiert wurden, die keinen Internetzugang hat, müssen Sie dies tun "Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

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

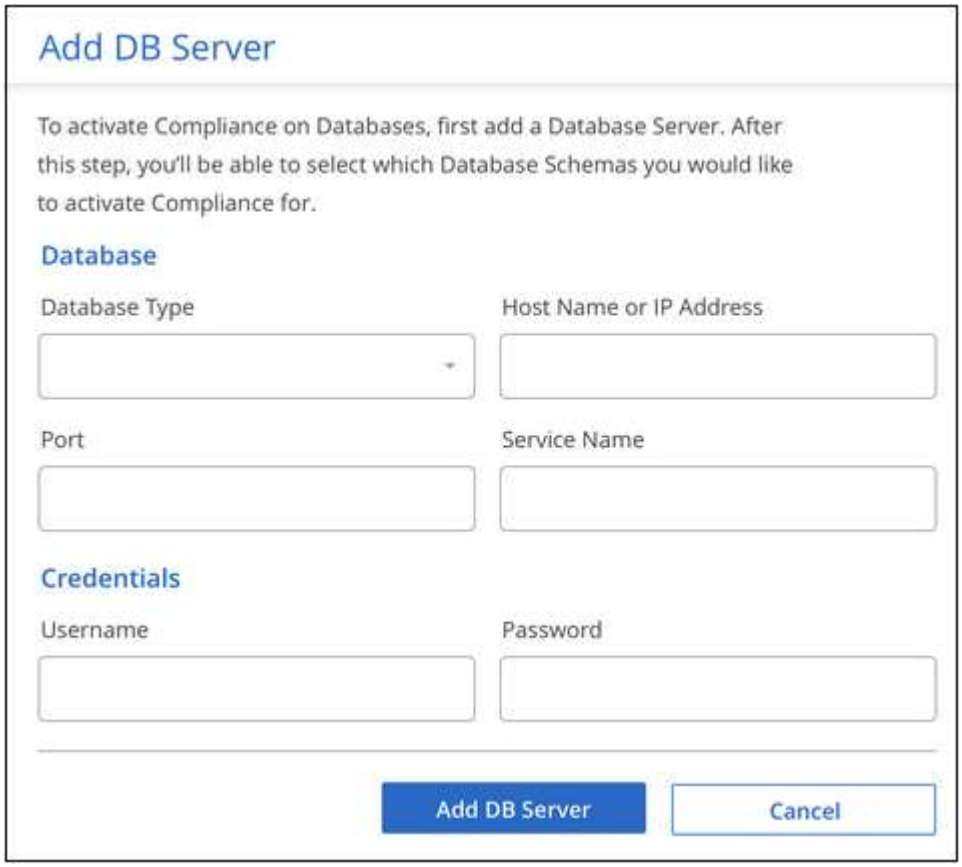
Fügen Sie den Datenbankserver hinzu

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

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen** > **Datenbank-Server hinzufügen**.



2. Geben Sie die erforderlichen Informationen ein, um den Datenbankserver zu identifizieren.
   a. Wählen Sie den Datenbanktyp aus.
   b. Geben Sie den Port und den Hostnamen oder die IP-Adresse ein, um eine Verbindung zur Datenbank herzustellen.
   c. Geben Sie für Oracle-Datenbanken den Dienstnamen ein.
   d. Geben Sie die Zugangsdaten ein, damit die BlueXP Klassifizierung auf den Server zugreifen kann.
   e. Klicken Sie auf **DB-Server hinzufügen**.



Die Datenbank wird zur Liste der Arbeitsumgebungen hinzugefügt.

Aktivieren und deaktivieren Sie Compliance-Scans für Datenbankschemas

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

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

1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Configuration** für die zu konfigurierende Datenbank.

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

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen aktivierten Datenbankschemas. Wenn Fehler auftreten, werden sie neben der erforderlichen Aktion zur Behebung des Fehlers in der Spalte Status angezeigt.

Die BlueXP Klassifizierung scannt Ihre Datenbanken einmal pro Tag – Datenbanken werden nicht wie andere Datenquellen fortlaufend gescannt.

OneDrive-Konten werden gescannt

Führen Sie ein paar Schritte durch, um mit der BlueXP Klassifizierung von Dateien in den OneDrive Ordnern eines Benutzers zu scannen.

Schnellstart

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

Alle Voraussetzungen für OneDrive prüfen

Stellen Sie sicher, dass Sie über die Administratoranmeldeinformationen verfügen, um sich beim OneDrive-Konto anzumelden.

Implementieren der BlueXP Klassifizierungsinstanz

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

Fügen Sie das OneDrive Konto hinzu

Melden Sie sich bei Verwendung der Admin-Benutzeranmeldeinformationen beim OneDrive-Konto an, auf das Sie zugreifen möchten, damit es als neue Arbeitsumgebung hinzugefügt wird.

Fügen Sie die Benutzer hinzu und wählen Sie den Scantyp aus

Fügen Sie die Liste der Benutzer aus dem OneDrive-Konto hinzu, das Sie scannen möchten, und wählen Sie den Scantyp aus. Sie können bis zu 100 Benutzer gleichzeitig hinzufügen.

OneDrive Anforderungen können Sie überprüfen

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

- Sie müssen über die Admin-Anmeldeinformationen für das OneDrive for Business-Konto verfügen, das Lesezugriff auf die Dateien des Benutzers bietet.
- Für alle Benutzer, deren OneDrive-Ordner Sie scannen möchten, benötigen Sie eine Liste mit den E-Mail-Adressen, die in einer Zeile getrennt sind.

Implementieren der BlueXP Klassifizierungsinstanz

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

Die BlueXP Klassifizierung kann dies sein "In der Cloud implementiert" Oder "In einer Anlage mit Internetzugang".

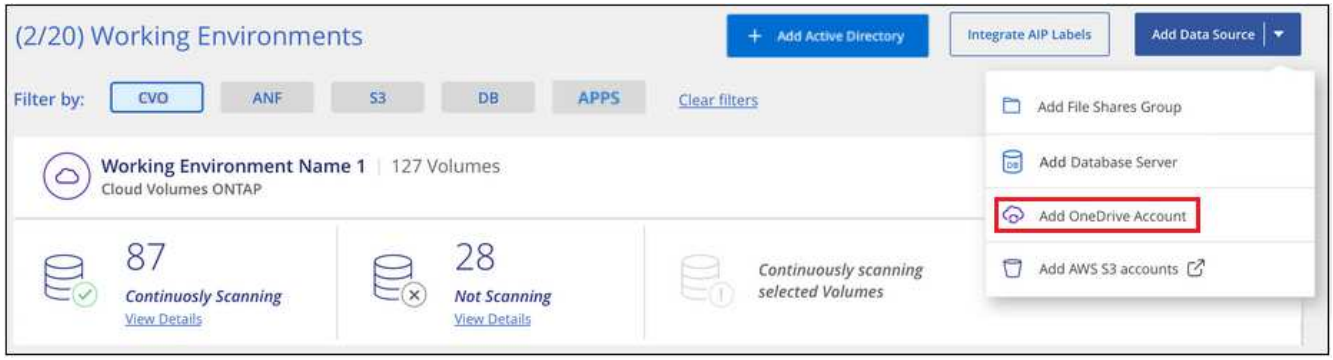
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des OneDrive Kontos

Fügen Sie das OneDrive-Konto hinzu, in dem sich die Benutzerdateien befinden.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen** > **OneDrive Konto hinzufügen**.



2. Klicken Sie im Dialogfeld „OneDrive-Konto hinzufügen“ auf **Anmelden bei OneDrive**.
3. Wählen Sie auf der angezeigten Microsoft-Seite das OneDrive-Konto aus, geben Sie den erforderlichen Admin-Benutzer und das Passwort ein, und klicken Sie dann auf **Accept**, damit die BlueXP-Klassifizierung Daten von diesem Konto lesen kann.

Das OneDrive-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

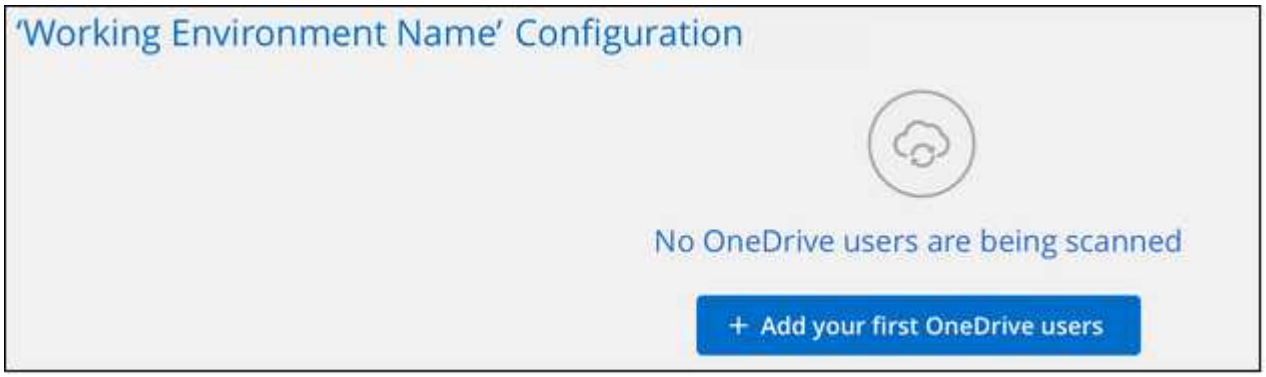
Hinzufügen von OneDrive Benutzern zu Compliance-Scans

Sie können einzelne OneDrive Benutzer oder alle OneDrive Benutzer hinzufügen, damit ihre Dateien durch die BlueXP Klassifizierung gescannt werden.

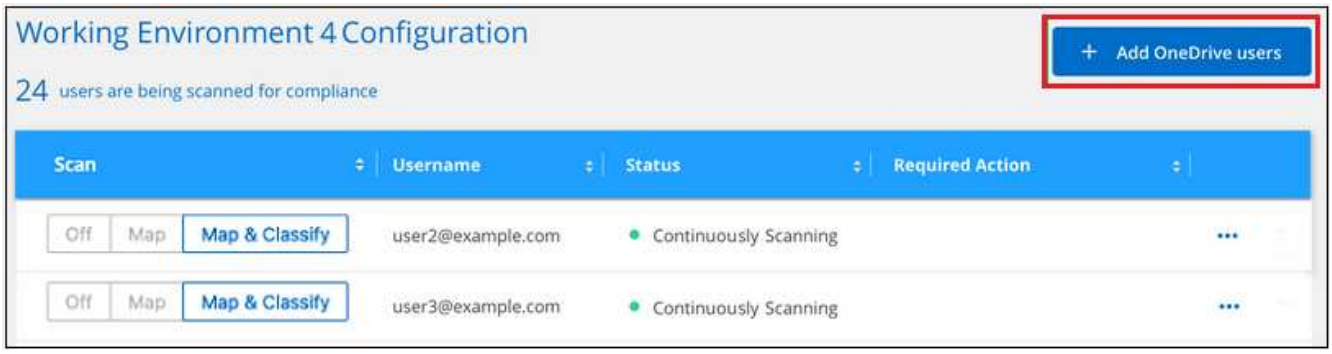
Schritte

1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Configuration** für das OneDrive-Konto.

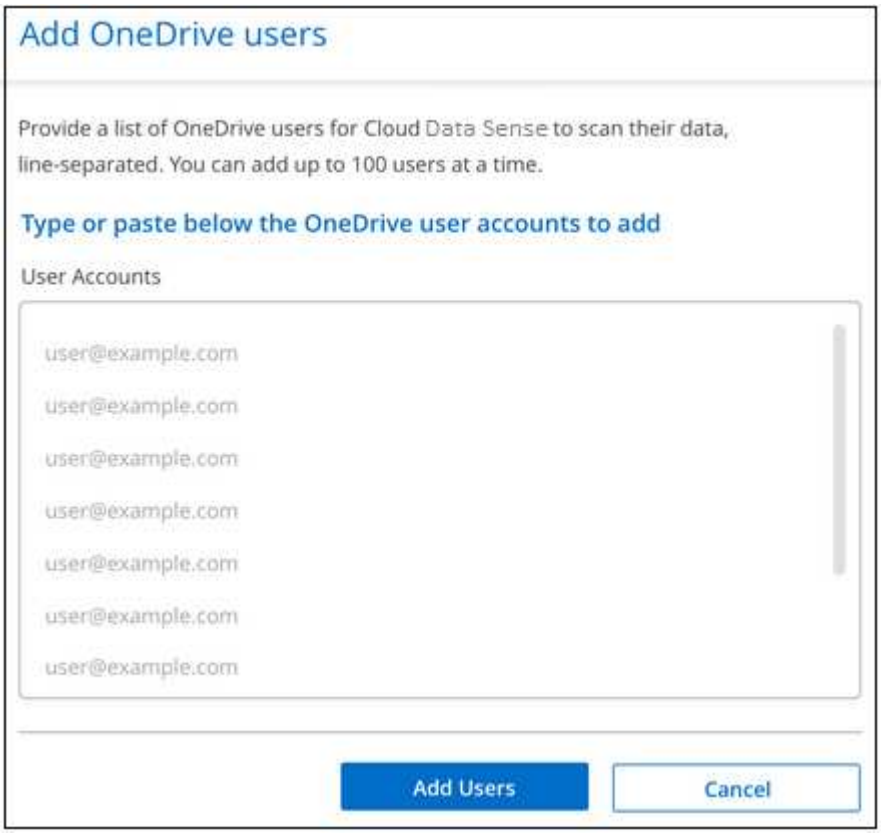
2. Wenn dies das erste Mal ist, Benutzer für dieses OneDrive-Konto hinzuzufügen, klicken Sie auf **Fügen Sie Ihre ersten OneDrive-Benutzer**.



Wenn Sie weitere Benutzer aus einem OneDrive-Konto hinzufügen möchten, klicken Sie auf **OneDrive Users hinzufügen**.



3. Fügen Sie die E-Mail-Adressen für die Benutzer hinzu, deren Dateien Sie scannen möchten - eine E-Mail-Adresse pro Zeile (bis zu 100 maximal pro Sitzung) - und klicken Sie auf **Benutzer hinzufügen**.



In einem Bestätigungsdialogfeld wird die Anzahl der Benutzer angezeigt, die hinzugefügt wurden.

Wenn im Dialogfeld Benutzer aufgeführt werden, die nicht hinzugefügt werden konnten, erfassen Sie diese Informationen, damit Sie das Problem beheben können. In einigen Fällen können Sie den Benutzer mit einer korrigierten E-Mail-Adresse erneut hinzufügen.

4. Ermöglichen Sie Scans, die nur zugeordnet werden können, oder Mapping- und Klassifizierungsprüfungen auf Benutzerdateien.

An:	Tun Sie dies:
Aktivieren Sie mappingonly Scans von Benutzerdateien	Klicken Sie Auf **Karte**
Aktivieren Sie vollständige Scans von Benutzerdateien	Klicken Sie Auf **Karte & Klassieren**

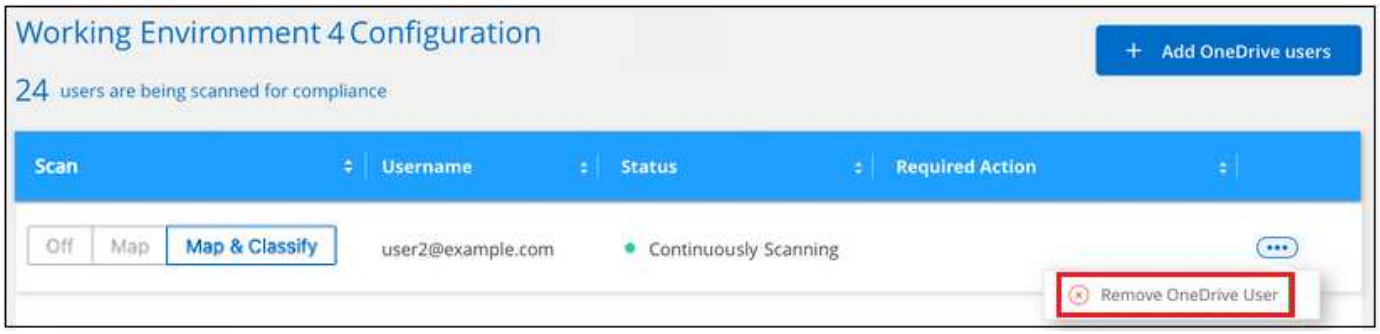
An:	Tun Sie dies:
Deaktivieren Sie das Scannen von Benutzerdateien	Klicken Sie Auf **Aus**

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der Dateien für die Benutzer, die Sie hinzugefügt haben. Die Ergebnisse werden im Dashboard und an anderen Orten angezeigt.

Entfernen eines OneDrive-Benutzers aus Compliance-Scans

Wenn Benutzer das Unternehmen verlassen oder sich ihre E-Mail-Adresse ändert, können Sie einzelne OneDrive Benutzer davon entfernen, dass ihre Dateien jederzeit gescannt werden können. Klicken Sie einfach auf **OneDrive User entfernen** von der Konfigurationsseite.



Beachten Sie, dass Sie können "Löschen Sie das gesamte OneDrive Konto aus der BlueXP Klassifizierung" Wenn Sie keine Benutzerdaten mehr aus dem OneDrive-Konto scannen möchten.

Scannen von SharePoint-Konten

Führen Sie ein paar Schritte durch, um mit dem Scannen von Dateien in Ihren lokalen SharePoint Online- und SharePoint-Konten mit BlueXP Klassifizierung zu beginnen.

Schnellstart

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

1. **SharePoint-Voraussetzungen prüfen**

Stellen Sie sicher, dass Sie über qualifizierte Anmeldeinformationen zur Anmeldung beim SharePoint-Konto verfügen und dass Sie über die URLs für die SharePoint-Sites verfügen, die Sie scannen möchten.

2. **Implementieren der BlueXP Klassifizierungsinstanz**

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

3. **Melden Sie sich beim SharePoint-Konto an**

Melden Sie sich mit qualifizierten Benutzeranmeldeinformationen beim SharePoint-Konto an, auf das Sie zugreifen möchten, um es als neue Datenquelle/Arbeitsumgebung hinzuzufügen.

4 Fügen Sie die URLs der SharePoint-Website zum Scannen hinzu

Fügen Sie die Liste der SharePoint-Website-URLs hinzu, die Sie im SharePoint-Konto scannen möchten, und wählen Sie den Scantyp aus. Sie können bis zu 100 URLs gleichzeitig hinzufügen - und bis zu 1,000 Sites insgesamt für jedes Konto.

Überprüfung der SharePoint Anforderungen

Prüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie die BlueXP Klassifizierung für ein SharePoint Konto aktivieren können.

- Sie müssen über die Anmeldeinformationen des Admin-Benutzers für das SharePoint-Konto verfügen, das Lesezugriff auf alle SharePoint-Sites bietet.
  - Für SharePoint Online können Sie ein nicht-Administratorkonto verwenden, aber dieser Benutzer muss über die Berechtigung verfügen, auf alle SharePoint-Sites zuzugreifen, die Sie scannen möchten.
- Für SharePoint vor Ort benötigen Sie auch die URL des SharePoint Servers.
- Für alle zu scannenden Daten benötigen Sie eine Liste der URLs der SharePoint-Website.

Implementieren der BlueXP Klassifizierungsinstanz

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

- Für SharePoint Online kann die BlueXP Klassifizierung erfolgen "In der Cloud implementiert".
- Für SharePoint vor Ort kann die BlueXP Klassifizierung installiert werden "In einer Anlage mit Internetzugang" Oder "In einem Hotel, das keinen Internetzugang hat".

Wenn die BlueXP-Klassifizierung auf einer Website ohne Internetzugang installiert ist, muss der BlueXP Connector auch ohne Internetzugang auf derselben Website installiert sein. "Weitere Informationen .".

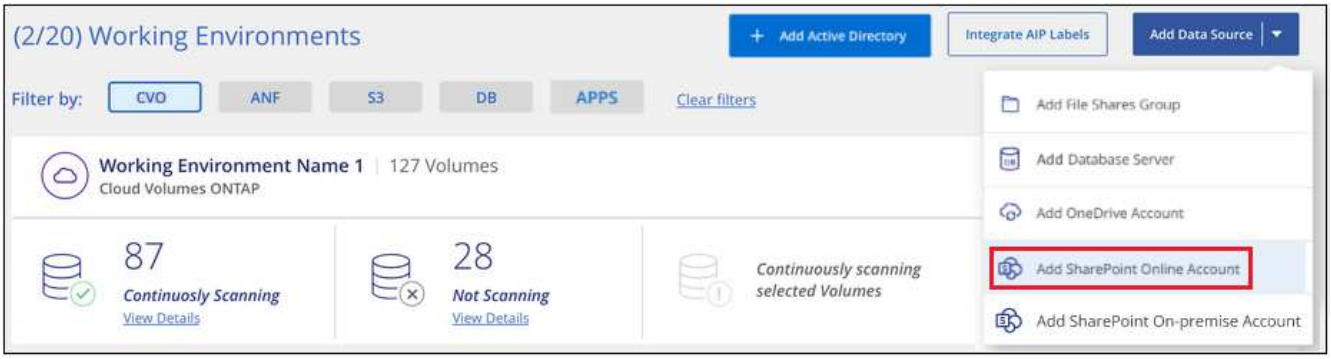
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen eines SharePoint Online-Kontos

Fügen Sie das SharePoint Online-Konto hinzu, in dem sich die Benutzerdateien befinden.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen** > **SharePoint Online-Konto hinzufügen**.



2. Klicken Sie im Dialogfeld SharePoint Online-Konto hinzufügen auf **in SharePoint anmelden**.
3. Wählen Sie auf der angezeigten Microsoft-Seite das SharePoint-Konto aus, geben Sie den Benutzer und das Passwort ein (Admin-Benutzer oder anderer Benutzer mit Zugriff auf die SharePoint-Sites), und klicken Sie dann auf **Accept**, damit die BlueXP-Klassifizierung Daten von diesem Konto lesen kann.

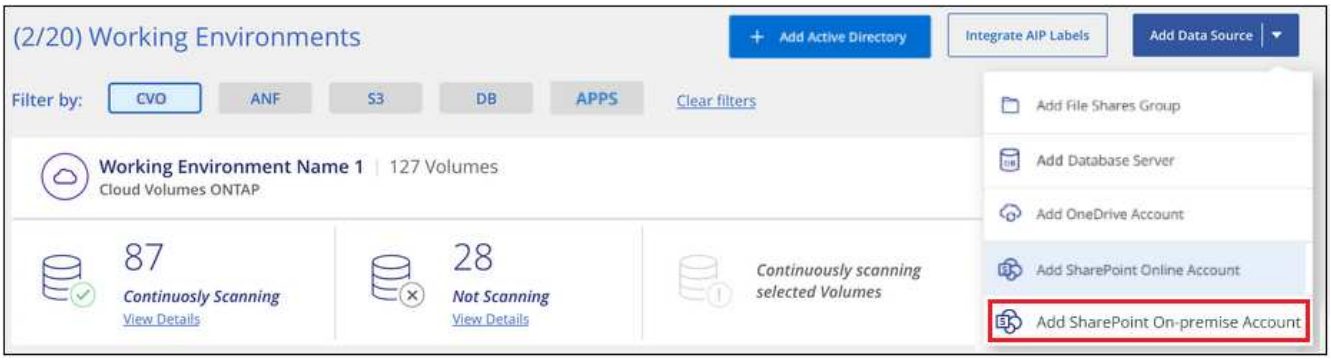
Das SharePoint Online-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

Hinzufügen eines SharePoint-Kontos vor Ort

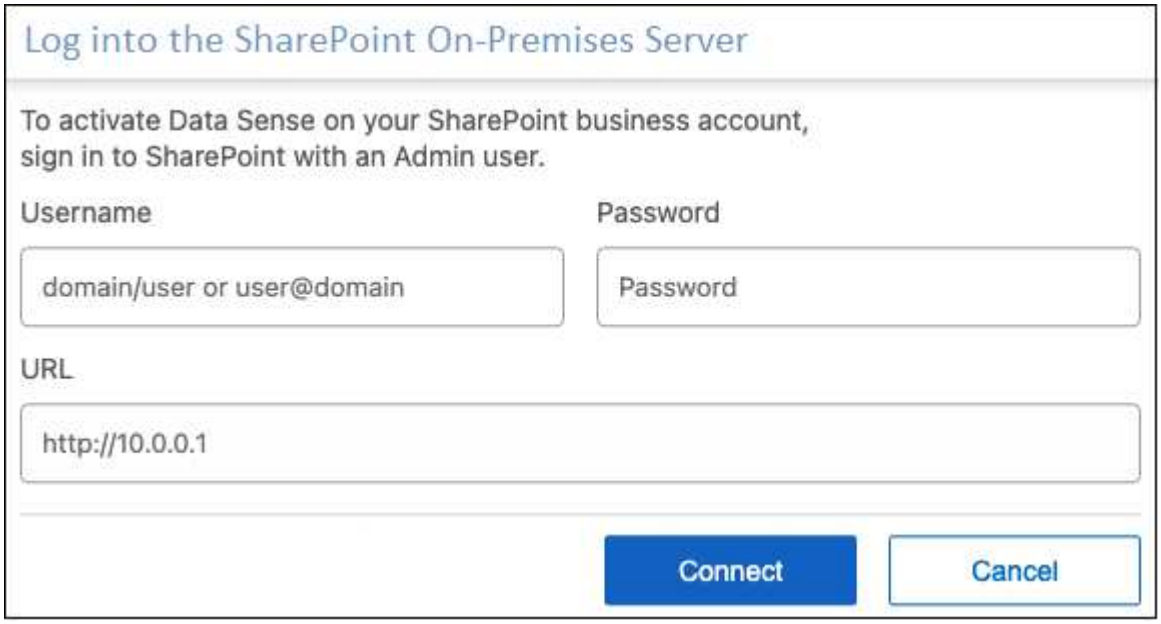
Fügen Sie das SharePoint-On-Premise-Konto hinzu, in dem sich die Benutzerdateien befinden.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen** > **SharePoint On-Premise-Konto hinzufügen**.



2. Geben Sie im Dialogfeld beim SharePoint-On-Premise-Server anmelden die folgenden Informationen ein:
   - Admin-Benutzer im Format „Domäne/Benutzer“ oder „Benutzer@Domäne“ und „Admin-Passwort“
   - URL des SharePoint Servers



3. Klicken Sie Auf **Verbinden**.

Das On-Premise-Konto SharePoint wird zur Liste der Arbeitsumgebungen hinzugefügt.

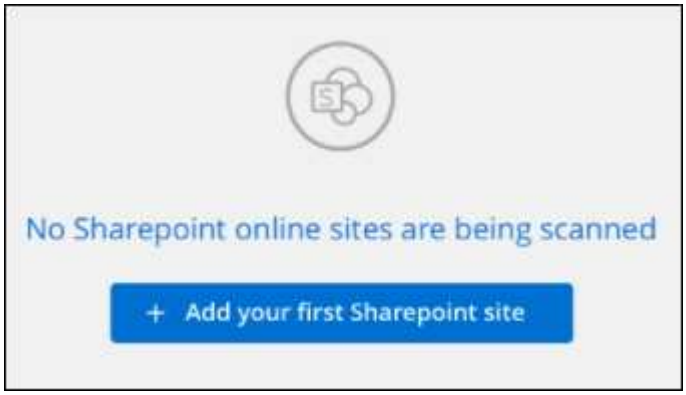
Hinzufügen von SharePoint Sites zu Compliance-Scans

Sie können dem Konto einzelne SharePoint Sites oder bis zu 1,000 SharePoint Sites hinzufügen, sodass die zugehörigen Dateien durch die BlueXP Klassifizierung gescannt werden. Unabhängig davon, ob Sie SharePoint Online oder SharePoint On-Premise-Websites hinzufügen, sind die Schritte gleich.

Schritte

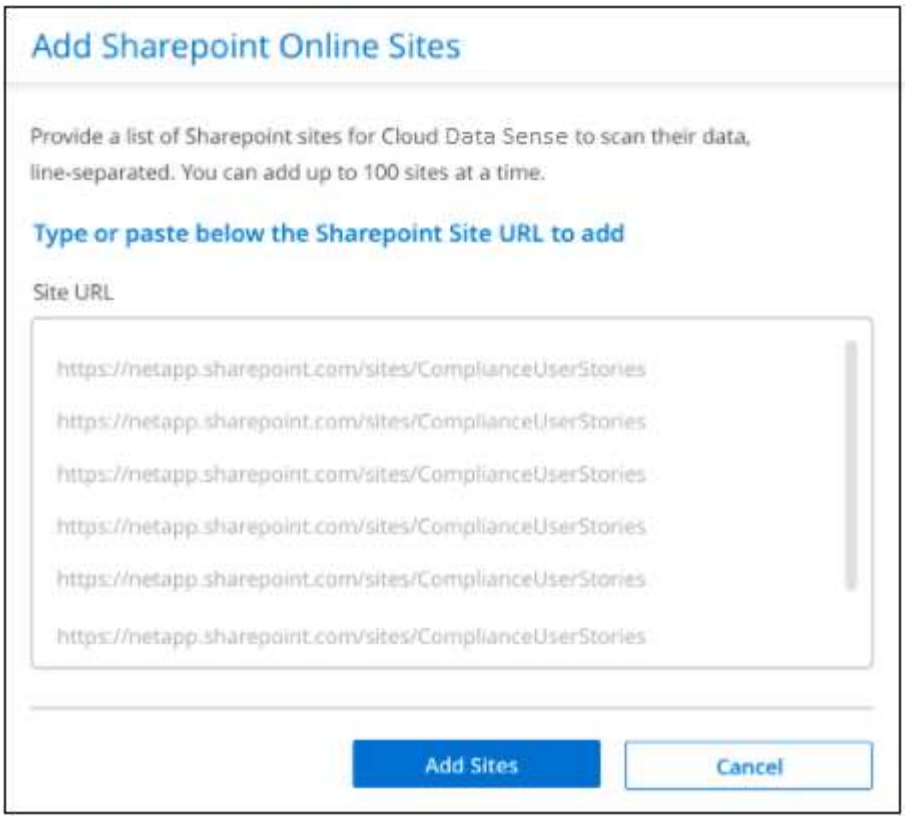
1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Configuration** für das SharePoint-Konto.

2. Wenn dies das erste Mal ist, Websites für dieses SharePoint-Konto hinzuzufügen, klicken Sie auf **Ihre erste SharePoint-Website hinzufügen**.



Wenn Sie weitere Benutzer von einem SharePoint-Konto hinzufügen, klicken Sie auf **SharePoint-Sites hinzufügen**.

3. Fügen Sie die URLs für die Seiten hinzu, deren Dateien Sie scannen möchten - eine URL pro Zeile (bis zu 100 maximal pro Sitzung) - und klicken Sie auf **Sites hinzufügen**.



In einem Bestätigungsdialogfeld wird die Anzahl der hinzugefügten Standorte angezeigt.

Wenn im Dialogfeld keine Sites aufgeführt sind, die nicht hinzugefügt werden konnten, erfassen Sie diese Informationen, damit Sie das Problem beheben können. In einigen Fällen können Sie die Site mit einer korrigierten URL erneut hinzufügen.

4. Wenn Sie mehr als 100 Sites für dieses Konto hinzufügen müssen, klicken Sie einfach erneut auf **SharePoint Sites hinzufügen**, bis Sie alle Ihre Sites für dieses Konto hinzugefügt haben (bis zu 1,000 Sites insgesamt für jedes Konto).
5. Ermöglichen Sie auf den Dateien auf den SharePoint-Sites Mapping- und Klassifizierungscans.

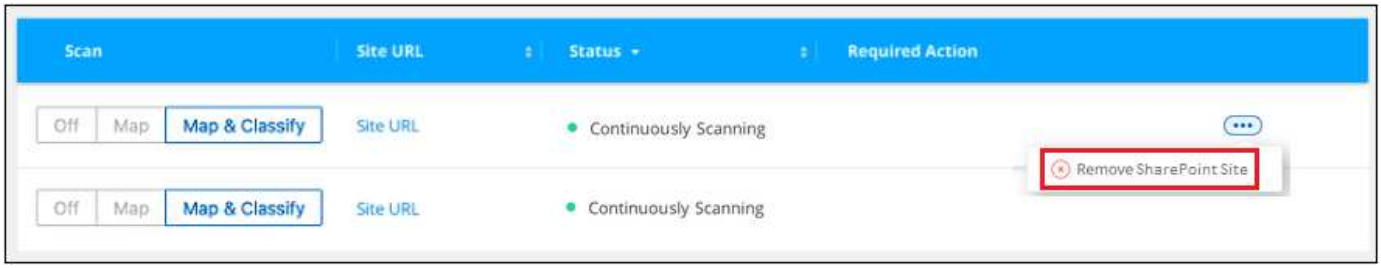
An:	Tun Sie dies:
Aktivieren Sie Mapping-Only-Scans auf Dateien	Klicken Sie Auf **Karte**
Aktivieren Sie vollständige Scans auf Dateien	Klicken Sie Auf **Karte & Klassieren**
Deaktivieren Sie das Scannen von Dateien	Klicken Sie Auf **Aus**

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der Dateien in den von Ihnen hinzugefügten SharePoint Sites. Die Ergebnisse werden im Dashboard und an anderen Orten angezeigt.

Entfernen einer SharePoint-Website aus Compliance-Scans

Wenn Sie eine SharePoint-Site in der Zukunft entfernen oder sich entscheiden, keine Dateien auf einer SharePoint-Site zu scannen, können Sie einzelne SharePoint-Sites davon entfernen, dass ihre Dateien jederzeit gescannt werden. Klicken Sie einfach auf **SharePoint-Website entfernen** von der Konfigurationsseite.



Beachten Sie, dass Sie können "Löschen Sie das gesamte SharePoint Konto aus der BlueXP Klassifizierung" Wenn Sie keine Benutzerdaten mehr vom SharePoint-Konto scannen möchten.

Google Drive-Konten werden durchsucht

Führen Sie ein paar Schritte durch, um mit dem Scannen von Benutzerdateien in Ihren Google-Laufwerkskonten mit BlueXP Klassifizierung zu beginnen.

Schnellstart

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

1. **Prüfen Sie die Voraussetzungen für Google Drive**

Stellen Sie sicher, dass Sie über die Administratoranmeldeinformationen verfügen, um sich beim Google Drive-Konto anzumelden.

2. **Implementieren Sie die BlueXP Klassifizierung**

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

3. **Melden Sie sich beim Google Drive-Konto an**

Wenn Sie Admin-Benutzeranmeldeinformationen verwenden, melden Sie sich beim Google Drive-Konto an, auf das Sie zugreifen möchten, damit es als neue Datenquelle hinzugefügt wird.

4. **Wählen Sie den Scantyp für die Benutzerdateien aus**

Wählen Sie den Scantyp aus, den Sie für die Benutzerdateien durchführen möchten; Zuordnen oder Zuordnen und Klassifizieren.

Überprüfen der Google-Laufwerksanforderungen

Überprüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie die BlueXP Klassifizierung für ein Google Drive Konto aktivieren können.

- Sie müssen über die Admin-Anmeldeinformationen für das Google Drive-Konto verfügen, das Lesezugriff auf die Dateien des Benutzers bietet

Aktuelle Einschränkungen

Die folgenden BlueXP Klassifizierungsfunktionen werden derzeit nicht von Google Drive Files unterstützt:

- Beim Anzeigen von Dateien auf der Seite „Datenuntersuchung“ sind die Aktionen in der Schaltflächenleiste nicht aktiv. Sie können keine Dateien kopieren, verschieben, löschen usw..
- Berechtigungen können nicht innerhalb von Dateien in Google Drive identifiziert werden, daher werden auf der Untersuchungsseite keine Berechtigungsinformationen angezeigt.

Implementieren der BlueXP Klassifizierung

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

Die BlueXP Klassifizierung kann dies sein "In der Cloud implementiert" Oder "In einer Anlage mit Internetzugang".

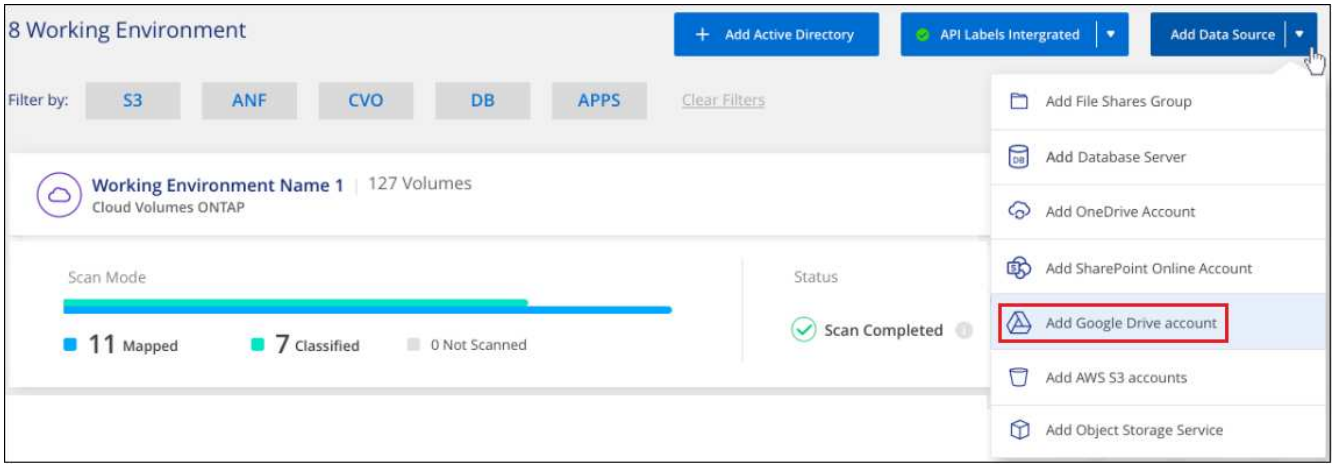
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des Google Drive-Kontos

Fügen Sie das Google Drive-Konto hinzu, in dem sich die Benutzerdateien befinden. Wenn Sie Dateien von mehreren Benutzern scannen möchten, müssen Sie diesen Schritt für jeden Benutzer ausführen.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen** > **Google Drive Account hinzufügen**.



2. Klicken Sie im Dialogfeld „Google Drive Account hinzufügen“ auf **beim Google Drive** anmelden.
3. Wählen Sie auf der angezeigten Google-Seite das Google Drive-Konto aus und geben Sie den gewünschten Admin-Benutzer und das Passwort ein. Klicken Sie dann auf **Akzeptieren**, damit die BlueXP-Klassifizierung Daten von diesem Konto lesen kann.

Das Google Drive-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

Auswählen des Scantyps für Benutzerdaten

Wählen Sie die Art des Scans aus, die die BlueXP Klassifizierung für die Benutzerdaten durchführen soll.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Konfiguration** für das Google Drive-Konto.

2. Aktivieren Sie mapping-only Scans oder Mapping- und Klassifizierungsscans auf den Dateien im Google Drive-Konto.

An:	Tun Sie dies:
Aktivieren Sie Mapping-Only-Scans auf Dateien	Klicken Sie Auf **Karte**
Aktivieren Sie vollständige Scans auf Dateien	Klicken Sie Auf **Karte & Klassieren**
Deaktivieren Sie das Scannen von Dateien	Klicken Sie Auf **Aus**

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der Dateien in dem von Ihnen hinzugefügten Google Drive-Konto, und die Ergebnisse werden im Dashboard und an anderen Orten angezeigt.

Entfernen eines Google Drive-Kontos aus Compliance-Scans

Da nur die Google Drive-Dateien eines einzigen Benutzers Teil eines einzigen Google Drive-Kontos sind, wenn Sie die Suche von Dateien von einem Benutzer Google Drive-Konto beenden möchten, dann sollten Sie "Löschen Sie das Google Drive-Konto aus der BlueXP Klassifizierung".

Scannen von Dateifreigaben

Führen Sie ein paar Schritte durch, um mit dem Scannen von nicht-NetApp NFS- oder CIFS-Dateifreigaben direkt mit der BlueXP Klassifizierung zu beginnen. Diese Dateifreigaben können lokal oder in der Cloud gespeichert werden.

Schnellstart

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

Prüfen Sie die Voraussetzungen für die Dateifreigabe

Stellen Sie für CIFS-Freigaben (SMB) sicher, dass Sie über Anmeldeinformationen für den Zugriff auf Freigaben verfügen.

2 **Implementieren der BlueXP Klassifizierungsinstanz**

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

3 **Erstellen Sie eine Gruppe, um die Dateifreigaben zu halten**

Die Gruppe ist ein Container für die Dateifreigaben, die Sie scannen möchten, und er wird als Name der Arbeitsumgebung für diese Dateifreigaben verwendet.

4 **Fügen Sie die Dateifreigaben der Gruppe hinzu**

Fügen Sie die Liste der zu scannenden Dateifreigaben hinzu und wählen Sie den Scantyp aus. Sie können bis zu 100 Dateifreigaben gleichzeitig hinzufügen.

Prüfen der Anforderungen für die Dateifreigabe

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

- Die Shares können überall gehostet werden, auch in der Cloud oder vor Ort. In den meisten Fällen handelt es sich hierbei um File Shares, die auf Storage-Systemen anderer Anbieter residieren. CIFS-Freigaben von älteren NetApp 7-Mode Storage-Systemen können jedoch als Dateifreigaben gescannt werden.

  Beachten Sie, dass die BlueXP Klassifizierung keine Berechtigungen oder die „Zeit des letzten Zugriffs“ aus 7-Mode Systemen extrahieren kann. Aufgrund eines bekannten Problems zwischen einigen Linux-Versionen und CIFS-Freigaben auf 7-Mode-Systemen müssen Sie die Freigabe zudem so konfigurieren, dass nur SMB v1 mit aktivierter NTLM-Authentifizierung verwendet wird.

- Zwischen der BlueXP Klassifizierungsinstanz und den Freigaben muss eine Netzwerkverbindung bestehen.
- Stellen Sie sicher, dass die Ports für die BlueXP Klassifizierungsinstanz offen sind:
  - Für NFS – die Ports 111 und 2049.
  - Für CIFS – die Ports 139 und 445.
- Sie können eine DFS-Freigabe (Distributed File System) als reguläre CIFS-Freigabe hinzufügen. Da die BlueXP Klassifizierung jedoch nicht bewusst ist, dass die Freigabe auf mehreren Servern/Volumes basiert, die als einzelne CIFS-Freigabe kombiniert werden, erhalten Sie möglicherweise Berechtigungen oder Verbindungsfehler bezüglich der Freigabe, wenn die Nachricht sich wirklich nur auf einen der Ordner/Freigaben bezieht, die sich auf einem anderen Server/Volume befinden.
- Stellen Sie für CIFS-Freigaben (SMB) sicher, dass Sie über Active Directory-Anmeldeinformationen verfügen, die Lesezugriff auf die Freigaben bieten. Anmeldedaten als Administrator sind bevorzugt, wenn die BlueXP Klassifizierung alle Daten scannt, die erhöhte Berechtigungen erfordern.

  Wenn Sie sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „Zeiten des letzten Zugriffs“ unverändert bleiben, empfehlen wir dem Benutzer Schreibattribute-Berechtigungen in CIFS oder Schreibberechtigungen in NFS. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

- Sie benötigen die Liste der Freigaben, die Sie im Format hinzufügen möchten

`<host_name>:/<share_path>`. Sie können die Freigaben einzeln eingeben oder eine Liste der Dateien, die Sie scannen möchten, mit einer Zeile angeben.

Implementieren der BlueXP Klassifizierungsinstanz

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

Wenn Sie nicht-NetApp NFS- oder CIFS-File Shares scannen, die über das Internet zugänglich sind, können Sie sie ausführen "Implementieren Sie die BlueXP Klassifizierung in der Cloud" Oder "Implementieren Sie die BlueXP Klassifizierung an einem lokalen Standort mit Internetzugang".

Wenn Sie nicht-NetApp NFS- oder CIFS-File Shares scannen, die in einer dunklen Site installiert wurden und über keinen Internetzugang verfügen, müssen Sie sie verwenden "Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

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

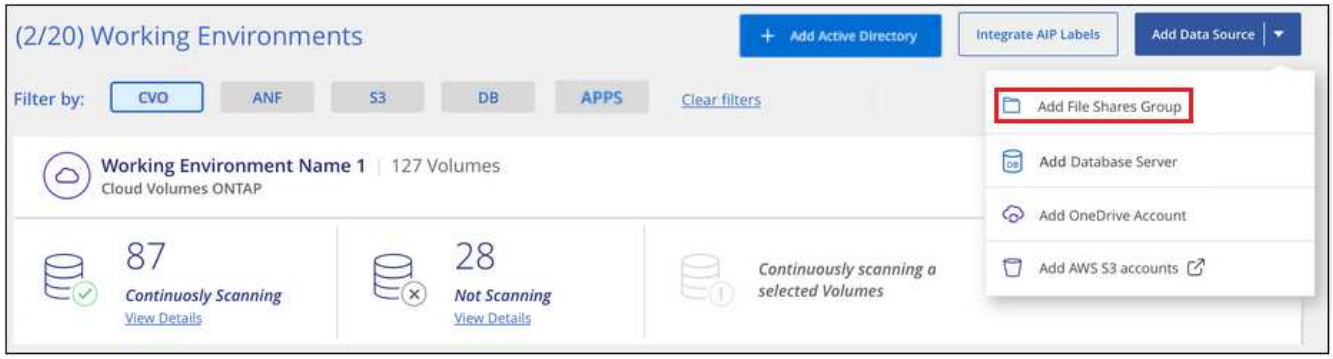
Erstellen der Gruppe für die Dateifreigaben

Sie müssen eine „Gruppe“ von Dateifreigaben für Dateien hinzufügen, bevor Sie Ihre Dateifreigaben hinzufügen können. Die Gruppe ist ein Container für die zu scannenden Dateifreigaben, und der Gruppenname wird als Name der Arbeitsumgebung für diese Dateifreigaben verwendet.

Sie können NFS- und CIFS-Freigaben in einer Gruppe kombinieren. Allerdings müssen alle CIFS-Dateifreigaben in einer Gruppe dieselben Active Directory-Anmeldedaten verwenden. Wenn Sie CIFS-Freigaben hinzufügen möchten, die unterschiedliche Anmeldedaten verwenden, müssen Sie für jeden eindeutigen Satz von Anmeldeinformationen eine separate Gruppe erstellen.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen** > **Datei-Shares-Gruppe hinzufügen**.



2. Geben Sie im Dialogfeld „Gruppe Dateien hinzufügen“ den Namen für die Gruppe der Freigaben ein, und klicken Sie auf **Weiter**.

Die neue File Shares-Gruppe wird der Liste der Arbeitsumgebungen hinzugefügt.

Hinzufügen von Dateifreigaben zu einer Gruppe

Sie fügen der Dateifreigaben-Gruppe Dateifreigaben hinzu, damit die Dateien in diesen Freigaben durch die BlueXP-Klassifizierung gescannt werden. Sie fügen die Freigaben im Format hinzu

`<host_name>:/<share_path>`.

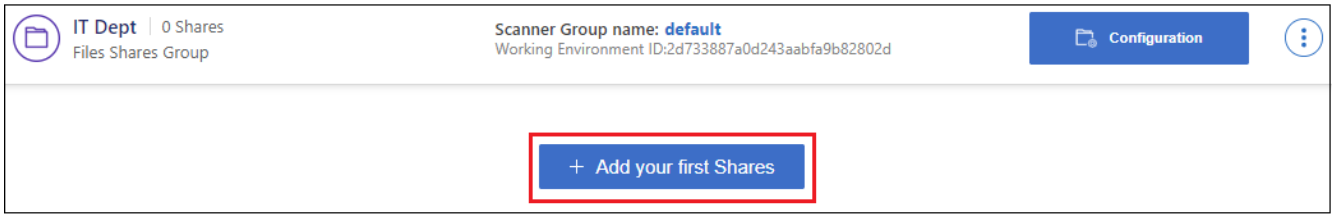
Sie können einzelne Dateifreigaben hinzufügen, oder Sie können eine Liste der Dateien, die Sie scannen möchten, mit einer Zeile eingeben. Sie können bis zu 100 Shares gleichzeitig hinzufügen.

Wenn Sie in einer einzelnen Gruppe sowohl NFS- als auch CIFS-Freigaben hinzufügen, müssen Sie diesen Prozess zweimal durchlaufen: Sobald Sie NFS-Freigaben hinzufügen, und dann erneut CIFS-Freigaben hinzufügen.

Schritte

1. Klicken Sie auf der Seite *Working Environments* auf die Schaltfläche **Konfiguration** für die File Shares Group.

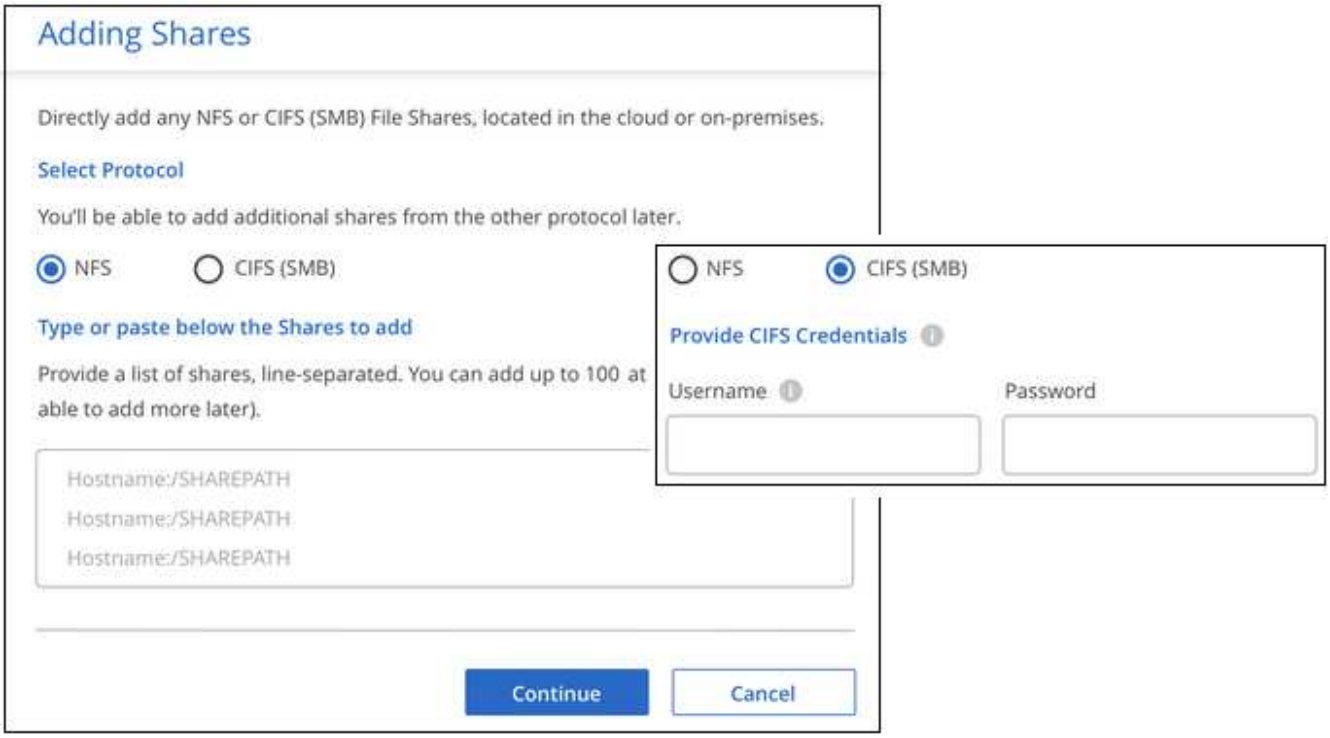
2. Wenn dies das erste Mal ist, um Dateifreigaben für diese File Shares-Gruppe hinzuzufügen, klicken Sie auf **erste Shares hinzufügen**.



Wenn Sie einer vorhandenen Gruppe File Shares hinzufügen, klicken Sie auf **Add Shares**.

3. Wählen Sie das Protokoll für die File Shares aus, die Sie hinzufügen, fügen Sie die File Shares hinzu, die Sie scannen möchten - eine Dateifreigabe pro Zeile - und klicken Sie auf **Weiter**.

   Beim Hinzufügen von CIFS (SMB)-Freigaben müssen Sie die Active Directory-Anmeldeinformationen eingeben, die Lesezugriff auf die Freigaben bieten. Anmeldedaten für Admin werden bevorzugt.



Ein Bestätigungsdialogfeld zeigt die Anzahl der hinzugefügten Freigaben an.

Wenn im Dialogfeld Freigaben aufgeführt werden, die nicht hinzugefügt werden konnten, erfassen Sie diese Informationen, damit Sie das Problem beheben können. In einigen Fällen können Sie die Freigabe mit einem korrigierten Hostnamen oder Freigabennamen erneut hinzufügen.

4. Aktivieren Sie für jede Dateifreigabe nur mappingbare Scans oder Mappings und Klassifizierungen.

An:	Tun Sie dies:
Aktivieren Sie Mapping-Only-Scans auf File Shares	Klicken Sie Auf **Karte**
Vollständige Scans auf Dateifreigaben ermöglichen	Klicken Sie Auf **Karte & Klassieren**
Deaktivieren Sie das Scannen von Dateifreigaben	Klicken Sie Auf **Aus**

Der Schalter oben auf der Seite für **Scan bei fehlenden "Schreibattributen"-Berechtigungen** ist standardmäßig deaktiviert. Das bedeutet, wenn die BlueXP Klassifizierung keine Schreibattributen-Berechtigungen in CIFS oder Schreibberechtigungen in NFS hat, dann wird das System die Dateien nicht scannen, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen egal ist, ob die letzte Zugriffszeit zurückgesetzt wird, schalten Sie den Schalter EIN, und alle Dateien werden unabhängig von den Berechtigungen gescannt. "Weitere Informationen .".

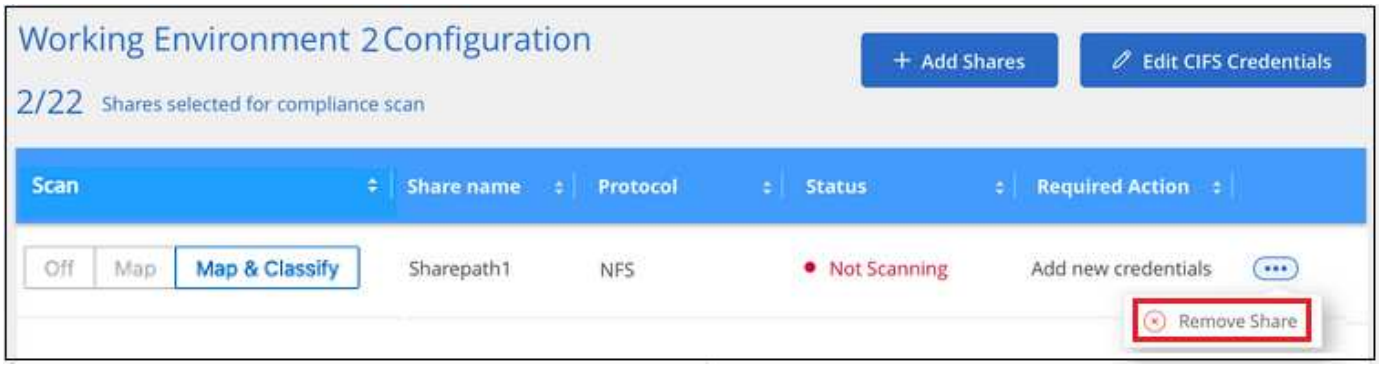
Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der Dateien in den von Ihnen hinzugefügten Dateifreigaben. Die Ergebnisse werden im Dashboard und an anderen Orten angezeigt.

Entfernen einer Dateifreigabe aus Compliance-Scans

Wenn Sie bestimmte Dateifreigaben nicht mehr scannen müssen, können Sie einzelne Dateifreigaben jederzeit aus dem Scannen ihrer Dateien entfernen. Klicken Sie einfach auf der Konfigurationsseite auf **Share**

entfernen.



Objekt-Storage wird mit S3-Protokoll gescannt

Führen Sie ein paar Schritte durch und starten Sie das Scannen von Daten innerhalb von Objekt-Storage direkt mit der BlueXP Klassifizierung. Die BlueXP Klassifizierung kann Daten von jedem beliebigen Objekt-Storage-Service scannen, der das S3-Protokoll (Simple Storage Service) verwendet. Dazu zählen NetApp StorageGRID, IBM Cloud Object Store, Linode, B2 Cloud Storage, Amazon S3 und vieles mehr.

Schnellstart

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

1. **Prüfen Sie die Voraussetzungen für den Objekt-Storage**

Es muss die Endpunkt-URL vorhanden sein, um eine Verbindung mit dem Objekt-Storage-Service herzustellen.

Sie müssen den Zugriffsschlüssel und den geheimen Schlüssel vom Objekt-Storage-Provider besitzen, damit die BlueXP Klassifizierung auf die Buckets zugreifen kann.

2. **Implementieren der BlueXP Klassifizierungsinstanz**

"Implementieren Sie die BlueXP Klassifizierung" Falls noch keine Instanz implementiert wurde.

3. **Fügen Sie den Objekt-Storage-Service hinzu**

Fügen Sie den Objekt-Storage-Service zur BlueXP Klassifizierung hinzu.

4. **Wählen Sie die zu scannenden Buckets aus**

Wählen Sie die Buckets aus, die Sie scannen möchten. Die BlueXP Klassifizierung beginnt mit dem Scannen.

Überprüfung der Objekt-Storage-Anforderungen

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

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

Implementieren der BlueXP Klassifizierungsinstanz

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

Wenn Sie Daten aus dem S3-Objektspeicher scannen, auf den über das Internet zugegriffen werden kann, ist die entsprechende Möglichkeit möglich "Implementieren Sie die BlueXP Klassifizierung in der Cloud" Oder "Implementieren Sie die BlueXP Klassifizierung an einem lokalen Standort mit Internetzugang".

Wenn Sie Daten vom S3 Objekt-Storage scannen, der auf einem dunklen Standort ohne Internetzugang installiert wurde, müssen Sie sie überprüfen "Implementieren Sie die BlueXP Klassifizierung an demselben lokalen Standort ohne Internetzugang". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

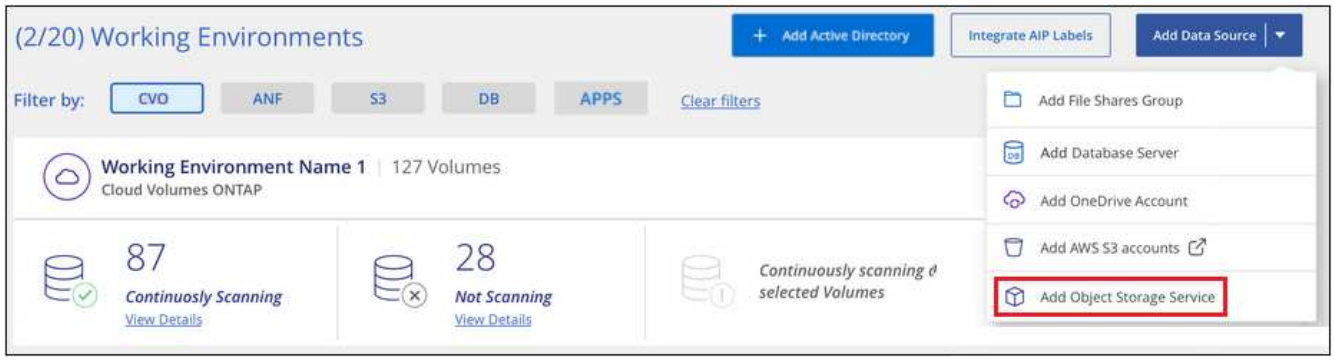
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des Objekt-Storage-Service zur BlueXP Klassifizierung

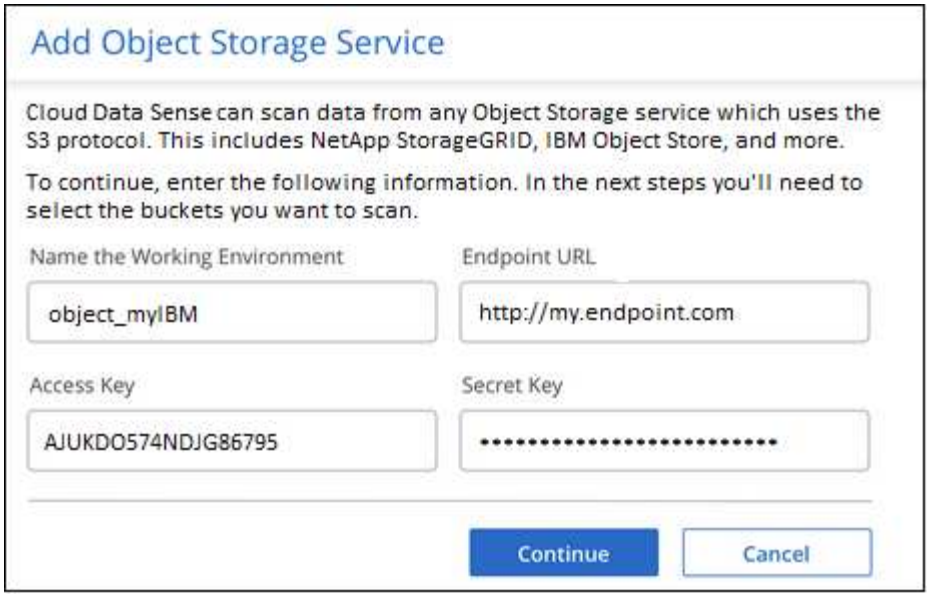
Fügen Sie den Objekt-Storage-Service hinzu.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen Konfiguration auf **Datenquelle hinzufügen** > **Objekt-Storage-Service hinzufügen**.



2. Geben Sie im Dialogfeld Add Object Storage Service die Details für den Objekt-Speicherdienst ein und klicken Sie auf **Continue**.
   a. Geben Sie den Namen ein, den Sie für die Arbeitsumgebung verwenden möchten. Dieser Name sollte den Namen des Objektspeicherdienstes widerspiegeln, mit dem Sie eine Verbindung herstellen.
   b. Geben Sie die Endpunkt-URL ein, um auf den Objekt-Storage-Service zuzugreifen.
   c. Geben Sie den Zugriffsschlüssel und den geheimen Schlüssel ein, damit die BlueXP Klassifizierung auf die Buckets im Objekt-Storage zugreifen kann.



Ergebnis

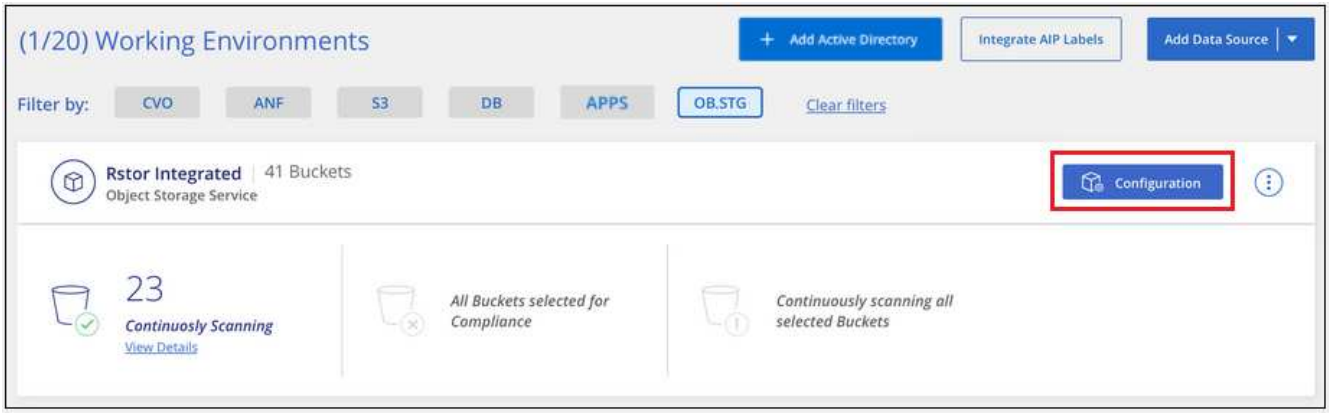
Der neue Objekt-Speicherdienst wird der Liste der Arbeitsumgebungen hinzugefügt.

Aktivieren und Deaktivieren von Compliance-Scans an Objekt-Storage-Buckets

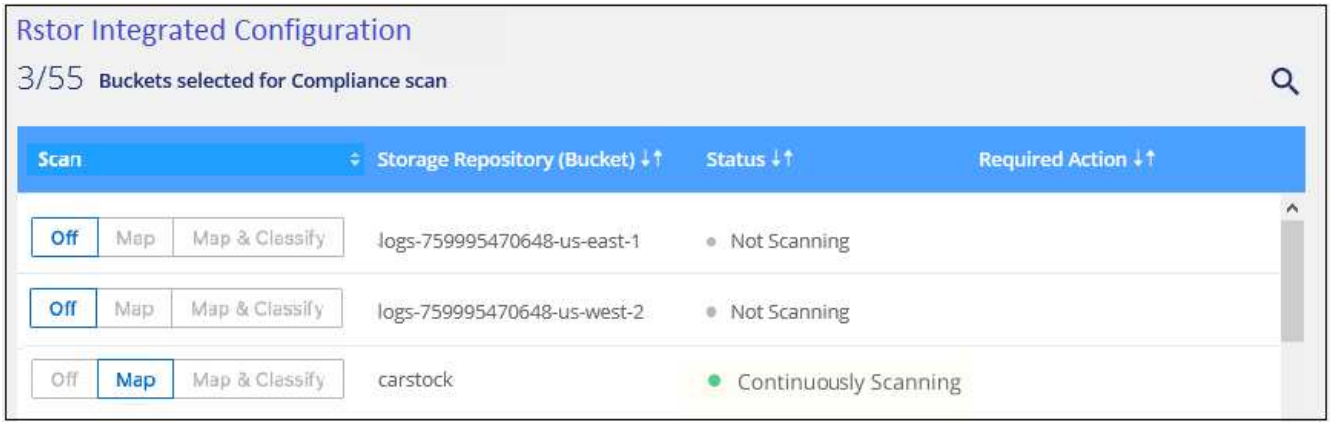
Nachdem Sie die BlueXP Klassifizierung für Ihren Objekt-Storage-Service aktiviert haben, müssen Sie im nächsten Schritt die Buckets konfigurieren, die Sie scannen möchten. Die BlueXP Klassifizierung erkennt diese Buckets und zeigt sie in der von Ihnen erstellten Arbeitsumgebung an.

Schritte

1. Klicken Sie auf der Konfigurationsseite in der Arbeitsumgebung Object Storage Service auf **Konfiguration**.



2. Aktivieren Sie Scans, die nur mappen oder Scans zuordnen und klassifizieren, auf Ihren Buckets.



An:	Tun Sie dies:
Ermöglichen Sie Mapping-Only-Scans auf einem Bucket	Klicken Sie Auf **Karte**
Aktivieren vollständiger Scans auf einem Bucket	Klicken Sie Auf **Karte & Klassieren**
Deaktivieren des Scans auf einem Bucket	Klicken Sie Auf **Aus**

Ergebnis

Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen aktivierten Buckets. Wenn Fehler auftreten, werden sie neben der erforderlichen Aktion zur Behebung des Fehlers in der Spalte Status angezeigt.

Integrieren Sie Active Directory in die BlueXP Klassifizierung

Sie können eine globale Active Directory-Klassifizierung mit BlueXP integrieren und so die Ergebnisse verbessern, die BlueXP Klassifizierungen von Dateieigentümern meldet und die Benutzer und Gruppen Zugriff auf Ihre Dateien haben.

Wenn Sie bestimmte (unten aufgeführte) Datenquellen einrichten, müssen Sie Active Directory-Anmeldeinformationen eingeben, um die BlueXP Klassifizierung zum Scannen von CIFS-Volumes zu ermöglichen. Diese Integration ermöglicht die Klassifizierung von BlueXP mit Angaben zu Dateieigentümerrechten und Berechtigungen für die Daten in diesen Datenquellen. Das für diese Datenquellen eingegebene Active Directory kann sich von den hier eingegebenen globalen Active Directory-Anmeldeinformationen unterscheiden. Die BlueXP Klassifizierung betrachtet in allen integrierten Active Directorys unter Angabe von Benutzer- und Berechtigungsdetails.

Diese Integration bietet zusätzliche Informationen an folgenden Standorten in der BlueXP Klassifizierung:

- Sie können den „Dateieigentümer“ verwenden. "Filtern" Und siehe die Ergebnisse in den Metadaten der Datei im Untersuchungsbereich. Anstelle des Dateieigentümers, der den SID (Security Identifier) enthält, wird er mit dem tatsächlichen Benutzernamen gefüllt.
- Sie sehen "Volldateiberechtigungen" Klicken Sie für jede Datei und jedes Verzeichnis auf die Schaltfläche „Alle Berechtigungen anzeigen“.
- Im "Governance-Dashboard", Das Fenster „Offene Berechtigungen“ zeigt eine größere Detailebene über Ihre Daten an.

Die SIDs des lokalen Benutzers und SIDs unbekannter Domänen werden nicht in den tatsächlichen Benutzernamen übersetzt.

Unterstützte Datenquellen

Durch eine Active Directory Integration mit BlueXP Klassifizierung können Daten aus den folgenden Datenquellen identifiziert werden:

- On-Premises ONTAP Systeme
- Cloud Volumes ONTAP
- Azure NetApp Dateien
- FSX für ONTAP
- CIFS-File-Shares von anderen Anbietern (keine NFS-File-Shares)
- OneDrive Accounts
- SharePoint Konten

Es wird keine Unterstützung für das Identifizieren von Benutzer- und Berechtigungsinformationen aus Datenbankschemas, Google Drive-Konten, Amazon S3-Konten oder Objekt-Storage mit dem S3-Protokoll (Simple Storage Service) angeboten.

Stellen Sie eine Verbindung zu Ihrem Active Directory-Server her

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

Die Active Directory-Zugangsdaten können schreibgeschützt sein, allerdings ist durch die Angabe von Administratorberechtigungen sichergestellt, dass die BlueXP Klassifizierung alle Daten lesen kann, die erhöhte Berechtigungen erfordern. Die Zugangsdaten werden in der BlueXP Klassifizierungsinstanz gespeichert.

Wenn Sie bei CIFS Volumes/Dateifreigaben sicherstellen möchten, dass Ihre Dateien durch BlueXP Klassifizierungs-Scans „zuletzt zugegriffen“ unverändert bleiben, empfehlen wir dem Benutzer die Berechtigung zum Schreiben von Attributen. Wenn möglich, empfehlen wir, den Active Directory-konfigurierten Benutzer in eine übergeordnete Gruppe in der Organisation mit Berechtigungen für alle Dateien zu integrieren.

Anforderungen

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

    Oder

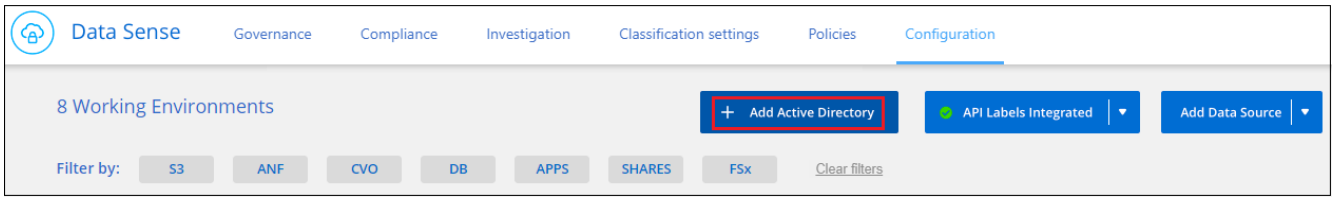
  LDAP-Server-IP-Adresse oder mehrere IP-Adressen
  - Benutzername und Kennwort für den Zugriff auf den Server
  - Domain-Name (Active Directory-Name)
  - Ob Sie Secure LDAP (LDAPS) verwenden oder nicht
  - LDAP-Server-Port (normalerweise 389 für LDAP und 636 für sicheres LDAP)

- Die folgenden Ports müssen für Outbound-Kommunikation durch die BlueXP Klassifizierungsinstanz offen sein:

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

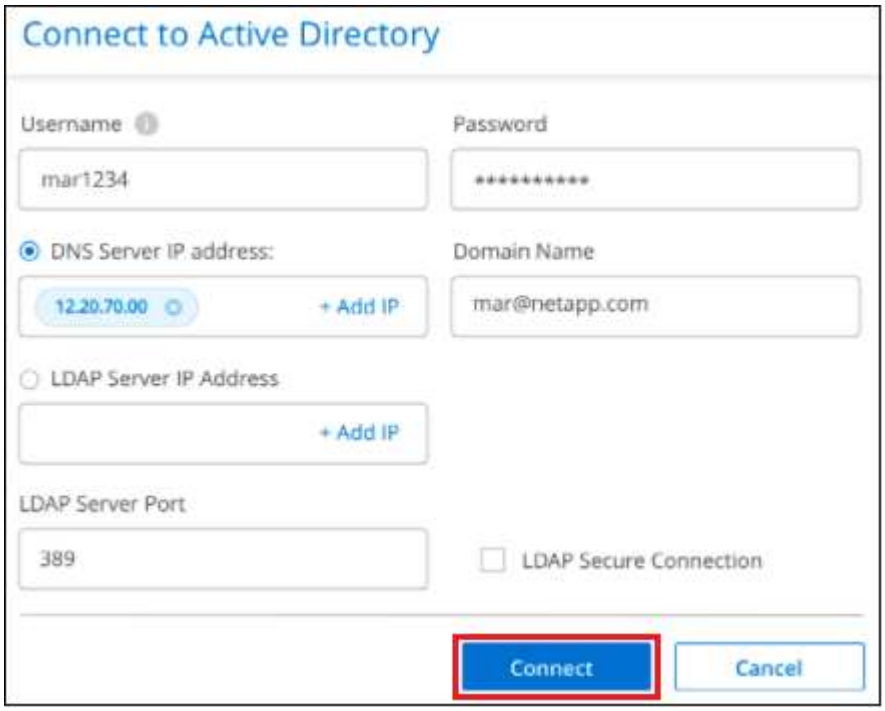
Schritte

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

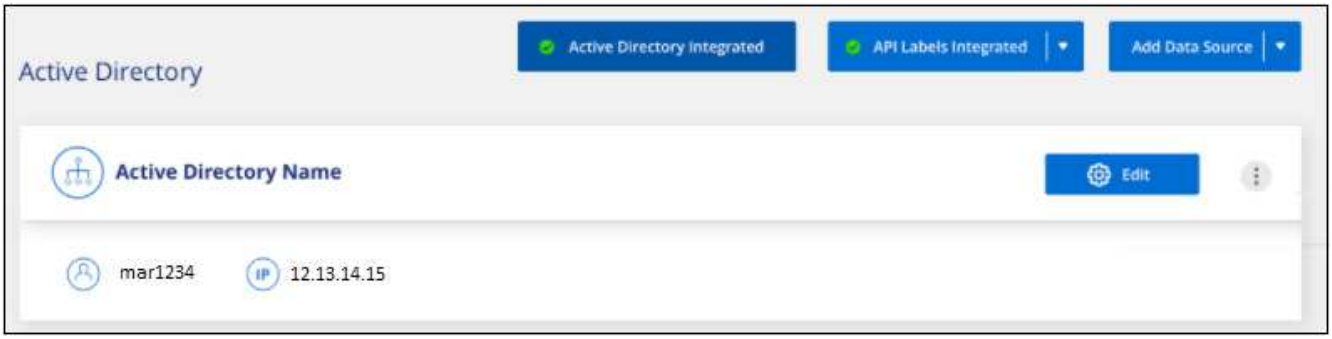


2. Geben Sie im Dialogfeld mit Active Directory verbinden die Active Directory-Details ein, und klicken Sie auf **Verbinden**.

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



   Die BlueXP Klassifizierung wird in Active Directory integriert. Anschließend wird der Konfigurationsseite ein neuer Abschnitt hinzugefügt.



Verwalten Sie Ihre Active Directory-Integration

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

Sie können die Integration auch löschen, wenn Sie sie nicht mehr benötigen, indem Sie auf die klicken Und dann **Active Directory entfernen**.

Lizenzierung für die BlueXP Klassifizierung einrichten

Die ersten 1 TB an Daten, die die BlueXP Klassifizierung in einem BlueXP Workspace scannt, sind 30 Tage lang kostenlos. Für den weiteren Scan der Daten ist eine BYOL-Lizenz von NetApp oder ein Abonnement vom Marketplace Ihres Cloud-Providers erforderlich.

Ein paar Notizen, bevor Sie weitere lesen:

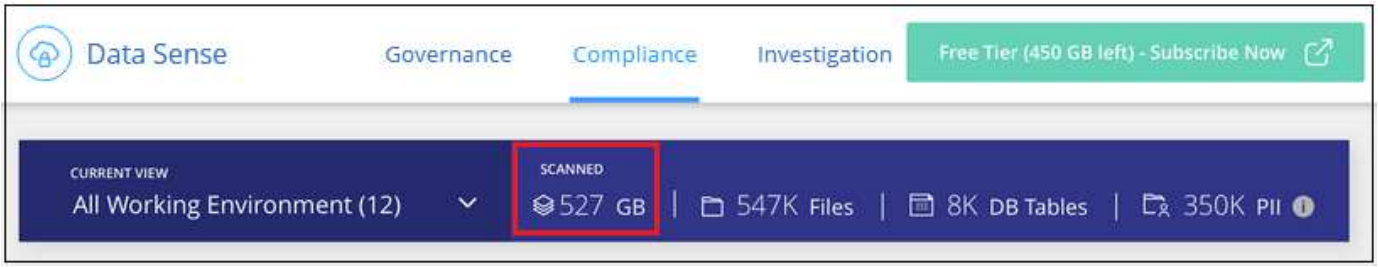
- Wenn Sie bereits das PAYGO-Abonnement (Pay-as-you-go) von BlueXP auf dem Marketplace Ihres Cloud-Providers abonniert haben, haben Sie auch die BlueXP Klassifizierung automatisch abonniert. Sie müssen sich nicht erneut anmelden.
- Die BlueXP Klassifizierung (Data Sense) von Bring-Your-Own-License (BYOL) ist eine Floating Lizenz, die Sie in allen Arbeitsumgebungen und Datenquellen des Workspace verwenden können, den Sie scannen möchten. Das Digital Wallet von BlueXP enthält ein aktives Abonnement.
- Die Datenmenge, die gescannt wird, basiert auf logischer Dateigröße, ohne Storage-Effizienz.

"Informieren Sie sich über die Lizenzierung und die Kosten der BlueXP Klassifizierung".

30 Tage kostenlos testen mit unserer

Es ist eine kostenlose 30-Tage-Testversion für bis zu 1 TB Daten verfügbar, die BlueXP Klassifizierung in einer BlueXP Umgebung scannt. Sie müssen eine BYOL-Lizenz von NetApp erwerben oder sich über den Marketplace Ihres Cloud-Providers für ein Abonnement anmelden, um nach diesem Zeitpunkt mit dem Scannen von Daten fortzufahren.

Sie können sich jederzeit anmelden und zahlen erst nach Ablauf der 30-Tage-Testsoftware oder nach mehr als 1 TB. Über das BlueXP Classification Governance Dashboard wird immer die Gesamtmenge der gescannten Daten angezeigt. Und die Schaltfläche *Jetzt abonnieren* erleichtert die Anmeldung, wenn Sie bereit sind.



Nutzen Sie ein PAYGO-Abonnement für die BlueXP Klassifizierung

Dank Pay-as-you-go-Abonnements über den Marketplace Ihres Cloud-Providers können Sie die Nutzung von Cloud Volumes ONTAP Systemen und vielen BlueXP Services lizenzieren, wie z. B. die BlueXP Klassifizierung. Sie bezahlen bei Ihrem Cloud-Provider den Umfang der Daten, die die BlueXP Klassifizierung überprüft, stündlich in einem einzelnen Abonnement.

Durch die Anmeldung wird sichergestellt, dass nach der kostenlosen Testversion keine Serviceunterbrechung erfolgt. Wenn die Testversion endet, werden Sie stündlich entsprechend der Menge der Daten, die Sie scannen, berechnet. Während der kostenlosen Testversion werden Ihnen keine Gebühren für Ihr Abonnement berechnet.

Schritte

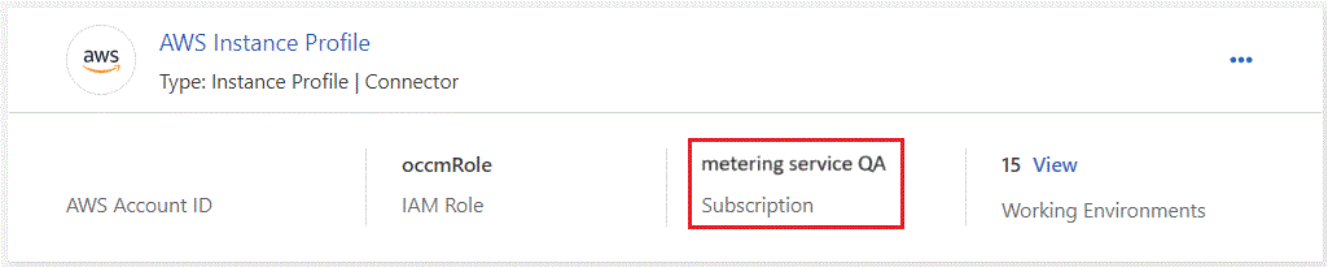
Diese Schritte müssen von einem Benutzer ausgeführt werden, der über die Rolle *Account Admin* verfügt.

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.

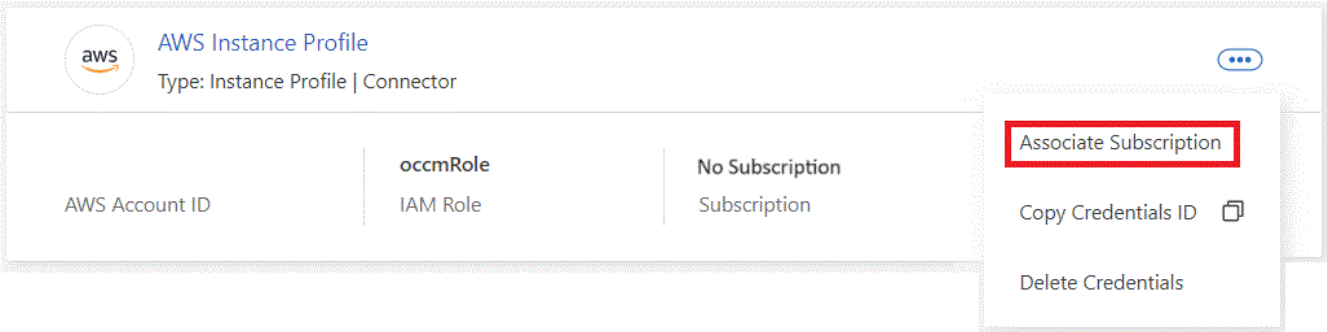
2. Klicken Sie auf **Credentials** und suchen Sie dann die Zugangsdaten für das AWS Instance Profile, Azure Managed Service Identity oder Google Project.

   Das Abonnement muss dem Instanzprofil, der Managed Service Identity oder dem Google Project hinzugefügt werden. Das Laden funktioniert nicht anders.

   Wenn Sie bereits über ein BlueXP Abonnement verfügen (wie unten für AWS dargestellt), haben Sie alle erforderlichen Schritte zur Auswahl. Außerdem brauchen Sie nichts anderes zu tun.



3. Wenn Sie noch kein Abonnement haben, klicken Sie auf das Aktionsmenü und dann auf **Associate Subscription**.



4. Wählen Sie ein vorhandenes Abonnement aus und klicken Sie auf **Associate**, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte.

   Das folgende Video zeigt, wie ein zugeordnet werden soll "AWS Marketplace" Abonnement eines AWS Abonnements:

   ► https://docs.netapp.com/de-de/bluexp-classification//media/video_subscribing_aws.mp4 *(video)*

   Das folgende Video zeigt, wie ein zugeordnet werden soll "Azure Marketplace" Abonnement eines Azure Abonnements:

   ► https://docs.netapp.com/de-de/bluexp-classification//media/video_subscribing_azure.mp4 *(video)*

   Das folgende Video zeigt, wie ein zugeordnet werden soll "Google Cloud Marketplace" Abonnement eines GCP-Abonnements:

   ► https://docs.netapp.com/de-de/bluexp-classification//media/video_subscribing_gcp.mp4 *(video)*

Verwenden Sie einen Jahresvertrag

Bezahlen Sie die BlueXP Klassifizierung jährlich durch den Erwerb eines Jahresvertrags. Das Angebot ist mit Laufzeiten von 1, 2 oder 3 Jahren erhältlich.

Wenn Sie einen Jahresvertrag von einem Markt haben, wird das gesamte Scannen von BlueXP Klassifizierungsdaten mit diesem Vertrag in Rechnung gestellt. Es ist nicht möglich, einen jährlichen Marktvertrag mit einem BYOL-Modell zu kombinieren.

- AWS, "Weitere Informationen zu Preisen finden Sie im BlueXP Marketplace Angebot".
- Azure: "Weitere Informationen zu Preisen finden Sie im BlueXP Marketplace Angebot".
- Google Cloud: Wenden Sie sich an Ihren NetApp Ansprechpartner, um einen Jahresvertrag zu erwerben. Der Vertrag ist als Privatangebot im Google Cloud Marketplace erhältlich. Nachdem NetApp das private Angebot an Sie weitergibt, können Sie den Jahresplan auswählen, wenn Sie während der Aktivierung der BlueXP Klassifizierung im Google Cloud Marketplace abonnieren.

Verwenden Sie eine BYOL-Lizenz für die BlueXP Klassifizierung

Mit den Bring-Your-Own-License-Lizenzen von NetApp erhalten Sie Vertragsbedingungen mit 1, 2 oder 3 Jahren. Die BYOL BlueXP Klassifizierungs- (Data Sense)-Lizenz ist eine Floating_-Lizenz, bei der die Gesamtkapazität von allen Arbeitsumgebungen und Datenquellen gemeinsam genutzt wird. Dies vereinfacht die erstmalige Lizenzierung und Verlängerung.

Wenn Sie keine BlueXP Klassifizierungslizenz haben, wenden Sie sich an uns, um eine zu erwerben:

- Mailto:ng-contact-data-sense@netapp.com?Subject=Lizenzierung[E-Mail senden, um eine Lizenz zu erwerben].
- Klicken Sie rechts unten auf das Chat-Symbol von BlueXP, um eine Lizenz anzufordern.

Wenn Sie optional eine nicht zugewiesene Node-basierte Lizenz für Cloud Volumes ONTAP haben, die Sie nicht verwenden werden, können Sie sie in eine BlueXP Klassifizierungslizenz mit derselben Dollar-Äquivalenz und demselben Ablaufdatum konvertieren. "Weitere Informationen finden Sie hier".

Sie nutzen das Digital Wallet von BlueXP, um die BYOL-Lizenzen der BlueXP Klassifizierung zu managen. Sie können über das BlueXP Digital Wallet neue Lizenzen hinzufügen, vorhandene Lizenzen aktualisieren und den Lizenzstatus einsehen.

Rufen Sie die BlueXP Klassifizierungs-Lizenzdatei ab

Nachdem Sie Ihre BlueXP Klassifizierungs- (Data Sense) Lizenz erworben haben, aktivieren Sie die Lizenz in BlueXP, indem Sie die BlueXP Klassifizierungs-Seriennummer und das NetApp NSS-Konto eingeben oder die NetApp Lizenzdatei hochladen. Die folgenden Schritte zeigen, wie Sie die Lizenzdatei NLF abrufen können, wenn Sie diese Methode verwenden möchten.

Wenn Sie die BlueXP Klassifizierung auf einem Host an einem lokalen Standort ohne Internetzugang implementiert haben, d. h., Sie haben den BlueXP Connector in implementiert "Privater Modus", Sie müssen die Lizenzdatei von einem mit dem Internet verbundenen System beziehen. Die Aktivierung der Lizenz unter Verwendung der Seriennummer und des NSS-Kontos ist für Installationen im Privatmodus nicht verfügbar.

Bevor Sie beginnen

Sie müssen die folgenden Informationen haben, bevor Sie beginnen:

- Seriennummer der BlueXP Klassifizierung

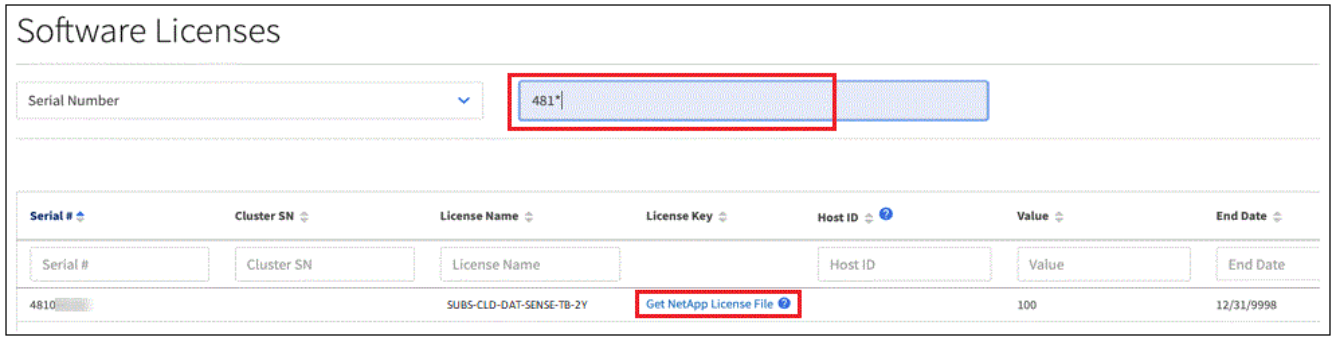
  Suchen Sie diese Nummer in Ihrem Auftrag, oder wenden Sie sich an das Account Team, um diese Informationen zu erhalten.

- BlueXP Konto-ID

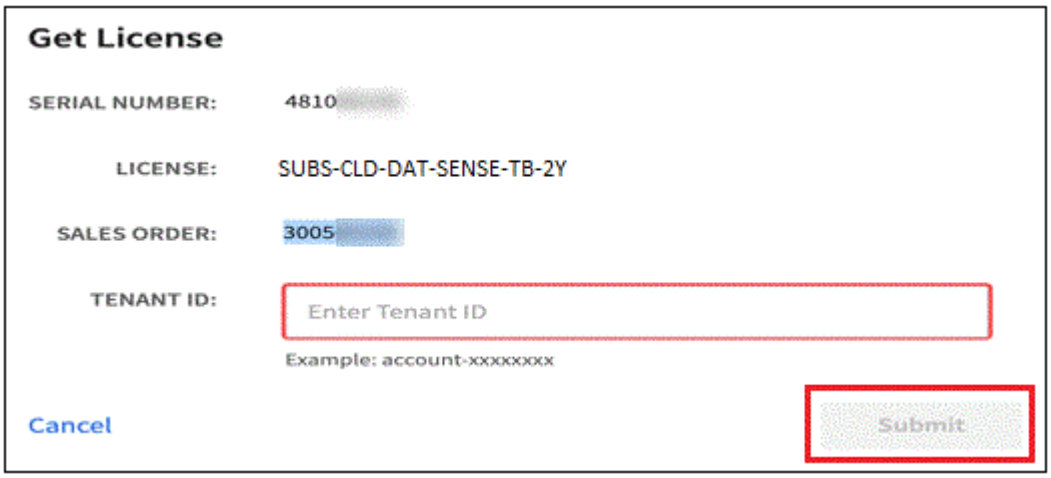
  Sie können Ihre BlueXP-Konto-ID finden, indem Sie oben in BlueXP das Dropdown-Menü **Konto** auswählen und dann neben Ihrem Konto auf **Konto verwalten** klicken. Ihre Account-ID wird auf der Registerkarte „Übersicht“ angezeigt. Verwenden Sie für Websites im privaten Modus ohne Internetzugang **Account-DARKSITE1**.

Schritte

1. Melden Sie sich beim an "NetApp Support Website" Klicken Sie anschließend auf **Systeme > Softwarelizenzen**.
2. Geben Sie die Seriennummer Ihrer BlueXP Klassifizierungs-Lizenz ein.



3. Klicken Sie in der Spalte **Lizenzschlüssel** auf **NetApp-Lizenzdatei abrufen**.
4. Geben Sie Ihre BlueXP-Konto-ID ein (dies wird als Mandanten-ID auf der Support-Website bezeichnet) und klicken Sie auf **Absenden**, um die Lizenzdatei herunterzuladen.



Fügen Sie Ihrem Konto BYOL-Lizenzen für die BlueXP Klassifizierung hinzu

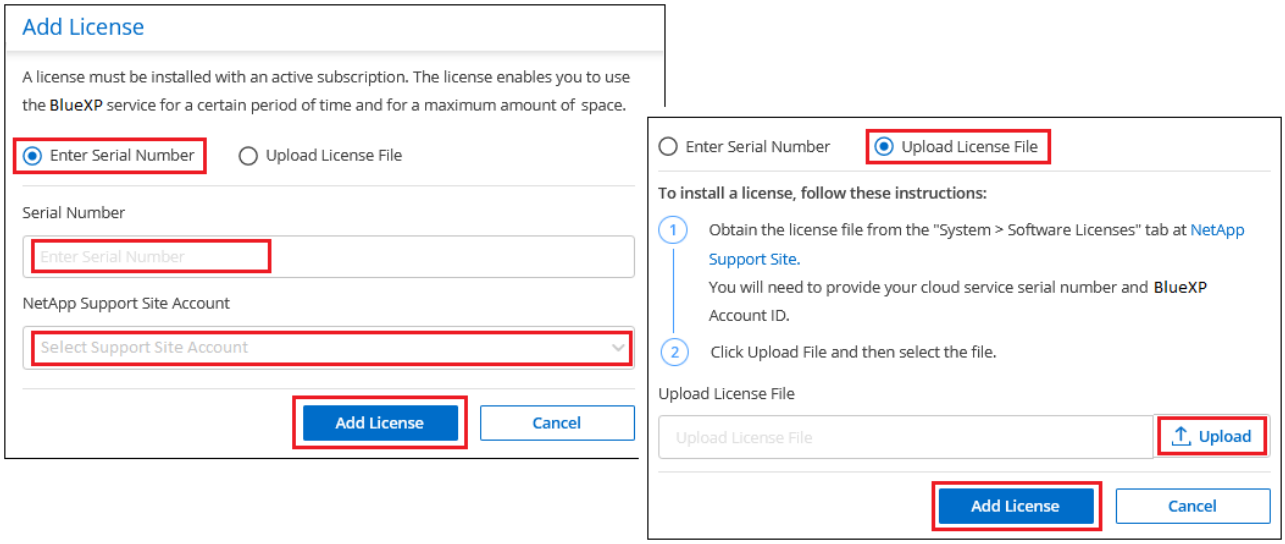
Nachdem Sie eine BlueXP Klassifizierungs-Lizenz (Data Sense) für Ihr BlueXP Konto erworben haben, müssen Sie die Lizenz zu BlueXP hinzufügen, um den BlueXP Klassifizierungsservice nutzen zu können.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Digital Wallet** und wählen Sie dann die Registerkarte **Data Services Licenses** aus.
2. Klicken Sie Auf **Lizenz Hinzufügen**.
3. Geben Sie im Dialogfeld „*Lizenz hinzufügen*“ die Lizenzinformationen ein, und klicken Sie auf **Lizenz hinzufügen**:
   - Wenn Sie die Seriennummer der BlueXP Klassifizierungslizenz haben und Ihr NSS-Konto kennen, wählen Sie die Option **Seriennummer eingeben** aus und geben Sie diese Information ein.

     Wenn Ihr NetApp Support Site Konto nicht in der Dropdown-Liste verfügbar ist, "Fügen Sie das NSS-Konto zu BlueXP hinzu".

   - Wenn Sie über die BlueXP-Klassifizierungslizenzdatei verfügen (erforderlich bei Installation auf einer dunklen Seite), wählen Sie die Option **Lizenzdatei hochladen** aus und folgen Sie den Anweisungen zum Anhängen der Datei.



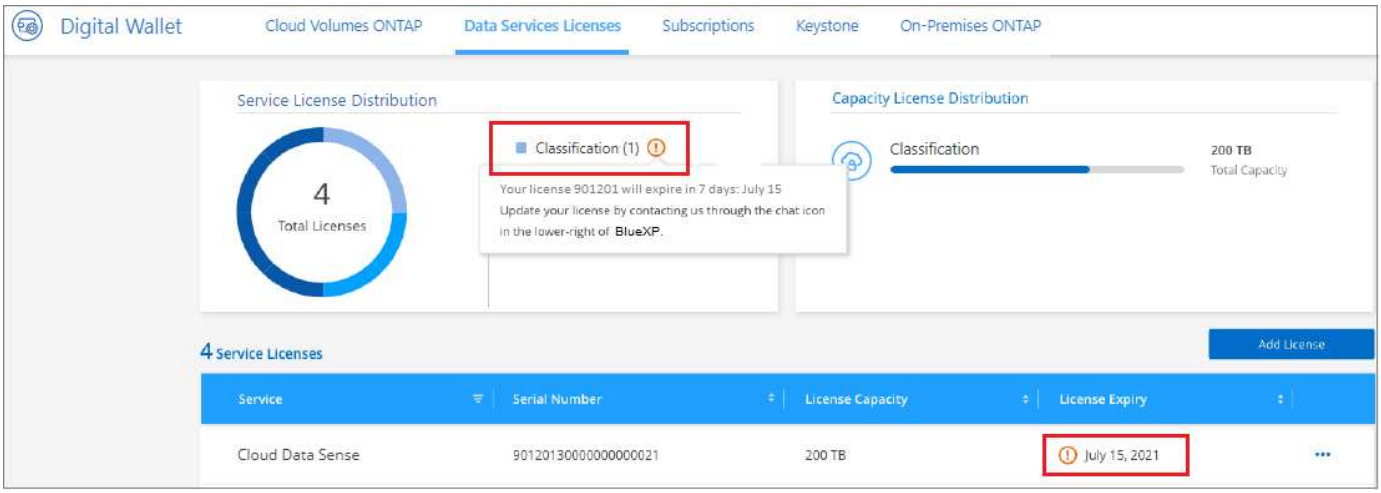
Ergebnis

BlueXP fügt die Lizenz hinzu, sodass Ihr BlueXP Klassifizierungsservice aktiv ist.

Aktualisieren einer BlueXP Klassifizierungs-BYOL-Lizenz

Wenn die Lizenzlaufzeit kurz vor dem Ablaufdatum steht oder die lizenzierte Kapazität das Limit erreicht, werden Sie über die Benutzeroberfläche „Klassifizierung“ benachrichtigt.

Dieser Status wird auch im Digital Wallet von BlueXP und in angezeigt "Benachrichtigungen".



Sie können Ihre BlueXP Klassifizierungslizenz bereits vor ihrem Ablauf aktualisieren, damit der Zugriff auf die gescannten Daten nicht unterbrochen wird.

Schritte

1. Klicken Sie auf das Chat-Symbol rechts unten bei BlueXP, um eine Erweiterung Ihres Termins oder zusätzliche Kapazität für Ihre Cloud Data Sense Lizenz für die jeweilige Seriennummer anzufordern. Sie können auch Senden Sie eine E-Mail.

Nachdem Sie für die Lizenz bezahlt und sie auf der NetApp Support-Website registriert ist, aktualisiert BlueXP automatisch die Lizenz im Digital Wallet von BlueXP. Auf der Seite „Data Services Licenses“ wird die Änderung in 5 bis 10 Minuten dargestellt.

2. Wenn BlueXP die Lizenz nicht automatisch aktualisieren kann (z. B. wenn sie auf einer dunklen Website installiert ist), müssen Sie die Lizenzdatei manuell hochladen.
   a. Das können Sie Beziehen Sie die Lizenzdatei über die NetApp Support-Website.
   b. Klicken Sie auf der Seite BlueXP Digital Wallet auf der Registerkarte *Data Services Licenses* auf ••• Klicken Sie für die Serviceseriennummer, die Sie aktualisieren, auf **Lizenz aktualisieren**.

   c. Laden Sie auf der Seite *Update License* die Lizenzdatei hoch und klicken Sie auf **Update License**.

Ergebnis

BlueXP aktualisiert die Lizenz, sodass Ihr BlueXP Klassifizierungsservice weiterhin aktiv ist.

Überlegungen zu BYOL-Lizenzen

Wenn Sie eine BlueXP Klassifizierungs-Lizenz (Data Sense) von BYOL verwenden, zeigt BlueXP in der BlueXP Klassifizierungs-UI und in der BlueXP Digital-Wallet-UI eine Warnung an, wenn die Größe aller gescannten Daten dem Kapazitätslimit nähert oder dem Ablaufdatum der Lizenz nähert. Sie erhalten folgende Warnungen:

- Wenn die Menge der Daten, die Sie scannen, erreicht hat 80% der lizenzierten Kapazität, und wieder, wenn Sie das Limit erreicht haben
- 30 Tage, bevor eine Lizenz abläuft, und wieder, wenn die Lizenz abläuft

Verwenden Sie das Chat-Symbol rechts unten in der BlueXP-Schnittstelle, um Ihre Lizenz zu verlängern, wenn diese Warnungen angezeigt werden.

Wenn Ihre Lizenz abläuft oder Sie das BYOL-Limit erreicht haben, wird die BlueXP Klassifizierung weiterhin ausgeführt, der Zugriff auf die Dashboards ist jedoch gesperrt, sodass Sie Informationen zu Ihren gescannten Daten nicht mehr anzeigen können. Nur die Seite *Configuration* steht zur Verfügung, wenn Sie die Anzahl der eingescannten Volumes reduzieren möchten, um die Kapazitätsnutzung unter das Lizenzlimit zu bringen.

Sobald Sie Ihre BYOL-Lizenz erneuern, aktualisiert BlueXP automatisch die Lizenz im Digital Wallet von BlueXP und bietet vollständigen Zugriff auf alle Dashboards. Wenn BlueXP nicht über die sichere Internetverbindung auf die Lizenzdatei zugreifen kann (z. B. bei Installation in einer dunklen Site), können Sie die Datei selbst beziehen und sie manuell auf BlueXP hochladen. Anweisungen hierzu finden Sie unter Aktualisieren einer BlueXP Klassifizierungslizenz.

Wenn für das von Ihnen verwendete Konto sowohl eine BYOL-Lizenz als auch ein PAYGO-Abonnement besteht, wird die BlueXP Klassifizierung *nicht* in das PAYGO-Abonnement verschieben, wenn die BYOL-Lizenz abläuft. Sie müssen die BYOL-Lizenz verlängern.

Häufig gestellte Fragen zur BlueXP Klassifizierung

Diese FAQ kann Ihnen helfen, wenn Sie nur nach einer schnellen Antwort auf eine Frage suchen.

BlueXP Klassifizierungsservice

Die folgenden Fragen bieten ein allgemeines Verständnis der BlueXP Klassifizierung.

Was ist die BlueXP Klassifizierung?

Die BlueXP Klassifizierung ist ein Cloud-Angebot, das auf KI-gestützter Technologie (künstliche Intelligenz) setzt, um den Datenkontext zu verstehen und sensible Daten in Ihren Storage-Systemen zu identifizieren. Bei den Systemen kann es sich um Arbeitsumgebungen handelt, die Sie in BlueXP Canvas hinzugefügt haben, sowie um viele Arten von Datenquellen, auf die BlueXP-Klassifizierung über Ihre Netzwerke zugreifen kann. "Die vollständige Liste finden Sie unten".

Die BlueXP Klassifizierung bietet vordefinierte Parameter (z. B. Arten von sensiblen Daten und Kategorien), um neue Daten-Compliance-Vorschriften für Datenschutz und -Sensibilität zu erfüllen, beispielsweise die DSGVO, CCPA oder HIPAA.

Wie funktioniert die BlueXP Klassifizierung?

Die BlueXP Klassifizierung implementiert eine weitere Schicht aus künstlicher Intelligenz zusammen mit Ihrem BlueXP System und Ihren Storage-Systemen. Anschließend werden die Daten auf Volumes, Buckets, Datenbanken und anderen Storage-Konten überprüft und die gefundenen Dateneinblicke indiziert. Die BlueXP Klassifizierung nutzt sowohl künstliche Intelligenz als auch natürliche Sprachverarbeitung, im Gegensatz zu alternativen Lösungen, die häufig auf regulären Ausdrücken und Mustervergleichen basieren.

Die BlueXP Klassifizierung verwendet KI, um ein kontextbezogenes Verständnis der Daten für eine genaue Erkennung und Klassifizierung zu ermöglichen. Der Fokus liegt auf KI, da sie für moderne Datentypen und Skalierungen konzipiert wurde. Er versteht auch den Datenkontext und sorgt so für starke, präzise, Erkennungs- und Klassifizierungsmöglichkeiten.

"Erfahren Sie mehr über die BlueXP Klassifizierung".

Was sind die gängigsten Anwendungsfälle für die BlueXP Klassifizierung?

- Ermitteln von personenbezogenen Daten
- Das Auffinden und Reporting von Daten zu bestimmten Daten als Antwort auf Betroffene kann ganz nach Bedarf auf DSGVO, CCPA, HIPAA und anderen Datenschutzvorschriften erfolgen.
- Einhaltung neuer und anstehender Datenschutzvorschriften
- Einhaltung von Daten-Compliance- und Datenschutzvorschriften
- Migrieren von Daten von Legacy-Systemen zur Cloud
- Einhaltung von Richtlinien zur Datenaufbewahrung.

"Weitere Informationen zu Anwendungsfällen für die BlueXP Klassifizierung".

Wie sieht es mit der Architektur der BlueXP Klassifizierung aus?

Die BlueXP Klassifizierung implementiert einen einzelnen Server oder Cluster unabhängig von Ihrer Wahl – in der Cloud oder lokal. Die Server verbinden sich über Standardprotokolle mit den Datenquellen und indizieren die Ergebnisse in einem Elasticsearch-Cluster, der ebenfalls auf denselben Servern implementiert wird. Dies ermöglicht die Unterstützung sowohl für Cloud-übergreifende Umgebungen als auch für Private-Cloud- und On-Premises-Umgebungen.

Welche Cloud-Provider werden unterstützt?

Die BlueXP Klassifizierung erfolgt als Teil von BlueXP und unterstützt AWS, Azure und GCP. Dadurch erhält Ihr Unternehmen Transparenz im Hinblick auf den Datenschutz bei verschiedenen Cloud-Providern.

Verfügt die BlueXP Klassifizierung über EINE REST-API, die auch mit Tools von Drittanbietern funktioniert?

BlueXP unterstützt REST-API-Funktionen für seine Services. Wenn BlueXP nicht der bevorzugte Managementpunkt ist, können Services wie die BlueXP Klassifizierung auch über eine REST-API genutzt werden. Jede Benutzeraktion hat eine REST-API, die in Systeme von Drittanbietern integriert werden kann. Siehe "BlueXP Klassifizierungs-APIs" Entsprechende Details.

Ist die BlueXP Klassifizierung über die Marktplätze verfügbar?

Ja, die Klassifizierung von BlueXP und BlueXP kann auf den AWS, Azure und GCP Marketplace abgerufen werden.

BlueXP Klassifizierungsscan und -Analysen

Die folgenden Fragen beziehen sich auf die Scan-Performance der BlueXP Klassifizierung sowie auf die für Anwender verfügbaren Analysen.

Wie oft werden meine Daten durch die BlueXP Klassifizierung gescannt?

Während der erste Scan Ihrer Daten etwas Zeit in Anspruch nehmen kann, untersuchen nachfolgende Scans nur die inkrementellen Änderungen, was die Systemscanzeiten verkürzt. Die BlueXP Klassifizierung scannt Ihre Daten kontinuierlich nach Round Robin-Verfahren und bietet Ihnen sechs Repositorys gleichzeitig, sodass alle geänderten Daten sehr schnell klassifiziert werden.

"Lesen Sie, wie Scans funktionieren".

Beachten Sie, dass die BlueXP Klassifizierung Datenbanken nur einmal pro Tag scannt – Datenbanken werden nicht wie andere Datenquellen fortlaufend gescannt.

Datenscans haben keine nennenswerten Auswirkungen auf Ihre Storage-Systeme und Ihre Daten. Wenn Sie jedoch auch nur geringe Auswirkungen haben, können Sie die BlueXP-Klassifizierung für „langsame“ Scans konfigurieren. "Erfahren Sie, wie Sie die Scangeschwindigkeit verringern".

Kann ich meine Daten mithilfe der BlueXP Klassifizierung durchsuchen?

Die BlueXP Klassifizierung bietet umfangreiche Suchfunktionen, die das Suchen nach einer bestimmten Datei oder einem Datenelement über alle verbundenen Quellen hinweg erleichtern. Die BlueXP Klassifizierung ermöglicht Benutzern eine umfassendere Suche als nur die Inhalte der Metadaten. Es ist ein sprachunabhängiger Dienst, der auch die Dateien lesen und eine Vielzahl sensibler Datentypen, wie Namen

und IDs, analysieren kann. So können Benutzer beispielsweise sowohl strukturierte als auch unstrukturierte Datenspeicher durchsuchen, um Daten zu finden, die von Datenbanken bis zu Benutzerdateien ausgetreten sind, und dies unter Verletzung von Unternehmensrichtlinien. Suchvorgänge können für einen späteren Zeitpunkt gespeichert werden. Richtlinien können erstellt werden, um die Ergebnisse zu einer festgelegten Häufigkeit zu suchen und entsprechend zu reagieren.

Sobald die entsprechenden Dateien gefunden wurden, können die Merkmale aufgelistet werden, einschließlich Tags, Konto der Arbeitsumgebung, Bucket, Dateipfad Kategorie (aus Klassifizierung), Dateigröße, letzte Änderung, Berechtigungsstatus, Duplikate, Empfindlichkeitsstufe, persönliche Daten, sensible Datentypen innerhalb der Datei, Eigentümer, Dateityp, Dateigröße, Erstellungszeit, Datei-Hash, unabhängig davon, ob die Daten einer Person zugewiesen wurden, die ihre Aufmerksamkeit sucht, und vieles mehr. Filter können auf Merkmale angewendet werden, die nicht relevant sind. Die BlueXP Klassifizierung verfügt außerdem über RBAC-Kontrollen. Damit können Dateien verschoben oder gelöscht werden, sofern entsprechende Berechtigungen vorhanden sind. Wenn die richtigen Berechtigungen nicht vorhanden sind, können die Aufgaben einer Person in der Organisation zugewiesen werden, die über die entsprechenden Berechtigungen verfügt.

Welche Art von Analysen bietet die BlueXP Klassifizierung?

Datenquellen können visuell dargestellt und Beziehungen definiert und grafisch dargestellt werden. Administratoren können beispielsweise alle veralteten, doppelten und nicht geschäftsbezogenen Daten aus allen Datenquellen im gesamten Unternehmen sehen (On-Premises-Systeme, Datenbanken, Dateifreigaben, S3-Speicher, OneDrive, Usw.). Anschließend können sie Daten kopieren, verschieben, löschen und managen, um so die Storage-Kosten zu optimieren und Risiken zu minimieren. Benutzer können Risiken minimieren, indem sie erkennen, welche sensitiven Daten offengelegt werden können. Sie können zudem Jobs zum Management der Berechtigungen für eine starke Datensicherung erstellen. Durch die BlueXP Klassifizierung werden auch alle verschiedenen Datentypen klassifiziert, sodass Administratoren Daten nach Typ untersuchen und sehen können, welche Aktionen wann an den Daten ausgeführt wurden.

Bietet die BlueXP Klassifizierung Berichte?

Ja. Die durch die Klassifizierung von BlueXP angebotenen Informationen können für andere Beteiligte in Ihrem Unternehmen relevant sein. Deshalb ermöglichen wir Ihnen die Erstellung von Berichten und die damit verbundene Nutzung. Die folgenden Berichte sind für die BlueXP Klassifizierung verfügbar:

Datenschutzrisiko-Assessment-Bericht

Bietet Einblicke in den Datenschutz und eine Bewertung des Datenschutzrisikos. "Weitere Informationen .".

Bericht für Anforderung von Datenfachzugriff

Ermöglicht Ihnen, einen Bericht aller Dateien zu extrahieren, die Informationen über den spezifischen Namen oder die persönliche Kennung eines Betroffenen enthalten. "Weitere Informationen .".

PCI DSS-Bericht

Unterstützt Sie bei der Identifizierung der Verteilung von Kreditkarteninformationen über Ihre Dateien. "Weitere Informationen .".

HIPAA-Bericht

Hilft Ihnen dabei, die Verteilung von Gesundheitsinformationen über Ihre Dateien hinweg zu identifizieren. "Weitere Informationen .".

Datenzuordnungsbericht

Stellt Informationen zur Größe und Anzahl der Dateien in Ihren Arbeitsumgebungen bereit. Dazu zählen Nutzungskapazität, Alter der Daten, Größe der Daten und Dateitypen. "Weitere Informationen .".

Data Discovery Assessment-Bericht

Bietet eine allgemeine Analyse der gescannten Umgebung, um die Ergebnisse des Systems hervorzuheben und Problembereiche und mögliche Schritte zur Problembehebung aufzuzeigen. "Lernmodus".

Berichte zu einem bestimmten Informationstyp

Es stehen Berichte zur Verfügung, die Details zu den identifizierten Dateien enthalten, die personenbezogene Daten und sensible personenbezogene Daten enthalten. Sie können auch Dateien nach Kategorie und Dateityp aufgeschlüsselt sehen. "Weitere Informationen .".

Ist die Scanleistung unterschiedlich?

Die Scan-Performance kann je nach Netzwerkbandbreite und durchschnittlicher Dateigröße in der Umgebung variieren. Es kann auch von der Größe des Host-Systems abhängen (entweder in der Cloud oder lokal). Siehe "Die BlueXP Klassifizierungsinstanz" Und "Implementieren der BlueXP Klassifizierung" Finden Sie weitere Informationen.

Beim ersten Hinzufügen neuer Datenquellen können Sie auch nur einen „Mapping"-Scan anstelle eines vollständigen „Classification"-Scans durchführen. Das Mapping kann auf Ihren Datenquellen sehr schnell durchgeführt werden, da es nicht auf Dateien zugegriffen wird, um die darin enthaltenen Daten zu sehen. "Sehen Sie den Unterschied zwischen einer Mapping- und Klassifizierungsscan".

BlueXP Klassifizierungsmanagement und Datenschutz

Die folgenden Fragen enthalten Informationen zum Management von BlueXP Klassifizierungs- und Datenschutzeinstellungen.

Wie lässt sich die BlueXP Klassifizierung aktivieren?

Zunächst müssen Sie eine Instanz der BlueXP Klassifizierung in BlueXP oder auf einem lokalen System implementieren. Sobald die Instanz ausgeführt wird, können Sie den Dienst auf vorhandenen Arbeitsumgebungen, Datenbanken und anderen Datenquellen über die Registerkarte **Konfiguration** oder durch Auswahl einer bestimmten Arbeitsumgebung aktivieren.

"Erste Schritte".

> Durch die Aktivierung der BlueXP Klassifizierung einer Datenquelle wird ein sofortiger erster Scan durchgeführt. Ergebnisse des Scans werden kurz danach angezeigt.

Wie deaktiviere ich die BlueXP-Klassifizierung?

Sie können die BlueXP Klassifizierung für das Scannen einzelner Arbeitsumgebungen, Datenbanken, Dateifreigabegruppen, OneDrive Konten oder SharePoint Konten auf der Seite BlueXP Klassifizierungskonfiguration deaktivieren.

"Weitere Informationen .".

> Um die BlueXP Klassifizierungsinstanz vollständig zu entfernen, können Sie die BlueXP Klassifizierungsinstanz manuell aus dem Portal Ihres Cloud-Providers oder Ihrem lokalen Standort entfernen.

Kann ich den Service an die Anforderungen meines Unternehmens anpassen?

Die BlueXP Klassifizierung bietet Ihnen sofort einsatzbereite Einblicke in Ihre Daten. Diese Erkenntnisse können extrahiert und für die Bedürfnisse Ihres Unternehmens verwendet werden.

Darüber hinaus bietet die BlueXP Klassifizierung Ihnen viele Möglichkeiten, eine benutzerdefinierte Liste mit „personenbezogenen Daten“ hinzuzufügen, die durch die BlueXP Klassifizierung in Scans identifiziert werden. So haben Sie alle Informationen darüber, wo sich potenziell sensible Daten in den Dateien Ihrer Unternehmen befinden.

- Sie können eindeutige Kennungen hinzufügen, die auf bestimmten Spalten in Datenbanken basieren, die Sie scannen - wir nennen dies **Data Fusion**.
- Sie können benutzerdefinierte Schlüsselwörter aus einer Textdatei hinzufügen.
- Sie können benutzerdefinierte Muster mit einem regulären Ausdruck (regex) hinzufügen.

"Weitere Informationen .".

Kann ich den Dienst anweisen, Scandaten in bestimmten Verzeichnissen auszuschließen?

Ja. Wenn die BlueXP Klassifizierung Scandaten in bestimmten Quellverzeichnissen ausschließen soll, können Sie der Klassifizierungs-Engine diese Liste bereitstellen. Nach Anwendung dieser Änderung schließt die BlueXP Klassifizierung Scandaten in den angegebenen Verzeichnissen aus.

"Weitere Informationen .".

Werden Snapshot-Kopien auf ONTAP Volumes gescannt?

Nein Durch die BlueXP Klassifizierung werden Snapshots nicht gescannt, da der Inhalt mit dem Inhalt des Volume identisch ist.

Was geschieht, wenn das Daten-Tiering auf Ihren ONTAP Volumes aktiviert ist?

Wenn die BlueXP Klassifizierung Volumes scannt, die kalte Daten in Objekt-Storage verschoben haben, scannt sie alle Daten auf lokalen Festplatten, während die kalten Daten in Objekt-Storage verschoben werden. Dies gilt auch für Produkte, die nicht von NetApp stammen und Tiering implementieren.

Der Scan heizt die kalten Daten nicht auf – sie bleiben kalt und verbleiben im Objekt-Storage.

Kann die BlueXP Klassifizierung Benachrichtigungen an mein Unternehmen senden?

Ja. In Verbindung mit der Funktion Richtlinien können Sie E-Mail-Benachrichtigungen an BlueXP-Benutzer (täglich, wöchentlich oder monatlich) oder andere E-Mail-Adressen senden, wenn eine Richtlinie Ergebnisse liefert, damit Sie Benachrichtigungen zum Schutz Ihrer Daten erhalten können. Weitere Informationen zu "Richtlinien".

Sie können auch Statusberichte von der Seite Governance und Untersuchung herunterladen, die Sie intern in Ihrem Unternehmen teilen können.

Kann die BlueXP Klassifizierung mit den in meine Dateien eingebetteten AIP-Labels funktionieren?

Ja. Sie können AIP-Etiketten in den Dateien managen, die die BlueXP Klassifizierung scannt, wenn Sie abonniert haben "Azure Information Protection (AIP)". Sie können die bereits zugewiesenen Beschriftungen anzeigen, Dateien Beschriftungen hinzufügen und vorhandene Beschriftungen ändern.

"Weitere Informationen .".

Arten von Quellsystemen und Datentypen

Die folgenden Fragen beziehen sich auf die Art des zu scannenden Speichers und die Arten der gescannten Daten.

Welche Datenquellen können mit der BlueXP Klassifizierung gescannt werden?

Die BlueXP Klassifizierung kann Daten aus Arbeitsumgebungen scannen, die Sie der BlueXP Leinwand hinzugefügt haben, sowie aus vielen Arten von strukturierten und unstrukturierten Datenquellen, auf die die BlueXP Klassifizierung über Ihre Netzwerke zugreifen kann.

- Arbeitsumgebungen:*
- Cloud Volumes ONTAP (implementiert in AWS, Azure oder GCP)
- On-Premises ONTAP Cluster
- Azure NetApp Dateien
- Amazon FSX für ONTAP
- Amazon S3

Datenquellen:

- File Shares von anderen Anbietern
- Objekt-Storage (nutzt S3-Protokoll)
- Datenbanken (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA, SQL SERVER)
- OneDrive Accounts
- SharePoint Online- und On-Premises-Accounts
- Google Drive-Konten

Die BlueXP Klassifizierung unterstützt NFS-Versionen 3.x und CIFS-Versionen 1.x, 2.0, 2.1 und 3.0.

Gibt es Einschränkungen bei der Bereitstellung in einer Regierungsregion?

Die BlueXP Klassifizierung wird unterstützt, wenn der Connector in einer Regierungsregion (AWS GovCloud, Azure Gov oder Azure DoD) bereitgestellt wird – auch als „eingeschränkter Modus“ bezeichnet. Bei einer solchen Implementierung unterliegt die BlueXP Klassifizierung folgenden Einschränkungen:

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

Welche Datenquellen kann ich scannen, wenn ich die BlueXP-Klassifizierung auf einer Website ohne Internetzugang installiere?

Die BlueXP Klassifizierung kann nur Daten aus lokalen Datenquellen am lokalen Standort scannen. Derzeit kann die BlueXP Klassifizierung folgende lokale Datenquellen scannen – im „privaten Modus“, auch als „dunkle“ Site bezeichnet:

- On-Premises ONTAP Systeme
- Datenbankschemas

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

Welche Dateitypen werden unterstützt?

Die BlueXP Klassifizierung scannt alle Dateien nach Kategorien- und Metadaten und zeigt alle Dateitypen im Abschnitt „Dateitypen“ des Dashboards an.

Wenn die BlueXP Klassifizierung personenbezogene Daten erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt:

```
.CSV, .DCM, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX,
Docs, Sheets, and Slides
```

Welche Arten von Daten und Metadaten werden durch die BlueXP Klassifizierung erfasst?

Die BlueXP Klassifizierung ermöglicht Ihnen die Durchführung eines allgemeinen „Mapping“-Scans oder eines vollständigen „Klassifizierungs“-Scans für Datenquellen. Das Mapping bietet nur einen Überblick über Ihre Daten auf hoher Ebene, während die Klassifizierung ein tiefes Scannen Ihrer Daten ermöglicht. Das Mapping kann auf Ihren Datenquellen sehr schnell durchgeführt werden, da es nicht auf Dateien zugegriffen wird, um die darin enthaltenen Daten zu sehen.

- Scan der Datenzuordnung

  Die BlueXP Klassifizierung scannt nur die Metadaten. Dies ist nützlich für das allgemeine Datenmanagement und die Datenverwaltung, für eine schnelle Projektabwicklung, für sehr große Bestände und für die Priorisierung. Die Datenzuordnung basiert auf Metadaten und gilt als **fast** Scan.

  Nach einem schnellen Scan können Sie einen Daten-Mapping-Bericht erstellen. Dieser Bericht bietet einen Überblick über die in Ihren Datenquellen gespeicherten Daten, um Sie bei Entscheidungen zu Ressourcenauslastung, Migration, Backup-, Sicherheits- und Compliance-Prozessen zu unterstützen.

- Scan der Datenklassifizierung (Deep):

  BlueXP Klassifizierungs-Scans mittels Standardprotokollen und schreibgeschützter Berechtigung in Ihrer gesamten Umgebung. Ausgewählte Dateien werden nach sensiblen Daten, privaten Informationen und Ransomware-Problemen geöffnet und gescannt, die damit verbunden sind.

  Nach einem vollständigen Scan gibt es zahlreiche zusätzliche BlueXP Klassifizierungsfunktionen, die Sie auf Ihre Daten anwenden können, beispielsweise das Anzeigen und Optimieren von Daten auf der Seite „Datenuntersuchung“, das Suchen nach Namen in Dateien, das Kopieren, Verschieben und Löschen von Quelldateien usw.

Die BlueXP Klassifizierung erfasst Metadaten wie z. B. Dateiname, -Berechtigungen, -Erstellungszeit, letzter Zugriff und letzte Änderung. Dies umfasst alle Metadaten, die auf der Seite „Datenermittlungsdetails“ und in „Datenermittlungsberichte“ angezeigt werden.

Die BlueXP Klassifizierung kann viele Arten von privaten Daten identifizieren, wie beispielsweise personenbezogene und sensible personenbezogene Daten. Weitere Informationen zu privaten Daten finden Sie unter "Kategorien von privaten Daten, die durch die BlueXP Klassifizierung gescannt werden".

Kann ich die BlueXP Klassifizierungsinformationen auf bestimmte Benutzer beschränken?

Ja, die BlueXP Klassifizierung ist vollständig in BlueXP integriert. BlueXP-Benutzer können nur Informationen für die Arbeitsumgebungen sehen, für die sie gemäß ihren Arbeitsbereichberechtigungen angezeigt werden können.

Wenn Sie bestimmten Benutzern darüber hinaus erlauben möchten, die Ergebnisse der BlueXP Klassifizierungsüberprüfung einfach anzuzeigen, ohne BlueXP Klassifizierungseinstellungen zu managen, können Sie diesen Benutzern die Rolle der Cloud Compliance Viewer zuweisen.

"Weitere Informationen .".

Kann jemand auf die privaten Daten zugreifen, die zwischen meinem Browser und der BlueXP Klassifizierung gesendet werden?

Nein Die privaten Daten, die zwischen Ihrem Browser und der BlueXP Klassifizierungsinstanz übertragen werden, sind durch End-to-End-Verschlüsselung mit TLS 1.2 geschützt. Dies bedeutet, dass NetApp und Drittanbieter die Daten nicht lesen können. Die BlueXP Klassifizierung gibt keine Daten oder Ergebnisse an NetApp weiter, es sei denn, Sie beantragen und genehmigen den Zugriff.

Die gescannten Daten verbleiben in Ihrer Umgebung.

Wie werden sensible Daten behandelt?

NetApp hat keinen Zugriff auf sensible Daten und zeigt sie nicht in der Benutzeroberfläche an. Sensible Daten werden maskiert, beispielsweise werden die letzten vier Zahlen für Kreditkarteninformationen angezeigt.

Wo werden die Daten gespeichert?

Die Scan-Ergebnisse werden in Elasticsearch innerhalb der BlueXP Klassifizierungsinstanz gespeichert.

Wie wird auf die Daten zugegriffen?

Die BlueXP Klassifizierung greift über API-Aufrufe, die eine Authentifizierung erfordern und mit AES-128 verschlüsselt sind, auf in Elasticsearch gespeicherte Daten zu. Für den direkten Zugriff auf Elasticsearch ist Root-Zugriff erforderlich.

Lizenzen und Kosten

Die folgenden Fragen beziehen sich auf Lizenzierung und Kosten der Nutzung der BlueXP Klassifizierung.

Wie hoch sind die Kosten für die Klassifizierung von BlueXP?

Die Kosten der BlueXP Klassifizierung hängen von der Datenmenge ab, die Sie scannen. Die ersten 1 TB an Daten, die die BlueXP Klassifizierung in einem BlueXP Workspace scannt, sind 30 Tage lang kostenlos. Wenn Sie eine der beiden Grenzwerte erreicht haben, benötigen Sie eine der folgenden Optionen, um mit dem Scannen der Daten fortzufahren:

- Ein Abonnement des BlueXP Marketplace-Abonnements von Ihrem Cloud-Provider oder
- Byol-Modell (Bring-Your-Own-License) von NetApp

Siehe "Preisgestaltung" Entsprechende Details.

Was geschieht, wenn ich das BYOL-Kapazitätslimit erreicht habe?

Wenn Sie eine BYOL-Kapazitätsgrenze erreichen, wird die BlueXP Klassifizierung weiter ausgeführt, der Zugriff auf die Dashboards ist jedoch gesperrt, sodass Informationen zu gescannten Daten nicht angezeigt werden können. Nur die Konfigurationsseite ist verfügbar, wenn Sie die Anzahl der eingescannten Volumes reduzieren möchten, um die Kapazitätsnutzung unter das Lizenzlimit zu bringen. Sie müssen Ihre BYOL-Lizenz verlängern, um wieder vollen Zugriff auf die BlueXP Klassifizierung zu erhalten.

Connector-Bereitstellung

Die folgenden Fragen beziehen sich auf den BlueXP Connector.

Was ist der Steckverbinder?

Der Connector ist eine Software, die auf einer Computing-Instanz entweder in Ihrem Cloud-Konto oder vor Ort ausgeführt wird und es BlueXP ermöglicht, Cloud-Ressourcen sicher zu managen. Sie müssen einen Connector implementieren, um die BlueXP-Klassifizierung zu verwenden.

Wo muss der Connector installiert werden?

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS, Amazon FSX für ONTAP oder in AWS S3 Buckets wird in AWS ein Connector verwendet.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konnektor in Azure.
- Beim Scannen von Daten in Cloud Volumes ONTAP in GCP wird ein Connector in GCP verwendet.
- Beim Scannen von Daten in lokalen ONTAP Systemen, File Shares anderer Anbieter, generischer S3 Objekt-Storage, Datenbanken, OneDrive Ordner, SharePoint Konten und Google Drive Konten können Sie einen Konnektor in jedem dieser Cloud-Standorte verwenden.

Wenn die Daten an vielen dieser Standorte gespeichert sind, müssen Sie eventuell verwenden "Mehrere Anschlüsse".

Ist für die BlueXP Klassifizierung Zugriff auf Zugangsdaten erforderlich?

Die BlueXP Klassifizierung selbst ruft keine Storage-Anmeldedaten ab. Stattdessen werden sie im BlueXP Connector gespeichert.

Die BlueXP Klassifizierung verwendet Daten-Ebenen-Anmeldedaten, zum Beispiel CIFS-Zugangsdaten, um Freigaben vor dem Scannen zu mounten.

Kann ich den Connector auf meinem eigenen Host bereitstellen?

Ja. Das können Sie "Stellen Sie den Connector vor Ort bereit" Auf einem Linux-Host in Ihrem Netzwerk oder auf einem Host in der Cloud. Wenn Sie die BlueXP Klassifizierung lokal implementieren möchten, sollten Sie den Connector möglicherweise auch On-Premises installieren. Dies ist aber nicht erforderlich.

Verwendet die Kommunikation zwischen dem Dienst und dem Connector HTTP?

Ja, die BlueXP Klassifizierung kommuniziert über HTTP mit dem BlueXP Connector.

Wie sieht es mit sicheren Websites ohne Internetzugang aus?

Ja, das wird auch unterstützt. Das können Sie "Stellen Sie den Connector auf einem lokalen Linux-Host bereit,

der keinen Internetzugang hat". "Dies wird auch als „Privatmodus“ bezeichnet.". Anschließend können Sie lokale ONTAP Cluster und andere lokale Datenquellen erkennen und die Daten mit der BlueXP Klassifizierung scannen.

Implementierung der BlueXP Klassifizierung

Die folgenden Fragen beziehen sich auf die separate BlueXP Klassifizierungsinstanz.

Welche Implementierungsmodelle werden von der BlueXP Klassifizierung unterstützt?

Mit BlueXP können Benutzer Systeme praktisch überall scannen und protokollieren, einschließlich On-Premises-, Cloud- und Hybridumgebungen. Die BlueXP Klassifizierung wird normalerweise mit einem SaaS-Modell implementiert. Bei diesem Modell ist der Service über die BlueXP Schnittstelle aktiviert, sodass keine Hardware- oder Softwareinstallation erforderlich ist. Selbst im Implementierungs-Modus mit einem Klick und einem Klick ist das Datenmanagement möglich, unabhängig davon, ob die Datenspeicher sich vor Ort oder in der Public Cloud befinden.

Welche Art von Instanz oder VM ist für die BlueXP Klassifizierung erforderlich?

Wenn "In der Cloud implementiert":

- In AWS wird die BlueXP Klassifizierung auf einer m6i.4xlarge-Instanz mit einer GP2-Festplatte mit 500 gib ausgeführt. Sie können während der Bereitstellung einen kleineren Instanztyp auswählen.
- In Azure wird die Klassifizierung von BlueXP auf einer Standard_D16s_v3 VM mit einer Festplatte von 500 gib ausgeführt.
- In GCP wird die BlueXP Klassifizierung auf einer VM gemäß n2-Standard-16 mit einer persistenten Standardfestplatte von 500 gib ausgeführt.

Beachten Sie, dass Sie die BlueXP Klassifizierung auf einem System mit weniger CPUs und weniger RAM implementieren können. Bei der Nutzung dieser Systeme bestehen jedoch Einschränkungen. Siehe "Verwenden eines kleineren Instanztyps" Entsprechende Details.

"Erfahren Sie mehr über die BlueXP Klassifizierung".

Kann ich die BlueXP Klassifizierung auf meinem eigenen Host implementieren?

Ja. Sie können die BlueXP Klassifizierungs-Software auf einem Linux-Host mit Internetzugang in Ihrem Netzwerk oder in der Cloud installieren. Alles funktioniert gleich, und Sie verwalten Ihre Scankonfiguration und -Ergebnisse weiterhin mit BlueXP. Siehe "Implementierung der BlueXP Klassifizierung vor Ort" Für die Systemanforderungen und Installationsdetails.

Wie sieht es mit sicheren Websites ohne Internetzugang aus?

Ja, das wird auch unterstützt. Das können Sie "Implementieren Sie die BlueXP Klassifizierung auf einer lokalen Website ohne Internetzugang" Für vollständig sichere Standorte.

BlueXP Klassifizierung nutzen

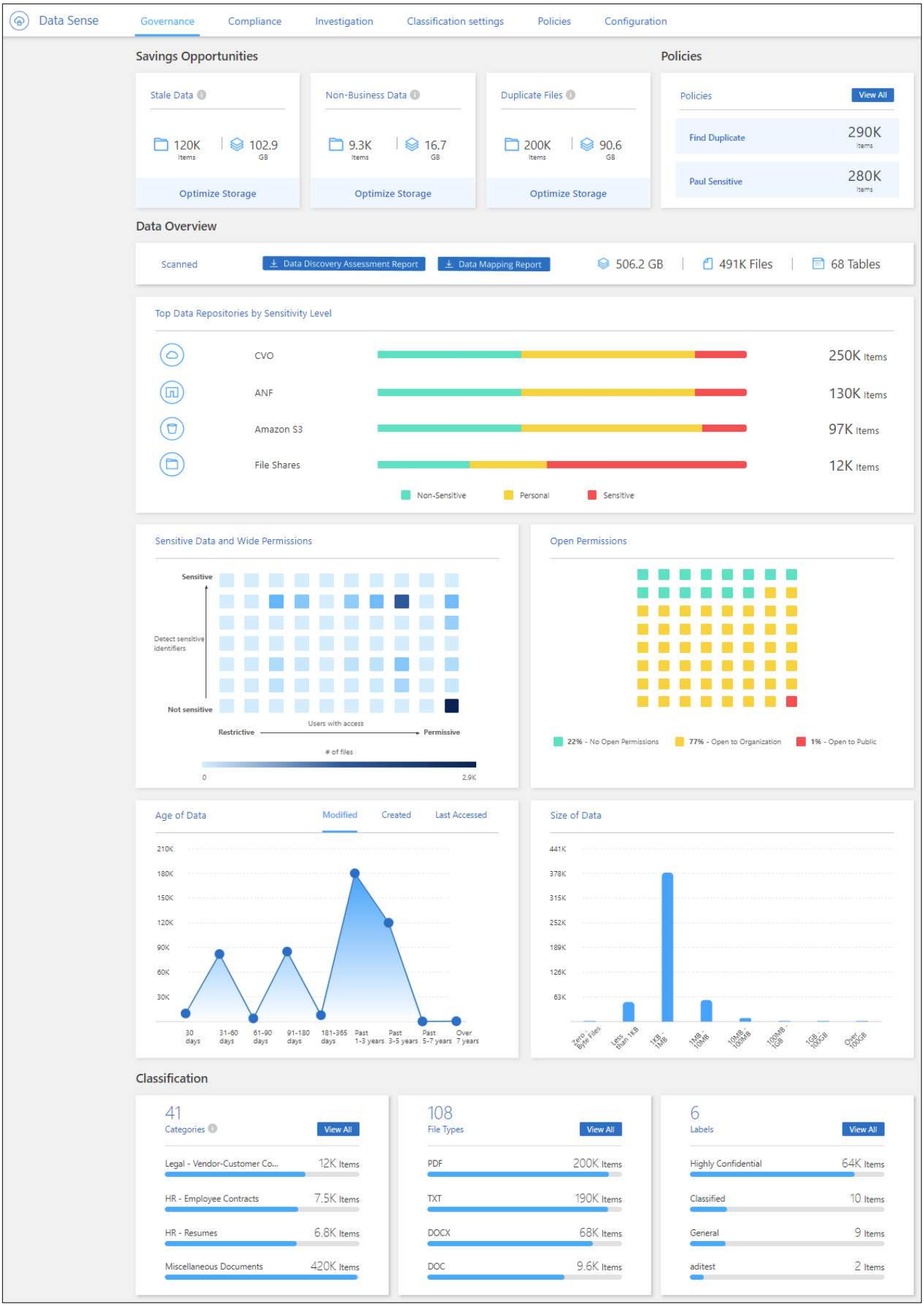
Zeigen Sie Governance-Details zu den in Ihrer Organisation gespeicherten Daten an

Behalten Sie die Kontrolle über die Kosten im Zusammenhang mit Daten auf den Storage-Ressourcen Ihres Unternehmens. Die BlueXP Klassifizierung ermittelt die Menge veralteter Daten, nicht geschäftsferner Daten, mehrfach vorhandener Dateien und sehr großer Dateien auf Ihren Systemen. So können Sie entscheiden, ob Sie einige Dateien entfernen oder auf kostengünstigeren Objekt-Storage verschieben möchten.

Wenn Sie Daten von On-Premises-Standorten in die Cloud migrieren möchten, können Sie vor der Verschiebung prüfen, ob einige der Daten vertrauliche Informationen beinhalten.

Dashboard für Governance

Das Governance-Dashboard liefert Informationen, mit denen Sie die Effizienz steigern und die Kosten für die in Ihren Storage-Ressourcen gespeicherten Daten kontrollieren können.


Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
120K Items
102.9 GB
Optimize Storage
Non-Business Data
9.3K Items
16.7 GB
Optimize Storage
Duplicate Files
200K Items
90.6 GB
Optimize Storage
Policies
Policies
View All
Find Duplicate 290K Items
Paul Sensitive 280K Items
Data Overview
Scanned
Data Discovery Assessment Report
Data Mapping Report
506.2 GB
491K Files
68 Tables
Top Data Repositories by Sensitivity Level
CVO 250K Items
ANF 130K Items
Amazon S3 97K Items
File Shares 12K Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detect sensitive identifiers
Not sensitive
Users with access
Restrictive
Permissive
# of files
0
2.9K
Open Permissions
22% - No Open Permissions
77% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
210K
180K
150K
120K
90K
60K
30K
30 days
31-60 days
61-90 days
91-180 days
181-365 days
Past 1-3 years
Past 3-5 years
Past 5-7 years
Over 7 years
Size of Data
441K
378K
315K
252K
189K
126K
63K
Zero Byte Files
Less than 1KB
1KB - 1MB
1MB - 10MB
10MB - 100MB
100MB - 1GB
1GB - 10GB
Over 10GB
Classification
41
Categories
View All
Legal - Vendor-Customer Co... 12K Items
HR - Employee Contracts 7.5K Items
HR - Resumes 6.8K Items
Miscellaneous Documents 420K Items
108
File Types
View All
PDF 200K Items
TXT 190K Items
DOCX 68K Items
DOC 9.6K Items
6
Labels
View All
Highly Confidential 64K Items
Classified 10 Items
General 9 Items
aditest 2 Items

Speichern Sie Opportunitys

Möglicherweise möchten Sie die Elemente im Bereich „*Saving Opportunities*“ untersuchen, um zu sehen, ob es Daten gibt, die Sie löschen oder zu kostengünstigerem Objekt-Storage Tier verschieben sollten. Klicken Sie auf die einzelnen Elemente, um die gefilterten Ergebnisse auf der Untersuchungsseite anzuzeigen.

- **Veraltete Daten** - Daten die zuletzt vor über 3 Jahren geändert wurden.
- **Nicht-Geschäftsdaten** - Daten, die aufgrund ihrer Kategorie oder ihres Dateityps als nicht geschäftsbezogen gelten. Hierzu zählen folgende Optionen:
  - Applikationsdaten
  - Audio
  - Ausführbare Dateien
  - Bilder
  - Protokolle
  - Videos
  - Sonstiges (allgemeine Kategorie „Sonstige“)
- **Doppelte Dateien** - Dateien, die an anderen Orten in den Datenquellen, die Sie scannen, dupliziert werden. "Sehen Sie, welche Arten von duplizierten Dateien angezeigt werden".

  HINWEIS

  Wenn eine Ihrer Datenquellen Daten-Tiering implementiert, werden alte Daten, die sich bereits im Objektspeicher befinden, möglicherweise in der Kategorie „veraltete Daten“ identifiziert.

Politik mit der größten Anzahl von Ergebnissen

Im Bereich *Policies* werden die Richtlinien mit der größten Anzahl von Ergebnissen oben in der Liste angezeigt. Klicken Sie auf den Namen einer Richtlinie, um die Ergebnisse auf der Untersuchungsseite anzuzeigen. Klicken Sie auf **Alle anzeigen**, um die Liste aller verfügbaren Richtlinien anzuzeigen.

Klicken Sie Auf "Hier" Um mehr über Richtlinien zu erfahren.

Datenüberblick

Der Abschnitt *Data Overview* bietet einen schnellen Überblick über alle zu scannenden Daten. Klicken Sie auf die Schaltfläche, um einen vollständigen Bericht zur Datenzuordnung herunterzuladen, der Nutzungskapazität, Alter der Daten, Datengröße und Dateitypen für alle Arbeitsumgebungen und Datenquellen enthält. Siehe Datenzuordnungsbericht Alle Details zu diesem Bericht.

Die wichtigsten Daten-Repositorys, die nach Sensibilität aufgeführt sind

Im Bereich *Top Data Repositories by Sensitivity Level* werden die vier wichtigsten Daten-Repositorys (Arbeitsumgebungen und Datenquellen) aufgeführt, die die sensibelsten Elemente enthalten. Das Balkendiagramm für jede Arbeitsumgebung ist in folgende Kategorien unterteilt:

- Nicht-sensible Daten
- Persönliche Daten
- Sensible personenbezogene Daten

Sie können mit der Maus auf jeden Abschnitt zeigen, um die Gesamtanzahl der Elemente in jeder Kategorie

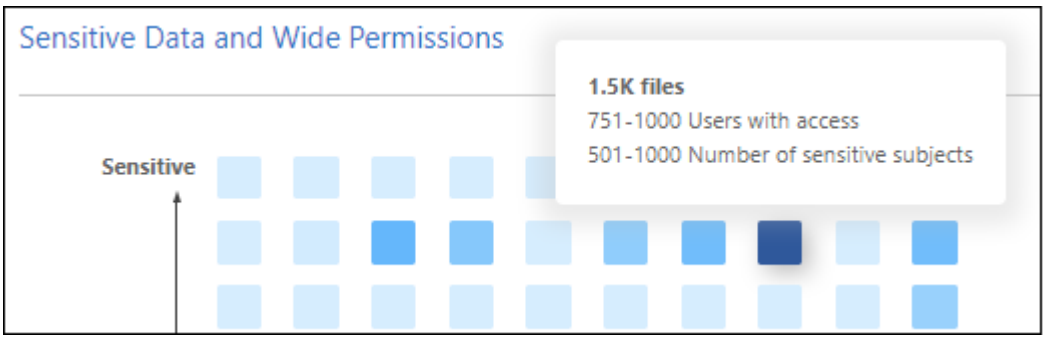
anzuzeigen.

Klicken Sie auf die einzelnen Bereiche, um die gefilterten Ergebnisse auf der Untersuchungsseite anzuzeigen, damit Sie weitere Untersuchungen machen können.

Daten, die nach Sensitivität und breiten Berechtigungen aufgelistet sind

Der Bereich *sensible Daten und Wide Permissions* bietet eine Heatmap von Dateien, die sensible Daten (einschließlich sensibler und sensibler personenbezogener Daten) enthalten und zu permissiv sind. So erkennen Sie, wo Sie möglicherweise Risiken mit sensiblen Daten haben.

Die Dateien werden anhand der Anzahl der Benutzer bewertet, die berechtigt sind, auf die Dateien auf der X-Achse (niedrigste bis höchste) zuzugreifen, und die Anzahl der sensiblen Kennungen innerhalb der Dateien auf der Y-Achse (niedrigste bis höchste). Die Blöcke stellen die Anzahl der Dateien dar, die mit den Elementen der X- und Y-Achsen übereinstimmen. Der hellere Block ist gut, da weniger Benutzer auf die Dateien zugreifen können und weniger sensible Kennungen pro Datei. Die dunkleren Blöcke sind die Elemente, die Sie untersuchen möchten. Auf dem folgenden Bildschirm wird beispielsweise der Mauszeiger für den dunkelblauen Block angezeigt. Es zeigt, dass Sie 1,500 Dateien haben, auf die 751-100 Benutzer zugreifen können und wo es 501-100 sensible Kennungen pro Datei gibt.



Sie können auf den Block klicken, für den Sie sich interessieren, um die gefilterten Ergebnisse der betroffenen Dateien auf der Untersuchungsseite anzuzeigen, damit Sie weitere Untersuchungen durchführen können.

Wenn Sie keinen Identitätsdienst mit BlueXP-Klassifizierung integriert haben, werden in diesem Bereich keine Daten angezeigt. "Erfahren Sie, wie Sie Ihren Active Directory-Service in die BlueXP Klassifizierung integrieren".

> Dieses Fenster unterstützt Dateien in CIFS-Freigaben, OneDrive und SharePoint-Datenquellen. Derzeit werden Datenbanken, Google Drive, Amazon S3 und generischer Objektspeicher nicht unterstützt.

Daten, die nach Typen der offenen Berechtigungen aufgeführt sind

Der Bereich „*Open Permissions*“ zeigt den Prozentsatz für jeden Berechtigungstyp an, der für alle Dateien vorhanden ist, die gescannt werden. Das Diagramm zeigt die folgenden Berechtigungstypen:

- Keine Offenen Berechtigungen
- Steht Unternehmen offen
- Öffentlich zugänglich
- Unbekannter Zugriff

Sie können mit der Maus auf jeden Abschnitt zeigen, um die Gesamtzahl der Dateien jeder Kategorie

anzuzeigen. Klicken Sie auf die einzelnen Bereiche, um die gefilterten Ergebnisse auf der Untersuchungsseite anzuzeigen, damit Sie weitere Untersuchungen machen können.

Alter der Daten und Größe der Diagramme

Möglicherweise möchten Sie die Elemente in den Diagrammen *Age* und *Size* untersuchen, um zu sehen, ob Daten gelöscht oder in kostengünstigeren Objektspeicher verschoben werden sollten.

Sie können den Mauszeiger über einen Punkt in den Diagrammen bewegen, um Details zum Alter oder zur Größe der Daten in dieser Kategorie anzuzeigen. Klicken Sie hier, um alle Dateien anzuzeigen, die nach diesem Alter oder Größenbereich gefiltert sind.

- **Alter der Daten Graph** - kategorisiert Daten basierend auf dem Zeitpunkt der Erstellung, dem letzten Zugriff oder der letzten Änderung.
- **Größe des Datengraphen** - kategorisiert Daten basierend auf der Größe.

  HINWEIS

  Wenn eine Ihrer Datenquellen Daten-Tiering implementiert, können im Diagramm „_Age of Data“ alte Daten, die sich bereits im Objektspeicher befinden, identifiziert werden.

Die meisten ermittelten Datenklassifizierungen

Der Bereich *Classification* enthält eine Liste der am häufigsten identifizierten "Kategorien", "Dateitypen", und "AIP-Etiketten" In den gescannten Daten.

Kategorien

Kategorien können Ihnen dabei helfen zu verstehen, was mit Ihren Daten passiert, indem Sie die Arten von Informationen anzeigen, die Sie haben. Beispielsweise kann eine Kategorie wie „Bewerbungen“ oder „Mitarbeiterverträge“ sensible Daten enthalten. Wenn Sie die Ergebnisse untersuchen, können Sie feststellen, dass Mitarbeiterverträge an einem unsicheren Ort gespeichert sind. Sie können das Problem dann beheben.

Siehe "Anzeigen von Dateien nach Kategorien" Finden Sie weitere Informationen.

Dateitypen

Die Überprüfung Ihrer Dateitypen kann Ihnen helfen, Ihre sensiblen Daten zu kontrollieren, da Sie möglicherweise feststellen können, dass bestimmte Dateitypen nicht richtig gespeichert sind.

Siehe "Anzeigen von Dateitypen" Finden Sie weitere Informationen.

AIP-Etiketten

Wenn Sie den Azure Information Protection (AIP) abonniert haben, können Sie Dokumente und Dateien klassifizieren und schützen, indem Sie Inhaltsetiketten anwenden. Durch die Überprüfung der am häufigsten verwendeten AIP-Etiketten, die Dateien zugeordnet sind, können Sie feststellen, welche Etiketten am häufigsten in Ihren Dateien verwendet werden.

Siehe "AIP-Etiketten" Finden Sie weitere Informationen.

Datenzuordnungsbericht

Der Daten-Mapping-Bericht bietet einen Überblick über die Daten, die in Ihren Datenquellen gespeichert werden, um Sie bei Entscheidungen zu Migrations-, Backup-, Sicherheits- und Compliance-Prozessen zu

unterstützen. Der Bericht enthält zunächst eine Übersicht, in der alle Arbeitsumgebungen und Datenquellen zusammengefasst sind, und enthält dann eine Aufschlüsselung für jede Arbeitsumgebung.

Der Bericht enthält die folgenden Informationen:

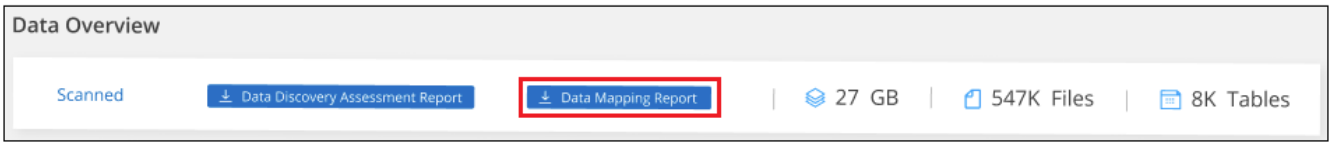
Kategorie	Beschreibung
Nutzung Von Kapazitäten	Für alle Arbeitsumgebungen: Listet die Anzahl der Dateien und die genutzte Kapazität für jede Arbeitsumgebung. Für einzelne Arbeitsumgebungen: Listet die Dateien auf, die die größte Kapazität nutzen.
Alter der Daten	Bietet drei Diagramme und Diagramme für den Zeitpunkt, an dem Dateien erstellt, zuletzt geändert oder zuletzt aufgerufen wurden. Listet die Anzahl der Dateien und deren verwendete Kapazität auf der Grundlage bestimmter Datumsbereiche auf.
Größe von Daten	Führt die Anzahl der Dateien auf, die in bestimmten Größenbereichen in Ihren Arbeitsumgebungen vorhanden sind.
Dateitypen	Listet die Gesamtzahl der Dateien und die genutzte Kapazität für jeden Dateityp auf, der in Ihren Arbeitsumgebungen gespeichert ist.

Generieren Sie den Bericht zur Datenzuordnung

Sie generieren diesen Bericht über die Registerkarte Governance in der BlueXP Klassifizierung.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Governance** und dann auf die Schaltfläche **Data Mapping Report**.



Ergebnis

Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Wenn der Bericht größer als 1 MB ist, wird die PDF-Datei auf der BlueXP Klassifizierungsinstanz beibehalten, und es wird eine Popup-Nachricht über den genauen Speicherort angezeigt. Wenn die BlueXP Klassifizierung auf einer lokalen Linux-Maschine oder auf einer Linux-Maschine, die Sie in der Cloud implementiert haben, installiert ist, können Sie direkt zur PDF-Datei navigieren. Wenn die BlueXP Klassifizierung in der Cloud implementiert wird, müssen Sie SSH zur BlueXP Klassifizierungsinstanz verwenden, um eine PDF-Datei herunterzuladen. "Informationen zum Zugriff auf Daten auf der Klassifikationsinstanz finden Sie unter".

Beachten Sie, dass Sie den Unternehmensnamen, der auf der ersten Seite des Berichts angezeigt wird, oben auf der BlueXP Klassifizierungsseite anpassen können, indem Sie auf klicken ⋮ Und dann auf **Firmenname ändern** klicken. Wenn Sie den Bericht das nächste Mal generieren, wird er den neuen Namen enthalten.

Data Discovery Assessment-Bericht

Der Data Discovery Assessment Report bietet eine allgemeine Analyse der gescannten Umgebung, um die Ergebnisse des Systems hervorzuheben und Problembereiche und mögliche Schritte zur Problembehebung

aufzuzeigen. Die Ergebnisse basieren sowohl auf der Zuordnung als auch auf der Klassifizierung Ihrer Daten. Mit diesem Bericht soll das Bewusstsein für drei wesentliche Aspekte Ihres Datensatzes gestärkt werden:

Merkmal	Beschreibung
Bedenken hinsichtlich der Daten-Governance	Ein detaillierter Überblick über alle Daten, die Sie besitzen, und Bereiche, in denen Sie die Datenmenge möglicherweise reduzieren und Kosten einsparen können.
Risiken im Hinblick auf die Datensicherheit	Bereiche, in denen Daten aufgrund umfassender Zugriffsberechtigungen für interne oder externe Angriffe verfügbar sind.
Lücken in der Daten-Compliance	Ihre personenbezogenen oder sensiblen personenbezogenen Daten sind sowohl aus Sicherheitsgründen als auch für DSLR-Zwecke (Zugriffsanfragen von Betroffenen) gespeichert.

Nach der Bewertung enthält dieser Bericht Bereiche, in denen Sie:

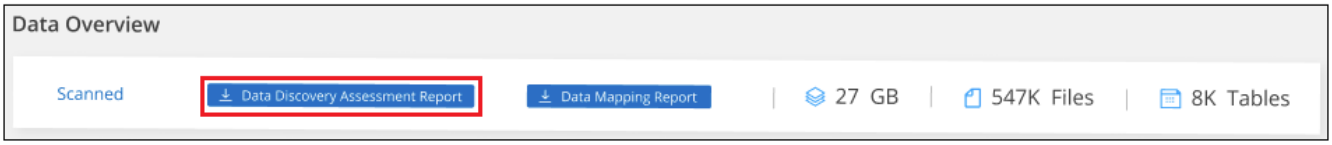
- Senkung der Storage-Kosten durch Ändern der Aufbewahrungsrichtlinie oder durch Verschieben oder Löschen bestimmter Daten (veraltete, doppelte oder nicht geschäftsfremde Daten)
- Schützen Sie Ihre berechtigen Daten durch eine Überarbeitung der globalen Richtlinien für das Gruppenmanagement
- Schützen Sie Ihre persönlichen oder sensiblen Daten, indem Sie personenbezogene Daten in sicherere Datenspeicher verlagern

Generieren Sie den Data Discovery Assessment Report

Sie generieren diesen Bericht über die Registerkarte Governance in der BlueXP Klassifizierung.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Governance** und dann auf die Schaltfläche **Data Discovery Assessment Report**.



Ergebnis

Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Beachten Sie, dass Sie den Unternehmensnamen, der auf der ersten Seite des Berichts angezeigt wird, oben auf der BlueXP Klassifizierungsseite anpassen können, indem Sie auf klicken Und dann auf **Firmenname ändern** klicken. Wenn Sie den Bericht das nächste Mal generieren, wird er den neuen Namen enthalten.

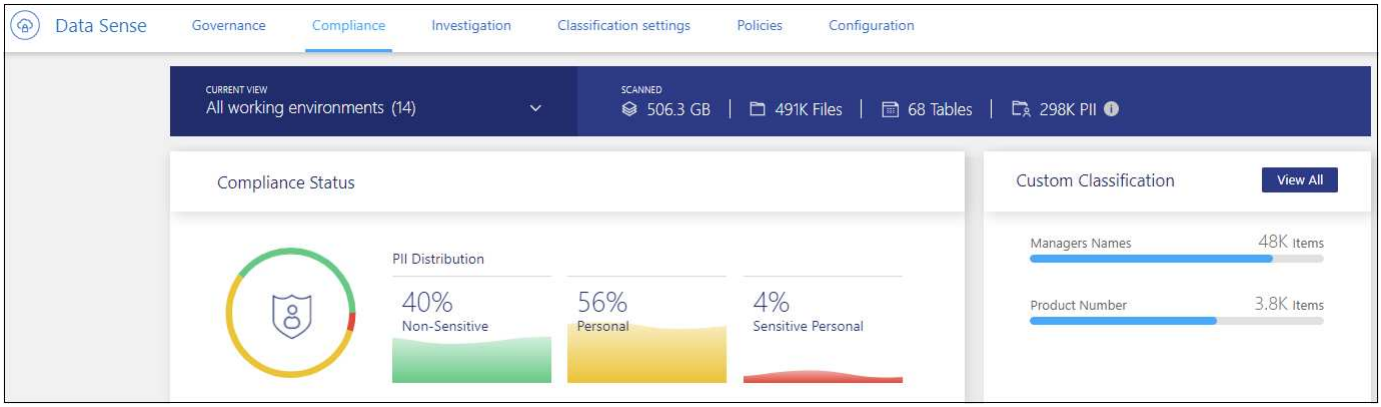
Zeigen Sie Compliance-Details zu den in Ihrem Unternehmen gespeicherten Daten an

Mehr Kontrolle über Ihre persönlichen Daten durch die Anzeige von Details zu den personenbezogenen Daten und vertraulichen personenbezogenen Daten in Ihrem

Unternehmen. Zusätzlich können Sie sich Sichtbarkeit verschaffen, indem Sie die Kategorien und Dateitypen überprüfen, die in Ihren Daten für die BlueXP Klassifizierung gefunden wurden.

> Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.

Im BlueXP Klassifizierungs-Dashboard werden standardmäßig Compliance-Daten für alle Arbeitsumgebungen und Datenbanken angezeigt.



Wenn Sie Daten nur für einige der Arbeitsumgebungen sehen möchten, Wählen Sie diese Arbeitsumgebungen aus.

Sie können die Ergebnisse auch auf der Seite Datenuntersuchung filtern und einen Bericht der Ergebnisse als CSV-Datei herunterladen. Siehe "Filtern von Daten auf der Seite „Datenuntersuchung“" Entsprechende Details.

Dateien anzeigen, die personenbezogene Daten enthalten

Durch die BlueXP Klassifizierung werden automatisch bestimmte Wörter, Strings und Muster (Regex) innerhalb der Daten identifiziert. Beispielsweise personenbezogene Daten (Personal Identification Information, PII), Kreditkartennummern, Sozialversicherungsnummern, Kontonummern, Passwörter, Und vieles mehr. "Die vollständige Liste finden Sie hier". Durch die BlueXP Klassifizierung wird diese Art von Informationen in einzelnen Dateien, in Dateien innerhalb von Verzeichnissen (Freigaben und Ordner) oder in Datenbanktabellen identifiziert.

Wenn Sie außerdem einen zu scannenden Datenbankserver hinzugefügt haben, können Sie mit der Funktion *Data Fusion* Ihre Dateien scannen, um festzustellen, ob eindeutige Identifikatoren aus Ihren Datenbanken in diesen Dateien oder anderen Datenbanken gefunden werden. Siehe "Hinzufügen von ID-Kennungen unter Verwendung von Data Fusion" Entsprechende Details.

Für einige Arten von personenbezogenen Daten verwendet die BlueXP Klassifizierung *Proximity Validation*, um ihre Ergebnisse zu validieren. Die Validierung erfolgt, indem ein oder mehrere vordefinierte Schlüsselwörter in der Nähe der gefundenen personenbezogenen Daten gesucht werden. Beispielsweise identifiziert die BlueXP Klassifizierung eine US Sozialversicherungsnummer (SSN) als SSN, wenn sie neben ihr ein Näherungswort sieht - zum Beispiel *SSN* oder *Sozialversicherung*. "Der Tisch der personenbezogenen Daten" Zeigt an, wann die BlueXP Klassifizierung die Validierung der Nähe verwendet.

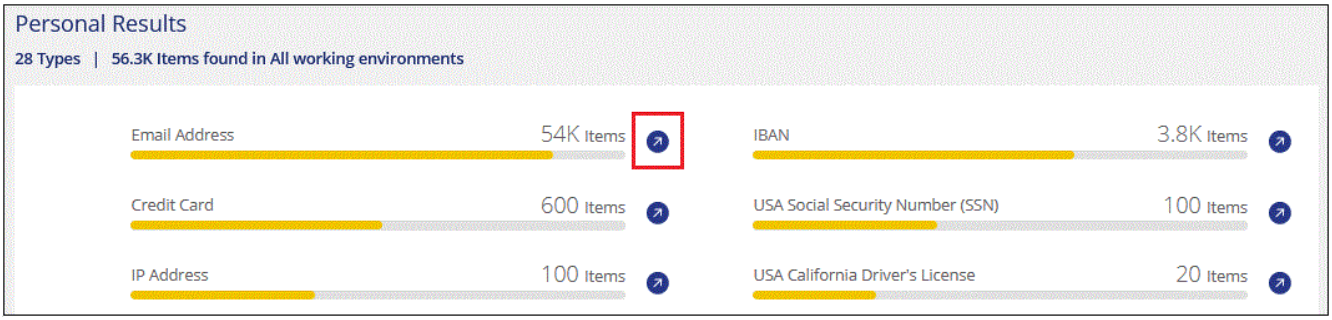
Schritte

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

Registerkarte **Compliance**.

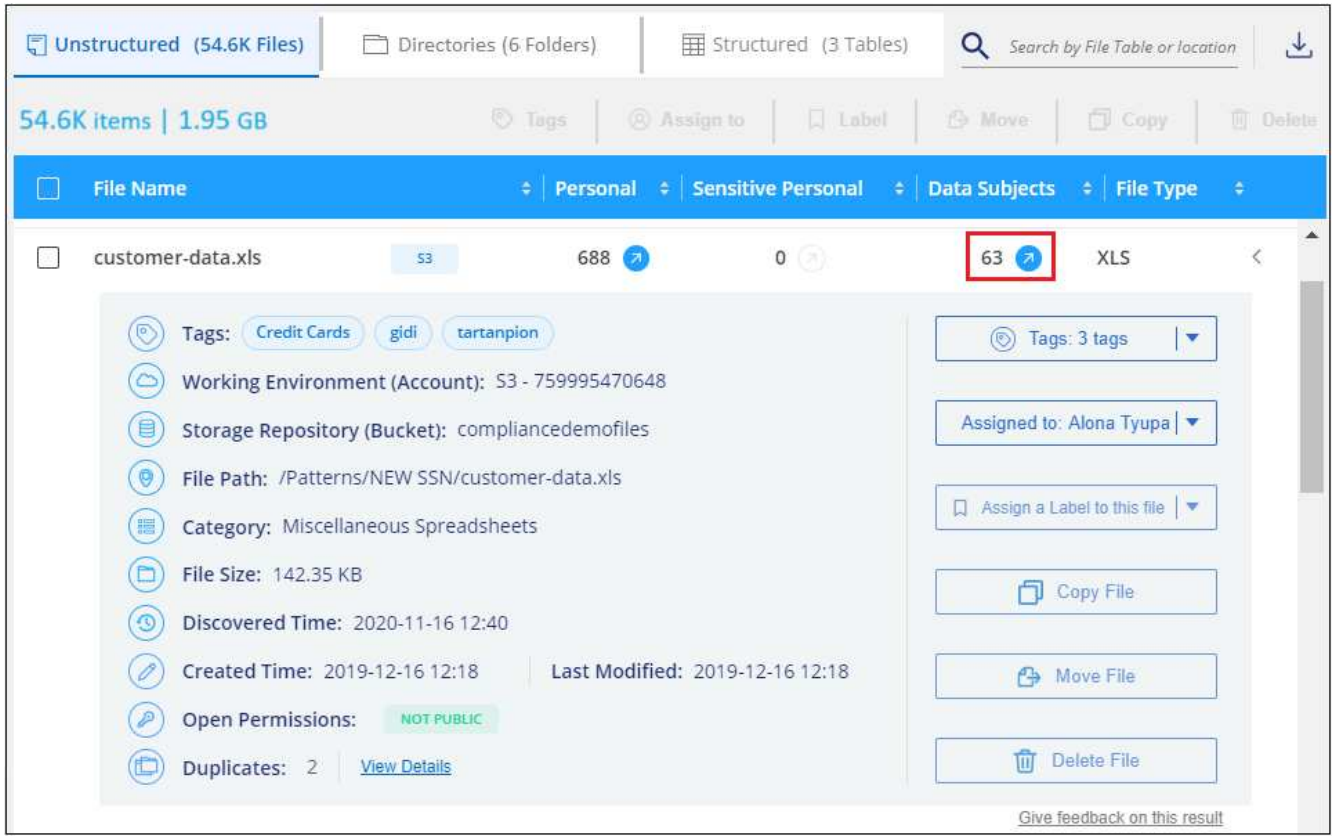
2. Um die Angaben zu allen personenbezogenen Daten zu untersuchen, klicken Sie auf das Symbol neben dem Prozentsatz der persönlichen Daten.

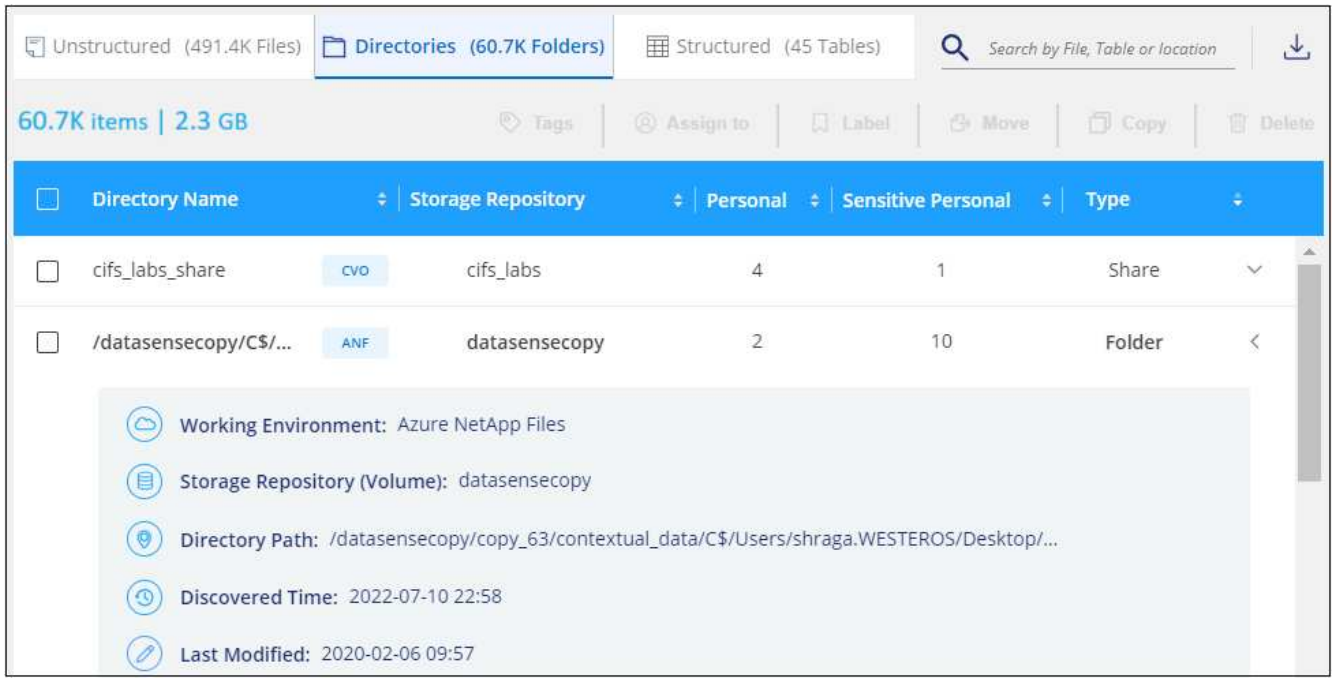
3. Um die Daten für eine bestimmte Art von personenbezogenen Daten zu untersuchen, klicken Sie auf **Alle anzeigen** und dann auf das Symbol **Ergebnisse untersuchen** für einen bestimmten Typ von personenbezogenen Daten, z. B. E-Mail-Adressen.



4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

   Die beiden Screenshots unten zeigen persönliche Daten in einzelnen Dateien gefunden, und in Dateien in Verzeichnissen (Freigaben und Ordner). Sie können auch die Registerkarte **Structured** auswählen, um persönliche Daten in Datenbanken anzuzeigen.





Dateien anzeigen, die sensible personenbezogene Daten enthalten

Die BlueXP Klassifizierung identifiziert automatisch besondere Arten von sensiblen personenbezogenen Daten, wie sie beispielsweise durch Datenschutzvorschriften definiert sind "Artikel 9 und 10 der DSGVO". Beispielsweise Informationen über die Gesundheit einer Person, ethnische Herkunft oder sexuelle Orientierung. "Die vollständige Liste finden Sie hier". Durch die BlueXP Klassifizierung wird diese Art von Informationen in einzelnen Dateien, in Dateien innerhalb von Verzeichnissen (Freigaben und Ordner) oder in Datenbanktabellen identifiziert.

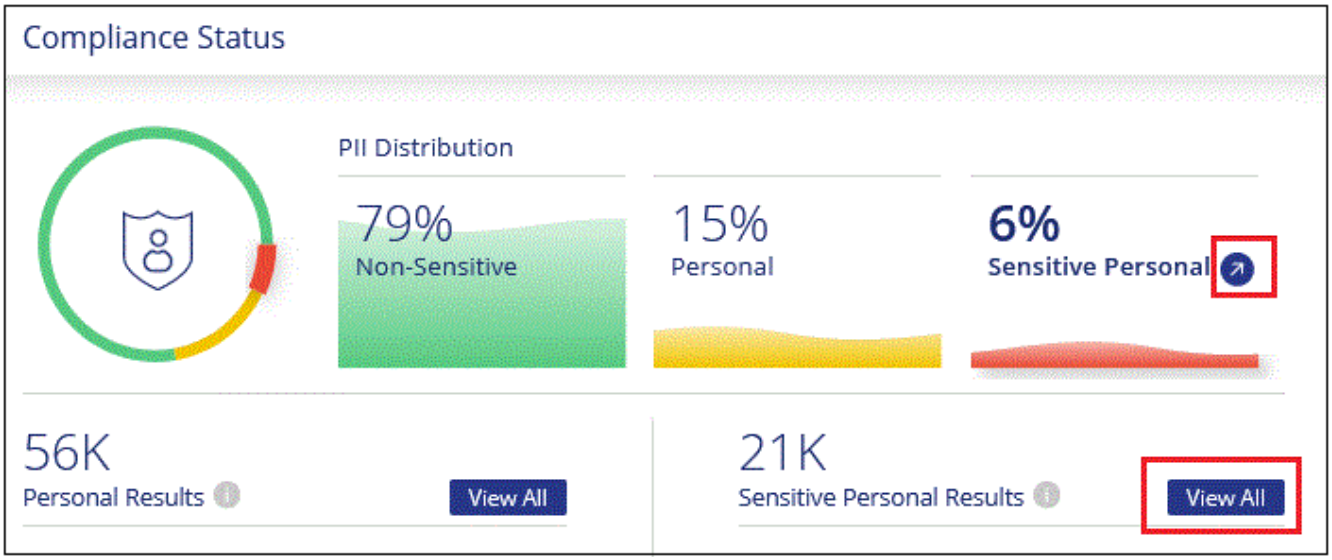
Die BlueXP Klassifizierung verwendet künstliche Intelligenz (KI), Natural Language Processing (NLP), Machine Learning (ML) und Cognitive Computing (CC), um die Bedeutung des gescannten Inhalts zu verstehen. Anhand dessen werden Entitäten extrahiert und entsprechend kategorisiert.

Beispielsweise ist eine sensitive DSGVO-Datenkategorie ethnisch Ursprungs. Aufgrund der NLP-Fähigkeiten kann die BlueXP Klassifizierung den Unterschied zwischen einem Satz unterscheiden: „George ist Mexikaner“ (sensible sensible sensible Daten gemäß DSGVO, Artikel 9) und „George isst Mexikanisch“.

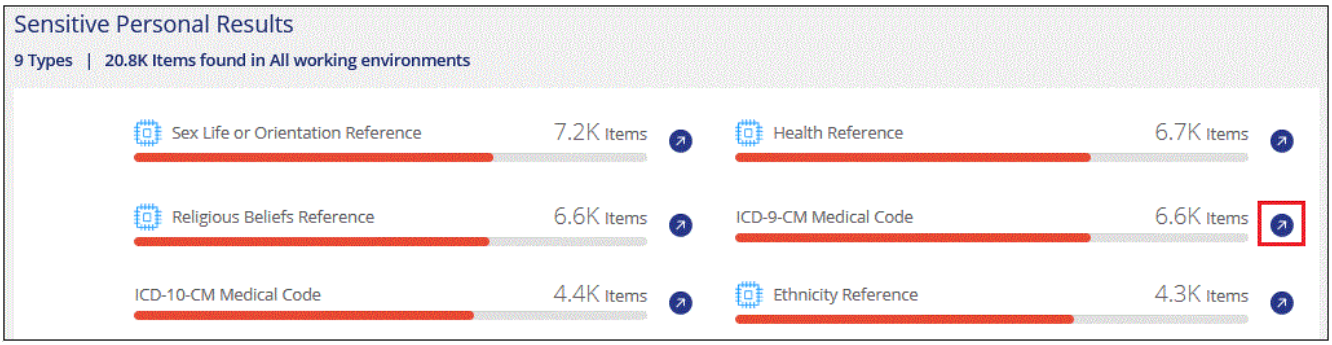
> Nur Englisch wird beim Scannen sensibler personenbezogener Daten unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Compliance**.
2. Um die Details für alle sensiblen persönlichen Daten zu untersuchen, klicken Sie auf das Symbol neben dem Prozentsatz sensibler personenbezogener Daten.



3. Um die Details für eine bestimmte Art sensibler personenbezogener Daten zu untersuchen, klicken Sie auf **Alle anzeigen** und klicken Sie dann auf das Symbol **Ergebnisse untersuchen** für einen bestimmten Typ sensibler personenbezogener Daten.



4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

Dateien nach Kategorien anzeigen

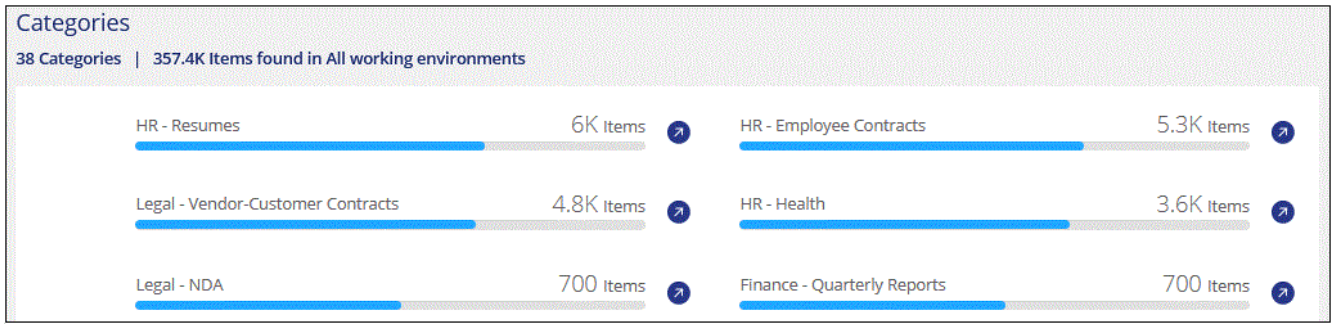
Die BlueXP Klassifizierung unterteilt die gescannten Daten in unterschiedliche Kategorien. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Siehe die Liste der Kategorien".

Kategorien können Ihnen dabei helfen zu verstehen, was mit Ihren Daten passiert, indem Sie die Arten von Informationen anzeigen, die Sie haben. Beispielsweise kann eine Kategorie wie Lebensläufe oder Mitarbeiterverträge sensible Daten enthalten. Wenn Sie die Ergebnisse untersuchen, können Sie feststellen, dass Mitarbeiterverträge an einem unsicheren Ort gespeichert sind. Sie können das Problem dann beheben.

> Englisch, Deutsch und Spanisch werden für Kategorien unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Compliance**.
2. Klicken Sie auf das Symbol **Ergebnisse untersuchen** für eine der 4 Top-Kategorien direkt im Hauptbildschirm oder klicken Sie auf **Alle anzeigen** und dann auf das Symbol für eine der Kategorien.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

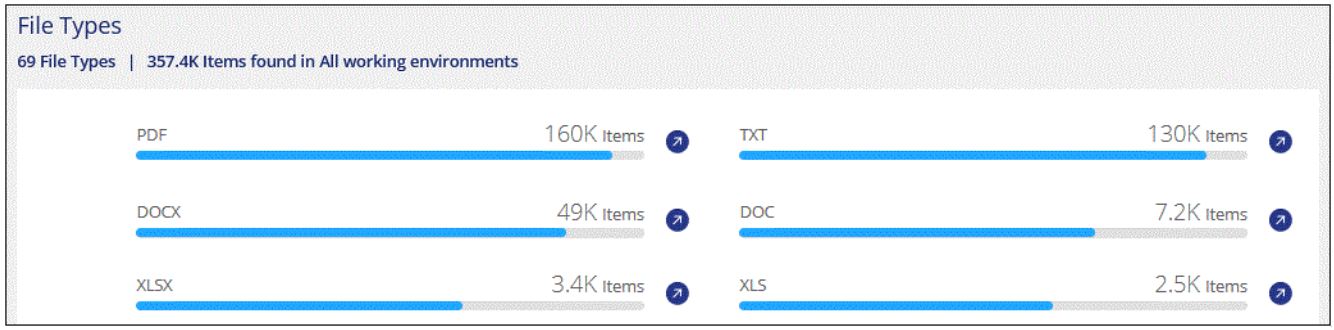
Dateien nach Dateitypen anzeigen

Die BlueXP Klassifizierung unterteilt die gescannten Daten nach Dateityp. Die Überprüfung Ihrer Dateitypen kann Ihnen helfen, Ihre sensiblen Daten zu kontrollieren, da Sie möglicherweise feststellen können, dass bestimmte Dateitypen nicht richtig gespeichert sind. "Siehe die Liste der Dateitypen".

Sie können beispielsweise CAD-Dateien speichern, die sehr sensible Informationen über Ihr Unternehmen enthalten. Wenn diese nicht gesichert sind, können Sie die Kontrolle über vertrauliche Daten übernehmen, indem Sie Berechtigungen beschränken oder Dateien an einen anderen Speicherort verschieben.

Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Compliance**.
2. Klicken Sie auf das Symbol **Ergebnisse untersuchen** für einen der 4 wichtigsten Dateitypen direkt vom Hauptbildschirm aus, oder klicken Sie auf **Alle anzeigen** und dann auf das Symbol für einen der Dateitypen.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

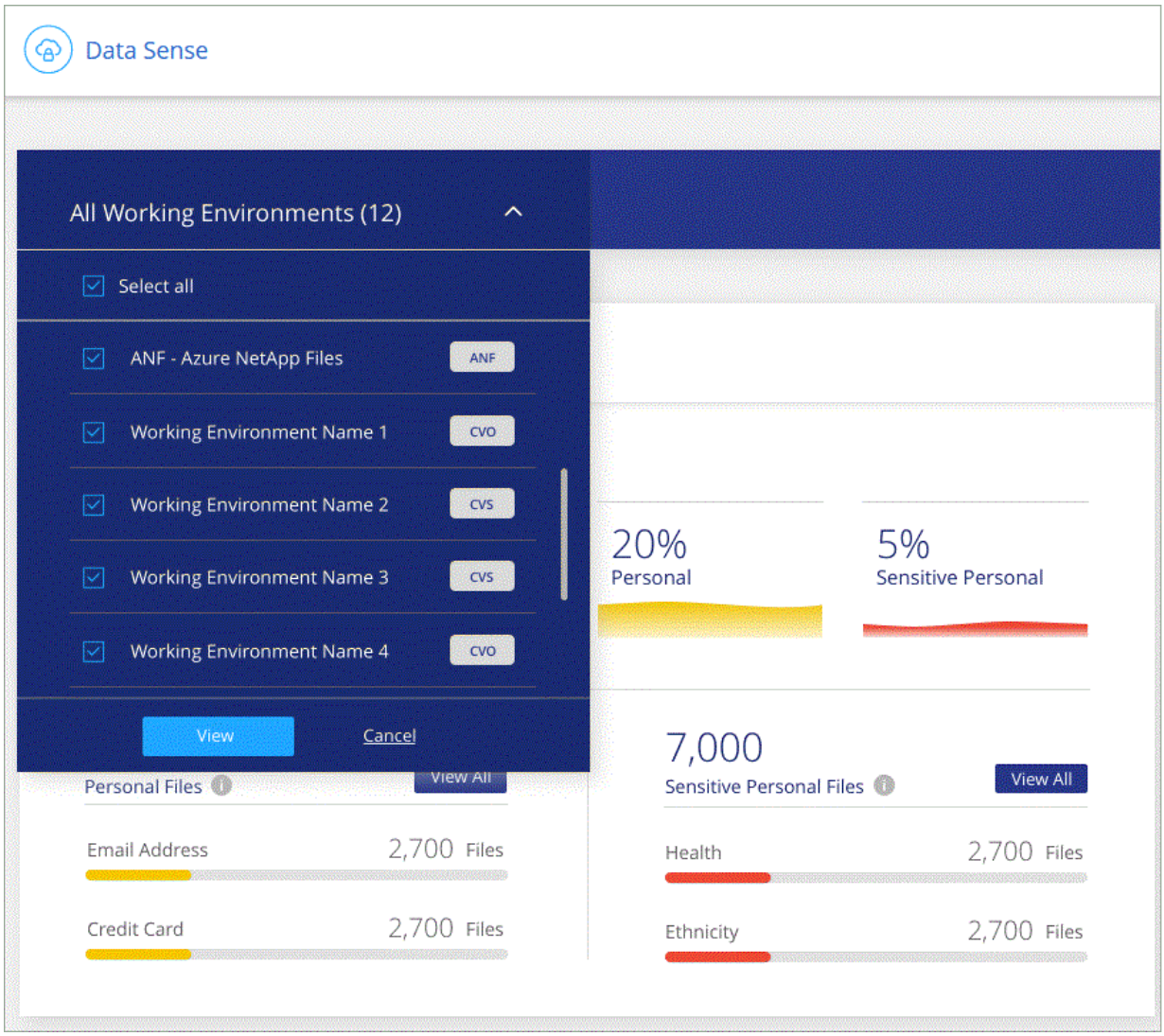
Anzeigen von Dashboard-Daten für bestimmte Arbeitsumgebungen

Sie können die Inhalte des BlueXP Klassifizierungs-Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur für bestimmte Arbeitsumgebungen einzusehen.

Wenn Sie das Dashboard filtern, erfasst die BlueXP Klassifizierung die Compliance-Daten und Berichte nur an die von Ihnen ausgewählten Applikationsumgebungen.

Schritte

1. Klicken Sie auf das Dropdown-Menü Filter, wählen Sie die Arbeitsumgebungen aus, für die Sie Daten anzeigen möchten, und klicken Sie auf **Ansicht**.



Kategorien von privaten Daten

Es gibt viele Arten von privaten Daten, die durch die BlueXP Klassifizierung in Ihren Volumes, Amazon S3 Buckets, Datenbanken, OneDrive-Ordnern, SharePoint-Konten identifiziert werden können. Und Google Drive-Konten. Sehen Sie sich die folgenden Kategorien an.

> Wenn Sie zur Identifizierung anderer privater Datentypen die Klassifizierung von BlueXP benötigen, z. B. zusätzliche nationale ID-Nummern oder Identifikatoren in Ihrem Gesundheitswesen, senden Sie eine E-Mail an ng-contact-data-sense@netapp.com.

Arten personenbezogener Daten

Die in Dateien gefundenen personenbezogenen Daten können allgemeine personenbezogene Daten oder nationale Kennungen sein. In der dritten Spalte der Tabelle unten wird angegeben, ob die BlueXP Klassifizierung verwendet "Prüfung der Nähe" Zum Validieren seiner Ergebnisse für die Kennung.

Die Sprachen, in denen diese Elemente erkannt werden können, sind in der Tabelle aufgeführt.

Beachten Sie, dass Sie der Liste der persönlichen Daten, die in Ihren Dateien gefunden werden, hinzufügen können. Wenn Sie einen Datenbankserver scannen, können Sie mit der Funktion *Data Fusion* zusätzliche Kennungen auswählen, nach denen die BlueXP-Klassifizierung in ihren Scans suchen wird, indem Sie Spalten in einer Datenbanktabelle auswählen. Sie können auch benutzerdefinierte Schlüsselwörter aus einer Textdatei oder benutzerdefinierte Muster mit einem regulären Ausdruck hinzufügen. Siehe "Hinzufügen persönlicher Daten-IDs zu Ihren BlueXP Klassifizierungs-Scans" Entsprechende Details.

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	Japanisch
Allgemein	Kreditkartennummer	Nein	✓	✓	✓		✓
	Betroffenen	Nein	✓	✓	✓		
	E-Mail-Adresse	Nein	✓	✓	✓		✓
	IBAN-Nummer (internationale Bankkontonummer)	Nein	✓	✓	✓		✓
	IP-Adresse	Nein	✓	✓	✓		✓
	Passwort	Ja.	✓	✓	✓		✓

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	Japanisch
Nationale Kennungen							

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	Japanisch
	Bankkontonummern						
	Sozialversicherungsnummer	Ja.	✓	✓	✓		
	Steuernummer (Steuerliche Identifikationsnummer)	Ja.	✓	✓	✓		
	Griechische ID	Ja.	✓	✓	✓		
	Ungarische Steuernummer	Ja.	✓	✓	✓		
	Irish ID (PPS)	Ja.	✓	✓	✓		
	Israelische ID	Ja.	✓	✓	✓		
	Italienische Steuernummer	Ja.	✓	✓	✓		
	Japanische Personal Identification Number (Privat- und Firmennummer)	Ja.	✓	✓	✓		✓
	Lettischer Ausweis	Ja.	✓	✓	✓		
	Litauische ID	Ja.	✓	✓	✓		
	Luxemburg-ID	Ja.	✓	✓	✓		
	Maltesische ID	Ja.	✓	✓	✓		
	NHS-Nummer (National Health Service)	Ja.	✓	✓	✓		
	Konto Einer Neuseeländischen Bank	Ja.	✓	✓	✓		
	Führerschein in Neuseeland	Ja.	✓	✓	✓		
	Neuseeland-IRD-Nummer (Steuernummer)	Ja.	✓	✓	✓		
	Neuseeland NHI (National Health Index) Nummer	Ja.	✓	✓	✓		
	Neuseeländische Passnummer	Ja.	✓	✓	✓		
	Polish ID (PESEL)	Ja.	✓	✓	✓		
	Portugiesische Steuernummer (NIF)	Ja.	✓	✓	✓		
	Rumänische ID (CNP)	Ja.	✓	✓	✓		
	Personalausweis für die nationale Registrierung in Singapur (NRIC)	Ja.	✓	✓	✓		
	Slowenische ID (EMSO)	Ja.	✓	✓	✓		
	Südafrikanischer Ausweis	Ja.	✓	✓	✓		
	Spanische Steuernummer	Ja.	✓	✓	✓		
	Schwedische ID	Ja.	✓	✓	✓		
	Texas Driver’s License	Ja.	✓	✓	✓		
	GROSSBRITANNIEN ID (NINO)	Ja.	✓	✓	✓		
	USA California Driver’s License	Ja.	✓	✓	✓		
	USA Indiana Führerschein	Ja.	✓	✓	✓		
	USA New York Führerschein	Ja.	✓	✓	✓		
	USA Sozialversicherungsnummer (SSN)	Ja.	✓	✓	✓		

Arten sensibler personenbezogener Daten

Die sensiblen personenbezogenen Daten, die die BlueXP Klassifizierung in Dateien finden kann, enthalten die folgende Liste.

Die Artikel in dieser Kategorie können derzeit nur auf Englisch erkannt werden.

Referenz Für Kriminelle Verfahren
: Daten zu strafrechtlichen Überzeugungen und Straftaten einer natürlichen Person.

Ethnische Referenz
: Daten über die rassische oder ethnische Herkunft einer natürlichen Person.

Systemzustand
: Daten über die Gesundheit einer natürlichen Person.

ICD-9-CM-Ärztliche Codes
: Codes, die in der Medizin- und Gesundheitsbranche verwendet werden.

ICD-10-CM-Ärztliche Codes
: Codes, die in der Medizin- und Gesundheitsbranche verwendet werden.

Philosophische Überzeugungen Referenz
: Daten über die philosophischen Überzeugungen einer natürlichen Person.

Politische Meinungen Referenz
: Daten über die politischen Meinungen einer natürlichen Person.

Religiöse Überzeugungen Referenz
: Daten über die religiösen Überzeugungen einer natürlichen Person.

Sexualleben oder Orientierung Referenz
: Daten über das Sexualleben einer natürlichen Person oder die sexuelle Orientierung.

Arten von Kategorien

Die BlueXP Klassifizierung kategorisiert Ihre Daten wie folgt.

Die meisten dieser Kategorien können in Englisch, Deutsch und Spanisch anerkannt werden.

Kategorie	Typ	Englisch	Deutsch	Spanisch
Finanzen	Bilanz	✓	✓	✓
	Bestellungen	✓	✓	✓
	Rechnungen	✓	✓	✓
	Vierteljährliche Berichte	✓	✓	✓

Kategorie	Typ	Englisch	Deutsch	Spanisch
HR	Background-Checks	✓		✓
	Vergütungspläne	✓	✓	✓
	Mitarbeiterverträge	✓		✓
	Mitarbeiterbewertung	✓		✓
	Systemzustand	✓		✓
	Wird Fortgesetzt	✓	✓	✓
Legal	NDAs	✓	✓	✓
	Verträge zwischen Anbietern und Kunden	✓	✓	✓
Marketing	Kampagnen	✓	✓	✓
	Konferenzen	✓	✓	✓
Betrieb	Audit-Berichte	✓	✓	✓
Vertrieb	Aufträge	✓	✓	
Services	RFI	✓		✓
	AUSSCHREIBUNG	✓		✓
	SOW	✓	✓	✓
	Schulung	✓	✓	✓
Unterstützung	Reklamationen und Tickets	✓	✓	✓

Die folgenden Metadaten werden ebenfalls kategorisiert und in den gleichen unterstützten Sprachen identifiziert:

- Applikationsdaten
- Archivdateien
- Audio
- Daten Von Business-Applikationen
- CAD-Dateien
- Codieren
- Beschädigt
- Datenbank- und Indexdateien
- BlueXP Klassifizierungs-Breadcrumbs
- Design-Dateien
- E-Mail-Anwendungsdaten
- Verschlüsselt (Dateien mit hohem Entropie-Wert)
- Ausführbare Dateien
- Daten Aus Finanzapplikationen

- Daten Der Integritätsanwendungen
- Bilder
- Protokolle
- Verschiedene Dokumente
- Diverse Präsentationen
- Verschiedene Tabellenkalkulationen
- Verschiedenes „Unbekannt“
- Passwortgeschützte Dateien
- Strukturierte Daten
- Videos
- Zero-Byte-Dateien

Dateitypen

Die BlueXP Klassifizierung scannt alle Dateien nach Kategorien- und Metadaten und zeigt alle Dateitypen im Abschnitt „Dateitypen“ des Dashboards an.

Wenn jedoch die BlueXP Klassifizierung personenbezogene Daten erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt:

```
.CSV, .DCM, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX,
Docs, Sheets, and Slides
```

Genauigkeit der gefundenen Informationen

NetApp kann die Genauigkeit der personenbezogenen Daten und sensiblen personenbezogenen Daten, die durch die BlueXP Klassifizierung identifiziert werden, nicht zu 100 % garantieren. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Basierend auf unseren Tests zeigt die folgende Tabelle die Genauigkeit der Informationen, die bei der BlueXP Klassifizierung als Ergebnis zu finden sind. Wir brechen es durch *Precision* und *Recall* ab:

Präzision

Die Wahrscheinlichkeit, dass die gefundenen Elemente der BlueXP Klassifizierung korrekt identifiziert wurden. Beispielsweise bedeutet eine Datengenauigkeit von 90% für personenbezogene Daten, dass 9 von 10 Dateien, die als personenbezogene Daten identifiziert werden, tatsächlich personenbezogene Daten enthalten. 1 von 10 Dateien wäre falsch positiv.

Rückruf

Die Wahrscheinlichkeit, dass die BlueXP Klassifizierung ihre Inhalte findet. Beispielsweise bedeutet eine Rückrufrate von 70 % für personenbezogene Daten, dass die BlueXP Klassifizierung 7 von 10 Dateien identifizieren kann, die tatsächlich personenbezogene Daten in Ihrem Unternehmen enthalten. Die BlueXP Klassifizierung würde 30 % der Daten verfehlen und wird dann nicht im Dashboard angezeigt.

Wir verbessern die Genauigkeit unserer Ergebnisse ständig. Diese Verbesserungen werden in zukünftigen BlueXP Klassifizierungs-Releases automatisch zur Verfügung stehen.

Typ	Präzision	Rückruf
Personenbezogene Daten - Allgemeines	90 % - 95 %	60 % - 80 %
Persönliche Daten – Länderkennungen	30 % - 60 %	40 % - 60 %
Sensible persönliche Daten	80 % - 95 %	20 % - 30 %
Kategorien	90 % - 97 %	60 % - 80 %

Untersuchen Sie die in Ihrem Unternehmen gespeicherten Daten

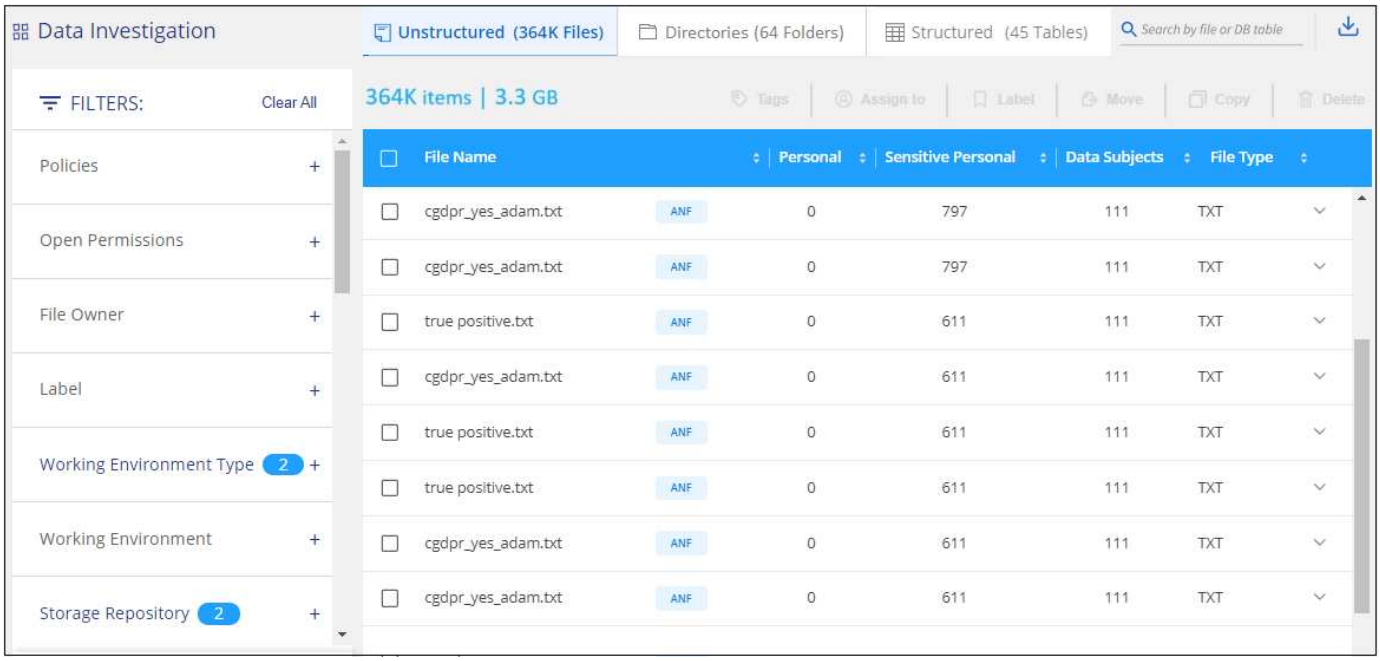
Sie können die Daten Ihres Unternehmens untersuchen, indem Sie Details auf der Seite „Datenuntersuchung“ anzeigen. Sie können diese Seite aus vielen Bereichen der BlueXP Klassifizierungs-UI aufrufen, einschließlich der Governance- und Compliance-Dashboards.

> Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.

Filtern Sie die Daten auf der Seite „Datenuntersuchung“

Sie können den Inhalt der Untersuchungsseite filtern, um nur die Ergebnisse anzuzeigen, die Sie sehen möchten. Dies ist eine sehr leistungsstarke Funktion, denn nachdem Sie die Daten verfeinert haben, können Sie die Buttonleiste oben auf der Seite verwenden, um eine Vielzahl von Aktionen durchzuführen, wie das Kopieren von Dateien, Verschieben von Dateien, Hinzufügen eines Tags oder AIP-Label zu den Dateien und vieles mehr.

Wenn Sie den Inhalt der Seite nach der Verarbeitung als Bericht herunterladen möchten, klicken Sie auf die Schaltfläche Schaltfläche. Einzelheiten zum Untersuchungsbericht zu Daten finden Sie hier.



- Auf den Registerkarten der obersten Ebene können Sie Daten aus Dateien (unstrukturierte Daten), Verzeichnissen (Ordner und Dateifreigaben) oder Datenbanken (strukturierte Daten) anzeigen.
- Mit den Steuerelementen oben in jeder Spalte können Sie die Ergebnisse in numerischer oder alphabetischer Reihenfolge sortieren.
- Mit den Filtern im linken Fensterbereich können Sie die Ergebnisse verfeinern, indem Sie die in den nächsten Abschnitten beschriebenen Attribute auswählen.

Filtern von Daten nach Sensitivität und Inhalt

Mithilfe der folgenden Filter können Sie anzeigen, wie viele vertrauliche Informationen in Ihren Daten enthalten sind.

Filtern	Details
Kategorie	Wählen Sie die aus "Arten von Kategorien".
Empfindlichkeitsstufe	Wählen Sie die Empfindlichkeitsstufe aus: Persönlich, sensibel persönlich oder nicht empfindlich.
Anzahl der Kennungen	Wählen Sie den Bereich der erkannten empfindlichen Kennungen pro Datei aus. Hierzu zählen personenbezogene Daten und sensible personenbezogene Daten. Beim Filtern in Verzeichnissen ergibt die BlueXP Klassifizierung insgesamt die Treffer aus allen Dateien in jedem Ordner (und in Unterordnern). HINWEIS: Die Veröffentlichung von Dezember 2023 (Version 1.26.6) hat die Möglichkeit, die Anzahl der personenbezogenen Daten (PII) nach Verzeichnissen zu berechnen, vorübergehend entfernt.
Persönliche Daten	Wählen Sie die aus "Arten personenbezogener Daten".
Sensible Personenbezogene Daten	Wählen Sie die aus "Arten sensibler personenbezogener Daten".
Betroffene Person	Geben Sie den vollständigen Namen oder die bekannte Kennung eines Betroffenen ein. "Weitere Informationen zu Datensubjekten finden Sie hier".

Filtern Sie Daten nach Benutzereigern und Benutzerberechtigungen

Verwenden Sie die folgenden Filter, um Dateibesitzer und Berechtigungen für den Zugriff auf Ihre Daten anzuzeigen.

Filtern	Details
Öffnen Sie Berechtigungen	Wählen Sie den Berechtigungstyp innerhalb der Daten und in Ordnern/Shares aus.
Benutzer-/Gruppenberechtigungen	Wählen Sie einen oder mehrere Benutzernamen und/oder Gruppennamen aus, oder geben Sie einen Teilnamen ein.
Dateieigentümer	Geben Sie den Namen des Dateieigentümers ein.
Anzahl der Benutzer mit Zugriff	Wählen Sie einen oder mehrere Kategoriebereiche aus, um anzuzeigen, welche Dateien und Ordner für eine bestimmte Anzahl von Benutzern geöffnet sind.

Filtern Sie Daten nach Zeit

Verwenden Sie die folgenden Filter, um Daten basierend auf den Zeitkriterien anzuzeigen.

Filtern	Details
Erstellungszeit	Wählen Sie einen Zeitbereich aus, in dem die Datei erstellt wurde. Sie können auch einen benutzerdefinierten Zeitbereich angeben, um die Suchergebnisse weiter zu verfeinern.
Entdeckte Zeit	Wählen Sie einen Zeitraum aus, in dem die BlueXP Klassifizierung die Datei erkannt hat. Sie können auch einen benutzerdefinierten Zeitbereich angeben, um die Suchergebnisse weiter zu verfeinern.
Zuletzt Geändert	Wählen Sie einen Zeitbereich aus, in dem die Datei zuletzt geändert wurde. Sie können auch einen benutzerdefinierten Zeitbereich angeben, um die Suchergebnisse weiter zu verfeinern.
Zuletzt Aufgerufen	Wählen Sie einen Zeitraum aus, in dem zuletzt auf die Datei oder das Verzeichnis (nur CIFS oder NFS) zugegriffen wurde. Sie können auch einen benutzerdefinierten Zeitbereich angeben, um die Suchergebnisse weiter zu verfeinern. Für die Dateitypen, die die BlueXP Klassifizierung scannt, wurde die Datei zuletzt durch die BlueXP Klassifizierung gescannt. Beachten Sie, dass die Klassifizierung durch BlueXP nicht zur Zeit des letzten Zugriffs aus den folgenden Datenquellen herangezogen wird: SharePoint Online, SharePoint On-Premises (SharePoint Server), OneDrive, Google Drive und Amazon S3.

Filtern Sie Daten nach Metadaten

Verwenden Sie die folgenden Filter, um Daten auf der Grundlage von Speicherort, Größe und Verzeichnis oder Dateityp anzuzeigen.

Filtern	Details
Dateipfad	Geben Sie bis zu 20 Teilpfade oder vollständige Pfade ein, die in die Abfrage einbezogen oder ausgeschlossen werden sollen. Wenn Sie beide Einschlusspfade eingeben und Pfade ausschließen, werden bei der BlueXP Klassifizierung zuerst alle Dateien in den eingeschlossenen Pfaden gefunden. Anschließend werden Dateien aus ausgeschlossenen Pfaden entfernt, und die Ergebnisse werden angezeigt. Beachten Sie, dass die Verwendung von "*" in diesem Filter keine Wirkung hat und dass Sie bestimmte Ordner nicht aus dem Scan ausschließen können - alle Verzeichnisse und Dateien unter einer konfigurierten Freigabe werden gescannt.
Verzeichnistyp	Wählen Sie den Verzeichnistyp aus, entweder „Share“ oder „Folder“.
Dateityp	Wählen Sie die aus "Dateitypen".
Dateigröße	Wählen Sie den Dateigrößenbereich aus.
Datei-Hash	Geben Sie den Hash der Datei ein, um eine bestimmte Datei zu finden, selbst wenn der Name anders ist.

Filtern Sie Ihre Daten nach Storage-Typ

Verwenden Sie die folgenden Filter, um Daten nach Speichertyp anzuzeigen.

Filtern	Details
Art Der Arbeitsumgebung	Wählen Sie den Typ der Arbeitsumgebung aus. OneDrive, SharePoint und Google Drive sind unter „Apps“ kategorisiert.
Name der Arbeitsumgebung	Wählen Sie spezielle Arbeitsumgebungen aus.
Storage Repository	Wählen Sie das Speicher-Repository aus, z. B. ein Volume oder ein Schema.

Filtern Sie Daten nach Tags, Labels, zugewiesenen Benutzern und Richtlinien

Verwenden Sie die folgenden Filter, um Daten nach AIP-Etiketten oder -Tags anzuzeigen.

Filtern	Details
Richtlinien	Wählen Sie eine Richtlinie oder Richtlinien aus. Los "Hier" Um die Liste der vorhandenen Richtlinien anzuzeigen und eigene Richtlinien zu erstellen.
Etikett	Wählen Sie "AIP-Etiketten" Die Ihren Dateien zugewiesen sind.
Tags	Wählen Sie "Das Tag oder die Tags" Die Ihren Dateien zugewiesen sind.
Zugewiesen Zu	Wählen Sie den Namen der Person aus, der die Datei zugeordnet ist.

Filtern Sie Daten nach Analysestatus

Verwenden Sie den folgenden Filter, um Daten nach dem BlueXP Klassifizierungs-Scan-Status anzuzeigen.

Filtern	Details
Analysestatus	Wählen Sie eine Option aus, um die Liste der Dateien anzuzeigen, die den ersten Scan ausstehend, den Scanvorgang abgeschlossen haben, den ausstehenden Rescan oder die nicht gescannt wurden.
Analyseereignis Scannen	Wählen Sie aus, ob Dateien angezeigt werden sollen, die nicht klassifiziert wurden, weil die BlueXP-Klassifizierung die Uhrzeit des letzten Zugriffs nicht rückgängig machen konnte, oder Dateien, die klassifiziert wurden, obwohl die BlueXP-Klassifizierung die Zeit des letzten Zugriffs nicht rückgängig machen konnte.

"Weitere Informationen zum Zeitstempel des letzten Zugriffs" Weitere Informationen zu den Elementen, die beim Filtern mit dem Ereignis Scananalyse auf der Seite Untersuchung angezeigt werden.

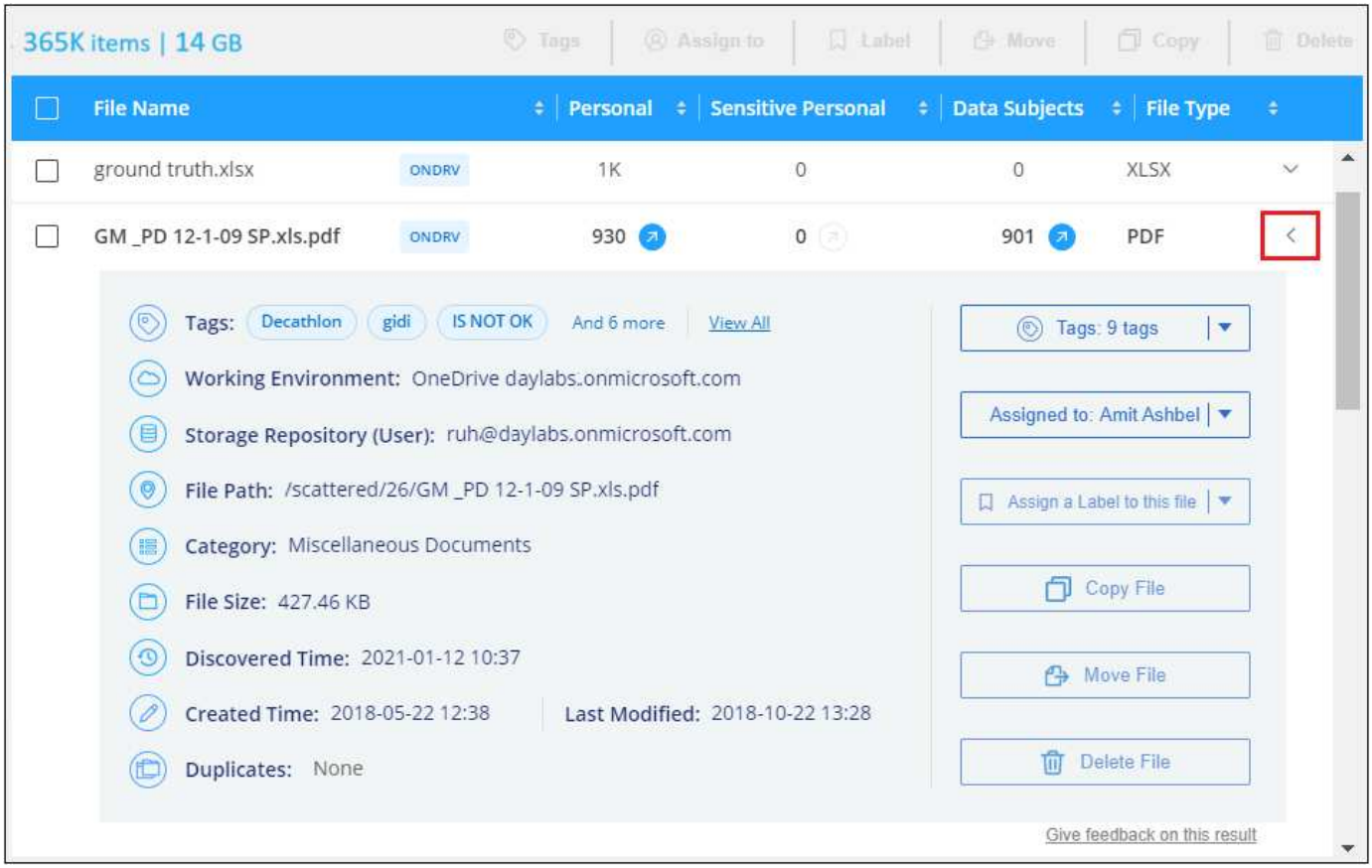
Daten nach Duplikaten filtern

Verwenden Sie den folgenden Filter, um Dateien anzuzeigen, die im Speicher dupliziert wurden.

Filtern	Details
Duplikate	Wählen Sie aus, ob die Datei in den Repositorys dupliziert wird.

Anzeigen von Datei-Metadaten

Klicken Sie im Bereich „Untersuchungsergebnisse“ auf ⌄ Für jede einzelne Datei, um die Dateimetadaten anzuzeigen.



Zusätzlich zur Anzeige der Arbeitsumgebung und des Volumes, in dem sich die Datei befindet, werden durch die Metadaten viel mehr Informationen angezeigt, einschließlich der Dateiberechtigungen, des Dateieigentümers, ob es Duplikate dieser Datei gibt und des zugewiesenen AIP-Etiketts (falls vorhanden) "Integrierte AIP in BlueXP Klassifizierung"). Diese Informationen sind hilfreich, wenn Sie Vorhaben "Erstellen von Richtlinien" Da Sie alle Informationen anzeigen können, die Sie zum Filtern Ihrer Daten verwenden können.

Beachten Sie, dass nicht alle Informationen für alle Datenquellen verfügbar sind – und genau die Informationen, die sich für diese Datenquelle eignen. Beispielsweise sind der Volume-Name, die Berechtigungen und AIP-Labels nicht für Datenbankdateien relevant.

Wenn Sie die Details für eine einzelne Datei anzeigen, gibt es einige Aktionen, die Sie für die Datei ergreifen können:

- Sie können die Datei verschieben oder in eine beliebige NFS-Freigabe kopieren. Siehe "Quelldateien werden in eine NFS-Freigabe verschoben" Und "Quelldateien werden in eine NFS-Freigabe kopiert" Entsprechende Details.
- Sie können die Datei löschen. Siehe "Quelldateien werden gelöscht" Entsprechende Details.
- Sie können der Datei einen bestimmten Status zuweisen. Siehe "Tags werden angewendet" Entsprechende Details.
- Sie können die Datei einem BlueXP-Benutzer zuweisen, damit er für alle Follow-up-Aktionen verantwortlich ist, die in der Datei ausgeführt werden müssen. Siehe "Zuweisen von Benutzern zu einer Datei"

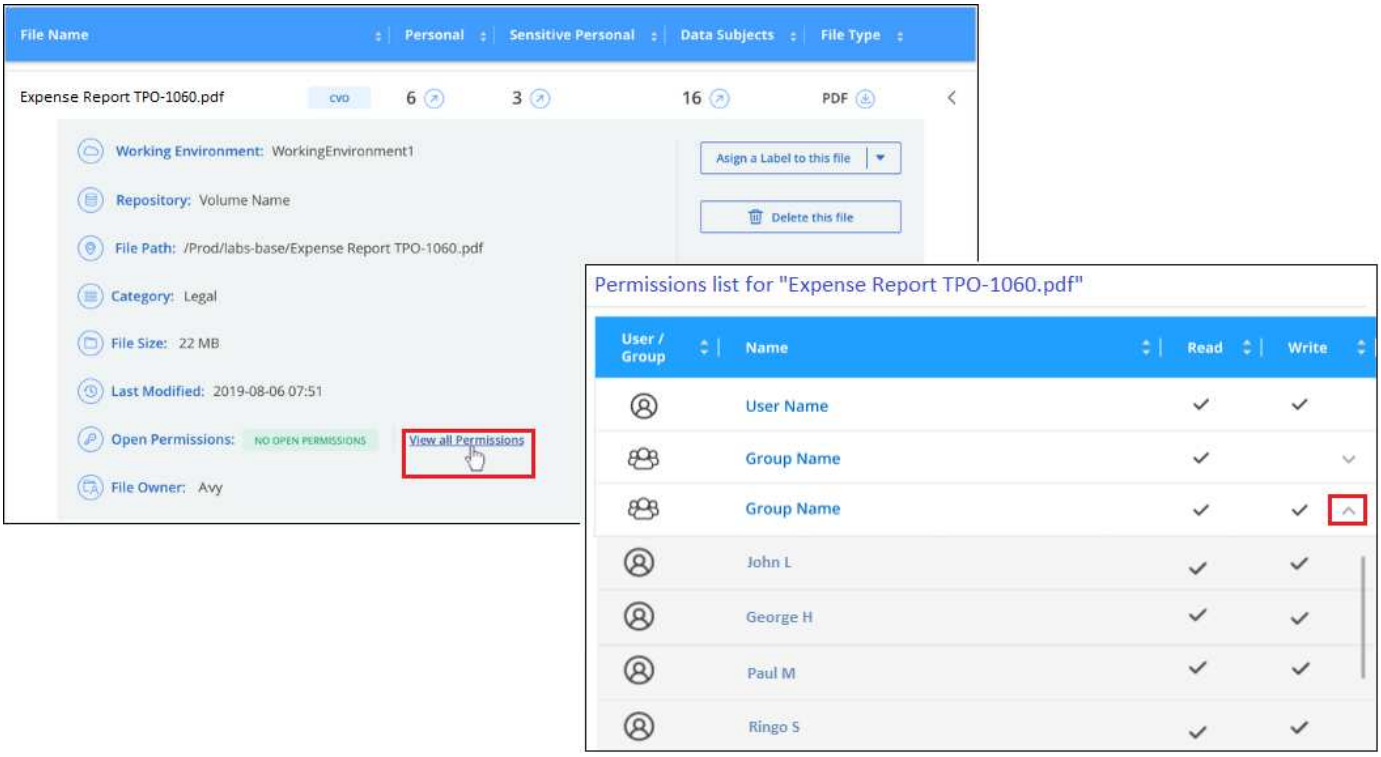
Entsprechende Details.

- Wenn Sie AIP-Labels mit der BlueXP-Klassifizierung integriert haben, können Sie dieser Datei eine Bezeichnung zuweisen oder, sofern vorhanden, zu einer anderen Bezeichnung wechseln. Siehe "Manuelles Zuweisen von AIP-Beschriftungen" Entsprechende Details.

Berechtigungen für Dateien und Verzeichnisse anzeigen

Um eine Liste aller Benutzer oder Gruppen anzuzeigen, die Zugriff auf eine Datei oder ein Verzeichnis haben, und die Arten von Berechtigungen, die sie haben, klicken Sie auf **Alle Berechtigungen anzeigen**. Diese Schaltfläche gilt nur für Daten in CIFS Shares, SharePoint Online, SharePoint On-Premises und OneDrive.

Wenn Sie SIDs (Security Identifiers) anstelle von Benutzer- und Gruppennamen sehen, sollten Sie Ihr Active Directory in die BlueXP Klassifizierung integrieren. "So geht's".



Klicken Sie auf ⌄ Für jede Gruppe, um die Liste der Benutzer anzuzeigen, die Teil der Gruppe sind.

Darüber Hinaus Sie können auf den Namen eines Benutzers oder einer Gruppe klicken und die Untersuchungsseite wird mit dem Namen dieses Benutzers oder dieser Gruppe angezeigt, der im Filter „Benutzer-/Gruppenberechtigungen“ ausgefüllt ist, sodass Sie alle Dateien und Verzeichnisse sehen können, auf die der Benutzer oder die Gruppe Zugriff hat.

Überprüfen Sie auf doppelte Dateien in Ihren Speichersystemen

Sie können sehen, ob doppelte Dateien auf Ihren Storage-Systemen gespeichert werden. Dies ist nützlich, wenn Sie Bereiche ermitteln möchten, in denen Sie Speicherplatz einsparen können. Zudem ist es hilfreich, sicherzustellen, dass Dateien mit bestimmten Berechtigungen oder vertraulichen Informationen in Ihren Speichersystemen nicht unnötig dupliziert werden.

Alle Ihre Dateien (ohne Datenbanken), die 1 MB oder größer sind und persönliche oder sensible personenbezogene Daten enthalten, werden verglichen, um zu sehen, ob es Duplikate gibt. Sie können die Filter auf der Untersuchungsseite „Dateigröße“ zusammen mit „Duplikate“ verwenden, um zu sehen, welche

Dateien eines bestimmten Größenbereichs in Ihrer Umgebung dupliziert werden.

Die BlueXP Klassifizierung verwendet Hashing-Technologie, um doppelte Dateien zu ermitteln. Wenn eine Datei den gleichen Hash-Code wie eine andere Datei hat, können wir zu 100% sicher sein, dass die Dateien exakte Duplikate sind - auch wenn die Dateinamen unterschiedlich sind.

Sie können die Liste mit doppelten Dateien herunterladen und an Ihren Storage-Administrator senden, damit er jederzeit entscheiden kann, welche Dateien gelöscht werden können. Oder Sie können "Löschen Sie die Datei" Wenn Sie sicher sind, dass keine bestimmte Version der Datei benötigt wird.

Alle duplizierten Dateien anzeigen

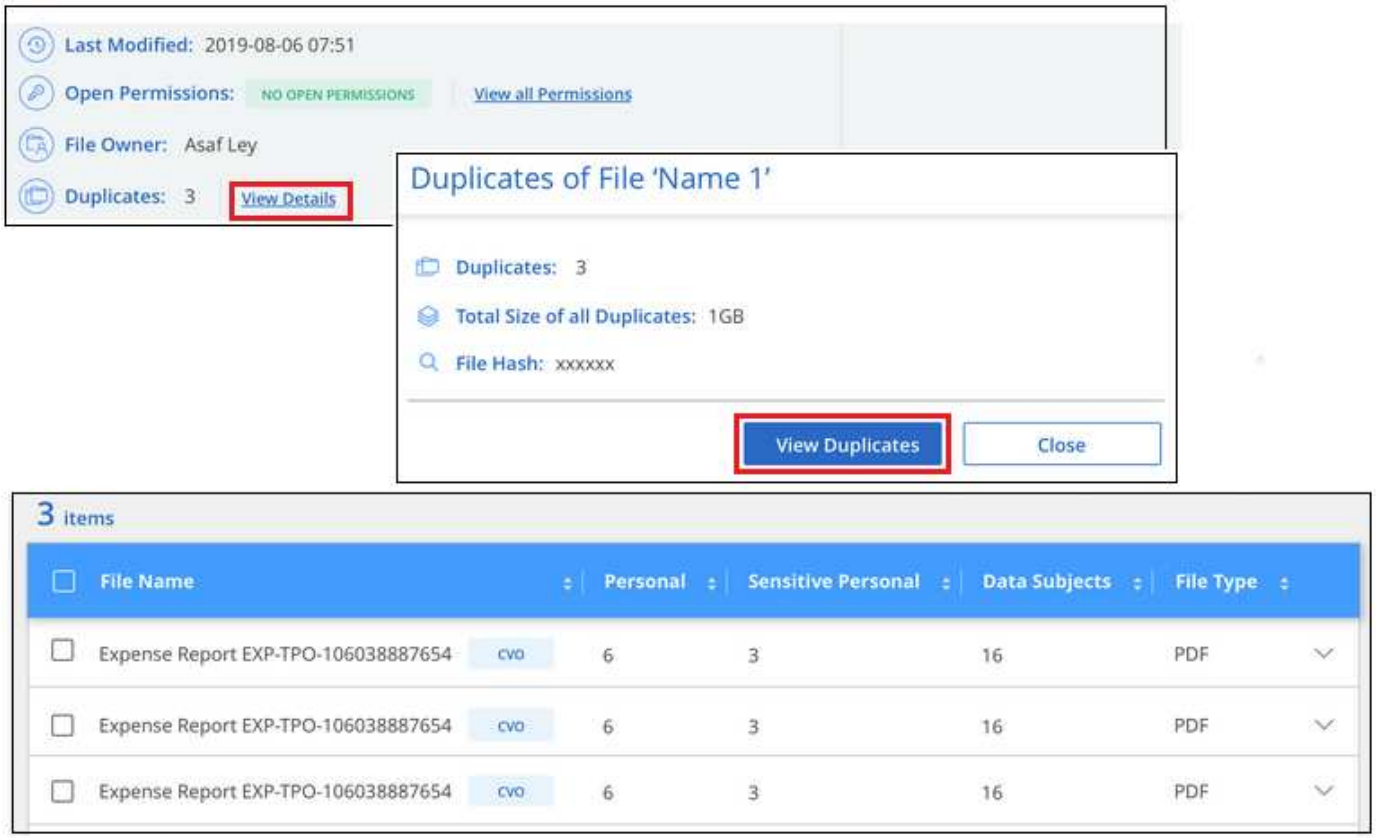
Wenn Sie eine Liste aller Dateien wünschen, die in den Arbeitsumgebungen und Datenquellen, die Sie scannen, dupliziert werden, können Sie den Filter **Duplicates > has Dubletten** auf der Seite Data Investigation verwenden.

Alle duplizierten Dateien werden auf der Ergebnisseite angezeigt.

Anzeigen, ob eine bestimmte Datei dupliziert wurde

Wenn Sie sehen möchten, ob eine einzelne Datei Duplikate enthält, klicken Sie im Bereich „Untersuchungsergebnisse“ auf ⌄ Für jede einzelne Datei, um die Dateimetadaten anzuzeigen. Wenn es Duplikate einer bestimmten Datei gibt, werden diese Informationen neben dem Feld *Duplicates* angezeigt.

Klicken Sie auf **Details anzeigen**, um die Liste der duplizierten Dateien anzuzeigen und wo sie sich befinden. Klicken Sie auf der nächsten Seite auf **Duplicates anzeigen**, um die Dateien auf der Untersuchungsseite anzuzeigen.



Sie können den auf dieser Seite angegebenen "Datei-Hash"-Wert verwenden und direkt auf der Untersuchungsseite eingeben, um jederzeit nach einer bestimmten doppelten Datei zu suchen - oder Sie können sie in einer Richtlinie verwenden.

Bericht Zur Datenuntersuchung

Der Untersuchungsbericht ist ein Download des gefilterten Inhalts der Seite Datenuntersuchung.

Der Bericht ist in zwei verschiedenen Formaten verfügbar:

- Als CSV-Datei, die Sie auf dem lokalen Computer speichern können.

  Dieser Bericht kann maximal 10,000 Datenzeilen enthalten.

- Als JSON-Datei, die Sie in eine NFS-Freigabe exportieren.

  Wenn mehr als 250,000 Datenzeilen vorhanden sind, werden zusätzliche JSON-Dateien erstellt.

  Stellen Sie beim Exportieren in eine Dateifreigabe sicher, dass die BlueXP Klassifizierung die richtigen Berechtigungen für den Exportzugriff hat.

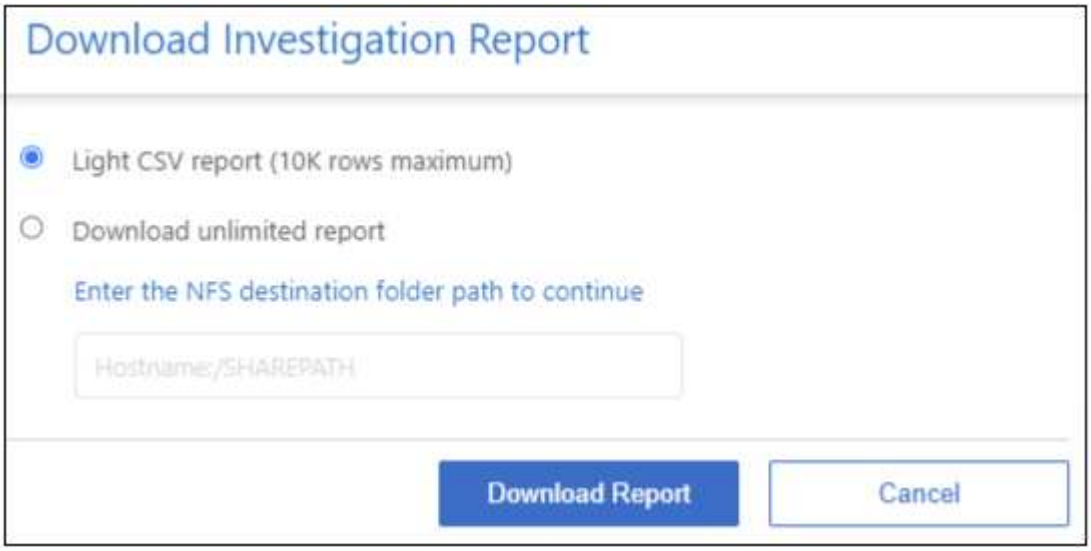
Es können bis zu drei Berichtsdateien heruntergeladen werden, wenn die BlueXP Klassifizierung Dateien (unstrukturierte Daten), Verzeichnisse (Ordner und Dateifreigaben) und Datenbanken (strukturierte Daten) scannt.

Generieren Sie den Bericht zur Datenermittlung

Schritte

1. Klicken Sie auf der Seite „Untersuchung von Daten“ auf Oben rechts auf der Seite klicken.
2. Wählen Sie aus, ob Sie einen .CSV-Bericht oder einen JSON-Bericht der Daten herunterladen möchten, und klicken Sie auf **Bericht herunterladen**.

   Geben Sie bei Auswahl eines JSON-Berichts den Namen der NFS-Freigabe ein, auf die der Bericht im Format heruntergeladen werden soll `<host_name>:/<share_path>`.



Ergebnis

Ein Dialogfeld zeigt eine Meldung an, dass die Berichte heruntergeladen werden.

Sie können den Fortschritt der JSON-Berichterstellung in anzeigen "Statusbereich Aktionen".

Was ist in den einzelnen Datenuntersuchungs-Berichten enthalten

Der Datenbericht **unstrukturierte Dateien** enthält folgende Informationen zu Ihren Dateien:

- Dateiname
- Positionstyp
- Name der Arbeitsumgebung
- Storage-Repository (z. B. Volume, Bucket, Shares)
- Repository-Typ
- Dateipfad
- Dateityp
- Dateigröße (in MB)
- Erstellungszeit
- Zuletzt geändert
- Zuletzt aufgerufen
- Dateibesitzer
- Kategorie
- Persönliche Angaben
- Sensible persönliche Daten
- Berechtigungen öffnen
- Fehler Bei Der Scananalyse
- Löscherkennung Datum

  Ein Löscherkennungsdatum gibt das Datum an, an dem die Datei gelöscht oder verschoben wurde. So können Sie feststellen, wann sensible Dateien verschoben wurden. Gelöschte Dateien sind nicht Teil der Anzahl der Dateinummern, die im Dashboard oder auf der Untersuchungsseite angezeigt wird. Die Dateien werden nur in den CSV-Berichten angezeigt.

Der Datenbericht für unstrukturierte Verzeichnisse* enthält die folgenden Informationen zu Ihren Ordnern und Dateifreigaben:

- Art der Arbeitsumgebung
- Name der Arbeitsumgebung
- Verzeichnisname
- Storage-Repository (beispielsweise ein Ordner oder Dateifreigaben)
- Verzeichniseigentümer
- Erstellungszeit
- Entdeckte Zeit

- Zuletzt geändert
- Zuletzt aufgerufen
- Berechtigungen öffnen
- Verzeichnistyp

Der **Structured Data Report** enthält die folgenden Informationen zu Ihren Datenbanktabellen:

- DB-Tabellenname
- Positionstyp
- Name der Arbeitsumgebung
- Storage-Repository (z. B. ein Schema)
- Anzahl der Spalten
- Zeilenanzahl
- Persönliche Angaben
- Sensible persönliche Daten

Private Daten organisieren

Die BlueXP Klassifizierung bietet Ihnen zahlreiche Möglichkeiten zum Managen und Organisieren Ihrer privaten Daten. Auf diese Weise können Sie die für Sie wichtigsten Daten besser einsehen.

- Wenn Sie abonniert sind "Azure Information Protection (AIP)" Um Ihre Dateien zu klassifizieren und zu schützen, können Sie diese AIP-Labels mit der BlueXP Klassifizierung managen.

> Mit der Veröffentlichung im Dezember 2023 (v1.26.6) wurde die Option zur Integration von Daten mit Azure Information Protection (AIP)-Labels vorübergehend aufgehoben.

- Sie können Tags zu Dateien hinzufügen, die Sie als Organisation oder für eine Art von Follow-up markieren möchten.
- Sie können einen BlueXP-Benutzer einer bestimmten Datei oder mehreren Dateien zuweisen, sodass diese Person für das Management der Datei verantwortlich ist.
- Mit der "Policy"-Funktion können Sie Ihre eigenen individuellen Suchanfragen erstellen, so dass Sie die Ergebnisse einfach durch Klicken auf eine Schaltfläche sehen können.
- Sie können E-Mail-Benachrichtigungen an BlueXP-Benutzer oder andere E-Mail-Adressen senden, wenn bestimmte kritische Richtlinien Ergebnisse liefern.

> Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.

Sollte ich Etiketten oder Etiketten verwenden?

Unten finden Sie einen Vergleich zwischen BlueXP Klassifizierungs-Tagging und Azure Information Protection Labelling.

Tags	Etiketten
Datei-Tags sind ein integrierter Teil der BlueXP Klassifizierung.	Voraussetzung ist, dass Sie den Azure Information Protection (AIP) abonniert haben.
Das Tag wird nur in der BlueXP Klassifizierungs-Datenbank aufbewahrt - es wird nicht in die Datei geschrieben. Die Datei oder die abgerufene oder geänderte Datei werden nicht geändert.	Die Bezeichnung ist Teil der Datei, und wenn sich die Bezeichnung ändert, ändert sich die Datei. Diese Änderung ändert auch die Zeiten, auf die zugegriffen wurde und die geändert wurden.
Sie können mehrere Tags für eine einzelne Datei haben.	Sie können eine Bezeichnung auf einer einzelnen Datei haben.
Das Tag kann für interne BlueXP-Klassifizierungsaktionen wie Kopieren, Verschieben, Löschen, Ausführen einer Richtlinie Usw.	Andere Systeme, die die Datei lesen können, können das Etikett sehen - welches für zusätzliche Automatisierung verwendet werden kann.
Nur ein einzelner API-Aufruf wird verwendet, um zu sehen, ob eine Datei ein Tag hat.	

Kategorisieren Sie Ihre Daten mit AIP-Etiketten

Sie können AIP-Etiketten in den Dateien managen, die die BlueXP Klassifizierung scannt, wenn Sie abonniert haben "Azure Information Protection (AIP)". Mit AIP können Sie Dokumente und Dateien klassifizieren und schützen, indem Sie Etiketten auf Inhalte anwenden. Mit der BlueXP Klassifizierung können Sie die Labels anzeigen, die bereits Dateien zugewiesen sind, Labels zu Dateien hinzufügen und Labels ändern, wenn bereits eine Labels vorhanden sind.

Die BlueXP Klassifizierung unterstützt AIP-Labels innerhalb der folgenden Dateitypen: .DOC, .DOCX, .PDF, .PPTX, .XLS, .XLSX:

- Sie können zurzeit keine Etiketten in Dateien ändern, die größer als 30 MB sind. Für OneDrive, SharePoint und Google Drive Konten die maximale Dateigröße beträgt 4 MB.
- Wenn eine Datei ein Label hat, das in AIP nicht mehr existiert, betrachtet die BlueXP Klassifizierung dieses Label als Datei ohne Label.
- Wenn Sie die BlueXP Klassifizierung in einer Regierungsregion oder an einem lokalen Standort ohne Internetzugang (auch als Dark Site bezeichnet) implementiert haben, ist die AIP-Label-Funktion nicht verfügbar.

Integrieren Sie AIP-Beschriftungen in Ihren Arbeitsbereich

Bevor Sie AIP-Labels managen können, müssen Sie die AIP-Label-Funktionalität in die BlueXP Klassifizierung integrieren, indem Sie sich in Ihr bestehendes Azure Konto anmelden. Nach der Aktivierung können Sie AIP-Beschriftungen in Dateien für alle verwalten "Datenquellen" In Ihrem BlueXP Workspace.

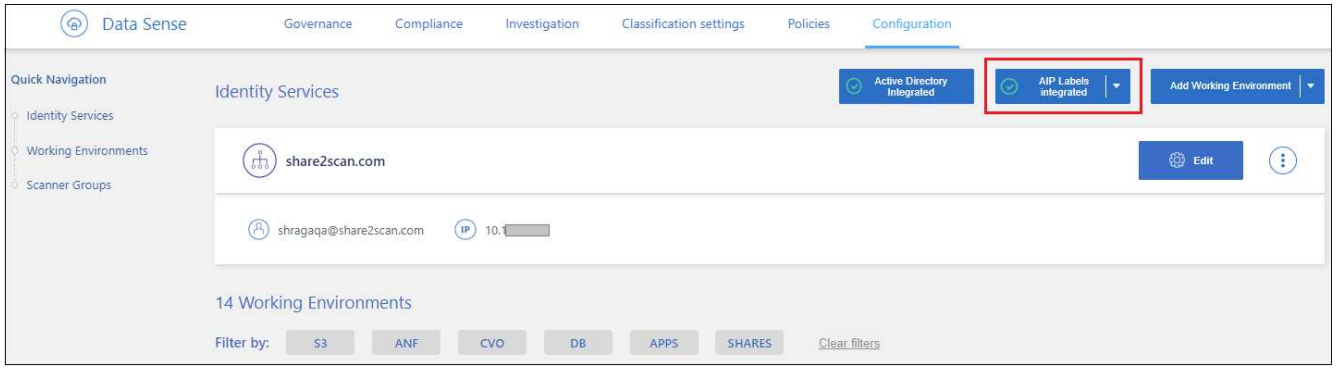
Anforderungen

- Sie benötigen ein Konto und eine Azure Information Protection-Lizenz.
- Sie müssen die Anmeldedaten für das Azure-Konto besitzen.
- Wenn Sie Etiketten in Dateien ändern möchten, die in Amazon S3 Buckets gespeichert sind, stellen Sie die Berechtigung sicher `s3:PutObject` Ist in der IAM-Rolle enthalten. Siehe "Einrichten der IAM-Rolle".

Schritte

1. Klicken Sie auf der Seite BlueXP classification Configuration auf **Integration AIP Labels**.

2. Klicken Sie im Dialogfeld AIP-Etiketten integrieren auf **in Azure anmelden**.
3. Wählen Sie auf der angezeigten Microsoft-Seite das Konto aus, und geben Sie die erforderlichen Anmeldedaten ein.
4. Kehren Sie zur Registerkarte BlueXP Klassifizierung zurück und Sie sehen die Meldung "*AIP-Labels was successfully integrated with the Account <account_name>*".
5. Klicken Sie auf **Schließen** und Sie sehen den Text *AIP Labels integriert* oben auf der Seite.



Ergebnis

Sie können AIP-Beschriftungen im Ergebnisbereich der Untersuchungsseite anzeigen und zuweisen. Außerdem können Sie Dateien mithilfe von Richtlinien AIP-Etiketten zuweisen.

AIP-Etiketten in Ihren Dateien anzeigen

Sie können die aktuelle AIP-Bezeichnung anzeigen, die einer Datei zugewiesen ist.

Klicken Sie im Bereich „Untersuchungsergebnisse“ auf ⌄ Für die Datei zum erweitern der Dateimetadaten.

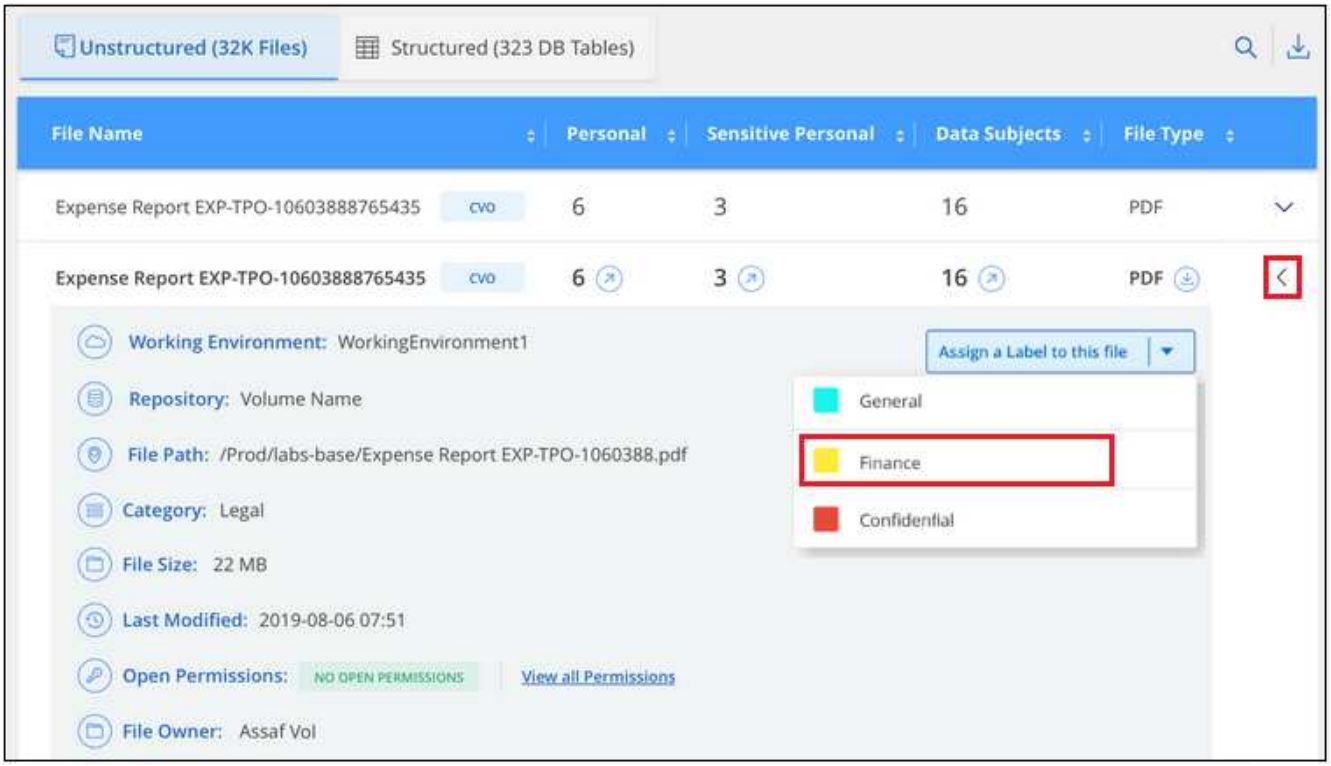
Weisen Sie AIP-Beschriftungen manuell zu

Mit der BlueXP Klassifizierung können Sie AIP-Labels zu Ihren Dateien hinzufügen, ändern und entfernen.

Führen Sie diese Schritte aus, um einer einzelnen Datei eine AIP-Bezeichnung zuzuweisen.

Schritte

1. Klicken Sie im Bereich „Untersuchungsergebnisse“ auf ⌄ Für die Datei zum erweitern der Dateimetadaten.



2. Klicken Sie auf **Etikett dieser Datei zuweisen** und wählen Sie dann die Beschriftung aus.

   Die Beschriftung wird in den Dateimetadaten angezeigt.

Führen Sie die folgenden Schritte aus, um mehreren Dateien eine AIP-Bezeichnung zuzuweisen. Beachten Sie, dass Sie maximal 20 Dateien gleichzeitig (eine Seite in der Benutzeroberfläche) eine AIP-Bezeichnung zuweisen können.

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie beschriften möchten.

- Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
- Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).

2. Klicken Sie in der Symbolleiste auf **Etikett** und wählen Sie die AIP-Bezeichnung:

Die AIP-Bezeichnung wird den Metadaten für alle ausgewählten Dateien hinzugefügt.

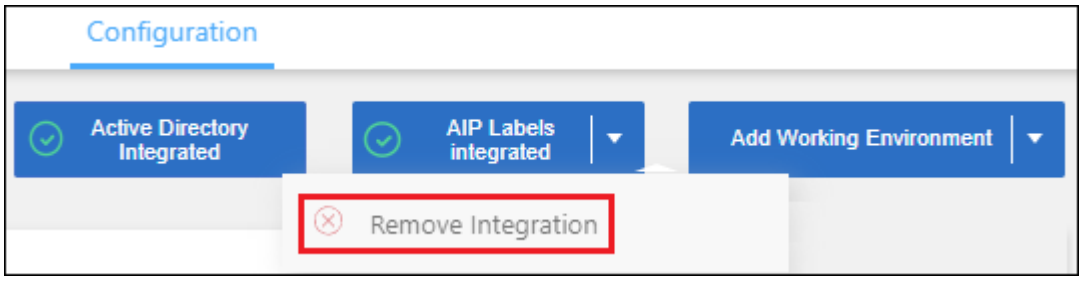
Entfernen Sie die AIP-Integration

Wenn Sie AIP-Labels in Dateien nicht mehr verwalten möchten, können Sie das AIP-Konto von der BlueXP Klassifizierungs-Schnittstelle entfernen.

Beachten Sie, dass an den Labels, die Sie mit der BlueXP Klassifizierung hinzugefügt haben, keine Änderungen vorgenommen werden. Die in Dateien vorhandenen Beschriftungen bleiben so, wie sie derzeit vorhanden sind.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf **AIP Labels integriert > Integration entfernen**.



2. Klicken Sie im Bestätigungsdialogfeld auf **Integration entfernen**.

Wenden Sie Tags an, um die gescannten Dateien zu verwalten

Sie können Dateien, die Sie für eine Art von Follow-up markieren möchten, ein Tag hinzufügen. Sie haben z. B. einige doppelte Dateien gefunden und möchten eine davon löschen, müssen aber überprüfen, welche Dateien gelöscht werden sollen. Sie könnten der Datei einen Tag mit "Prüfen zum Löschen" hinzufügen, damit Sie wissen, dass diese Datei eine Recherche und eine Art von zukünftigen Aktionen erfordert.

Mit der BlueXP Klassifizierung können Sie die Tags anzeigen, die Dateien zugewiesen sind, Tags aus Dateien hinzufügen oder entfernen sowie den Namen ändern oder ein vorhandenes Tag löschen.

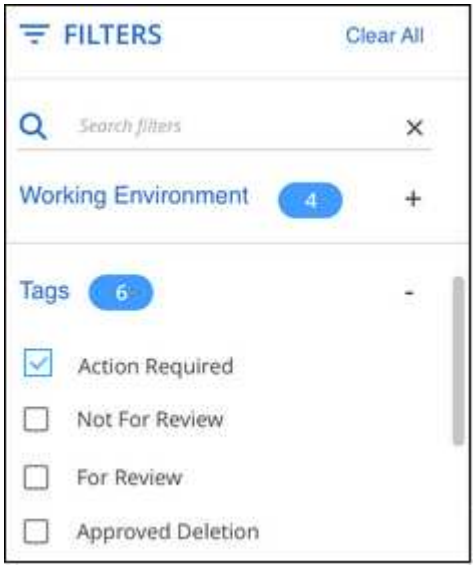
Beachten Sie, dass das Tag der Datei nicht auf die gleiche Weise hinzugefügt wird wie AIP-Etiketten Teil der Dateimetadaten sind. Das Tag wird gerade von BlueXP Benutzern angezeigt, die die BlueXP Klassifizierung verwenden. Sie können also erkennen, ob eine Datei gelöscht oder auf eine bestimmte Art von Follow-up überprüft werden muss.

> Die Tags, die Dateien in der BlueXP Klassifizierung zugewiesen sind, stehen nicht mit den Tags zusammen, die Sie zu Ressourcen wie Volumes oder Instanzen von Virtual Machines hinzufügen können. BlueXP Klassifizierungs-Tags werden auf Dateiebene angewendet.

Zeigen Sie Dateien an, auf die bestimmte Tags angewendet wurden

Sie können alle Dateien anzeigen, denen bestimmte Tags zugewiesen sind.

1. Klicken Sie in der BlueXP-Klassifizierung auf die Registerkarte **Investigation**.
2. Klicken Sie auf der Seite Datenuntersuchung im Bereich Filter auf **Tags** und wählen Sie die gewünschten Tags aus.



Im Bereich Untersuchungsergebnisse werden alle Dateien angezeigt, denen diese Tags zugewiesen sind.

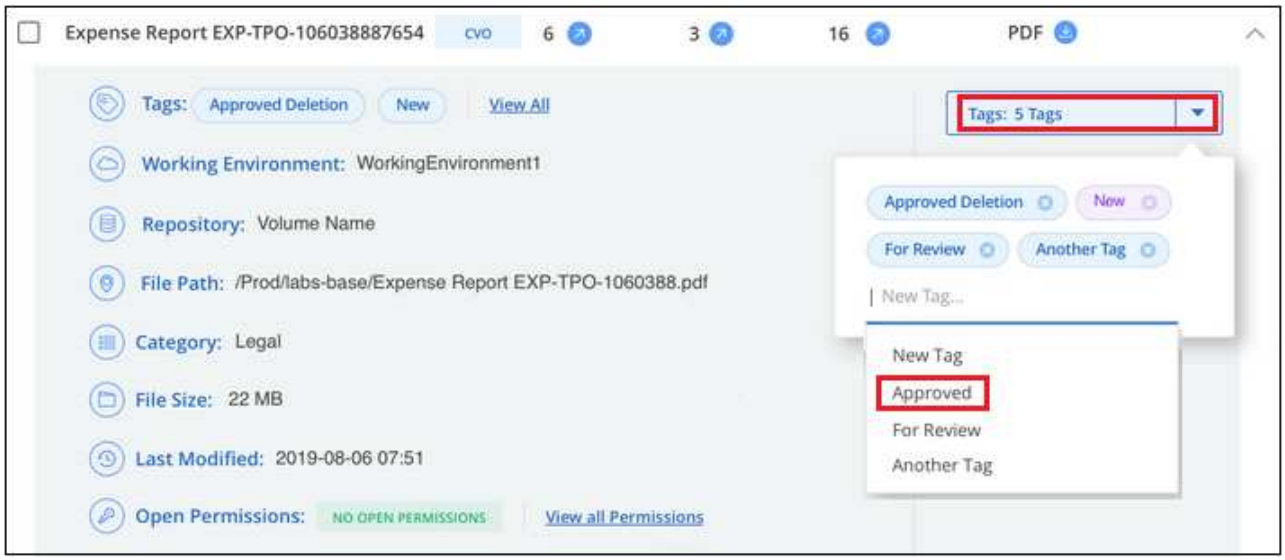
Weisen Sie Dateien Tags zu

Sie können Tags zu einer einzelnen Datei oder zu einer Gruppe von Dateien hinzufügen.

So fügen Sie einer einzelnen Datei ein Tag hinzu:

Schritte

1. Klicken Sie im Bereich „Untersuchungsergebnisse“ auf ⌄ Für die Datei zum erweitern der Dateimetadaten.
2. Klicken Sie auf das Feld **Tags** und die aktuell zugewiesenen Tags werden angezeigt.
3. Tag oder Tags hinzufügen:
   - Um ein vorhandenes Tag zuzuweisen, klicken Sie in das Feld **Neues Tag…** und geben den Namen des Tags ein. Wenn das gesuchte Tag angezeigt wird, wählen Sie es aus, und drücken Sie **Enter**.
   - Um ein neues Tag zu erstellen und es der Datei zuzuweisen, klicken Sie in das Feld **New Tag…**, geben Sie den Namen des neuen Tags ein und drücken Sie **Enter**.



Das Tag wird in den Dateimetadaten angezeigt.

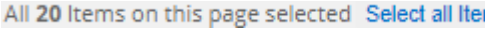
So fügen Sie einem mehrere Dateien ein Tag hinzu:

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die markiert werden sollen.

   - Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (☑ Volume_1).
   - Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (☑ File Name).

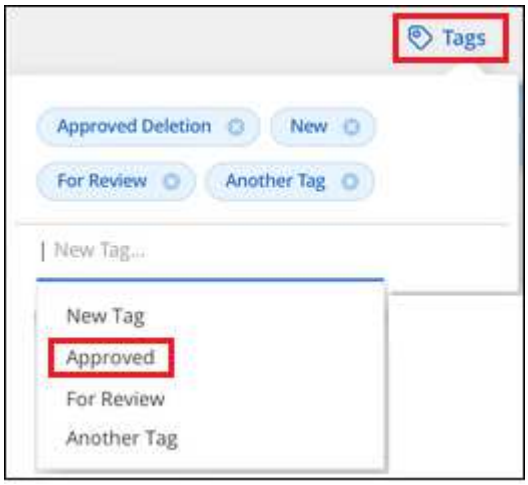
- Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (

), und dann in der Pop-up-Nachricht 

Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.

  Sie können Tags auf maximal 100,000 Dateien gleichzeitig anwenden.

2. Klicken Sie in der Buttonleiste auf **Tags** und die aktuell zugewiesenen Tags werden angezeigt.
3. Tag oder Tags hinzufügen:
   - Um ein vorhandenes Tag zuzuweisen, klicken Sie in das Feld **Neues Tag…** und geben den Namen des Tags ein. Wenn das gesuchte Tag angezeigt wird, wählen Sie es aus, und drücken Sie **Enter**.
   - Um ein neues Tag zu erstellen und es der Datei zuzuweisen, klicken Sie in das Feld **New Tag…**, geben Sie den Namen des neuen Tags ein und drücken Sie **Enter**.



4. Genehmigen Sie das Hinzufügen der Tags im Bestätigungsdialogfeld, und die Tags werden den Metadaten für alle ausgewählten Dateien hinzugefügt.

Tags aus Dateien löschen

Sie können ein Tag löschen, wenn Sie es nicht mehr verwenden müssen.

Klicken Sie einfach auf das **x** für ein vorhandenes Tag.

Wenn Sie mehrere Dateien ausgewählt haben, wird das Tag aus allen Dateien entfernt.

Weisen Sie Benutzer zu, um bestimmte Dateien zu verwalten

Sie können einen BlueXP-Benutzer einer bestimmten Datei oder mehreren Dateien zuweisen, so dass diese Person für alle Follow-up-Aktionen verantwortlich sein kann, die in der Datei ausgeführt werden müssen. Diese Funktion wird häufig zusammen mit der Funktion verwendet, um einer Datei benutzerdefinierte Status-Tags hinzuzufügen.

Sie können beispielsweise eine Datei mit bestimmten personenbezogenen Daten haben, die zu vielen Benutzern Lese- und Schreibzugriff (offene Berechtigungen) ermöglicht. Sie können also das Status-Tag "Berechtigungen ändern" zuweisen und diese Datei dem Benutzer "Joan Smith" zuweisen, damit er

entscheiden kann, wie das Problem behoben werden kann. Wenn sie das Problem behoben haben, könnten sie die Status-Tag-Nummer auf „Abgeschlossen“ ändern.

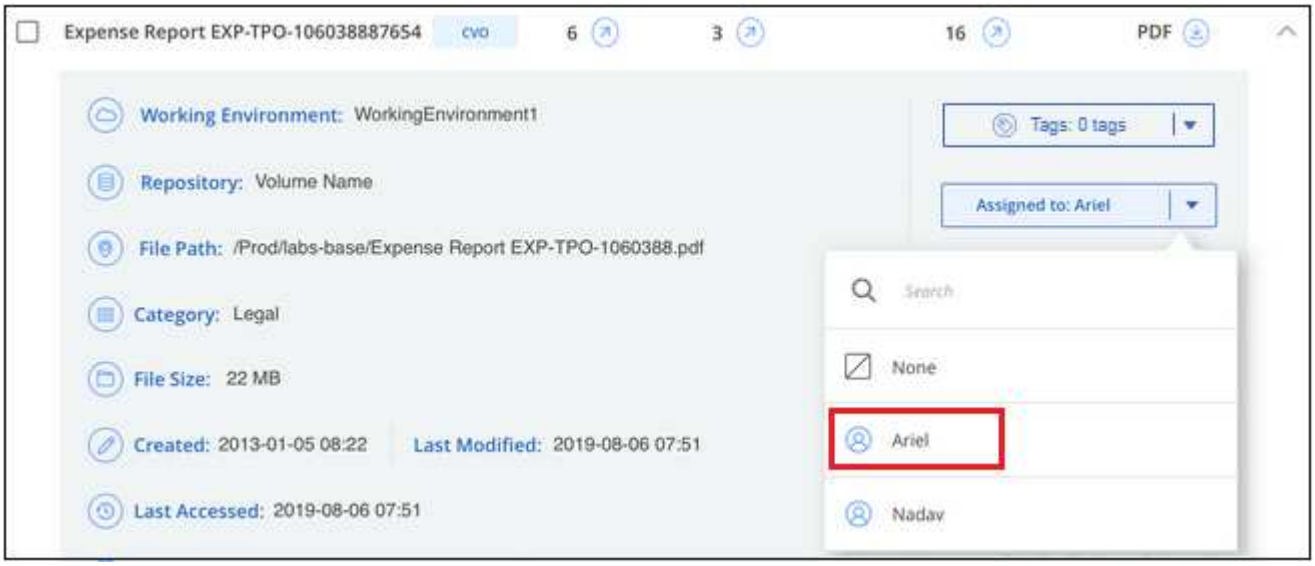
Beachten Sie, dass der Benutzername nicht als Teil der Datei-Metadaten zur Datei hinzugefügt wird. Er wird gerade von BlueXP Benutzern bei der Nutzung der BlueXP Klassifizierung gesehen.

Mit einem neuen Filter auf der Untersuchungsseite können Sie problemlos alle Dateien anzeigen, die dieselbe Person im Feld „Assigned to“ haben.

Führen Sie die folgenden Schritte aus, um einen Benutzer einer einzelnen Datei zuzuweisen.

Schritte

1. Klicken Sie im Bereich „Untersuchungsergebnisse“ auf ⌄ Für die Datei zum erweitern der Dateimetadaten.
2. Klicken Sie auf das Feld **Assigned to** und wählen Sie den Benutzernamen aus.



Der Benutzername wird in den Dateimetadaten angezeigt.

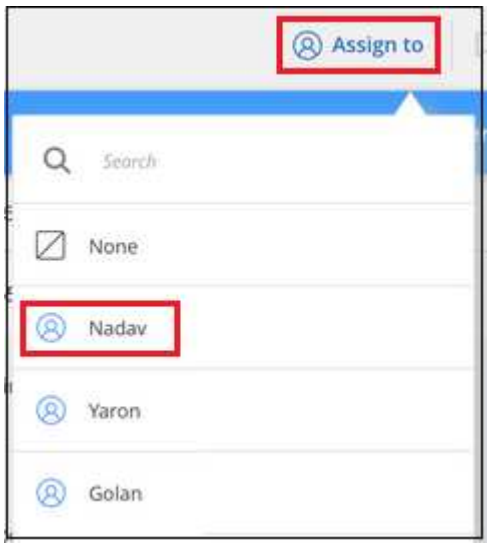
Führen Sie diese Schritte aus, um einen Benutzer mehreren Dateien zuzuweisen. Beachten Sie, dass Sie einen Benutzer maximal 20 Dateien gleichzeitig zuweisen können (eine Seite in der Benutzeroberfläche).

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie einem Benutzer zuweisen möchten.

- Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
- Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).

2. Klicken Sie in der Symbolleiste auf **Zuweisen zu** und wählen Sie den Benutzernamen aus:



Der Benutzer wird den Metadaten für alle ausgewählten Dateien hinzugefügt.

Weisen Sie Daten Richtlinien zu

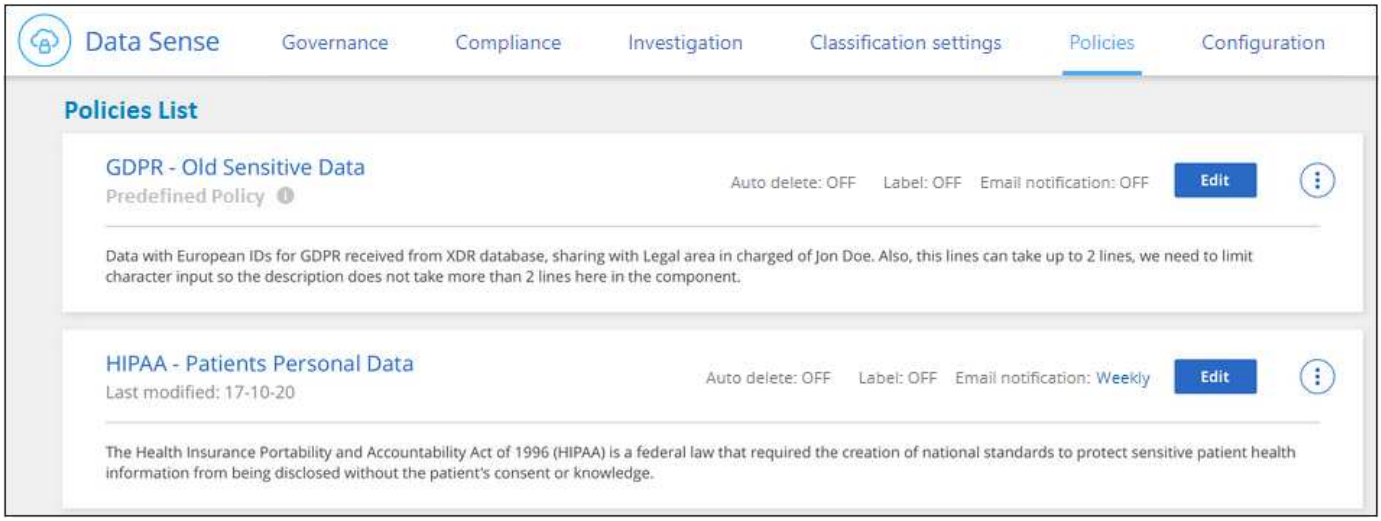
Richtlinien sind wie eine Favoritenliste mit benutzerdefinierten Filtern, die Suchergebnisse auf der Untersuchungsseite für häufig angeforderte Compliance-Abfragen liefern. Die BlueXP Klassifizierung bietet einen Satz vordefinierter Richtlinien auf der Basis allgemeiner Kundenanfragen. Sie können benutzerdefinierte Richtlinien erstellen, die Ergebnisse für die Suche liefern, die speziell auf Ihr Unternehmen zugeschnitten sind.

Richtlinien bieten folgende Funktionen:

- Vordefinierte Richtlinien Von NetApp basierend auf Benutzeranfragen
- Möglichkeit, eigene benutzerdefinierte Richtlinien zu erstellen

- Starten Sie die Untersuchungsseite mit den Ergebnissen Ihrer Richtlinien mit nur einem Klick
- Senden Sie E-Mail-Benachrichtigungen an BlueXP-Benutzer oder andere E-Mail-Adressen, wenn bestimmte kritische Richtlinien Ergebnisse liefern, damit Sie Benachrichtigungen zum Schutz Ihrer Daten erhalten können
- Weisen Sie AIP-Etiketten (Azure Information Protection) automatisch allen Dateien zu, die den in einer Richtlinie definierten Kriterien entsprechen
- Löschen Sie Dateien automatisch (einmal pro Tag), wenn bestimmte Richtlinien Ergebnisse zurückgeben, damit Sie Ihre Daten automatisch schützen können

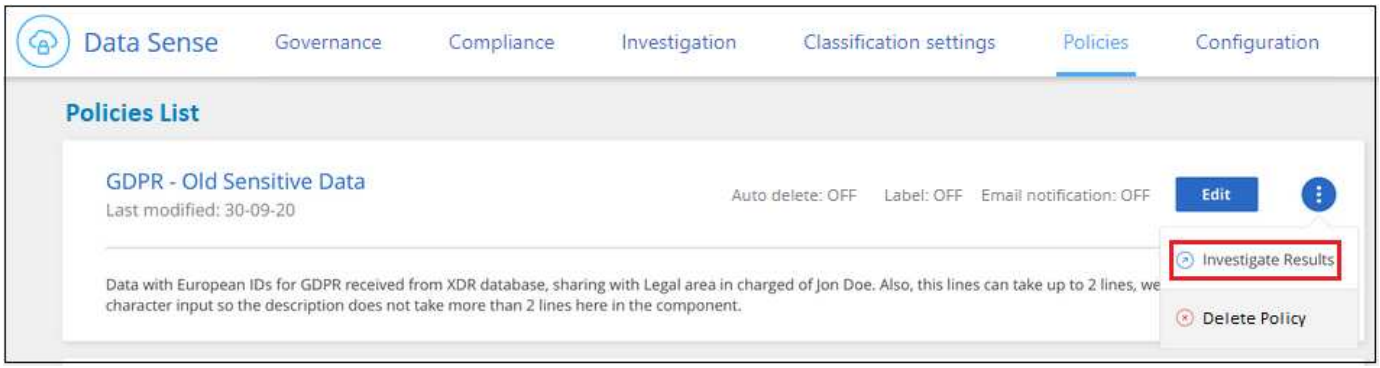
Auf der Registerkarte **Policies** im Compliance Dashboard werden alle vordefinierten und benutzerdefinierten Richtlinien aufgelistet, die auf dieser Instanz der BlueXP-Klassifizierung verfügbar sind.



Darüber hinaus werden Richtlinien in der Liste der Filter auf der Untersuchungsseite angezeigt.

Zeigen Sie die Ergebnisse der Richtlinie auf der Seite Untersuchung an

Um die Ergebnisse für eine Richtlinie auf der Untersuchungsseite anzuzeigen, klicken Sie auf die ⋮ Klicken Sie für eine bestimmte Richtlinie, und wählen Sie dann **Ergebnisse untersuchen**.



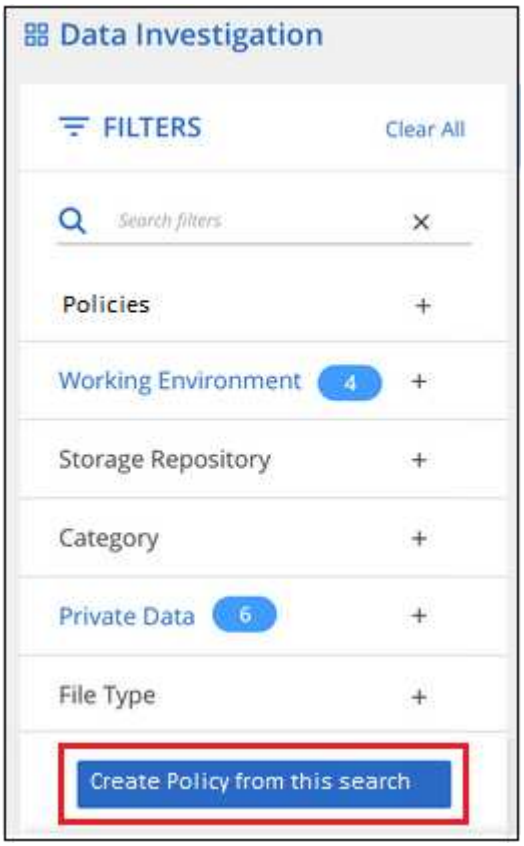
Erstellen Sie benutzerdefinierte Richtlinien

Sie können eigene benutzerdefinierte Richtlinien erstellen, die Ergebnisse für spezifische Suchen in Ihrem Unternehmen liefern. Die Ergebnisse werden für alle Dateien und Verzeichnisse (Freigaben und Ordner) zurückgegeben, die den Suchkriterien entsprechen.

Beachten Sie, dass die Aktionen zum Löschen von Daten und zum Zuweisen von AIP-Etiketten auf der Grundlage der Richtlinienergebnisse nur für Dateien gültig sind. Verzeichnisse, die den Suchkriterien entsprechen, können nicht automatisch gelöscht oder AIP-Bezeichnungen zugewiesen werden.

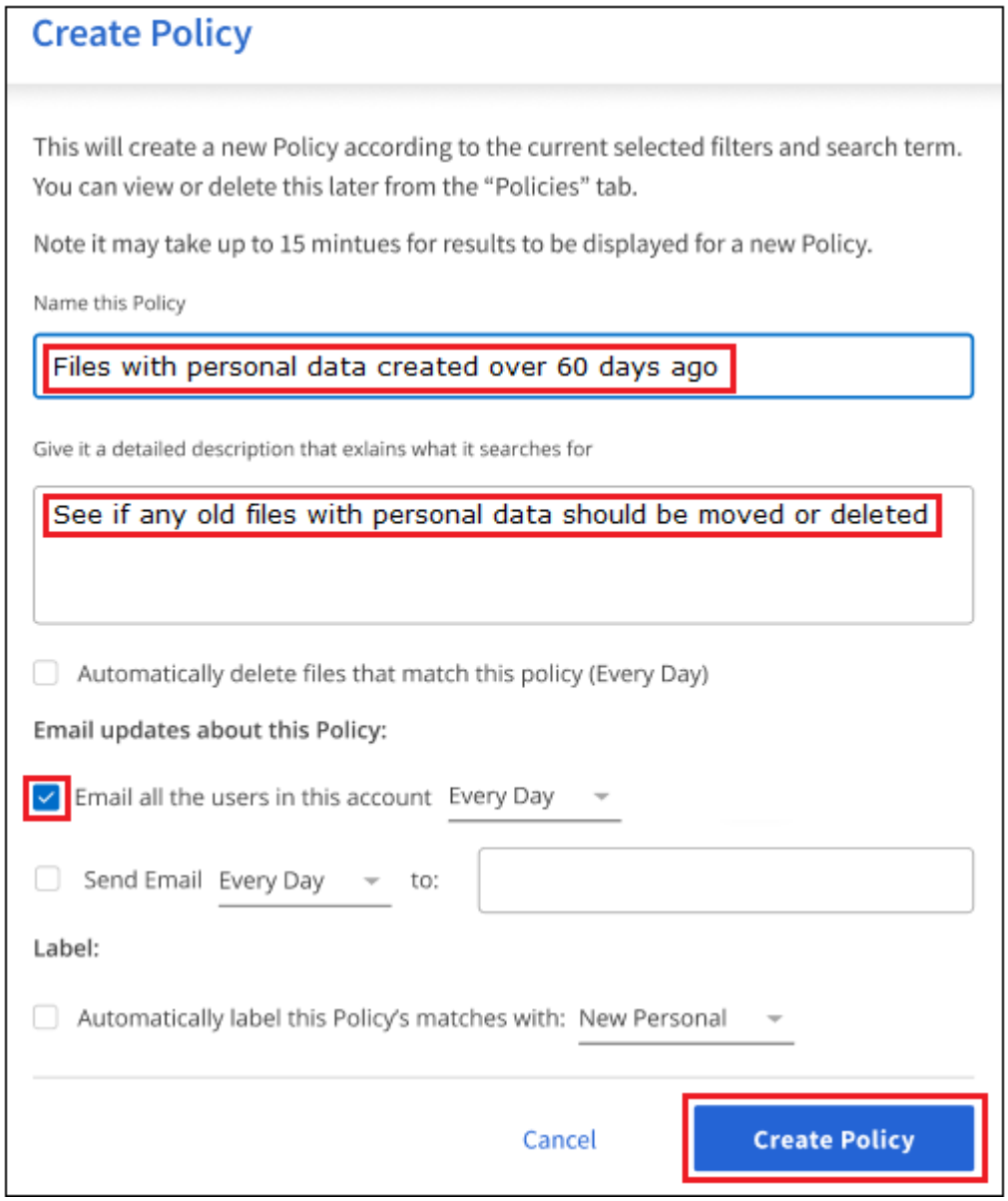
Schritte

1. Definieren Sie auf der Seite „Untersuchung von Daten“ die Suche, indem Sie alle Filter auswählen, die Sie verwenden möchten. Siehe "Filtern von Daten auf der Seite „Datenuntersuchung“" Entsprechende Details.
2. Wenn Sie alle Filtereigenschaften genau so haben, wie Sie sie wollen, klicken Sie auf **Create Policy von dieser Suche**.



3. Benennen Sie die Richtlinie, und wählen Sie andere Aktionen aus, die von der Richtlinie ausgeführt werden können:
   a. Geben Sie einen eindeutigen Namen und eine eindeutige Beschreibung ein.
   b. Aktivieren Sie optional das Kontrollkästchen, um Dateien automatisch zu löschen, die mit den Richtlinieparametern übereinstimmen. Weitere Informationen zu Quelldateien mit einer Richtlinie löschen.
   c. Aktivieren Sie optional das Kontrollkästchen, wenn Sie Benachrichtigungen-E-Mails an BlueXP-Benutzer in Ihrem Konto senden möchten, und wählen Sie das Intervall aus, in dem die E-Mail gesendet wird. Weitere Informationen zu wenn nicht konforme Daten gefunden werden,Senden von E-Mail-Warnmeldungen anhand von Richtlinienergebnissen.
   d. Aktivieren Sie optional das Kontrollkästchen, wenn Sie Benachrichtigungs-E-Mails an andere Benutzer senden möchten, geben Sie bis zu 20 E-Mail-Adressen ein und wählen Sie das Intervall aus, in dem die E-Mail gesendet wird.
   e. Aktivieren Sie optional das Kontrollkästchen, um Dateien, die den Richtlinieparametern entsprechen, automatisch AIP-Etiketten zuzuweisen, und wählen Sie die Beschriftung aus. (Nur wenn Sie bereits AIP-Etiketten integriert haben. Weitere Informationen zu "AIP-Etiketten".)

f. Klicken Sie Auf **Create Policy**.



Ergebnis

Die neue Richtlinie wird auf der Registerkarte Richtlinien angezeigt.

Senden Sie E-Mail-Warnungen, wenn nicht konforme Daten gefunden werden

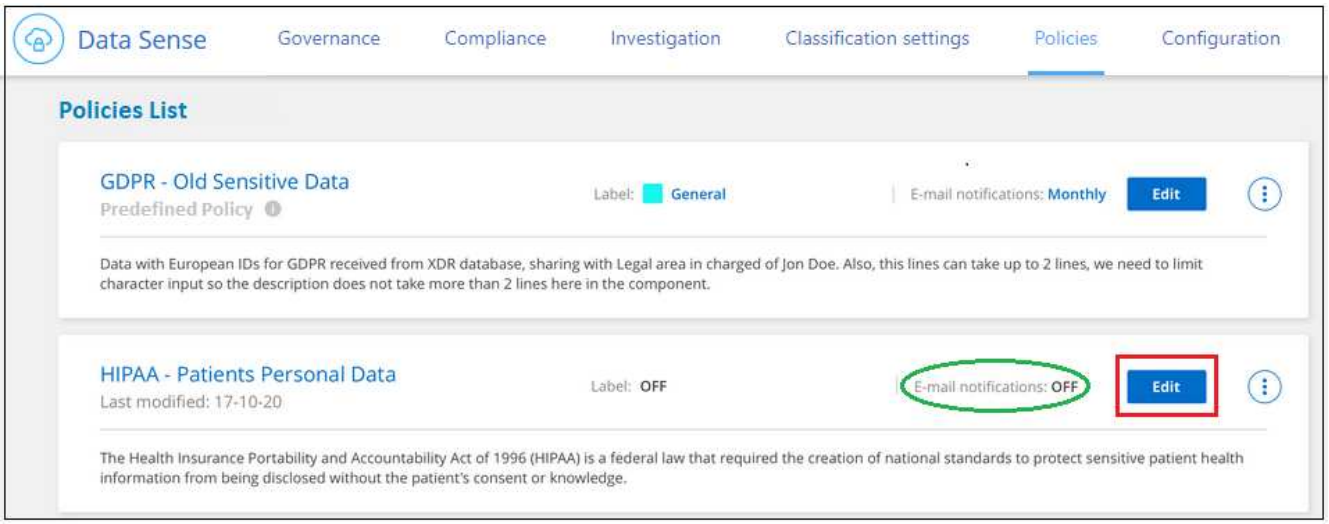
Die BlueXP Klassifizierung kann E-Mail-Benachrichtigungen an BlueXP Benutzer in Ihrem Konto senden, wenn bestimmte kritische Richtlinien Ergebnisse liefern, sodass Sie Benachrichtigungen zum Schutz Ihrer Daten erhalten. Sie können die E-Mail-Benachrichtigungen täglich, wöchentlich oder monatlich versenden. Sie können auch E-Mail-Benachrichtigungen an eine andere E-Mail-Adresse senden - bis zu 20 E-Mail-Adressen - nicht in Ihrem BlueXP-Konto.

Sie können diese Einstellung beim Erstellen der Richtlinie oder beim Bearbeiten einer Richtlinie konfigurieren.

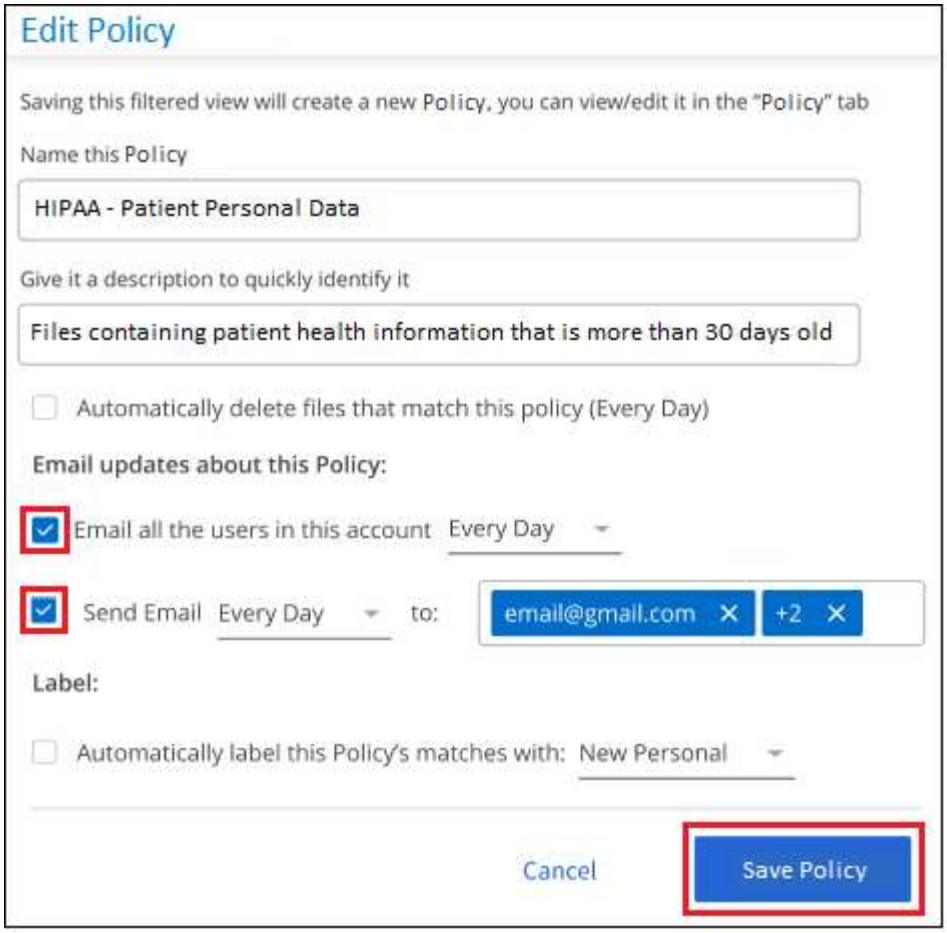
Befolgen Sie diese Schritte, um E-Mail-Updates zu einer bestehenden Richtlinie hinzuzufügen.

Schritte

1. Klicken Sie auf der Liste Richtlinien auf **Bearbeiten** für die Richtlinie, in der Sie die E-Mail-Einstellung hinzufügen (oder ändern) möchten.



2. Auf der Seite Richtlinie bearbeiten:
   a. Aktivieren Sie das Kontrollkästchen „E-Mail all the users in this Account“, wenn Sie Benachrichtigungen-E-Mails an Benutzer in Ihrem BlueXP-Konto senden möchten, und wählen Sie das Intervall aus, in dem die E-Mail gesendet wird (z. B. **every Day**).
   b. Aktivieren Sie das Kontrollkästchen „E-Mail senden“, wenn Sie Benachrichtigungs-E-Mails an weitere Benutzer senden möchten, wählen Sie das Intervall aus, in dem die E-Mail gesendet wird, und geben Sie bis zu 20 E-Mail-Adressen ein.



3. Klicken Sie auf **Save Policy** und das Intervall, in dem die E-Mail gesendet wird, wird in der Policy description angezeigt.

Ergebnis

Die erste E-Mail wird jetzt gesendet, wenn Ergebnisse aus der Richtlinie vorliegen - aber nur, wenn Dateien die Kriterien der Richtlinie erfüllen. Es werden keine personenbezogenen Daten in die Benachrichtigungs-E-Mails gesendet. Die E-Mail zeigt an, dass es Dateien gibt, die den Kriterien der Richtlinie entsprechen, und sie enthält einen Link zu den Ergebnissen der Richtlinie.

Löschen Sie Quelldateien automatisch mithilfe von Richtlinien

Sie können eine benutzerdefinierte Richtlinie erstellen, um Dateien zu löschen, die der Richtlinie entsprechen. Beispielsweise können Sie Dateien löschen, die sensible Informationen enthalten und von der BlueXP Klassifizierung in den letzten 30 Tagen erkannt wurden.

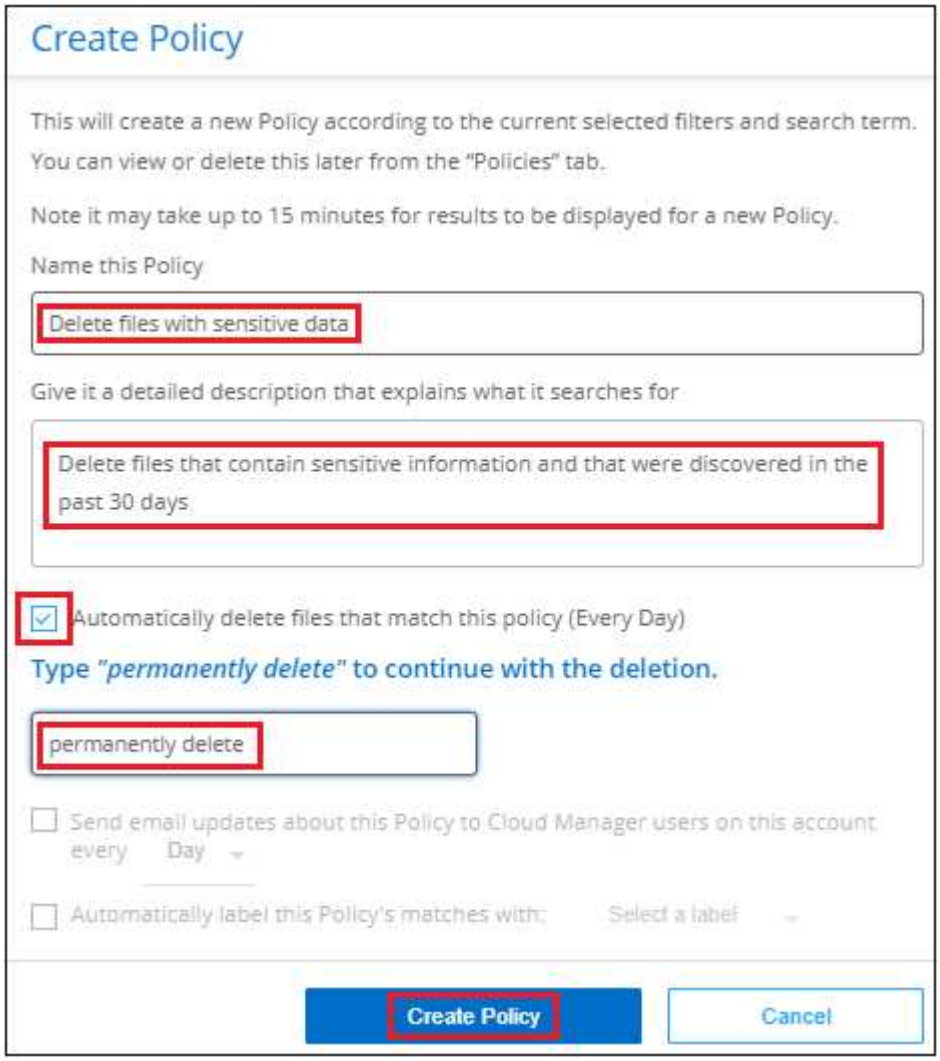
Nur Kontoadministratoren können eine Richtlinie zum automatischen Löschen von Dateien erstellen.

> Alle Dateien, die der Richtlinie entsprechen, werden einmal am Tag dauerhaft gelöscht.

Schritte

1. Definieren Sie auf der Seite „Untersuchung von Daten“ die Suche, indem Sie alle Filter auswählen, die Sie verwenden möchten. Siehe "Filtern von Daten auf der Seite „Datenuntersuchung“" Entsprechende Details.
2. Wenn Sie alle Filtereigenschaften genau so haben, wie Sie sie wollen, klicken Sie auf **Create Policy von dieser Suche**.

3. Benennen Sie die Richtlinie, und wählen Sie andere Aktionen aus, die von der Richtlinie ausgeführt werden können:
   a. Geben Sie einen eindeutigen Namen und eine eindeutige Beschreibung ein.
   b. Aktivieren Sie das Kontrollkästchen "Dateien, die dieser Richtlinie entsprechen automatisch löschen" und geben Sie **dauerhaft löschen** ein, um zu bestätigen, dass Dateien dauerhaft von dieser Richtlinie gelöscht werden sollen.
   c. Klicken Sie Auf **Create Policy**.



Ergebnis

Die neue Richtlinie wird auf der Registerkarte Richtlinien angezeigt. Dateien, die der Richtlinie entsprechen, werden einmal pro Tag gelöscht, wenn die Richtlinie ausgeführt wird.

Sie können die Liste der Dateien anzeigen, die im gelöscht wurden "Statusbereich Aktionen".

Weisen Sie AIP-Etiketten automatisch mit Richtlinien zu

Sie können allen Dateien, die die Kriterien der Richtlinie erfüllen, eine AIP-Beschriftung zuweisen. Sie können beim Erstellen der Richtlinie das AIP-Etikett angeben oder die Beschriftung beim Bearbeiten einer Richtlinie hinzufügen.

Während die BlueXP Klassifizierung Ihre Dateien scannt, werden Labels fortlaufend in Dateien hinzugefügt oder aktualisiert.

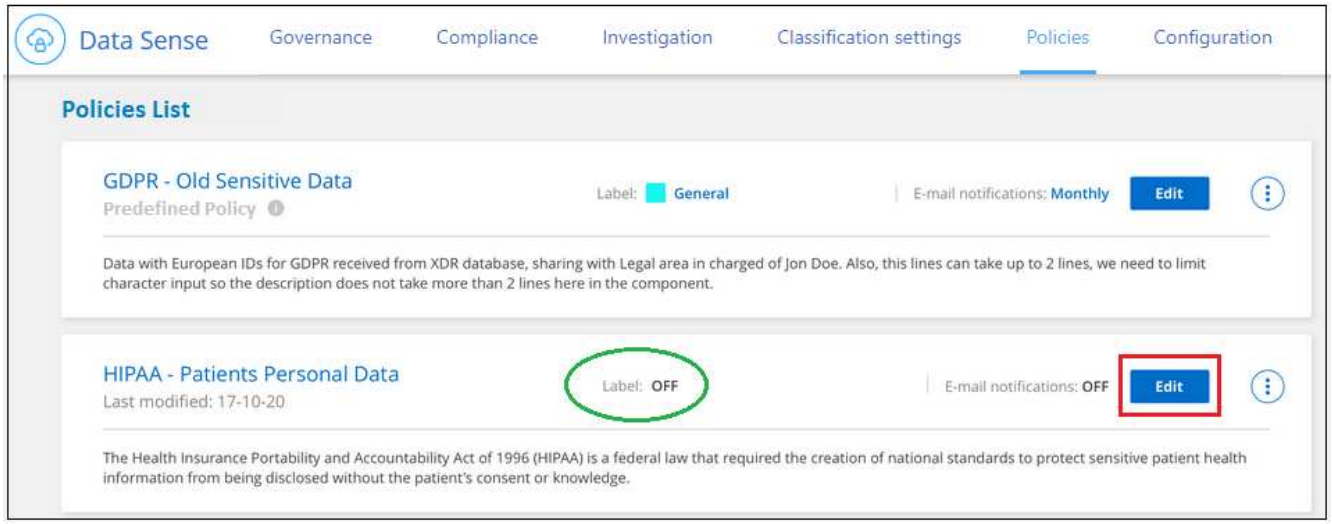
Je nachdem, ob bereits ein Label auf eine Datei und die Klassifizierungsstufe des Etiketts angewendet wurde, werden beim Ändern einer Bezeichnung folgende Aktionen ausgeführt:

Wenn die Datei…	Dann…
Hat kein Etikett	Die Beschriftung wird hinzugefügt
Verfügt über ein bereits vorhandenes Etikett mit einer niedrigeren Klassifizierungsstufe	Das Etikett der höheren Ebene wird hinzugefügt
Verfügt über ein bereits vorhandenes Etikett mit einer höheren Klassifizierungsstufe	Das Etikett der höheren Ebene bleibt erhalten
Wird eine Bezeichnung sowohl manuell als auch von einer Richtlinie zugewiesen	Das Etikett der höheren Ebene wird hinzugefügt
Ist zwei Richtlinien zugewiesen	Das Etikett der höheren Ebene wird hinzugefügt

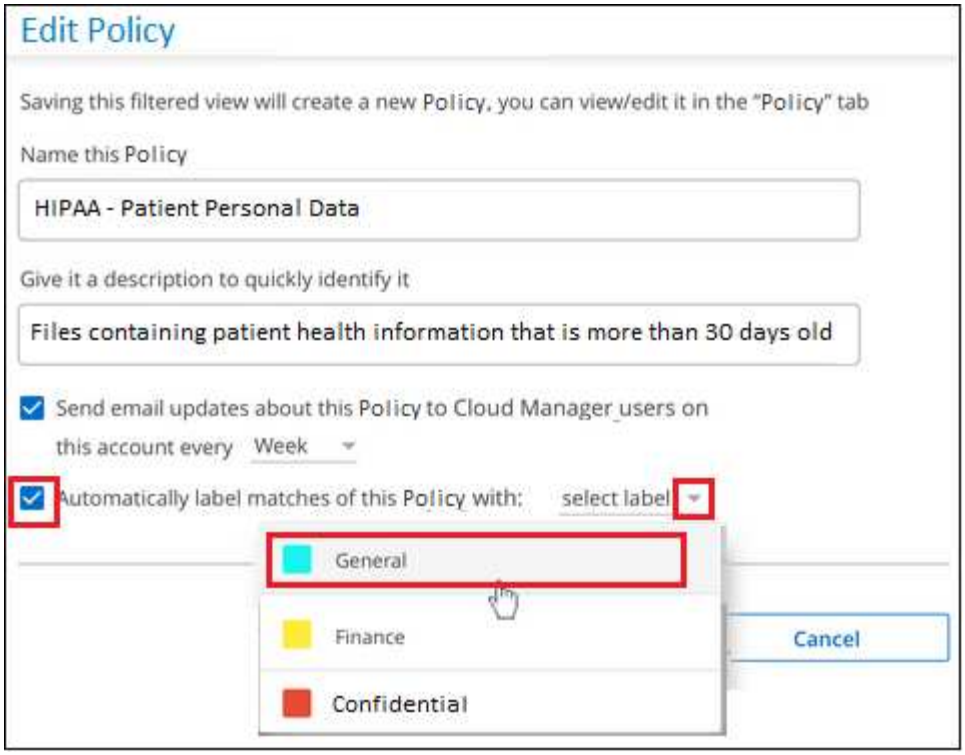
Führen Sie diese Schritte aus, um einer vorhandenen Richtlinie eine AIP-Beschriftung hinzuzufügen.

Schritte

1. Klicken Sie auf der Liste Richtlinien auf **Bearbeiten** für die Richtlinie, in der Sie die AIP-Bezeichnung hinzufügen (oder ändern) möchten.



2. Aktivieren Sie auf der Seite Richtlinie bearbeiten das Kontrollkästchen, um automatische Beschriftungen für Dateien zu aktivieren, die den Richtlinieparametern entsprechen, und wählen Sie die Beschriftung aus (z. B. **Allgemein**).



3. Klicken Sie auf **Save Policy** und das Etikett wird in der Policy description angezeigt.

> Wenn eine Richtlinie mit einem Etikett konfiguriert wurde, die Bezeichnung aber seitdem von AIP entfernt wurde, wird der Name der Bezeichnung auf AUS gesetzt und die Bezeichnung nicht mehr zugewiesen.

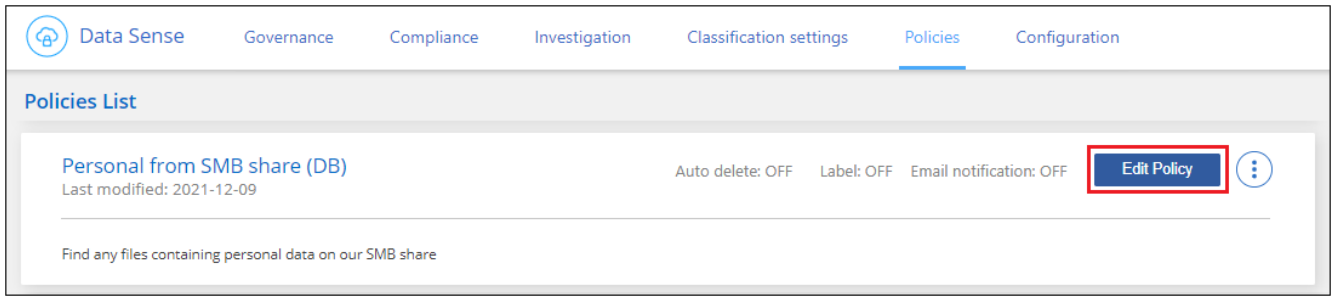
Richtlinien Bearbeiten

Sie können alle Kriterien für eine vorhandene Richtlinie ändern, die Sie zuvor erstellt haben. Dies kann besonders nützlich sein, wenn Sie die Abfrage (die Elemente, die Sie mit Filtern definiert haben) ändern möchten, um bestimmte Parameter hinzuzufügen oder zu entfernen.

Beachten Sie, dass Sie für vordefinierte Richtlinien nur ändern können, ob E-Mail-Benachrichtigungen gesendet werden und ob AIP-Beschriftungen hinzugefügt werden. Andere Werte können nicht geändert werden.

Schritte

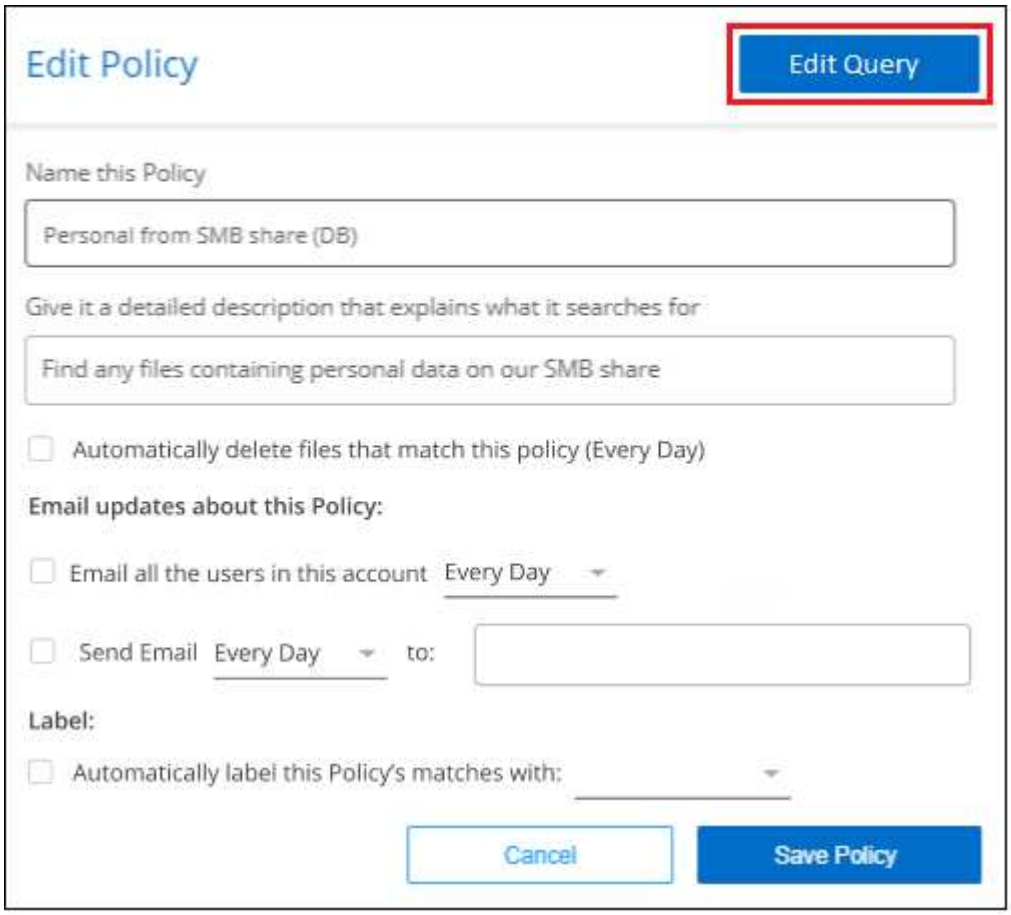
1. Klicken Sie auf der Liste Richtlinien auf **Bearbeiten** für die Richtlinie, die Sie ändern möchten.



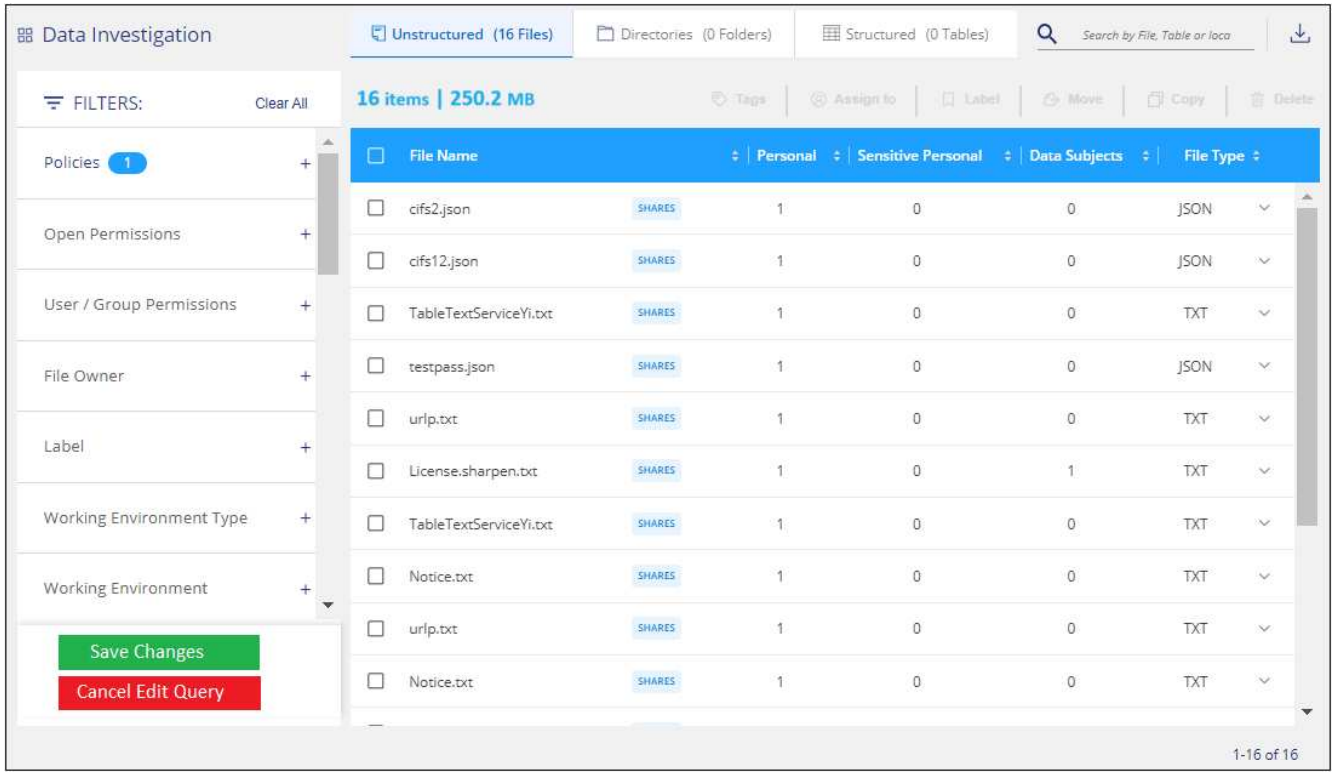
2. Wenn Sie nur die Elemente auf dieser Seite ändern möchten (Name, Beschreibung, ob E-Mail-Benachrichtigungen gesendet werden, und ob AIP-Beschriftungen hinzugefügt werden), ändern Sie die

Änderung und klicken Sie auf **Richtlinie speichern**.

Wenn Sie die Filter für die gespeicherte Abfrage ändern möchten, klicken Sie auf **Abfrage bearbeiten**.



3. Bearbeiten Sie auf der Untersuchungsseite, die diese Abfrage definiert, die Abfrage durch Hinzufügen, Entfernen oder Anpassen der Filter und klicken Sie auf **Änderungen speichern** .



Ergebnis

Die Richtlinie wird sofort geändert. Alle Aktionen, die für diese Richtlinie zum Senden einer E-Mail, Hinzufügen von AIP-Etiketten oder Löschen von Dateien definiert sind, werden im nächsten internen ausgeführt.

Richtlinien Löschen

Sie können alle benutzerdefinierten Richtlinien löschen, die Sie erstellt haben, wenn Sie sie nicht mehr benötigen. Sie können keine der vordefinierten Richtlinien löschen.

Zum Löschen einer Richtlinie klicken Sie auf das ⋮ Klicken Sie für eine bestimmte Richtlinie auf **Richtlinie löschen**, und klicken Sie dann im Bestätigungsdialogfeld erneut auf **Richtlinie löschen**.

Liste der vordefinierten Richtlinien

Die BlueXP Klassifizierung bietet die folgenden systemdefinierten Richtlinien:

Name	Beschreibung	Logik
S3 öffentlich - offengelegte private Daten	S3 Objekte mit persönlichen oder sensiblen persönlichen Daten, mit offenem öffentlichen Lesezugriff.	S3 Public ENTHÄLT persönliche ODER sensible persönliche Informationen
PCI DSS – veraltete Daten über 30 Tage	Dateien mit Kreditkarteninformationen, zuletzt geändert vor mehr als 30 Tagen.	Enthält Kreditkarte UND zuletzt geändert über 30 Tage
HIPAA – veraltete Daten über 30 Tage	Dateien mit Gesundheitsinformationen, zuletzt geändert vor mehr als 30 Tagen.	Enthält Gesundheitsdaten (wie in HIPAA-Berichten definiert) UND die letzte Änderung über 30 Tage

Name	Beschreibung	Logik
Private Daten - veraltet über 7 Jahre	Dateien mit persönlichen oder sensiblen persönlichen Daten, zuletzt geändert vor über 7 Jahren.	Dateien mit persönlichen oder sensiblen persönlichen Daten, zuletzt geändert vor über 7 Jahren
DSGVO: Die europäischen Bürger	Dateien mit mehr als 5 Kennungen von EU-Bürgern oder DB-Tabellen, die Kennungen von EU-Bürgern enthalten	Dateien mit mehr als 5 Kennungen von (einem) EU-Bürgern oder DB-Tabellen, die Zeilen mit mehr als 15 % der Spalten mit den EU-Kennungen eines Landes enthalten. (Eine der nationalen Kennungen der europäischen Länder. Beinhaltet keine Brasilien, Kalifornien, USA SSN, Israel, Südafrika)
CCPA – Einwohner Kaliforniens	Dateien, die über 10 California Driver's License Identifier oder DB-Tabellen mit dieser Kennung enthalten.	Dateien mit mehr als 10 California Driver's License Identifier ODER DB-Tabellen mit California Driver's License
Namen der Betroffenen - hohes Risiko	Dateien mit mehr als 50 Namen des Betroffenen.	Dateien mit mehr als 50 Namen des Betroffenen
E-Mail-Adressen – hohes Risiko	Dateien mit über 50 E-Mail-Adressen oder DB-Spalten mit über 50 % ihrer Zeilen, die E-Mail-Adressen enthalten	Dateien mit über 50 E-Mail-Adressen oder DB-Spalten mit über 50 % ihrer Zeilen, die E-Mail-Adressen enthalten
Personenbezogene Daten - hohes Risiko	Dateien mit mehr als 20 Identifikatoren für persönliche Daten oder Datenbankspalten mit über 50 % ihrer Zeilen, die Identifikatoren für persönliche Daten enthalten.	Dateien mit über 20 persönlichen oder DB-Spalten mit über 50% ihrer Zeilen, die persönliche enthalten
Sensible personenbezogene Daten - hohes Risiko	Dateien mit über 20 vertraulichen personenbezogenen Daten-IDs oder DB-Spalten mit über 50 % ihrer Zeilen, die vertrauliche personenbezogene Daten enthalten.	Dateien mit über 20 sensiblen persönlichen oder DB-Spalten mit über 50% ihrer Zeilen, die sensible persönliche Daten enthalten

Management privater Daten

Die BlueXP Klassifizierung bietet Ihnen viele Möglichkeiten für das Management Ihrer privaten Daten. Einige Funktionen erleichtern die Vorbereitung auf die Migration Ihrer Daten, während andere Funktionen können Sie Änderungen an den Daten.

- Sie können Dateien in eine Ziel-NFS-Freigabe kopieren, wenn Sie eine Kopie bestimmter Daten erstellen und sie an einen anderen NFS-Speicherort verschieben möchten.
- Sie können ein ONTAP Volume auf einem neuen Volume klonen und dabei nur ausgewählte Dateien aus dem Quell-Volume im neuen geklonten Volume eingeschlossen. Dies ist nützlich für Situationen, in denen Sie Daten migrieren und bestimmte Dateien vom ursprünglichen Volume ausschließen möchten.
- Sie können Dateien aus einem Quell-Repository in ein Verzeichnis an einem bestimmten Zielspeicherort kopieren und synchronisieren. Dies ist nützlich in Situationen, in denen Sie Daten von einem Quellsystem zu einem anderen migrieren, während noch einige letzte Aktivitäten in den Quelldateien vorliegen.
- Sie können Quelldateien, die von der BlueXP Klassifizierung gescannt werden, auf jede beliebige NFS-Freigabe verschieben.

- Sie können Dateien löschen, die als unsicher oder zu riskant erscheinen, um in Ihrem Speichersystem zu verbleiben, oder die Sie als Duplikat identifiziert haben.

> - Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.
> - Daten von Google Drive-Konten können derzeit keine dieser Funktionen nutzen.

Quelldateien kopieren

Sie können beliebige Quelldateien kopieren, die von der BlueXP Klassifizierung gescannt werden. Es gibt drei Arten von Kopiervorgängen, je nachdem, was Sie erreichen möchten:

- **Kopieren Sie Dateien** aus den gleichen oder anderen Volumes oder Datenquellen in eine Ziel-NFS-Freigabe.

  Dies ist nützlich, wenn Sie eine Kopie bestimmter Daten erstellen und sie an einen anderen NFS-Speicherort verschieben möchten.

- **Ein ONTAP-Volume** zu einem neuen Volume im selben Aggregat klonen, aber nur ausgewählte Dateien aus dem Quell-Volume in das neue geklonte Volume einbeziehen.

  Dies ist nützlich für Situationen, in denen Sie Daten migrieren und bestimmte Dateien vom ursprünglichen Volume ausschließen möchten. Diese Aktion verwendet das "NetApp FlexClone" Funktionalität zum schnellen Duplizieren des Volumes und dann entfernen Sie die Dateien, die Sie **nicht** ausgewählt haben.

- **Kopieren und Synchronisieren von Dateien** aus einem Quell-Repository (ONTAP-Volume, S3-Bucket, NFS-Freigabe usw.) zu einem Verzeichnis in einem bestimmten Ziel-Speicherort (Ziel).

  Dies ist besonders nützlich, wenn Sie Daten von einem Quellsystem zu einem anderen migrieren. Nach der ersten Kopie synchronisiert der Service alle geänderten Daten auf der Grundlage des von Ihnen festgelegten Zeitplans. Diese Aktion verwendet das "NetApp BlueXP Kopier- und Synchronisierungsfunktion" Funktion zum Kopieren und Synchronisieren von Daten von einer Quelle an ein Ziel

Kopieren Sie Quelldateien auf eine NFS-Freigabe

Sie können Quelldateien, die von der BlueXP Klassifizierung gescannt werden, auf eine beliebige NFS-Freigabe kopieren. Die NFS-Freigabe muss nicht in die BlueXP Klassifizierung integriert werden – Sie müssen nur den Namen der NFS-Freigabe kennen, von der alle ausgewählten Dateien im Format kopiert werden `<host_name>:/<share_path>`.

> Sie können keine Dateien kopieren, die sich in Datenbanken befinden.

Anforderungen

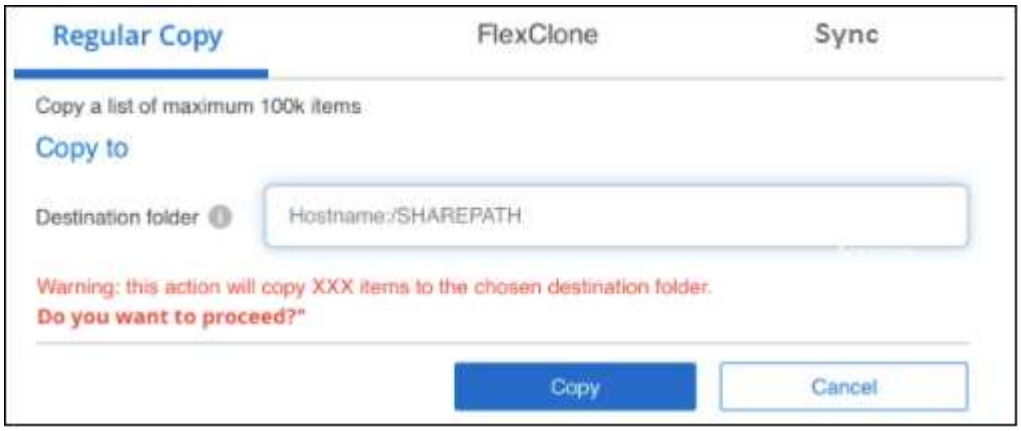
- Sie müssen über die Rolle „Kontoadministrator“ oder „Workspace-Admin“ verfügen, um Dateien zu kopieren.
- Für das Kopieren von Dateien muss die NFS-Zielfreigabe den Zugriff über die BlueXP Klassifizierungsinstanz ermöglichen.
- Sie können zwischen 1 und 100,000 Dateien gleichzeitig kopieren.

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie kopieren möchten, und klicken Sie auf **Kopieren**.

   - Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
   - Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).
   - Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name), und dann in der Pop-up-Nachricht All **20** Items on this page selected Select all Items in list (63K Items)Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.

2. Wählen Sie im Dialogfeld „ Dateien kopieren “ die Registerkarte **normale Kopie** aus.



3. Geben Sie den Namen der NFS-Freigabe ein, auf die alle ausgewählten Dateien in das Format kopiert werden sollen `<host_name>:/<share_path>`, Und klicken Sie auf **Kopieren**.

   Ein Dialogfeld mit dem Status des Kopiervorgangs wird angezeigt.

Sie können den Fortschritt des Kopiervorgangs in anzeigen "Statusbereich Aktionen".

Beachten Sie, dass Sie bei der Anzeige der Metadatendetails für eine Datei auch eine einzelne Datei kopieren können. Klicken Sie einfach auf **Datei kopieren**.

Volume-Daten auf ein neues Volume klonen

Sie können ein vorhandenes ONTAP Volume klonen, das von der BlueXP Klassifizierung gescannt wird, mit der NetApp *FlexClone* Funktion. So können Sie das Volume schnell duplizieren, während nur die von Ihnen ausgewählten Dateien enthalten sind. Dies ist nützlich, wenn Sie Daten migrieren und bestimmte Dateien vom ursprünglichen Volume ausschließen möchten oder wenn Sie eine Kopie eines Volumes zu Testzwecken erstellen möchten.

Das neue Volume wird im selben Aggregat erstellt wie das Quell-Volume. Stellen Sie vor Beginn dieser Aufgabe sicher, dass genügend Platz für dieses neue Volume im Aggregat vorhanden ist. Wenden Sie sich bei Bedarf an Ihren Storage-Administrator.

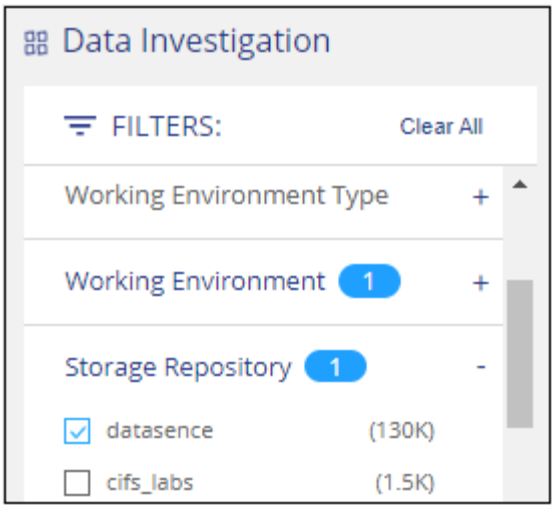
Hinweis: FlexGroup Volumes können nicht geklont werden, da sie nicht von FlexClone unterstützt werden.

Anforderungen

- Sie müssen über die Rolle „Kontoadministrator“ oder „Workspace-Admin“ verfügen, um Dateien zu kopieren.
- Sie müssen mindestens 20 Dateien auswählen.
- Alle ausgewählten Dateien müssen sich vom selben Volume befinden, und das Volume muss online sein.
- Das Volume muss aus einem Cloud Volumes ONTAP oder einem lokalen ONTAP System stammen. Derzeit werden keine anderen Datenquellen unterstützt.
- Die FlexClone Lizenz muss auf dem Cluster installiert sein. Diese Lizenz wird standardmäßig auf Cloud Volumes ONTAP-Systemen installiert.

Schritte

1. Erstellen Sie im Bereich Datenuntersuchung einen Filter, indem Sie eine einzige **Arbeitsumgebung** und ein einziges **Speicher-Repository** auswählen, um sicherzustellen, dass alle Dateien vom selben ONTAP-Volume stammen.

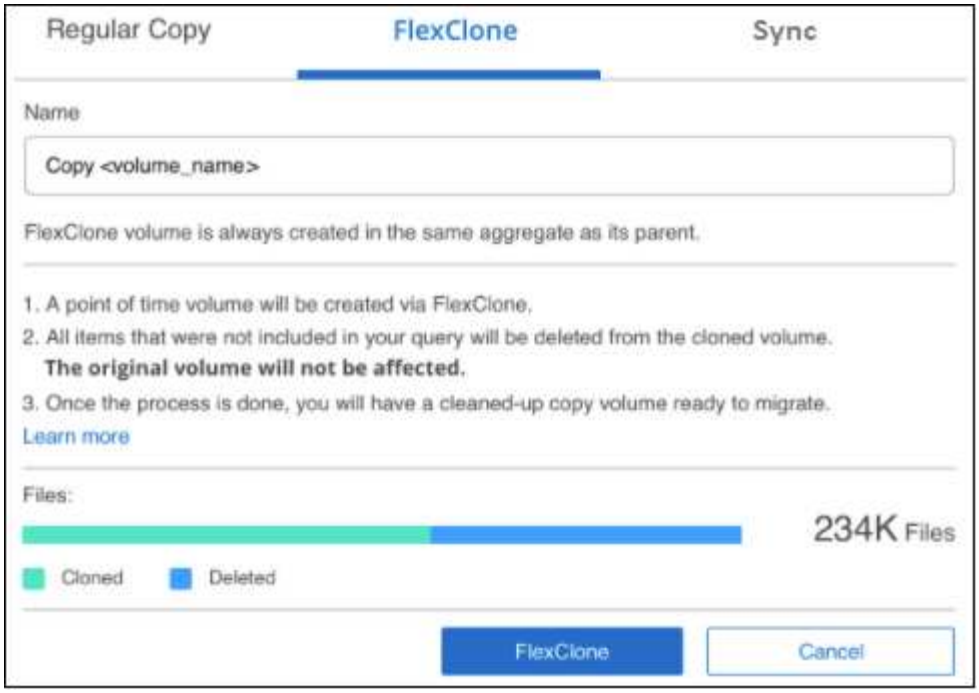


Wenden Sie alle anderen Filter an, sodass nur die Dateien zu sehen sind, die Sie auf dem neuen Volume klonen möchten.

2. Wählen Sie im Bereich Untersuchungsergebnisse die Dateien aus, die Sie klonen möchten, und klicken Sie auf **Kopieren**.

- Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
- Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).
- Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name), und dann in der Pop-up-Nachricht All **20** Items on this page selected Select all Items in list (63K Items)Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.

3. Wählen Sie im Dialogfeld *Dateien kopieren* die Registerkarte **FlexClone** aus. Diese Seite zeigt die Gesamtzahl der Dateien, die aus dem Volume geklont werden (die von Ihnen ausgewählten Dateien) und die Anzahl der Dateien, die nicht enthalten bzw. gelöscht sind (die Dateien, die Sie nicht ausgewählt haben), aus dem geklonten Volume.



4. Geben Sie den Namen des neuen Volume ein und klicken Sie auf **FlexClone**.

   Ein Dialogfeld mit dem Status des Klonvorgangs wird angezeigt.

Ergebnis

Das neue geklonte Volume wird in demselben Aggregat erstellt wie das Quell-Volume.

Sie können den Status des Klonvorgangs in anzeigen "Statusbereich Aktionen".

Wenn Sie zunächst **Alle Volumes zuweisen** oder **alle Volumes zuordnen und klassifizieren** ausgewählt haben, wenn Sie die BlueXP-Klassifizierung für die Arbeitsumgebung aktiviert haben, in der sich das Quell-Volume befindet, wird die BlueXP-Klassifizierung das neue geklonte Volume automatisch scannen. Wenn Sie eine dieser Optionen zunächst nicht verwendet haben, müssen Sie dieses neue Volume scannen "Aktivieren Sie manuell das Scannen auf dem Volumen".

Kopieren und synchronisieren Sie Quelldateien auf ein Zielsystem

Sie können Quelldateien, die von der BlueXP Klassifizierung gescannt werden, von einer unterstützten unstrukturierten Datenquelle in ein Verzeichnis an einem bestimmten Zielspeicherort kopieren ("Zielorte, die von der BlueXP Kopier- und Synchronisierungsfunktion unterstützt werden"). Nach der ersten Kopie werden alle geänderten Daten in den Dateien gemäß dem von Ihnen konfigurierten Zeitplan synchronisiert.

Dies ist besonders nützlich, wenn Sie Daten von einem Quellsystem zu einem anderen migrieren. Diese Aktion verwendet das "NetApp BlueXP Kopier- und Synchronisierungsfunktion" Funktion zum Kopieren und Synchronisieren von Daten von einer Quelle an ein Ziel

> Dateien, die sich in Datenbanken, OneDrive-Konten oder SharePoint Konten befinden, können nicht kopiert und synchronisiert werden.

Anforderungen

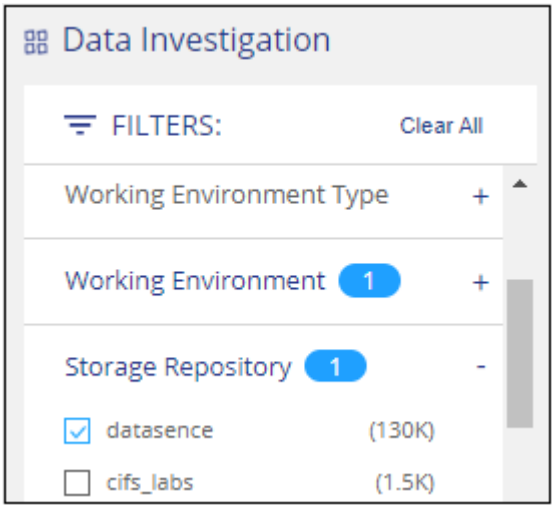
- Zum Kopieren und Synchronisieren von Dateien müssen Sie über die Rolle „Kontoadministrator“ oder „Arbeitsbereichsadministrator“ verfügen.

- Sie müssen mindestens 20 Dateien auswählen.
- Alle ausgewählten Dateien müssen aus demselben Quell-Repository stammen (ONTAP Volume, S3 Bucket, NFS oder CIFS-Freigabe usw.).
- Sie müssen den BlueXP Kopier- und Synchronisierungsservice aktivieren und mindestens einen Daten-Broker konfigurieren, mit dem Dateien zwischen Quell- und Zielsystemen übertragen werden können. Prüfen Sie die BlueXP Kopier- und Synchronisierungsanforderungen beginnend mit "Kurzanleitung".

  Beachten Sie, dass für den BlueXP Kopier- und Synchronisierungsservice unterschiedliche Servicegebühren für Ihre Synchronisierungsbeziehungen anfallen und Ressourcengebühren anfallen, wenn Sie den Daten-Broker in der Cloud implementieren.

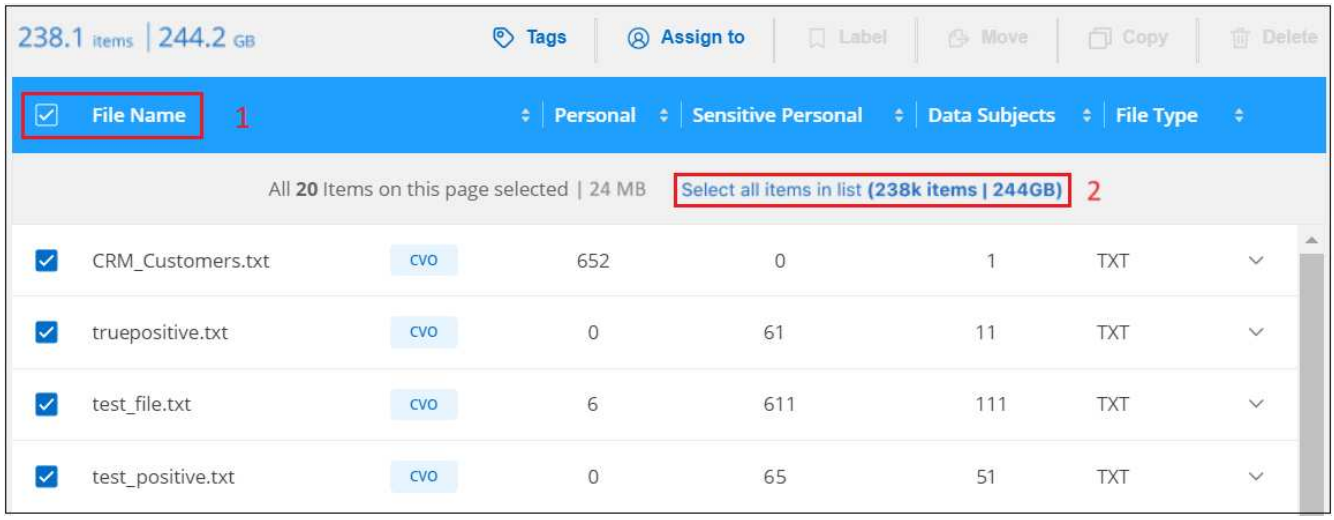
Schritte

1. Erstellen Sie im Bereich Datenuntersuchung einen Filter, indem Sie eine einzige * Arbeitsumgebung* und ein einziges **Speicher-Repository** auswählen, um sicherzustellen, dass alle Dateien aus demselben Repository stammen.

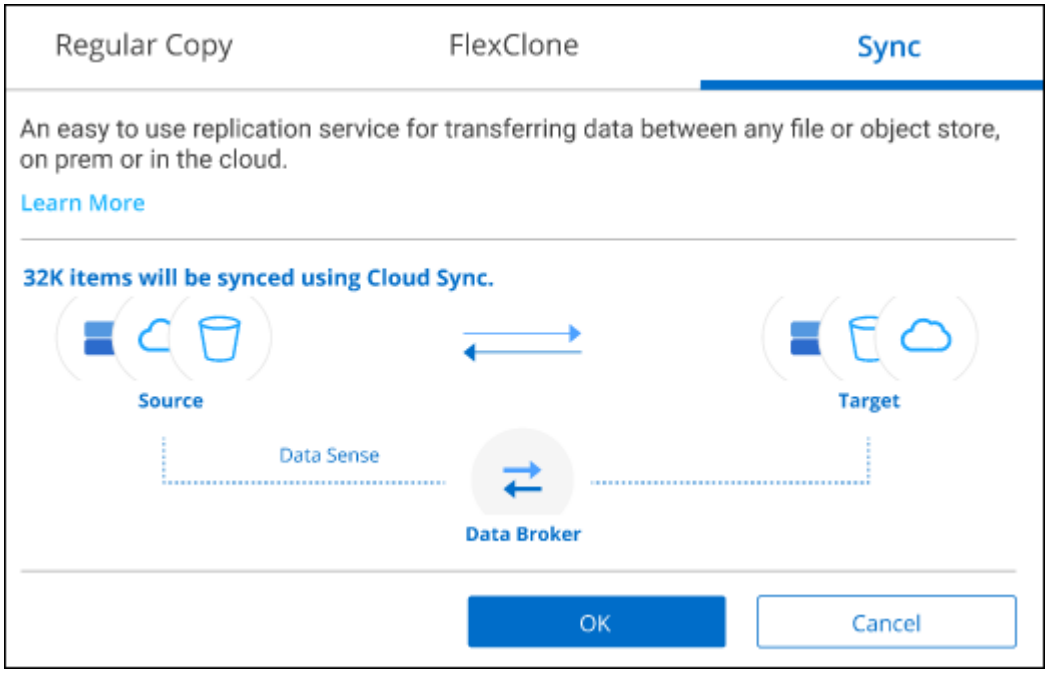


   Wenden Sie alle anderen Filter an, sodass nur die Dateien zu sehen sind, die Sie kopieren und mit dem Zielsystem synchronisieren möchten.

2. Wählen Sie im Bereich Untersuchungsergebnisse alle Dateien auf allen Seiten aus, indem Sie das Kästchen in der Titelzeile (aktivieren File Name), dann in der Pop-up-Nachricht All **20** Items on this page selected Select all Items in list (63K Items) Klicken Sie auf **Wählen Sie alle Elemente aus der Liste aus (xxx Elemente)**, und klicken Sie dann auf **Kopieren**.



3. Wählen Sie im Dialogfeld „ Dateien kopieren “ die Registerkarte **Sync** aus.



4. Wenn Sie sicher sind, dass Sie die ausgewählten Dateien mit einem Zielort synchronisieren möchten, klicken Sie auf **OK**.

   Die BlueXP Kopier- und Synchronisierungs-UI wird in BlueXP geöffnet.

   Sie werden aufgefordert, die Synchronisierungsbeziehung zu definieren. Das Quellsystem basiert auf dem Repository und den Dateien, die Sie bereits in der BlueXP Klassifizierung ausgewählt haben, und wird entsprechend vorausgefüllt.

5. Sie müssen das Zielsystem auswählen und dann den zu verwendenden Daten-Broker (oder erstellen) auswählen. Prüfen Sie die BlueXP Kopier- und Synchronisierungsanforderungen beginnend mit "Kurzanleitung".

Ergebnis

Die Dateien werden in das Zielsystem kopiert und auf der Grundlage des von Ihnen definierten Zeitplans synchronisiert. Wenn Sie eine einmalige Synchronisierung auswählen, werden die Dateien nur einmal kopiert

und synchronisiert. Wenn Sie eine regelmäßige Synchronisierung auswählen, werden die Dateien auf Grundlage des Zeitplans synchronisiert. Beachten Sie, dass wenn das Quellsystem neue Dateien hinzufügt, die mit der Abfrage übereinstimmen, die Sie mit Filtern erstellt haben, diese *neuen*-Dateien in das Ziel kopiert und in Zukunft synchronisiert werden.

Beachten Sie, dass einige der üblichen BlueXP Kopier- und Synchronisierungsvorgänge deaktiviert sind, wenn sie aus der BlueXP Klassifizierung aufgerufen werden:

- Sie können die Schaltflächen **Dateien auf Quelle löschen** oder **Dateien auf Ziel** löschen nicht verwenden.
- Ausführen eines Berichts ist deaktiviert.

Verschieben Sie Quelldateien auf eine NFS-Freigabe

Sie können Quelldateien, die von der BlueXP Klassifizierung gescannt werden, auf jede beliebige NFS-Freigabe verschieben. Die NFS-Freigabe muss nicht in die BlueXP Klassifizierung integriert werden.

Optional können Sie eine Breadcrumb-Datei am Speicherort der verschobenen Datei belassen. Eine Breadcrumb-Datei hilft Ihren Benutzern zu verstehen, warum eine Datei vom ursprünglichen Speicherort verschoben wurde. Für jede verschobene Datei erstellt das System eine Breadcrumb-Datei im Quellspeicherort mit dem Namen `<filename>-breadcrumb-<date>.txt`. Sie können Text in das Dialogfeld einfügen, das der Breadcrumb-Datei hinzugefügt wird, um den Speicherort anzugeben, an dem die Datei verschoben wurde, und den Benutzer, der die Datei verschoben hat.

Beachten Sie, dass die Unterverzeichnisstruktur aus der Quelldatei beim Verschieben der Datei auf der Zielfreigabe neu erstellt wird, sodass Sie leichter verstehen können, woher die Datei verschoben wurde. Wenn eine Datei mit dem gleichen Namen am Zielspeicherort vorhanden ist, wird die Datei nicht verschoben.

Sie können keine Dateien verschieben, die sich in Datenbanken befinden.

Anforderungen

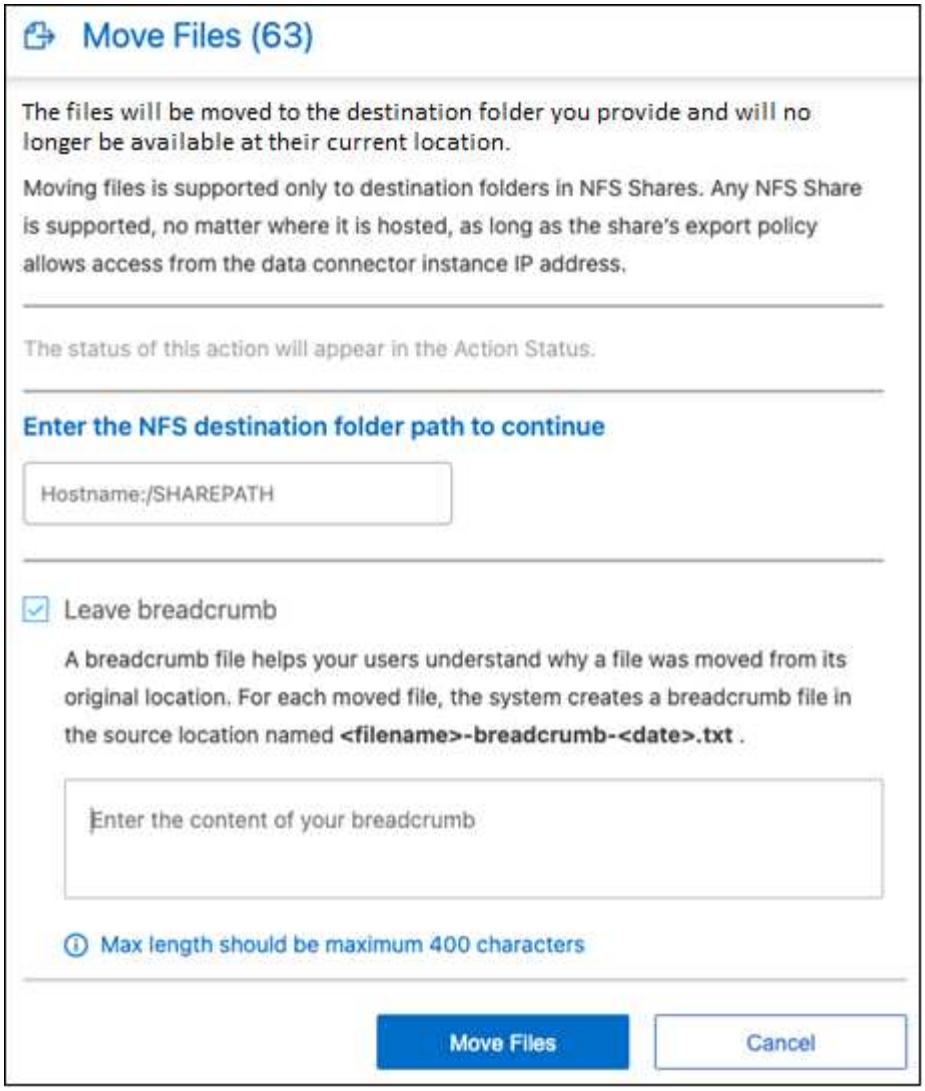
- Sie müssen über die Rolle „Kontoadministrator“ oder „Arbeitsbereichsadministrator“ verfügen, um Dateien zu verschieben.
- Die Quelldateien lassen sich in den folgenden Datenquellen befinden: On-Premises ONTAP, Cloud Volumes ONTAP, Azure NetApp Files, File Shares und SharePoint Online.
- Sie können maximal 15 Millionen Dateien gleichzeitig verschieben.
- Es werden nur Dateien verschoben, die 50 MB oder kleiner sind.
- Die NFS-Zielfreigabe muss den Zugriff von der IP-Adresse der BlueXP Klassifizierungsinstanz ermöglichen.

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie verschieben möchten.

- Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
- Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).
- Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name), und dann in der Pop-up-Nachricht All **20** Items on this page selected Select all Items in list (63K Items)Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.

2. Klicken Sie in der Tastenleiste auf **Move**.



3. Geben Sie im Dialogfeld „ Dateien verschieben “ den Namen der NFS-Freigabe ein, bei der alle ausgewählten Dateien im Format verschoben werden `<host_name>:/<share_path>`.
4. Wenn Sie eine Breadcrumb-Datei verlassen möchten, aktivieren Sie das Kontrollkästchen *Breadcrumb* verlassen. Sie können Text in das Dialogfeld eingeben, um den Speicherort anzugeben, an dem die Datei verschoben wurde, sowie den Benutzer, der die Datei verschoben hat, und weitere Informationen, z. B. den Grund, aus dem die Datei verschoben wurde.
5. Klicken Sie Auf **Dateien Verschieben**.

Beachten Sie, dass Sie auch eine einzelne Datei verschieben können, wenn Sie sich die Metadatendetails für eine Datei ansehen. Klicken Sie einfach auf **Datei verschieben**.

Quelldateien löschen

Sie können Quelldateien dauerhaft entfernen, die unsicher oder zu riskant erscheinen, um in Ihrem Speichersystem zu verbleiben, oder dass Sie als Duplikat identifiziert haben. Diese Aktion ist permanent und es gibt kein Rückgängigmachen oder Wiederherstellen.

Sie können Dateien manuell aus dem Untersuchungsbereich löschen, oder "Automatische Verwendung von Richtlinien".

> Sie können keine Dateien löschen, die sich in Datenbanken befinden. Alle anderen Datenquellen werden unterstützt.

Das Löschen von Dateien erfordert die folgenden Berechtigungen:

- Für NFS-Daten: Die Exportrichtlinie muss mit Schreibberechtigungen definiert werden.
- Für CIFS-Daten - die CIFS-Anmeldeinformationen benötigen Schreibberechtigungen.
- Für S3-Daten muss die IAM-Rolle die folgende Berechtigung enthalten: `s3:DeleteObject`.

Quelldateien manuell löschen

Anforderungen

- Zum Löschen von Dateien müssen Sie über die Rolle „Kontoadministrator“ oder „Workspace-Admin“ verfügen.
- Sie können maximal 100,000 Dateien gleichzeitig löschen.

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie löschen möchten.

- Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
- Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).
- Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name), und dann in der Pop-up-Nachricht All **20** Items on this page selected Select all Items in list (63K Items)Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.

2. Klicken Sie in der Tastenleiste auf **Löschen**.
3. Da der Löschvorgang dauerhaft ist, müssen Sie "**permanent delete**" in das folgende Dialogfeld *Datei löschen* eingeben und auf **Datei löschen** klicken.

Sie können den Fortschritt des Löschvorgangs in der anzeigen "Statusbereich Aktionen".

Beachten Sie, dass Sie auch eine einzelne Datei löschen können, wenn Sie sich die Metadatendetails für eine Datei ansehen. Klicken Sie einfach auf **Datei löschen**.

Anzeigen von Compliance-Berichten

Die BlueXP Klassifizierung bietet Berichte, die Sie verwenden können, um besseren Einblick in den Status Ihres Unternehmenskonzepts zum Datenschutz zu erhalten.

Standardmäßig zeigen die BlueXP Klassifizierungs-Dashboards Compliance- und Governance-Daten für alle Arbeitsumgebungen, Datenbanken und Datenquellen an. Wenn Sie Berichte anzeigen möchten, die Daten nur für einige Arbeitsumgebungen enthalten, Wählen Sie diese Arbeitsumgebungen aus.

- Die in diesem Abschnitt beschriebenen Berichte sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan durchgeführt wurde, können nur den Daten-Mapping-Bericht generieren.
- NetApp kann die Genauigkeit der personenbezogenen Daten und sensiblen personenbezogenen Daten, die durch die BlueXP Klassifizierung identifiziert werden, nicht zu 100 % garantieren. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Datenschutzrisiko-Assessment-Bericht

Der Datenschutzrisiko-Assessment-Bericht bietet einen Überblick über den Datenschutz-Risikostatus Ihres Unternehmens, wie durch Datenschutzvorschriften wie DSGVO und CCPA erforderlich. Der Bericht enthält die folgenden Informationen:

Compliance-Status

A Schweregrad Und die Verteilung von Daten, ganz gleich, ob es sich um unempfindliche, personenbezogene oder sensible Daten handelt.

Assessment-Übersicht

Eine Aufschlüsselung der gefundenen Arten von personenbezogenen Daten sowie der Kategorien von Daten.

Betroffene in dieser Beurteilung

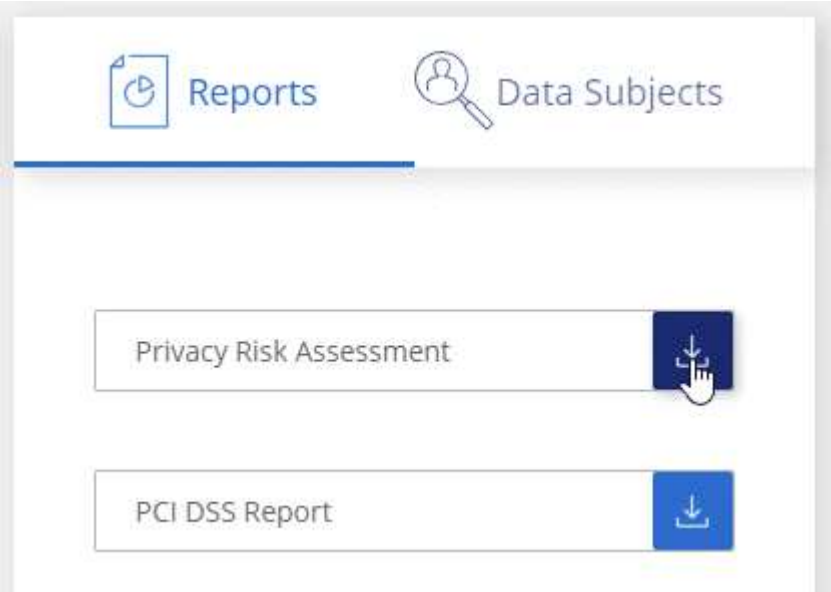
Die Anzahl der Personen, nach Ort, für die nationale Kennungen gefunden wurden.

Erstellen Sie den Bericht zur Risikoanalyse für den Datenschutz

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Compliance** und dann auf das Download-Symbol neben **Privacy Risk Assessment** unter **Reports**.



Ergebnis

Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Schweregrad

Die BlueXP Klassifizierung berechnet die Bewertung des Schweregrads für den Bericht zur Risikoanalyse personenbezogener Daten auf der Basis von drei Variablen:

- Der Prozentsatz der personenbezogenen Daten aus allen Daten.
- Der Prozentsatz sensibler personenbezogener Daten aus allen Daten.
- Der Prozentsatz der Dateien, die betroffene Daten enthalten, die durch nationale Kennungen wie nationale IDs, Sozialversicherungsnummern und Steuerkennzahlen bestimmt werden.

Die folgende Logik dient zur Ermittlung der Punktzahl:

Schweregrad	Logik
0	Alle drei Variablen sind genau 0%
1	Eine der Variablen ist größer als 0 %
2	Eine der Variablen ist größer als 3%
3	Zwei der Variablen sind größer als 3%
4	Drei der Variablen sind größer als 3 %
5	Eine der Variablen ist größer als 6%
6	Zwei der Variablen sind größer als 6%
7	Drei der Variablen sind größer als 6 %
8	Eine der Variablen ist größer als 15%
9	Zwei der Variablen sind größer als 15%
10	Drei der Variablen sind größer als 15 %

PCI DSS-Bericht

Der PCI DSS-Bericht (Payment Card Industry Data Security Standard) hilft Ihnen bei der Identifizierung der Verteilung von Kreditkarteninformationen über Ihre Dateien hinweg. Der Bericht enthält die folgenden Informationen:

Überblick

Wie viele Dateien enthalten Kreditkarteninformationen und in welchen Arbeitsumgebungen.

Verschlüsselung

Der Prozentsatz der Dateien, die Kreditkartendaten in verschlüsselten oder nicht verschlüsselten Arbeitsumgebungen enthalten. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Schutz Vor Ransomware

Der Prozentsatz von Dateien mit Kreditkarteninformationen, die in Arbeitsumgebungen gespeichert sind, für die der Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Aufbewahrung

Der Zeitrahmen, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, weil Sie Ihre Kreditkartendaten nicht länger aufbewahren sollten, als Sie sie bearbeiten müssen.

Verteilung der Kreditkarteninformationen

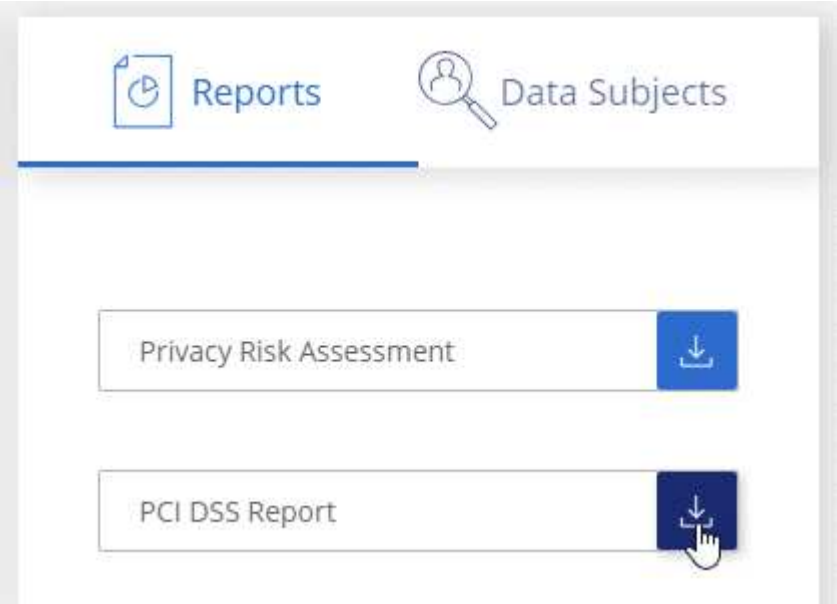
Die Arbeitsumgebungen, in denen Kreditkartendaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

Erstellen Sie den PCI DSS-Bericht

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Compliance** und dann auf das Download-Symbol neben **PCI DSS Report** unter **Reports**.



Ergebnis

Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

HIPAA-Bericht

Der HIPAA-Bericht (Health Insurance Portability and Accountability Act) hilft Ihnen bei der Identifizierung von Dateien, die Gesundheitsdaten enthalten. Er unterstützt Ihr Unternehmen bei der Einhaltung der HIPAA-Datenschutzgesetze. Die Informationen, für die die BlueXP Klassifizierung geeignet ist, umfassen:

- Zustandsreferenzmuster
- ICD-10 CM medizinischer Code
- ICD-9 CM medizinischer Code
- HR – Kategorie Gesundheit
- Datenkategorie für Gesundheitsanwendungen

Der Bericht enthält die folgenden Informationen:

Überblick

Wie viele Dateien enthalten Gesundheitsinformationen und in welchen Arbeitsumgebungen.

Verschlüsselung

Der Prozentsatz der Dateien, die Gesundheitsinformationen in verschlüsselten oder nicht verschlüsselten Arbeitsumgebungen enthalten. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Schutz Vor Ransomware

Der Prozentsatz von Dateien mit Gesundheitsinformationen in Arbeitsumgebungen, in denen Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Aufbewahrung

Der Zeitrahmen, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, weil Sie Gesundheitsinformationen nicht länger aufbewahren sollten, als Sie sie verarbeiten müssen.

Verteilung von Gesundheitsinformationen

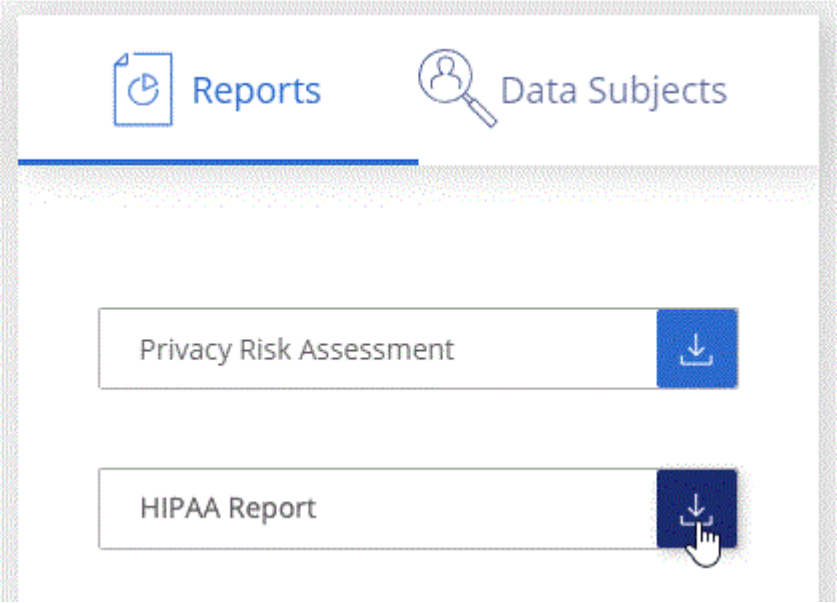
In den Arbeitsumgebungen, in denen die Gesundheitsdaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

Erstellen Sie den HIPAA-Bericht

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Compliance** und dann auf das Download-Symbol neben **HIPAA Report** unter **Reports**.



Ergebnis

Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Was ist ein Antrag auf Zugang für betroffene Person?

Datenschutzvorschriften wie die Europäische DSGVO erteilen Betroffenen (wie Kunden oder Mitarbeitern) das Recht, auf ihre personenbezogenen Daten zuzugreifen. Wenn eine betroffene Person diese Informationen anfordert, wird dies als DSAR (Zugriffsanfrage für betroffene Person) bezeichnet. Unternehmen sind verpflichtet, auf diese Anfragen „ohne übermäßige Verzögerung“ und spätestens innerhalb eines Monats nach Eingang zu reagieren.

Sie können auf einen DSAR antworten, indem Sie nach dem vollständigen Namen eines Studienteilnehmers oder einer bekannten Kennung (z. B. einer E-Mail-Adresse) suchen und dann einen Bericht herunterladen. Der Bericht soll Ihrem Unternehmen helfen, die Vorgaben der DSGVO oder ähnlicher Datenschutzgesetze einzuhalten.

Wie kann die BlueXP Klassifizierung Ihnen helfen, auf eine DSAR zu reagieren?

Wenn Sie eine Suche nach einer bestimmten Person durchführen, findet die BlueXP Klassifizierung alle Dateien, Buckets, OneDrive und SharePoint Konten, die den Namen oder die Kennung dieser Person enthalten. Die BlueXP Klassifizierung überprüft die aktuellsten vorab indizierten Daten nach dem Namen oder der Kennung. Es wird kein neuer Scan gestartet.

Nachdem die Suche abgeschlossen ist, können Sie die Liste der Dateien für einen Bericht für die Anforderung von Datensubjekten herunterladen. Der Bericht sammelt Erkenntnisse aus den Daten und stellt die Daten zu rechtlichen Bedingungen bereit, die Sie an die Person zurücksenden können.

> Die Suche nach Betroffenen wird derzeit in Datenbanken nicht unterstützt.

Suche nach betroffenen Personen und Download von Berichten

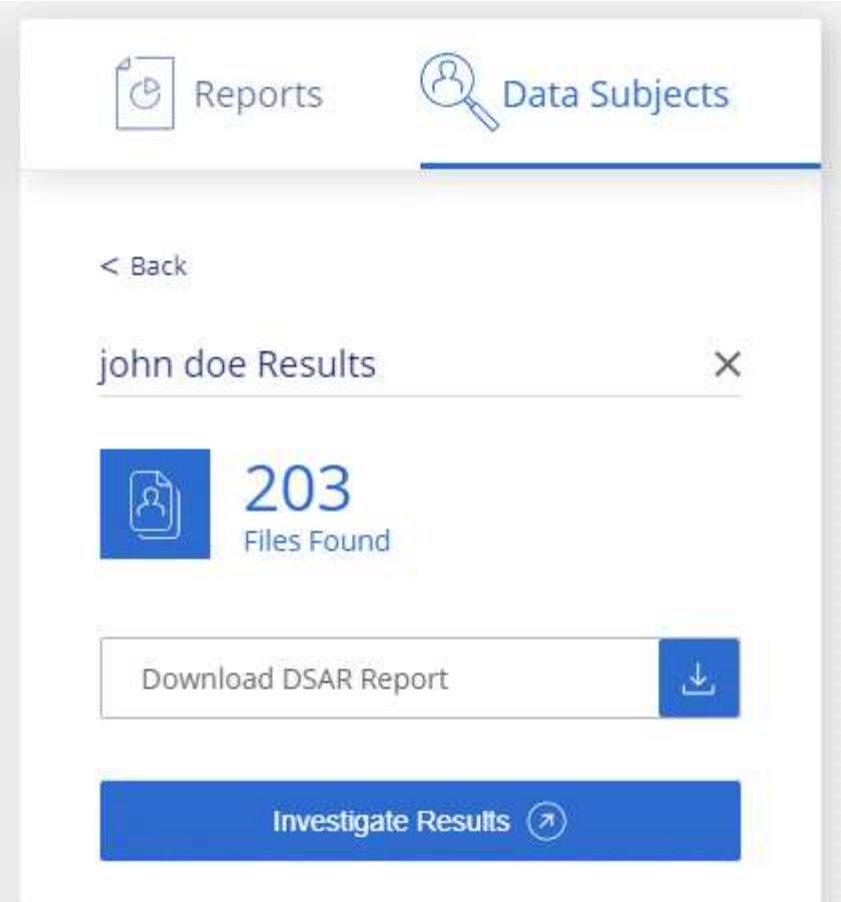
Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen, und laden Sie dann einen Dateilistenbericht oder einen DSAR-Bericht herunter. Suchen Sie nach "Alle persönlichen Informationstypen".

> Bei der Suche nach den Namen der betroffenen Personen werden Englisch, Deutsch, Japanisch und Spanisch unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie Auf **Data Subjects**.
3. Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen.

   Hier ein Beispiel, das eine Suche nach dem Namen *john doe* zeigt:



4. Wählen Sie eine der folgenden Optionen:
   - **Download DSAR Report**: Eine formelle Antwort auf die Zugriffsanfrage, die Sie an den Betroffenen senden können. Dieser Bericht enthält automatisch generierte Informationen, die auf Daten basieren, deren BlueXP-Klassifizierung für den Betroffenen gefunden wurde und als Vorlage dienen. Füllen Sie das Formular aus und überprüfen Sie es intern, bevor Sie es an den Betroffenen senden.
   - **Ergebnisse untersuchen**: Eine Seite, auf der Sie die Daten untersuchen können, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern und die Dateiliste herunterladen.

     Wenn es mehr als 10,000 Ergebnisse gibt, werden nur die Top 10,000 in der Dateiliste angezeigt.

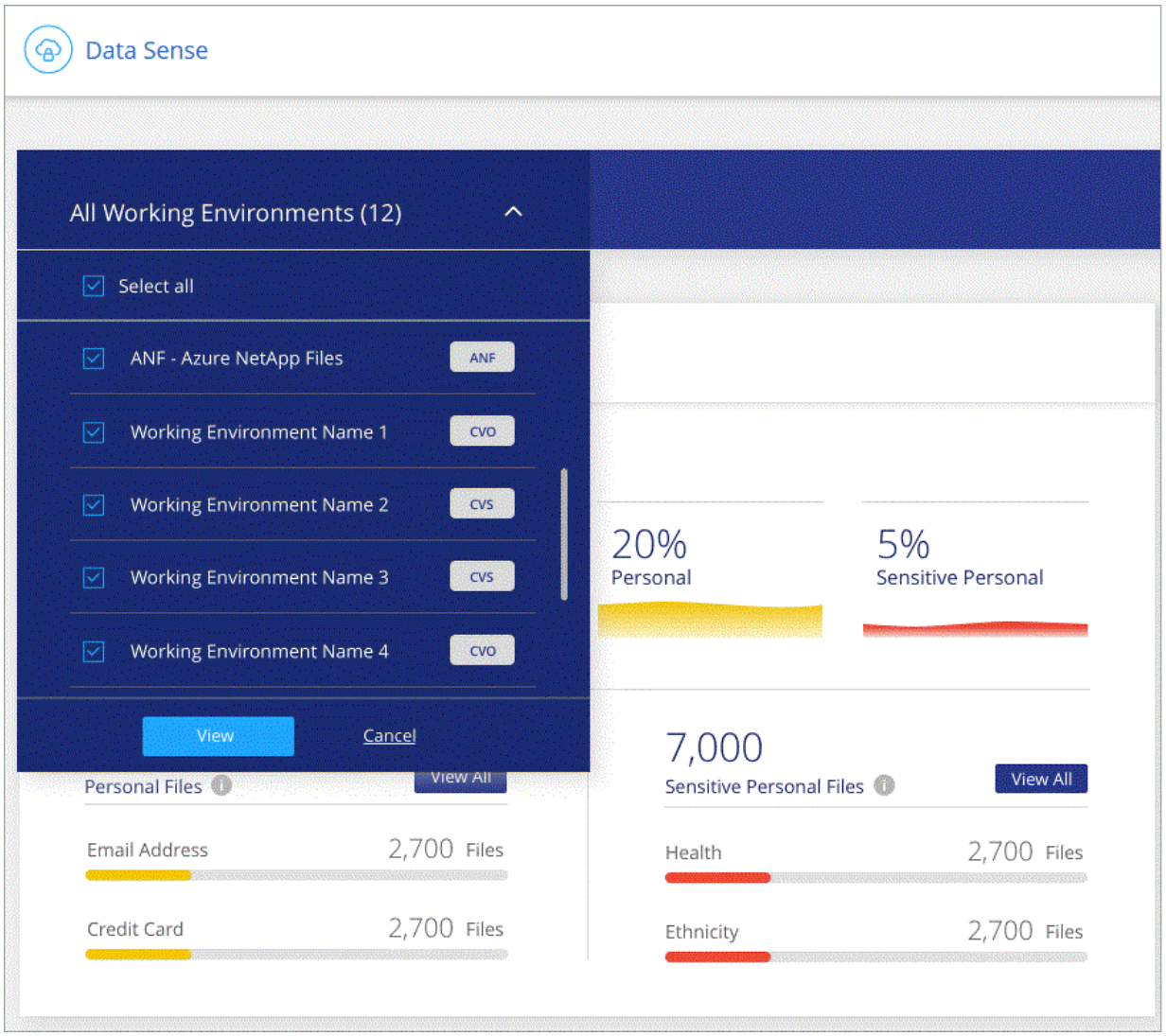
Wählen Sie die Arbeitsumgebungen für Berichte aus

Sie können die Inhalte des BlueXP Klassifizierungs-Compliance-Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur für bestimmte Arbeitsumgebungen einzusehen.

Wenn Sie das Dashboard filtern, erfasst die BlueXP Klassifizierung die Compliance-Daten und Berichte nur an die von Ihnen ausgewählten Applikationsumgebungen.

Schritte

1. Klicken Sie auf das Dropdown-Menü Filter, wählen Sie die Arbeitsumgebungen aus, für die Sie Daten anzeigen möchten, und klicken Sie auf **Ansicht**.


Data Sense
All Working Environments (12)
Select all
ANF - Azure NetApp Files
ANF
Working Environment Name 1
CVO
Working Environment Name 2
CVS
Working Environment Name 3
CVS
Working Environment Name 4
CVO
View
Cancel
20%
Personal
5%
Sensitive Personal
Personal Files
View All
Email Address
2,700 Files
Credit Card
2,700 Files
7,000
Sensitive Personal Files
View All
Health
2,700 Files
Ethnicity
2,700 Files

BlueXP Klassifizierung managen

Ergänzen Sie Ihre BlueXP Klassifizierungs-Scans um persönliche Daten-IDs

Die BlueXP Klassifizierung bietet Ihnen viele Möglichkeiten, eine benutzerdefinierte Liste mit „personenbezogenen Daten“ hinzuzufügen, die durch die BlueXP Klassifizierung bei zukünftigen Scans identifiziert werden. So haben Sie alle Informationen darüber, wo sich möglicherweise sensible Daten in den Dateien Ihrer Unternehmen befinden.

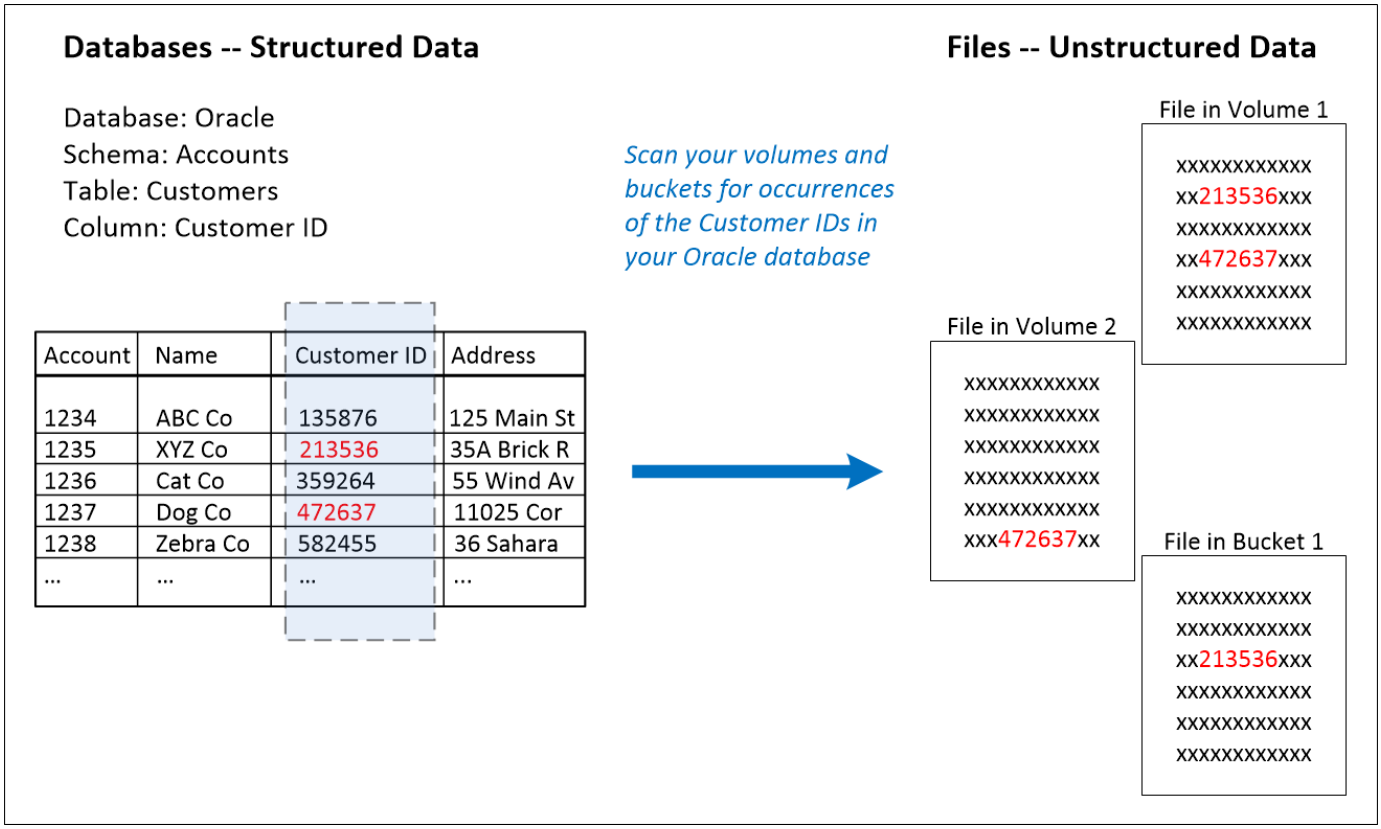
- Sie können eindeutige Kennungen basierend auf bestimmten Spalten in Datenbanken hinzufügen, die Sie scannen.
- Sie können benutzerdefinierte Schlüsselwörter aus einer Textdatei hinzufügen - diese Wörter werden in Ihren Daten identifiziert.
- Sie können ein persönliches Muster mit einem regulären Ausdruck (regex) hinzufügen — der Regex wird den bestehenden vordefinierten Mustern hinzugefügt.
- Sie können benutzerdefinierte Kategorien hinzufügen, um zu ermitteln, wo bestimmte Informationskategorien in Ihren Daten gefunden werden.

Alle diese Mechanismen zum Hinzufügen benutzerdefinierter Scankriterien werden in allen Sprachen unterstützt.

> Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.

Fügen Sie benutzerdefinierte ID-Daten aus Ihren Datenbanken hinzu

Eine Funktion, die wir *Data Fusion* nennen, ermöglicht Ihnen, die Daten Ihres Unternehmens zu überprüfen, um zu ermitteln, ob eindeutige IDs aus Ihren Datenbanken in einer Ihrer anderen Datenquellen gefunden werden. Sie können die zusätzlichen Identifikatoren auswählen, nach denen die BlueXP Klassifizierung in ihren Scans suchen soll, indem Sie eine bestimmte Spalte oder Spalte in einer Datenbanktabelle auswählen. Das folgende Diagramm zeigt beispielsweise, wie Daten-Fusion zur Überprüfung von Volumes, Buckets und Datenbanken eingesetzt wird, um vor allen Kunden-IDs aus der Oracle Datenbank zu kommen.



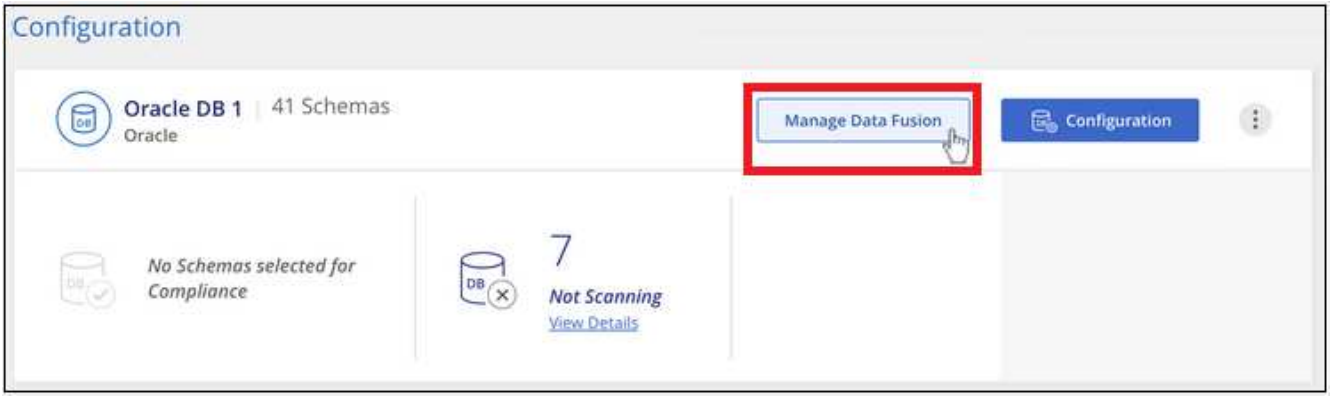
Wie Sie sehen, wurden in zwei Volumes und in einem S3-Bucket zwei eindeutige Kunden-IDs gefunden. Alle Übereinstimmungen in Datenbanktabellen werden ebenfalls identifiziert.

Da Sie Ihre eigenen Datenbanken scannen, können Sie mit jeder Sprache, in der Ihre Daten gespeichert sind, Daten bei zukünftigen BlueXP Klassifizierungs-Scans erkennen.

Schritte

Dieser muss unbedingt vorhanden sein "Hat mindestens einen Datenbankserver hinzugefügt" Bis zur BlueXP Klassifizierung vor dem Hinzufügen von Fusion-Datenquellen

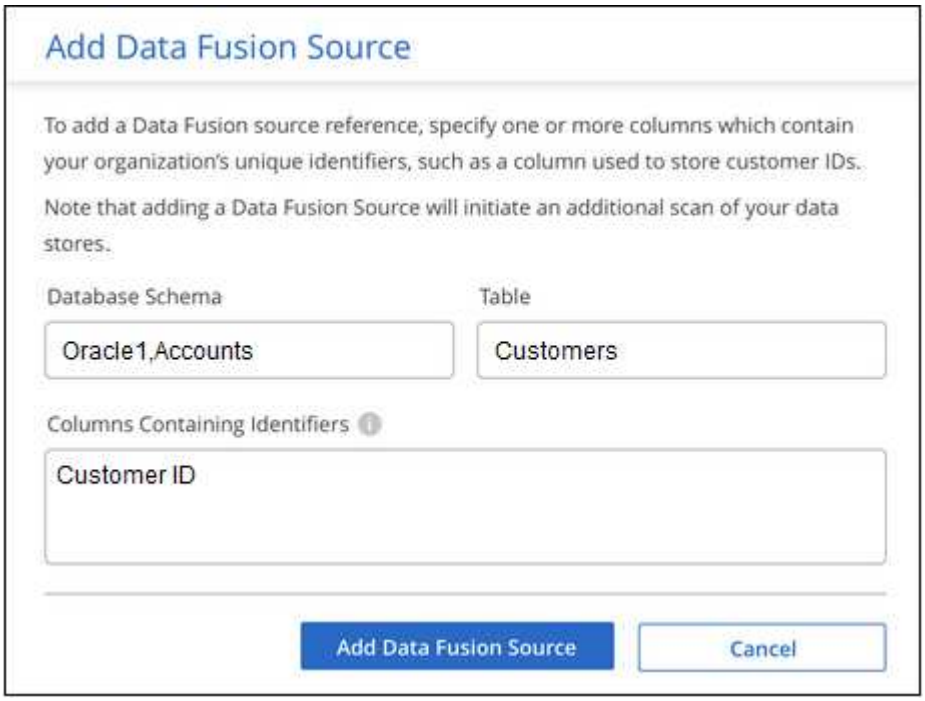
1. Klicken Sie auf der Konfigurationsseite in der Datenbank, in der sich die Quelldaten befinden, auf **Daten-Fusion verwalten**.



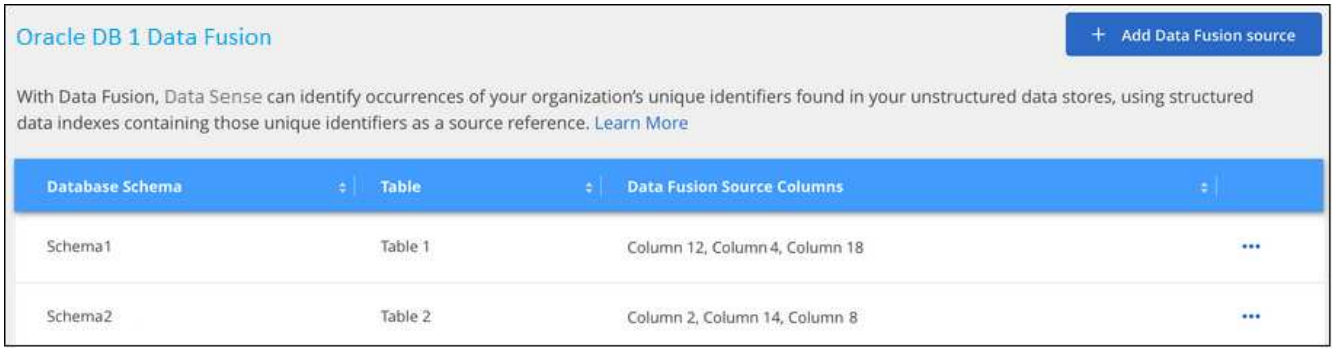
2. Klicken Sie auf der nächsten Seite auf **Data Fusion Source hinzufügen**.
3. Klicken Sie auf der Seite „ Fusion-Quelle hinzufügen “ auf die Seite „

a. Wählen Sie das Datenbankschema aus dem Dropdown-Menü aus.
b. Geben Sie den Tabellennamen in dieses Schema ein.
c. Geben Sie die Spalte oder Spalten ein, die die eindeutigen Kennungen enthalten, die Sie verwenden möchten.

   Wenn Sie mehrere Spalten hinzufügen, geben Sie jeden Spaltennamen oder Namen der Tabellenansicht in einer separaten Zeile ein.

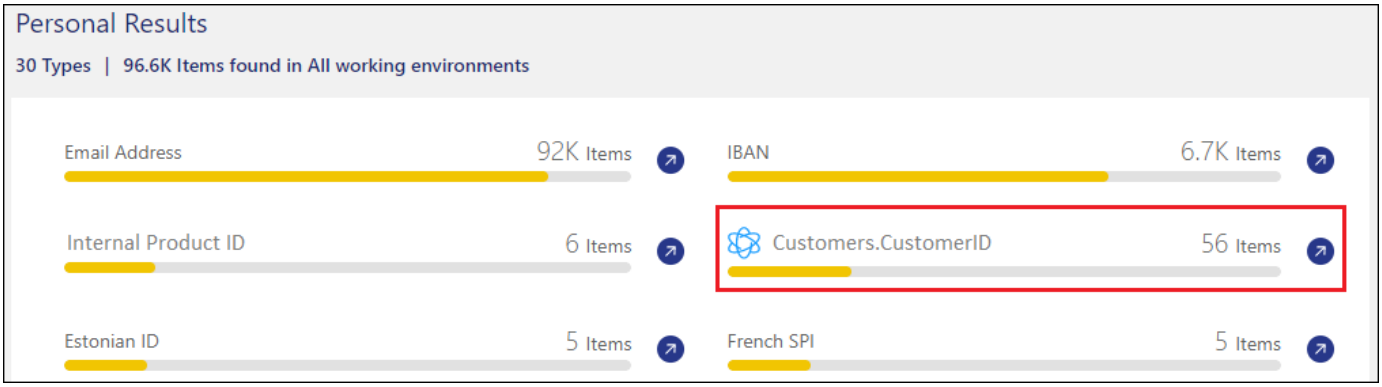


4. Klicken Sie Auf **Data Fusion-Quelle Hinzufügen**.



Ergebnisse

Nach dem nächsten Scan werden diese neuen Informationen im Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Untersuchungsseite im Filter „Persönliche Daten“ angezeigt. Der Name, den Sie für den Klassifikator verwendet haben, wird z. B. in der Filterliste angezeigt `Customers.CustomerID`.



Löschen Sie eine Data Fusion-Quelle

Wenn Sie sich irgendwann entscheiden, Ihre Dateien nicht mit einer bestimmten Data Fusion Quelle zu scannen, können Sie die Quellzeile auf der Seite Data Fusion Inventory auswählen und auf **Daten löschen Fusion Source** klicken.

Fügen Sie benutzerdefinierte Schlüsselwörter aus einer Wortliste hinzu

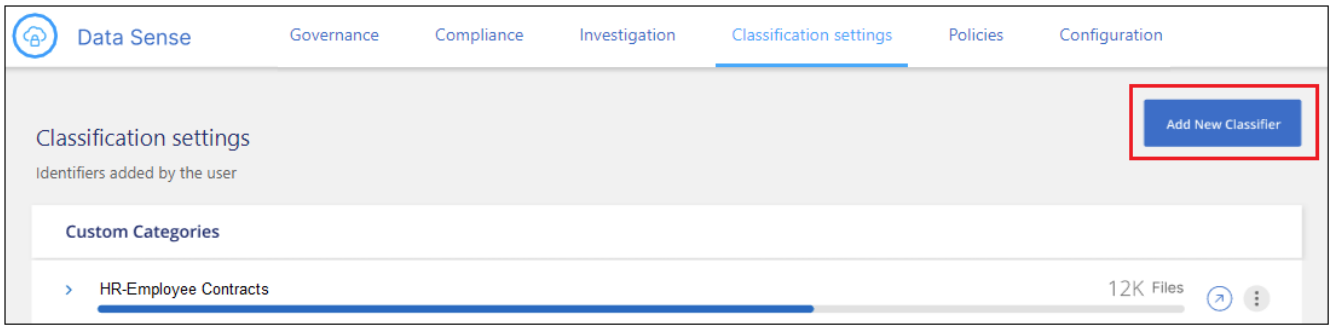
Sie können der BlueXP Klassifizierung benutzerdefinierte Schlüsselwörter hinzufügen, um den Speicherort der Daten bestimmen zu können. Fügen Sie die Schlüsselwörter einfach ein, indem Sie jedes Wort eingeben, das die BlueXP Klassifizierung wiedererkennen soll. Die Schlüsselwörter werden zu den vorhandenen vordefinierten Schlüsselwörtern hinzugefügt, die bereits von der BlueXP-Klassifizierung verwendet werden, und die Ergebnisse werden im Abschnitt „Persönliche Muster“ angezeigt.

Sie können z. B. sehen, wo interne Produktnamen in allen Dateien erwähnt werden, um sicherzustellen, dass diese Namen nicht an Orten zugänglich sind, die nicht sicher sind.

Nach der Aktualisierung der benutzerdefinierten Schlüsselwörter wird die BlueXP Klassifizierung neu gestartet und alle Datenquellen werden gescannt. Nach Abschluss des Scans werden die neuen Ergebnisse im BlueXP Classification Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Untersuchungsseite im Filter „Persönliche Daten“ angezeigt.

Schritte

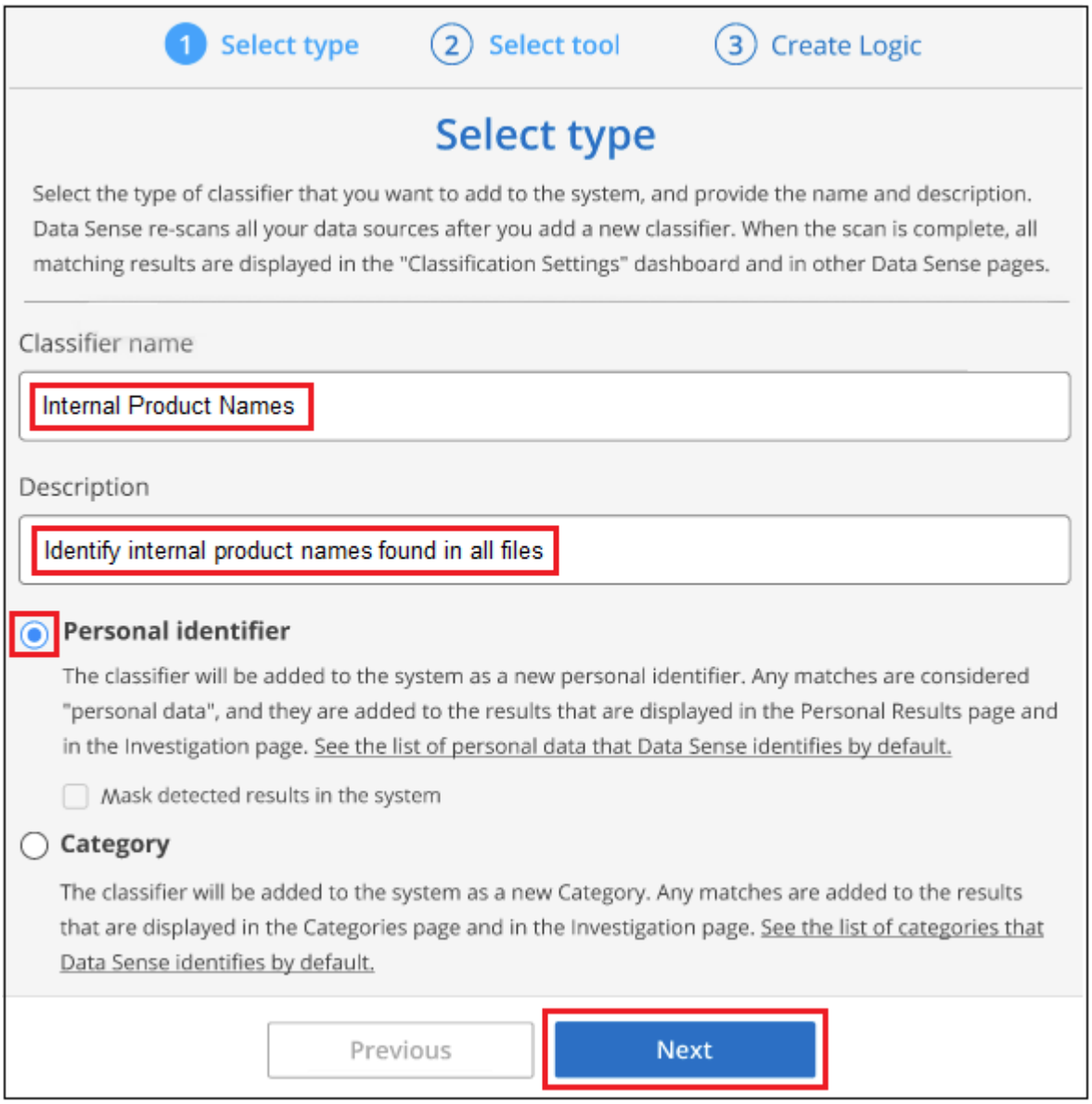
1. Klicken Sie auf der Registerkarte *Classification settings* auf **Add New Classifier**, um den Assistenten *Add Custom Classifier* zu starten.



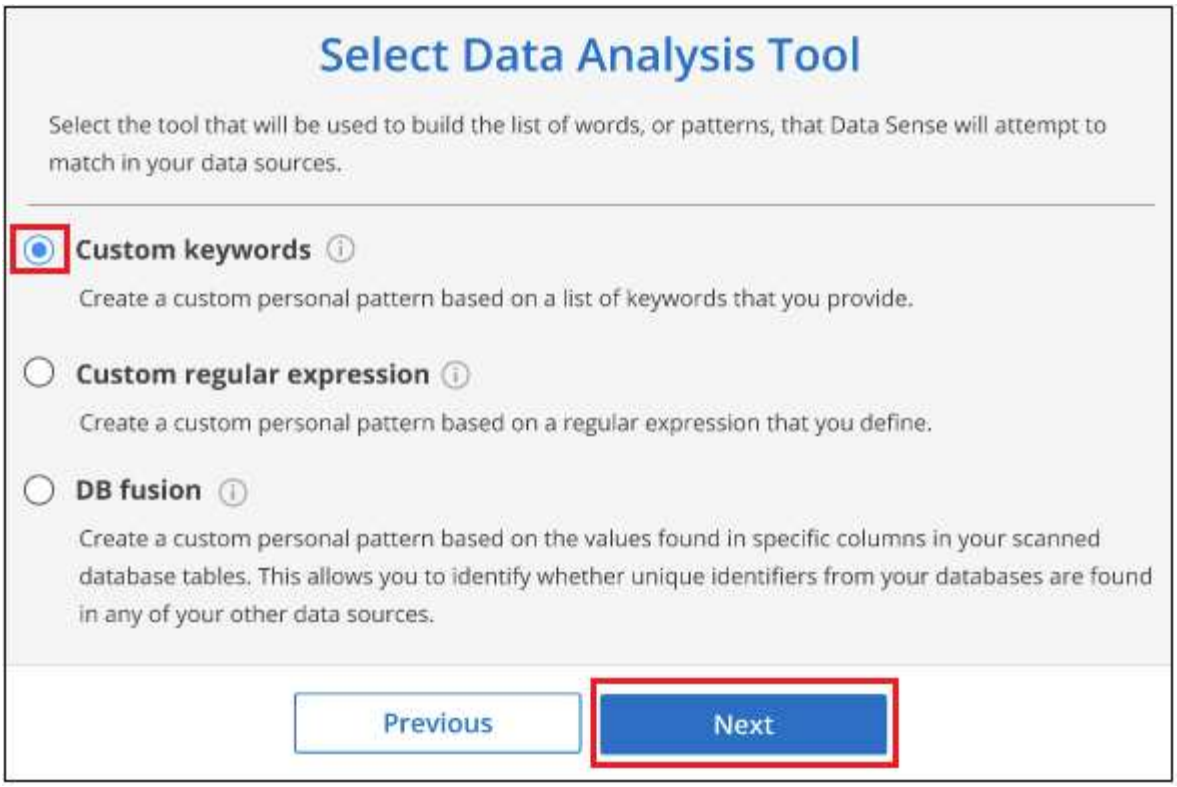
2. Geben Sie auf der Seite *Typ auswählen* den Namen des Klassifikators ein, geben Sie eine kurze Beschreibung ein, wählen Sie **Persönliche Kennung** aus und klicken Sie dann auf **Weiter**.

   Der eingegebene Name wird in der BlueXP-Klassifizierungs-UI als Überschrift für gescannte Dateien angezeigt, die den Anforderungen des Klassifikators entsprechen, und als Name des Filters auf der Seite Untersuchung.

   Sie können das Kontrollkästchen auch aktivieren, um „erkannte Ergebnisse im System maskieren“ zu aktivieren, damit das vollständige Ergebnis nicht in der Benutzeroberfläche angezeigt wird. So können Sie beispielsweise vollständige Kreditkartennummern oder ähnliche persönliche Daten ausblenden (die Maske erscheint in der Benutzeroberfläche wie folgt: "Pass:[***] Pass:[] Pass:[] Pass:[***]" 3434).

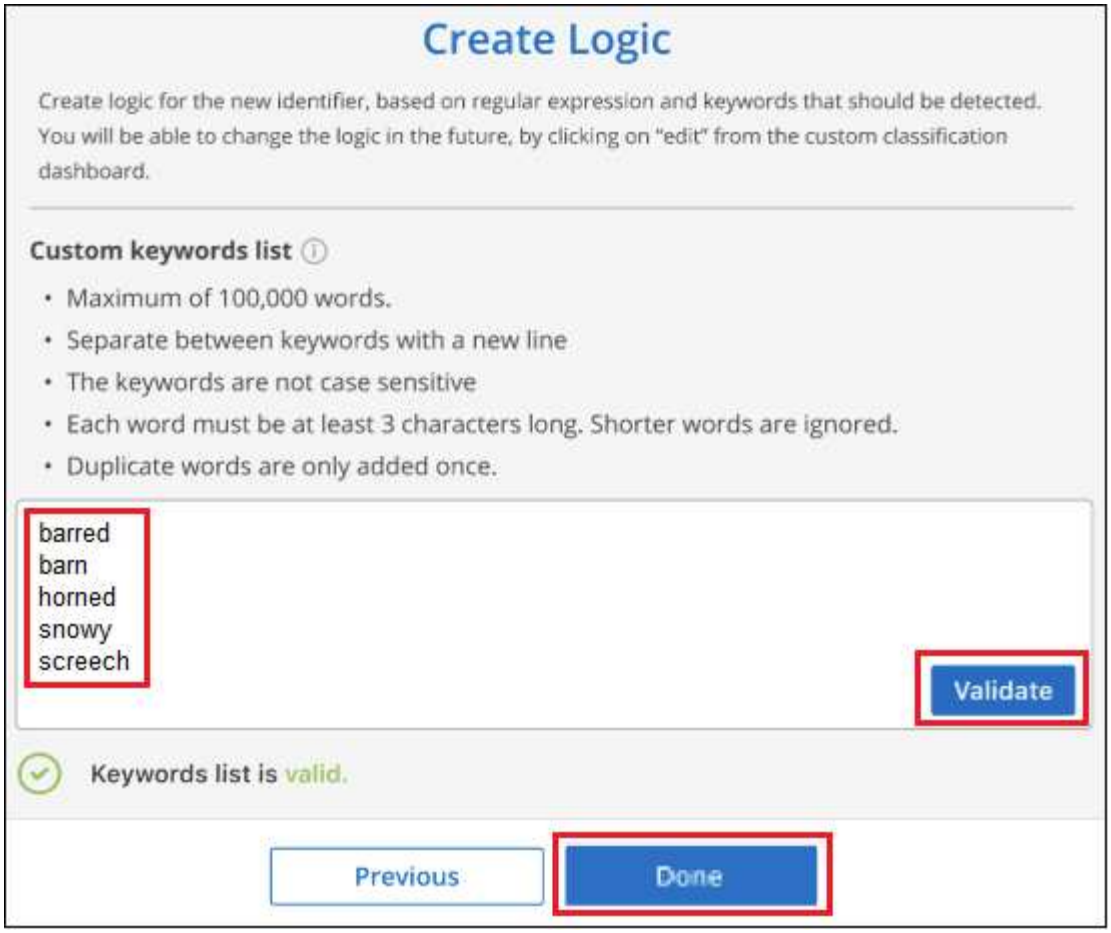


3. Wählen Sie auf der *Select Data Analysis Tool* -Seite **Custom Keywords** als Methode aus, mit der Sie den Klassifikator definieren möchten, und klicken Sie dann auf **Next**.



4. Geben Sie auf der Seite *Create Logic* die Schlüsselwörter ein, die Sie erkennen möchten - jedes Wort in einer separaten Zeile - und klicken Sie auf **Validate**.

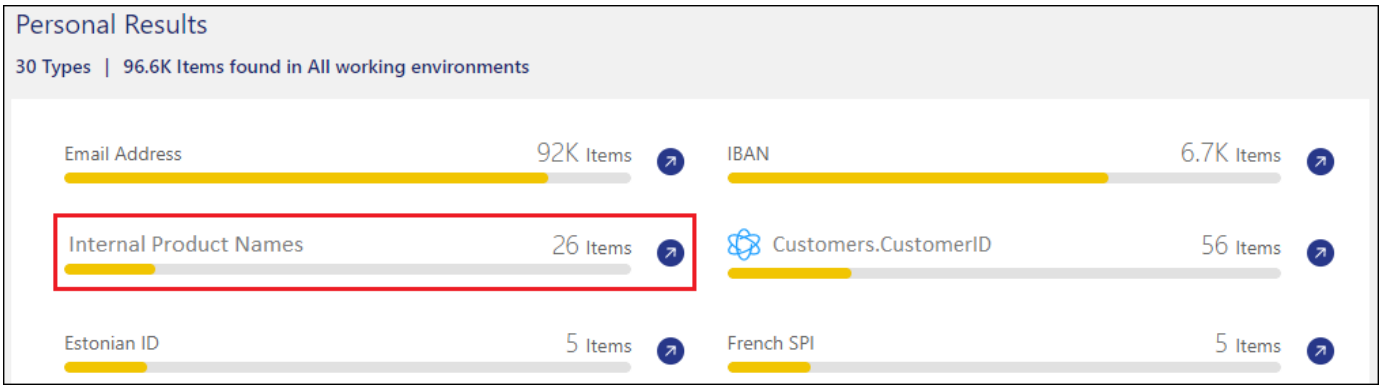
   Die Abbildung unten zeigt interne Produktnamen (verschiedene Arten von Eulen). Bei der BlueXP Klassifizierungssuche für diese Elemente wird die Groß-/Kleinschreibung nicht berücksichtigt.



5. Klicken Sie auf **done** und die BlueXP Klassifizierung beginnt mit der erneuten Überprüfung Ihrer Daten.

Ergebnisse

Nach Abschluss des Scans werden diese neuen Informationen im Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Seite „Untersuchung“ im Filter „Persönliche Daten“ angezeigt.



Wie Sie sehen, wird der Name des Klassifikators als Name im Fenster „Persönliche Ergebnisse“ verwendet. Auf diese Weise können Sie viele verschiedene Gruppen von Schlüsselwörtern aktivieren und die Ergebnisse für jede Gruppe anzeigen.

Fügen Sie mithilfe eines Regex benutzerdefinierte Kennungen für persönliche Daten hinzu

Mit einem benutzerdefinierten regulären Ausdruck (regex) können Sie ein persönliches Muster hinzufügen, um bestimmte Informationen in Ihren Daten zu identifizieren. Auf diese Weise können Sie ein neues benutzerdefiniertes Regex erstellen, um neue persönliche Informationselemente zu identifizieren, die noch nicht im System vorhanden sind. Der regex wird zu den vorhandenen vordefinierten Mustern hinzugefügt, die die BlueXP-Klassifizierung bereits verwendet, und die Ergebnisse werden im Abschnitt „Persönliche Muster“ angezeigt.

Sie können beispielsweise sehen, wo Ihre internen Produkt-IDs in allen Dateien erwähnt werden. Wenn die Produkt-ID z. B. eine klare Struktur hat, ist es eine 12-stellige Nummer, die mit 201 beginnt, können Sie die benutzerdefinierte regex-Funktion verwenden, um sie in Ihren Dateien zu suchen. Der reguläre Ausdruck für dieses Beispiel lautet **\b201\d{9}\b**.

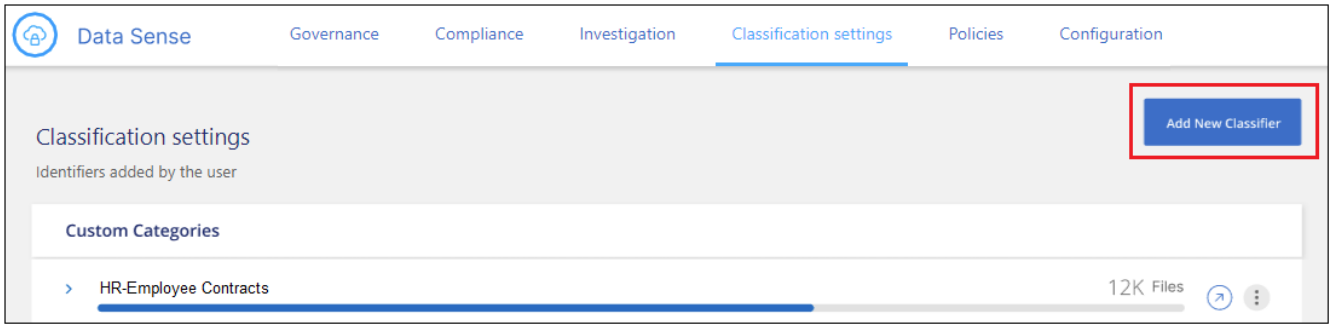
Nach Hinzufügen des regex wird die BlueXP Klassifizierung neu gestartet und scannt alle Datenquellen. Nach Abschluss des Scans werden die neuen Ergebnisse im BlueXP Classification Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Untersuchungsseite im Filter „Persönliche Daten“ angezeigt.

Wenn Sie beim Erstellen des regulären Ausdrucks Hilfe benötigen, lesen Sie "Reguläre Ausdrücke 101". Wählen Sie **Python** für den Geschmack, um zu sehen, welche Arten von Ergebnissen die BlueXP-Klassifikation vom regulären Ausdruck entspricht. Der "Seite „Python Regex Tester“" Ist auch nützlich, indem Sie eine grafische Darstellung Ihrer Muster anzeigen.

> Derzeit erlauben wir die Verwendung von Pattern Flags beim Erstellen eines Regex nicht - das bedeutet, dass Sie "/" nicht verwenden sollten.

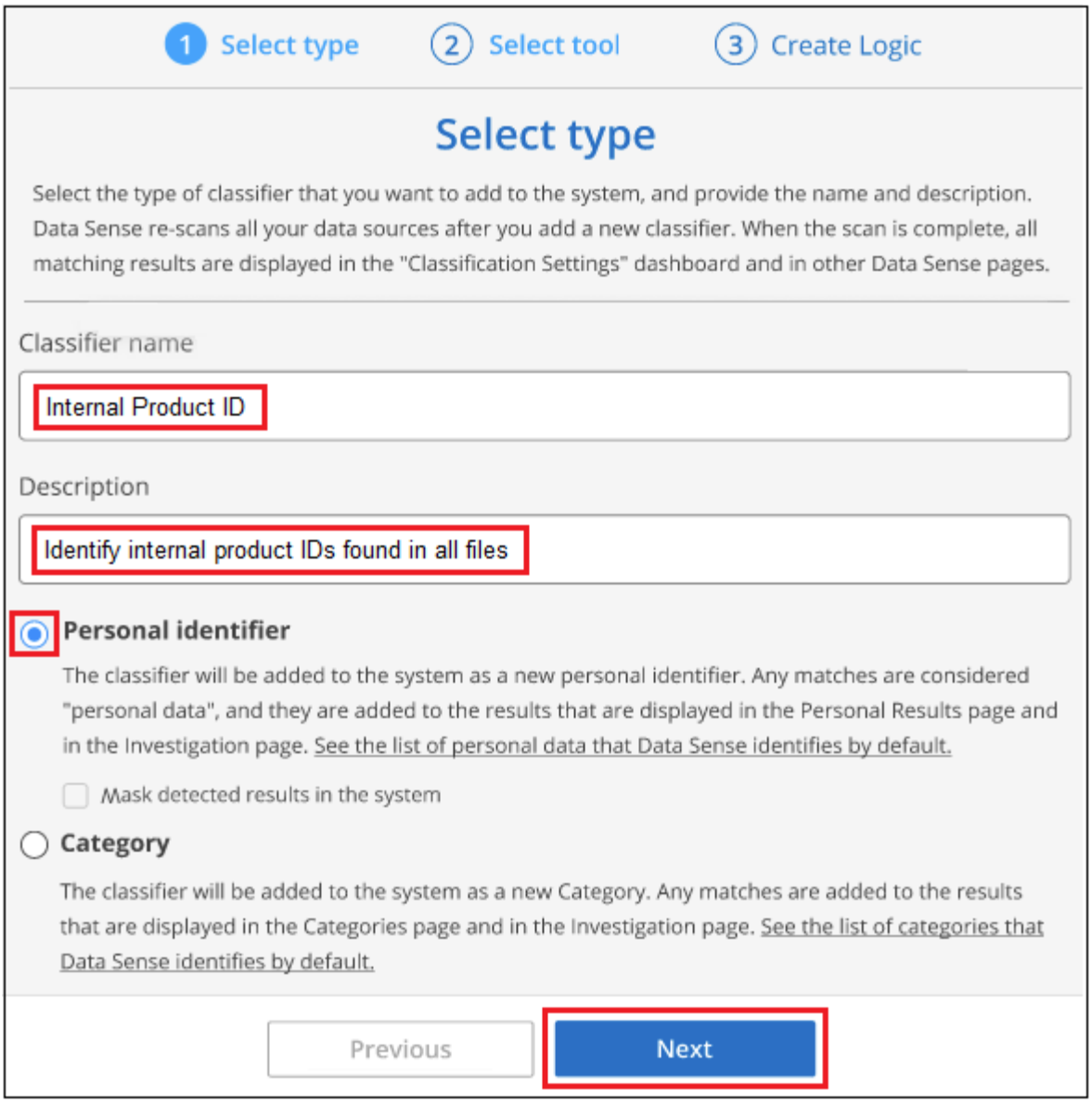
Schritte

1. Klicken Sie auf der Registerkarte *Classification settings* auf **Add New Classifier**, um den Assistenten *Add Custom Classifier* zu starten.

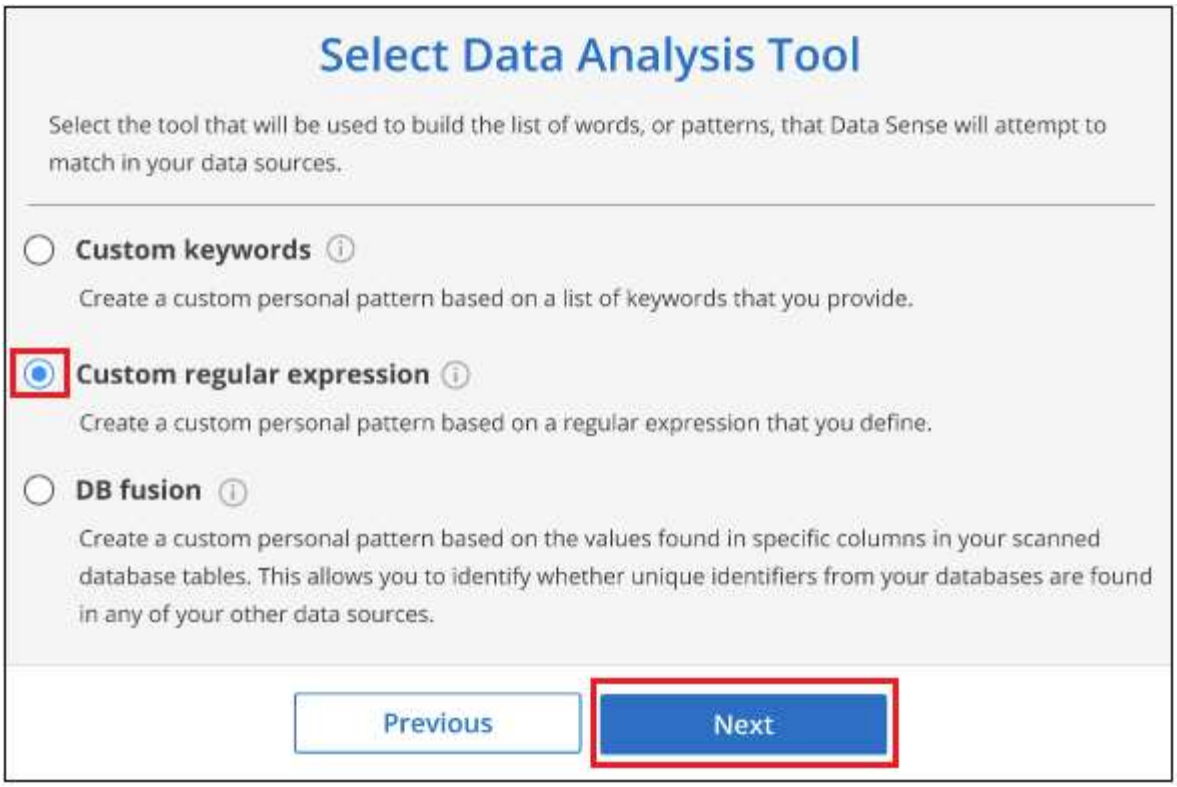


2. Geben Sie auf der Seite *Typ auswählen* den Namen des Klassifikators ein, geben Sie eine kurze Beschreibung ein, wählen Sie **Persönliche Kennung** aus und klicken Sie dann auf **Weiter**.

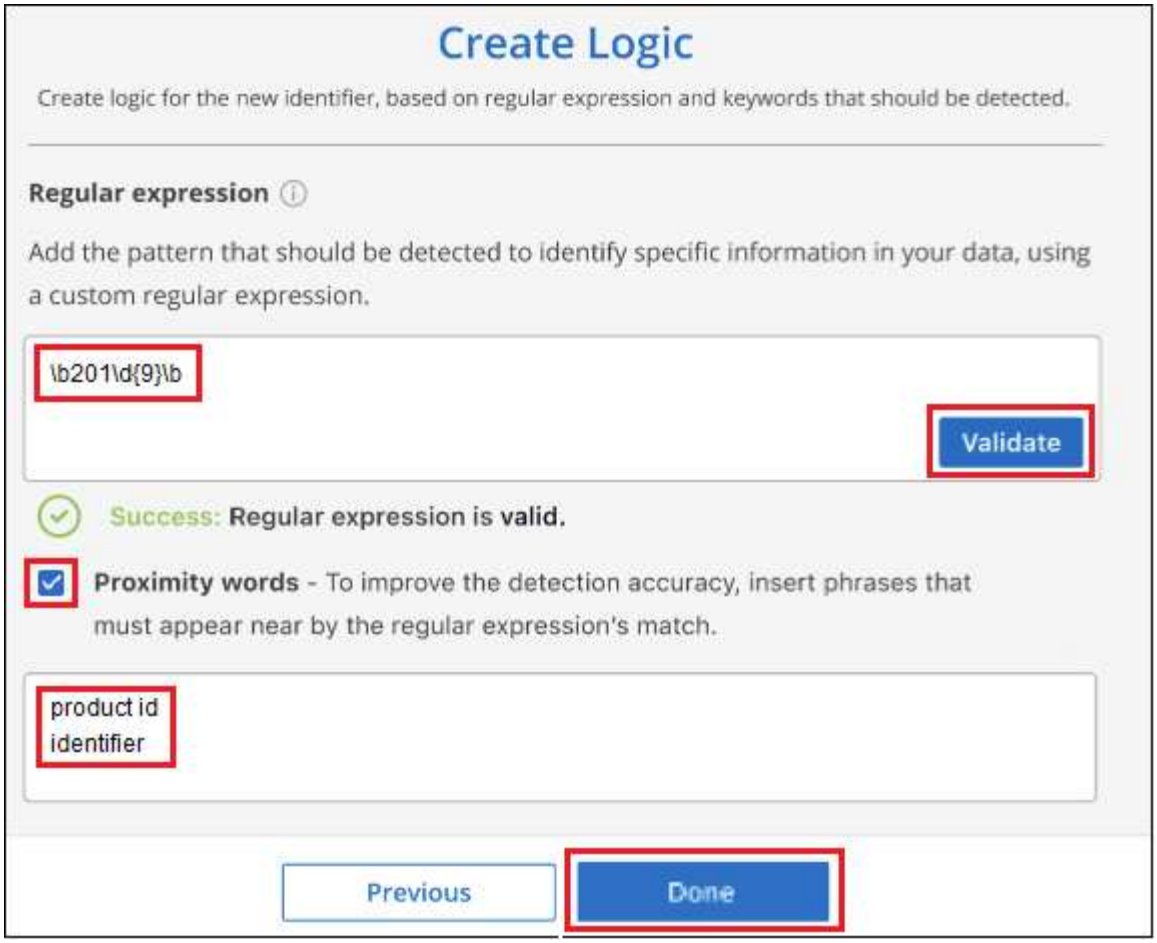
   Der eingegebene Name wird in der BlueXP-Klassifizierungs-UI als Überschrift für gescannte Dateien angezeigt, die den Anforderungen des Klassifikators entsprechen, und als Name des Filters auf der Seite Untersuchung. Sie können das Kontrollkästchen auch aktivieren, um „erkannte Ergebnisse im System maskieren“ zu aktivieren, damit das vollständige Ergebnis nicht in der Benutzeroberfläche angezeigt wird. Sie können dies beispielsweise tun, um vollständige Kreditkartennummern oder ähnliche persönliche Daten zu verbergen.



3. Wählen Sie auf der Seite Datenanalyse-Tool_ **Benutzerdefinierter regulärer Ausdruck** als Methode, mit der Sie den Klassifikator definieren möchten, und klicken Sie dann auf **Weiter**.

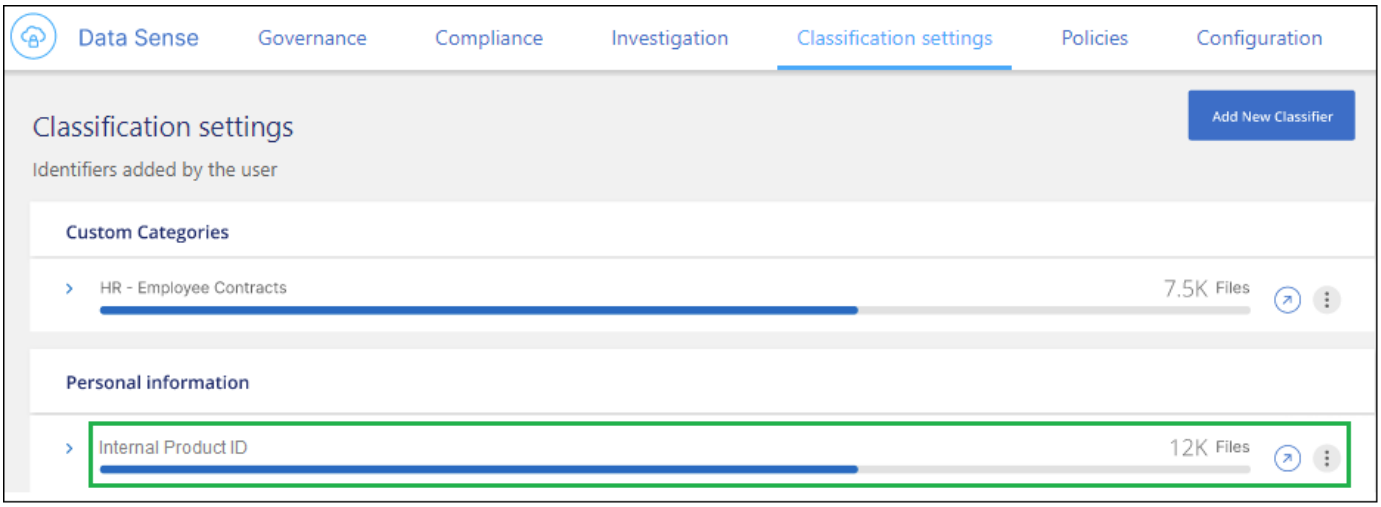


4. Geben Sie auf der Seite *Create Logic* den regulären Ausdruck und beliebige Annäherungswörter ein, und klicken Sie auf **Fertig**.
   a. Sie können jeden beliebigen regulären Ausdruck eingeben. Klicken Sie auf die Schaltfläche **Validieren**, um die BlueXP-Klassifizierung zu überprüfen, ob der reguläre Ausdruck gültig ist und nicht zu breit ist — das bedeutet, dass zu viele Ergebnisse zurückgegeben werden.
   b. Optional können Sie einige Annäherungsworte eingeben, um die Genauigkeit der Ergebnisse zu verbessern. Das sind Wörter, die in der Regel innerhalb von 300 Zeichen des Musters gefunden werden, nach dem Sie suchen (entweder vor oder nach dem gefundenen Muster). Geben Sie jedes Wort oder jede Phrase in eine separate Zeile ein.



Ergebnisse

Der Klassifikator wird hinzugefügt, und die BlueXP Klassifizierung beginnt, alle Datenquellen erneut zu scannen. Sie gelangen zurück zur Seite Benutzerdefinierte Klassifizierungsmerkmale, auf der Sie die Anzahl der Dateien anzeigen können, die Ihrem neuen Klassifikator entsprechen. Die Ergebnisse aus dem Scannen aller Ihrer Datenquellen werden je nach Anzahl der zu scannenden Dateien einige Zeit in Anspruch nehmen.



Benutzerdefinierte Kategorien hinzufügen

Die BlueXP Klassifizierung unterteilt die gescannten Daten in unterschiedliche Kategorien. Kategorien sind Themenbereiche, die auf der künstlichen Intelligenz Analyse der Inhalte und Metadaten der einzelnen Dateien

basieren. "Sehen Sie sich die Liste der vordefinierten Kategorien an".

Kategorien können Ihnen dabei helfen zu verstehen, was mit Ihren Daten passiert, indem Sie die Arten von Informationen anzeigen, die Sie haben. Beispielsweise kann eine Kategorie wie *Lebensläufe* oder *Mitarbeiterverträge* sensible Daten enthalten. Wenn Sie die Ergebnisse untersuchen, können Sie feststellen, dass Mitarbeiterverträge an einem unsicheren Ort gespeichert sind. Sie können das Problem dann beheben.

Sie können der BlueXP Klassifizierung benutzerdefinierte Kategorien hinzufügen, damit Sie erkennen können, in welchen Kategorien von Informationen Sie Ihre Daten finden, die speziell für Ihren Datenbestand sind. Jede Kategorie fügen Sie hinzu, indem Sie „Trainingsdateien“ erstellen, die die Datenkategorien enthalten, die Sie identifizieren möchten. Anschließend lässt die BlueXP Klassifizierung diese Dateien scannen, um sie über KI zu „lernen“, damit die Daten in Ihren Datenquellen identifiziert werden können. Die Kategorien werden zu den vorhandenen vordefinierten Kategorien hinzugefügt, die durch die BlueXP Klassifizierung bereits identifiziert werden. Die Ergebnisse sind im Abschnitt „Kategorien“ sichtbar.

Sie können beispielsweise sehen, wo sich komprimierte Installationsdateien im .gz-Format in Ihren Dateien befinden, damit Sie sie bei Bedarf entfernen können.

Nach der Aktualisierung der benutzerdefinierten Kategorien wird die BlueXP Klassifizierung alle Datenquellen neu gescannt. Nach Abschluss des Scans werden die neuen Ergebnisse im BlueXP Klassifizierungs-Compliance-Dashboard im Abschnitt „Kategorien“ und auf der Untersuchungsseite im Filter „Kategorie“ angezeigt. "Lesen Sie, wie Sie Dateien nach Kategorien anzeigen".

Was Sie benötigen

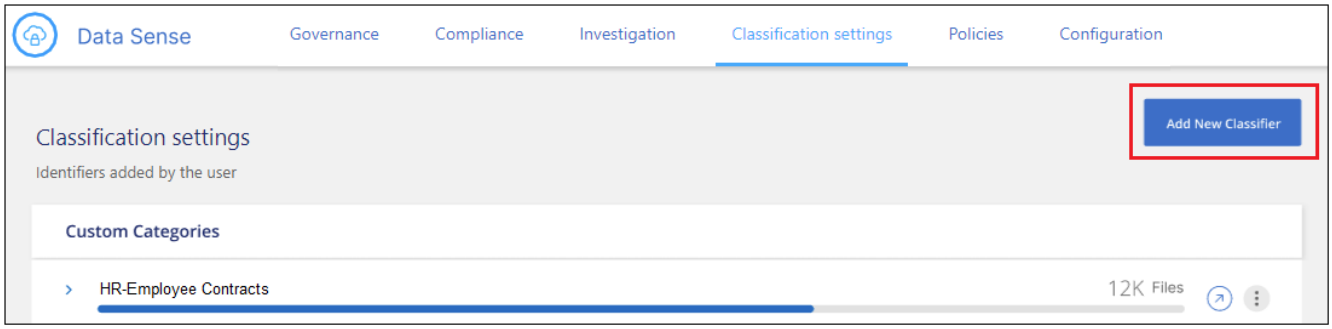
Sie müssen mindestens 25 Trainingsdateien erstellen, die Beispiele für die Datenkategorien enthalten, die von der BlueXP Klassifizierung erkannt werden sollen. Die folgenden Dateitypen werden unterstützt:

```
.CSV, .DOC, .DOCX, .GZ, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs,
Sheets, and Slides
```

Die Dateien müssen mindestens 100 Byte groß sein und sich in einem Ordner befinden, auf den BlueXP Zugriff bietet.

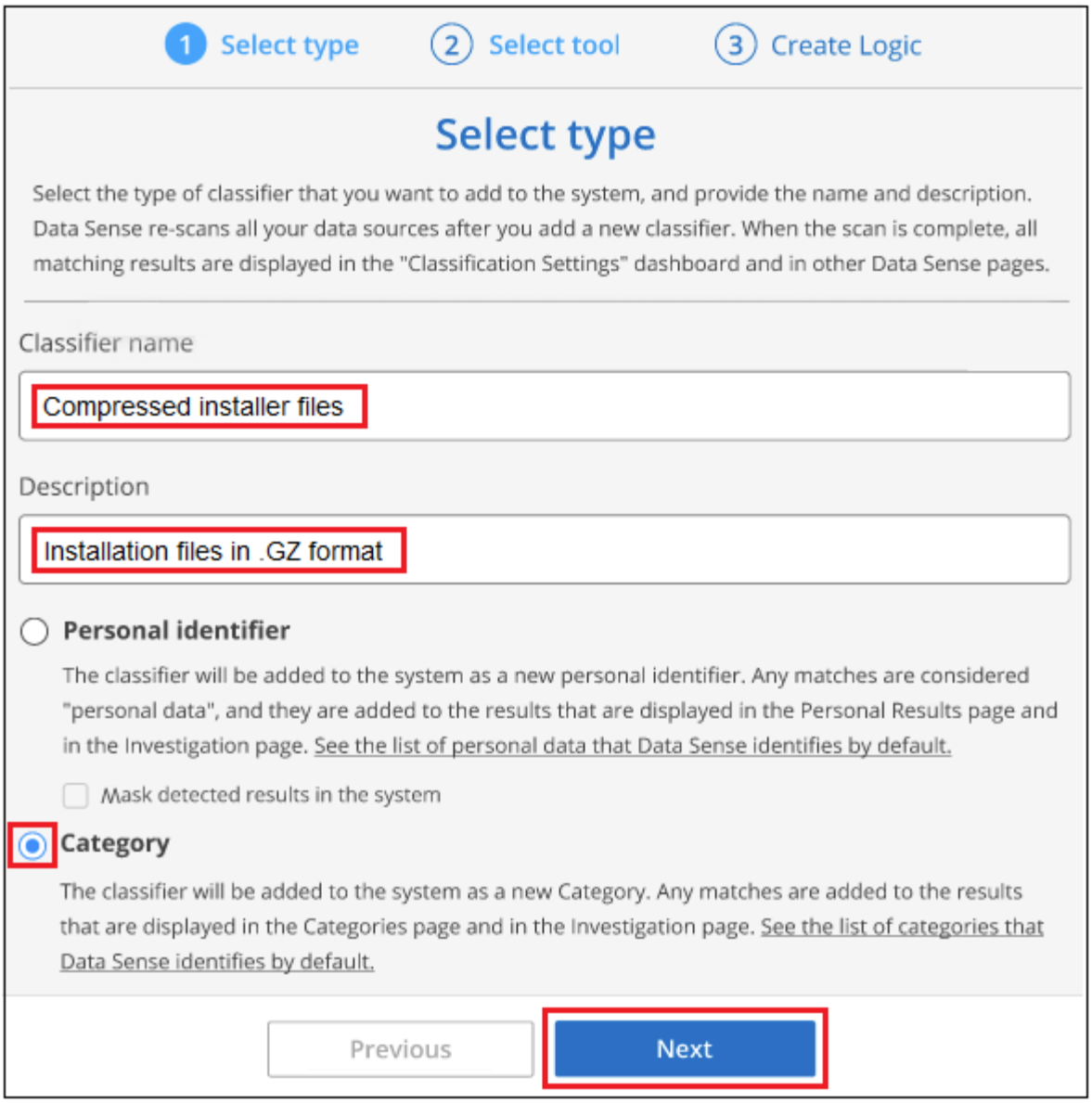
Schritte

1. Klicken Sie auf der Registerkarte *Classification settings* auf **Add New Classifier**, um den Assistenten *Add Custom Classifier* zu starten.

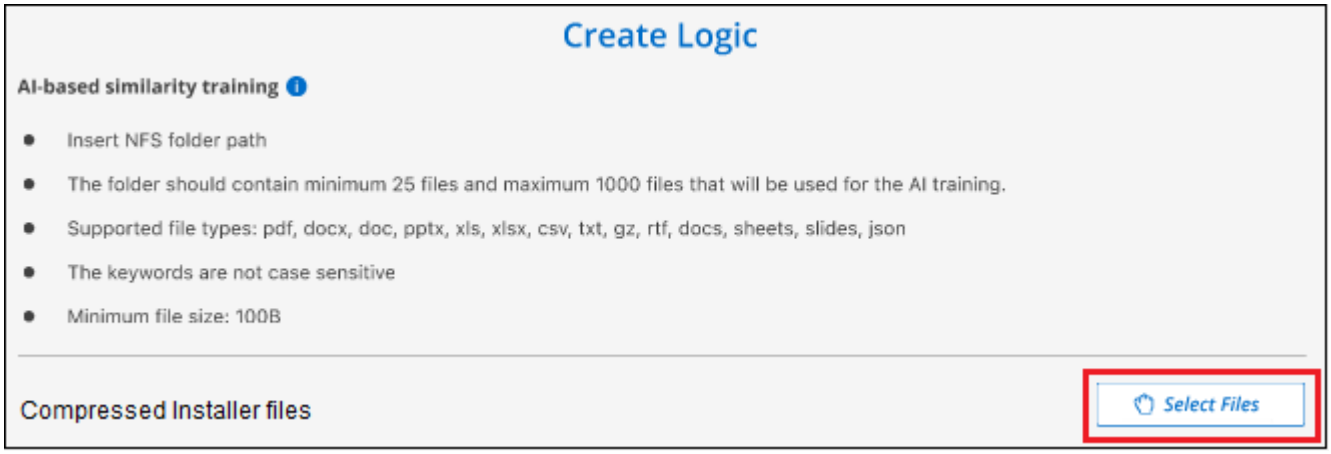


2. Geben Sie auf der Seite *Select type* den Namen des Klassifikators ein, geben Sie eine kurze Beschreibung ein, wählen Sie **Category** aus und klicken Sie dann auf **Next**.

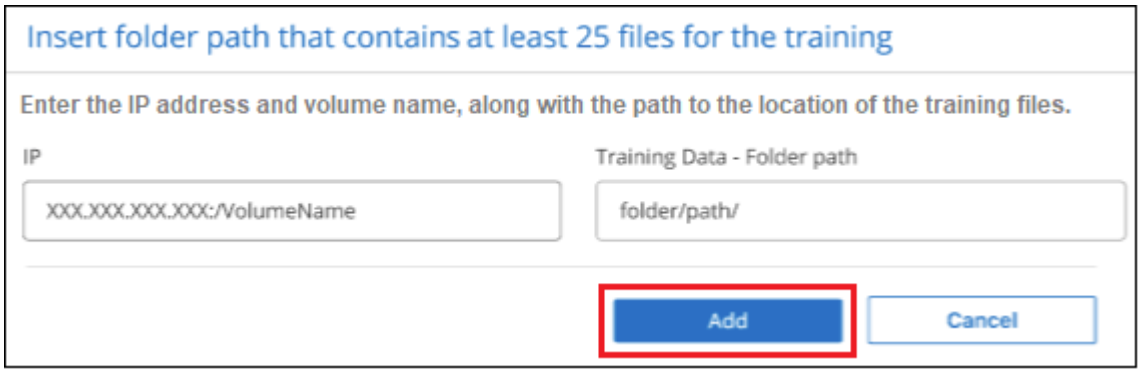
   Der eingegebene Name wird in der BlueXP Klassifizierungs-UI als Überschrift für gescannte Dateien angezeigt, die der von Ihnen definierten Datenkategorie entsprechen, und als Name des Filters auf der Seite Untersuchung.



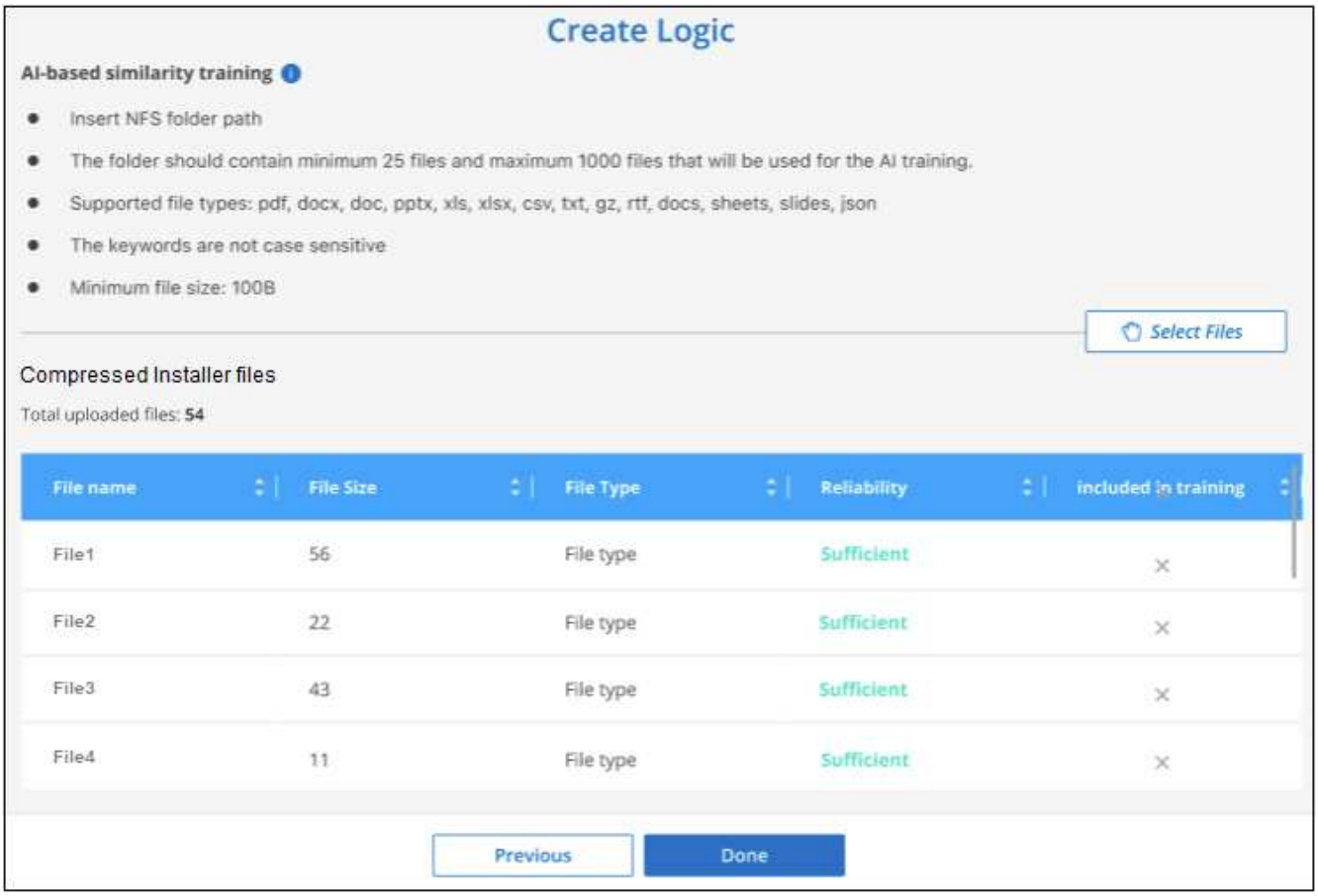
3. Stellen Sie auf der Seite *Create Logic* sicher, dass Sie die Lerndateien vorbereitet haben, und klicken Sie dann auf **Select files**.



4. Geben Sie die IP-Adresse des Volumes und den Pfad ein, in dem sich die Trainingsdateien befinden, und klicken Sie auf **Hinzufügen**.



5. Überprüfen Sie, ob die Trainingsdateien von der BlueXP Klassifizierung erkannt wurden. Klicken Sie auf **x**, um alle Trainingsdateien zu entfernen, die nicht den Anforderungen entsprechen. Klicken Sie dann auf **Fertig**.

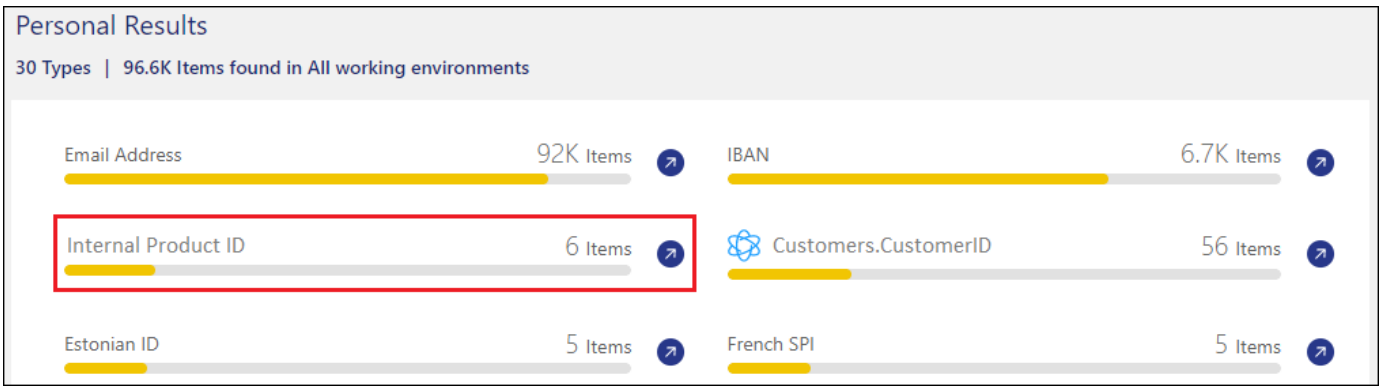


Ergebnisse

Die neue Kategorie wird gemäß den Trainingsdateien erstellt und der BlueXP Klassifizierung hinzugefügt. Die BlueXP Klassifizierung beginnt dann, alle Datenquellen neu zu scannen, um Dateien zu identifizieren, die in diese neue Kategorie passen. Sie kehren zur Seite Benutzerdefinierte Klassifikatoren zurück, auf der Sie die Anzahl der Dateien anzeigen können, die Ihrer neuen Kategorie entsprechen. Die Ergebnisse aus dem Scannen aller Ihrer Datenquellen werden je nach Anzahl der zu scannenden Dateien einige Zeit in Anspruch nehmen.

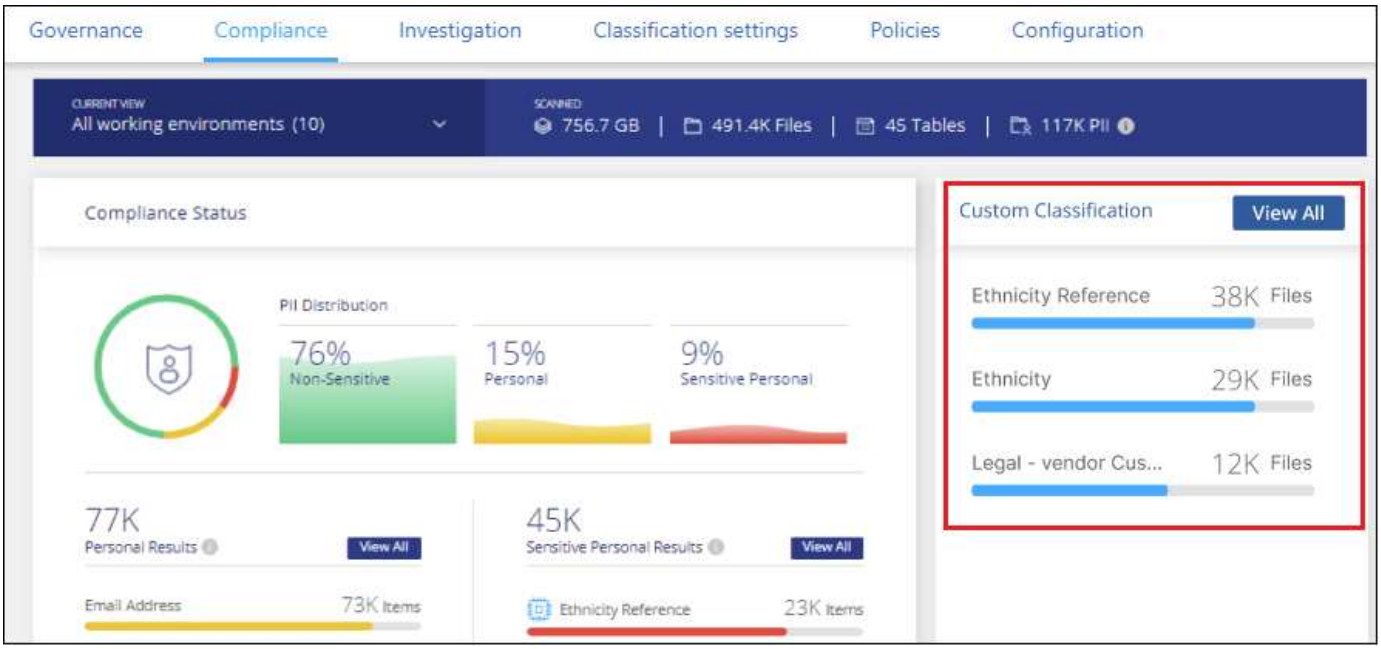
Ergebnisse von Ihren benutzerdefinierten Klassifikatoren anzeigen

Sie können die Ergebnisse von einem Ihrer benutzerdefinierten Klassifikatoren im Compliance Dashboard und auf der Untersuchungsseite anzeigen. In diesem Screenshot werden beispielsweise die übereinstimmenden Informationen im Compliance-Dashboard im Abschnitt „Persönliche Ergebnisse“ angezeigt.



Klicken Sie auf das Um die detaillierten Ergebnisse auf der Untersuchungsseite anzuzeigen.

Darüber hinaus werden alle benutzerdefinierten Klassifikatorergebnisse auf der Registerkarte Benutzerdefinierte Klassifikatoren angezeigt, und die oberen 6 benutzerdefinierten Klassifikatorergebnisse werden wie unten gezeigt im Compliance Dashboard angezeigt.



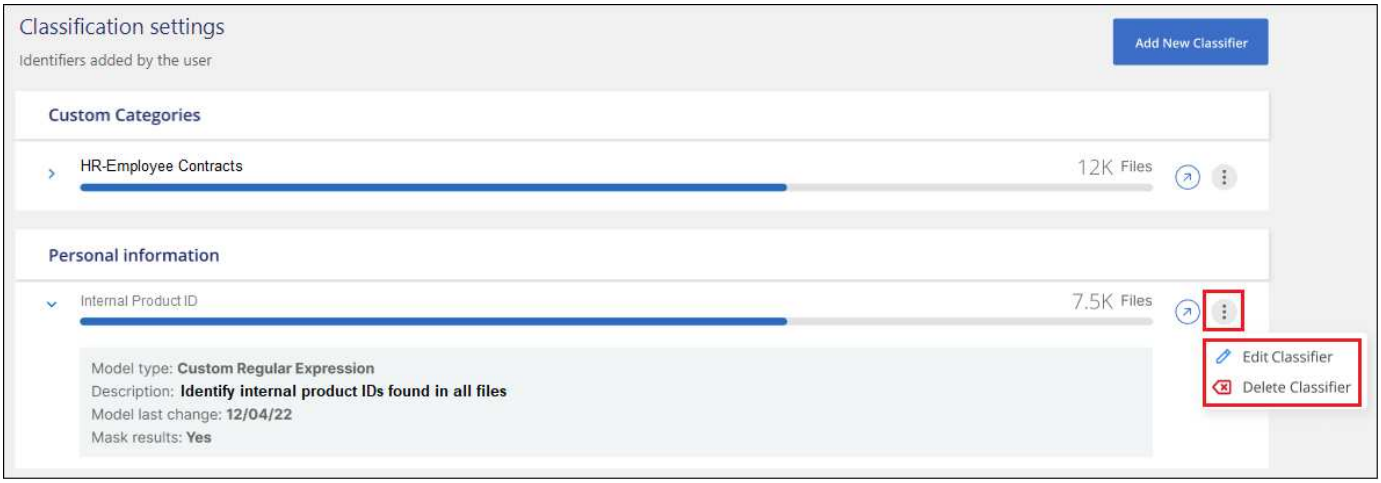
Benutzerdefinierte Klassifikatoren verwalten

Sie können alle benutzerdefinierten Klassifikatoren ändern, die Sie mit der Schaltfläche **Klassifikator bearbeiten** erstellt haben.

Sie können derzeit keine Data Fusion-Klassifikatoren bearbeiten.

Und wenn Sie zu einem späteren Zeitpunkt entscheiden, dass Sie keine BlueXP-Klassifizierung benötigen, um die von Ihnen hinzugefügten benutzerdefinierten Muster zu identifizieren, können Sie die Schaltfläche

Klassifikator löschen verwenden, um jedes Element zu entfernen.



Ausschließen bestimmter Verzeichnisse von den Klassifikationsscans von BlueXP

Wenn die BlueXP Klassifizierung Scandaten in bestimmten Datenquellen-Verzeichnissen ausschließen soll, können Sie diese Verzeichnisnamen zu einer Konfigurationsdatei hinzufügen. Nachdem Sie diese Änderung angewendet haben, schließt die BlueXP Klassifizierungs-Engine Scandaten in diesen Verzeichnissen aus.

Beachten Sie, dass die BlueXP Klassifizierung standardmäßig so konfiguriert ist, dass die Scan-Volume-Snapshot-Daten ausgeschlossen werden, da dieser Inhalt mit dem Inhalt des Volumes identisch ist.

Diese Funktion ist ab Version 1.29 der BlueXP Klassifizierung verfügbar (ab März 2024).

Unterstützte Datenquellen

Der Ausschluss bestimmter Verzeichnisse aus der BlueXP Klassifizierungs-Scans wird für NFS- und CIFS-Freigaben in den folgenden Datenquellen unterstützt:

- On-Premises-ONTAP
- Cloud Volumes ONTAP
- Amazon FSX für NetApp ONTAP
- Azure NetApp Dateien
- Allgemeine Dateifreigaben

Definieren Sie die Verzeichnisse, die vom Scannen ausgeschlossen werden sollen

Bevor Sie Verzeichnisse von der Klassifizierungsüberprüfung ausschließen können, müssen Sie sich beim BlueXP Klassifizierungssystem anmelden, damit Sie eine Konfigurationsdatei bearbeiten und ein Skript ausführen können. Informieren Sie sich darüber "Melden Sie sich beim BlueXP Klassifizierungssystem an" Je nachdem, ob Sie die Software manuell auf einem Linux-Rechner installiert haben oder ob Sie die Instanz in der Cloud bereitgestellt haben.

- Pro BlueXP Klassifizierungssystem können Sie maximal 50 Verzeichnispfade ausschließen.
- Das Ausschließen von Verzeichnispfaden kann sich auf die Scanzeiten auswirken.

Schritte

1. Öffnen Sie auf dem BlueXP Klassifizierungssystem die Datei unter „/opt/netapp/config/Custom_Configuration“ `data_provider.yaml`.
2. Geben Sie im Bereich „Data_Providers“ unter der Zeile „exclude:“ die auszuschließenden Verzeichnispfade ein. Beispiel:

   ```
   exclude:
   - "folder1"
   - "folder2"
   ```

   Ändern Sie nichts anderes in dieser Datei.

3. Speichern Sie die Änderungen in der Datei.
4. Gehen Sie zu „/opt/netapp/Datense/Tools/Customer_Configuration/Data_Providers“ und führen Sie das folgende Skript aus:

   ```
   update_data_providers_from_config_file.sh
   ```

   Mit diesem Befehl werden die Verzeichnisse, die vom Scannen ausgeschlossen werden sollen, an die Klassifizierungs-Engine übergeben.

Ergebnis

Alle nachfolgenden Scans Ihrer Daten schließen das Scannen dieser angegebenen Verzeichnisse aus.

Mit den gleichen Schritten können Sie Elemente aus der Ausschlussliste hinzufügen, bearbeiten oder löschen. Die überarbeitete Ausschlussliste wird aktualisiert, nachdem Sie das Skript ausgeführt haben, um Ihre Änderungen zu übernehmen.

Beispiele

Konfiguration 1:

Jeder Ordner, der an einer beliebigen Stelle im Namen „folder1“ enthält, wird von allen Datenquellen ausgeschlossen.

```
data_providers:
   exclude:
   - "folder1"
```

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO1/folder1
- /CVO1/folder1Name

- /CVO1/folder10
- /CVO1/*folder1
- /CVO1/+folder1Name
- /CVO1/notfolder10
- /CVO22/folder1
- /CVO22/folder1Name
- /CVO22/folder10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO1/*Ordner
- /CVO1/Ordnername
- /CVO22/*folder20

Konfiguration 2:

Jeder Ordner, der "*folder1" nur am Anfang des Namens enthält, wird ausgeschlossen.

```
data_providers:
   exclude:
   - "\\*folder1"
```

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO/*folder1
- /CVO/*folder1Name
- /CVO/*folder10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO/folder1
- /CVO/folder1Name
- /CVO/Not*folder10

Konfiguration 3:

Jeder Ordner in der Datenquelle „CVO22“, der „folder1“ irgendwo im Namen enthält, wird ausgeschlossen.

```
data_providers:
   exclude:
   - "CVO22/folder1"
```

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO22/folder1
- /CVO22/folder1Name
- /CVO22/folder10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO1/folder1
- /CVO1/folder1Name
- /CVO1/folder10

Sonderzeichen in Ordnernamen werden entfernt

Wenn Sie einen Ordnernamen haben, der eines der folgenden Sonderzeichen enthält und Sie Daten in diesem Ordner vom Scannen ausschließen möchten, müssen Sie die Escape-Sequenz \\ vor dem Ordnernamen verwenden.

```
 ., +, *, ?, ^, $, (, ), [, ], {, }, |
Beispiel:
```

Pfad in Quelle: `/project/*not_to_scan`

Syntax in Ausschlussdatei: `"\\*not_to_scan"`

Aktuelle Ausschlussliste anzeigen

Es ist möglich für den Inhalt des `data_provider.yaml` Die Konfigurationsdatei muss sich von der Datei unterscheiden, die nach dem Ausführen des festgelegt wurde `update_data_providers_from_config_file.sh` Skript: Um die aktuelle Liste der Verzeichnisse anzuzeigen, die Sie nicht beim Klassifizierungs-Scan von BlueXP berücksichtigt haben, führen Sie den folgenden Befehl von „/opt/netapp/Datense/Tools/Customer_Configuration/Data_Providers“ aus:

```
get_data_providers_configuration.sh
```

Anzeigen des Status Ihrer Compliance-Aktionen

Wenn Sie eine asynchrone Aktion aus dem Bereich Untersuchungsergebnisse über viele Dateien ausführen, z. B. das Verschieben oder Löschen von 100 Dateien, kann der Prozess einige Zeit in Anspruch nehmen. Sie können den Status dieser Aktionen im Fenster „*Action Status* “ überwachen, sodass Sie wissen, wann sie auf alle Dateien angewendet wurde.

Auf diese Weise können Sie die Aktionen sehen, die erfolgreich abgeschlossen wurden, die derzeit in Bearbeitung sind und die, die nicht erfolgreich waren, damit Sie Probleme diagnostizieren und beheben können. Beachten Sie, dass kurze Vorgänge, die schnell abgeschlossen werden, z. B. das Verschieben einer einzelnen Datei, nicht im Bereich Aktionsstatus angezeigt werden.

Der Status kann lauten:

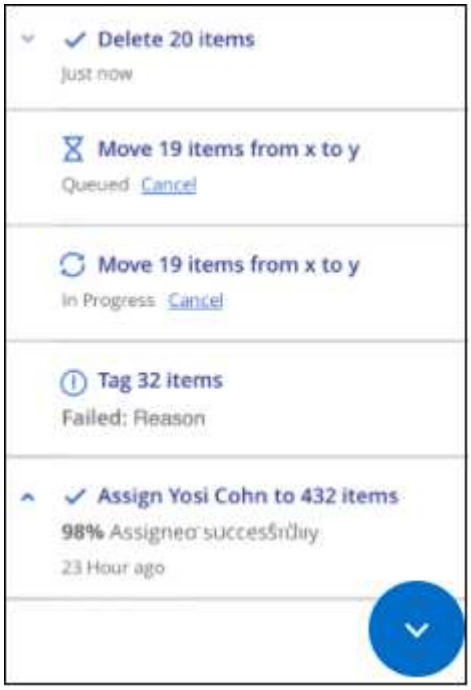
- Erfolg – Eine BlueXP Klassifizierungsaktion wurde abgeschlossen und alle Elemente erfolgreich abgeschlossen.
- Teilweiser Erfolg: Eine BlueXP-Klassifizierungsaktion ist abgeschlossen, einige Elemente sind fehlgeschlagen, einige erfolgreich.

- In Bearbeitung – die Aktion läuft noch.
- Warteschlange: Die Aktion wurde nicht gestartet.
- Storniert: Die Aktion wurde abgebrochen.
- Fehlgeschlagen - die Aktion ist fehlgeschlagen.

Beachten Sie, dass Sie alle Aktionen mit dem Status „in Bearbeitung“ oder „in Bearbeitung“ abbrechen können.

Schritte

1. Rechts unten auf der BlueXP-Klassifikations-UI sehen Sie die Schaltfläche **Actions Status** .
2. Klicken Sie auf diese Schaltfläche, und die letzten 20 Aktionen werden aufgelistet.



Sie können auf den Namen einer Aktion klicken, um die entsprechenden Details anzuzeigen.

Definieren Sie zusätzliche Gruppen-IDs als für die Organisation offen

Wenn Gruppen-IDs (GIDs) an Dateien oder Ordner in NFS-Dateifreigaben angehängt werden, definieren sie die Berechtigungen für die Datei oder den Ordner, z. B. ob sie „für die Organisation offen“ sind. Wenn einige Gruppen-IDs (GIDs) zunächst nicht mit der Berechtigungsebene „für Organisation öffnen“ eingerichtet wurden, können Sie diese Berechtigung zur GID hinzufügen, sodass alle Dateien und Ordner, die mit dieser GID verknüpft sind, als „für die Organisation offen“ gelten.

Nachdem Sie diese Änderung vorgenommen und die BlueXP-Klassifizierung Ihre Dateien und Ordner erneut scannt, werden alle Dateien und Ordner, denen diese Gruppen-IDs angehängt sind, auf der Seite

„Ermittlungsdetails“ diese Berechtigung angezeigt. Sie werden auch in Berichten angezeigt, in denen Sie Dateiberechtigungen anzeigen.

Um diese Funktion zu aktivieren, müssen Sie sich beim BlueXP Klassifizierungssystem anmelden, damit Sie eine Konfigurationsdatei bearbeiten und ein Skript ausführen können. Informieren Sie sich darüber "Melden Sie sich beim BlueXP Klassifizierungssystem an" Je nachdem, ob Sie die Software manuell auf einem Linux-Rechner installiert haben oder ob Sie die Instanz in der Cloud bereitgestellt haben.

Fügen Sie den Gruppen-IDs die Berechtigung „für Organisation öffnen“ hinzu

Sie müssen die Gruppen-ID-Nummern (GIDs) haben, bevor Sie diese Aufgabe starten.

Schritte

1. Öffnen Sie auf dem BlueXP Klassifizierungssystem die Datei unter „/opt/netapp/config/Custom_Configuration“ `data_provider.yaml`.
2. Fügen Sie in der Zeile "Organisation_Group_ids: []" die Gruppen-IDs hinzu. Beispiel:

   ```
   organization_group_ids: [1014, 1015, 21, 2021, 1013, 2020, 1018, 1019]
   ```

   Ändern Sie nichts anderes in dieser Datei.

3. Speichern Sie die Änderungen in der Datei.
4. Gehen Sie zu „/opt/netapp/Datense/Tools/Customer_Configuration/Data_Providers“ und führen Sie das folgende Skript aus:

   ```
   update_data_providers_from_config_file.sh
   ```

   Mit diesem Befehl werden die überarbeiteten Gruppen-ID-Berechtigungen für die Klassifizierungs-Engine übertragen.

Ergebnis

Bei allen nachfolgenden Scans Ihrer Daten werden Dateien oder Ordner identifiziert, bei denen diese Gruppen-IDs als „für Unternehmen offen“ angehängt sind.

Mit den gleichen Schritten können Sie die Liste der Gruppen-IDs bearbeiten und alle Gruppen-IDs löschen, die Sie in der Vergangenheit hinzugefügt haben. Die überarbeitete Liste der Gruppen-IDs wird aktualisiert, nachdem Sie das Skript ausgeführt haben, um Ihre Änderungen zu übernehmen.

Die aktuelle Liste der Gruppen-IDs anzeigen

Es ist möglich für den Inhalt des `data_provider.yaml` Die Konfigurationsdatei muss sich von der Datei unterscheiden, die nach dem Ausführen des festgelegt wurde `update_data_providers_from_config_file.sh` Skript: Um die aktuelle Liste der Gruppen-IDs anzuzeigen, die Sie der BlueXP Klassifizierung hinzugefügt haben, führen Sie den folgenden Befehl von „/opt/netapp/Datense/Tools/Customer_Configuration/Data_Providers“ aus:

```
get_data_providers_configuration.sh
```

Audit der Historie der BlueXP Klassifizierungsaktionen

Die BlueXP Klassifizierungs-Logs managen-Aktivitäten, die an Dateien aus allen Arbeitsumgebungen und Datenquellen ausgeführt wurden, die von der BlueXP Klassifizierung gescannt werden. Die BlueXP Klassifizierung protokolliert auch die Aktivitäten, wenn Sie eine BlueXP Klassifizierungsinstanz implementieren.

Sie können den Inhalt der BlueXP Klassifizierungs-Audit-Protokolldateien anzeigen oder herunterladen, um festzustellen, welche Dateiänderungen wann vorgenommen wurden. Beispielsweise können Sie sehen, welche Anfrage erstellt wurde, wann die Anfrage gestellt wurde, und Details wie den Quellspeicherort für das Löschen einer Datei oder den Quell- und Zielstandort, falls eine Datei verschoben wurde.

Inhalt der Protokolldatei protokollieren

Jede Zeile im Auditprotokoll enthält Informationen in diesem Format:

```
<full date> | <status> | ds_audit_logger | <module> | 0 | 0 | File <full file
path> deleted from device <device path> - <result>
```

- Datum und Uhrzeit: Vollständiger Zeitstempel für das Ereignis
- Status - INFO, WARNUNG
- Aktionstyp (Löschen, Kopieren, Verschieben, Erstellen einer Richtlinie, Aktualisieren der Richtlinie, Dateien erneut scannen, JSON-Bericht herunterladen usw.)
- Dateiname (wenn die Aktion für eine Datei relevant ist)
- Details zur Aktion - was getan wurde: Hängt von der Aktion ab
  - Name der Richtlinie
  - Für Move - Quelle und Ziel
  - Für Copy - Quelle und Ziel
  - Für Tag - Tag-Name
  - Zum Zuweisen an - Benutzername
  - Für E-Mail Alert - E-Mail-Adresse / Konto

Beispielsweise zeigen die folgenden Zeilen aus der Protokolldatei einen erfolgreichen Kopiervorgang und einen fehlerhaften Kopiervorgang an.

```
2022-06-06 15:23:08,910 | INFO | ds_audit_logger | es_scanned_file | 237 |
49 | Copy file /CIFS_share/data/dop1/random_positives.tsv from device
10.31.133.183 (type: SMB_SHARE) to device 10.31.130.133:/export_reports
(NFS_SHARE) - SUCCESS
2022-06-06 15:23:08,968 | WARNING | ds_audit_logger | es_scanned_file |
239 | 153 | Copy file /CIFS_share/data/compliance-netapp.tar.gz from
device 10.31.133.183 (type: SMB_SHARE) to device
10.31.130.133:/export_reports (NFS_SHARE) - FAILURE
```

Speicherorte der Protokolldateien

Die Management-Audit-Log-Dateien befinden sich auf der BlueXP Klassifizierungs-Maschine in: `/opt/netapp/audit_logs/`

Die Audit-Protokolldateien für die Installation werden in geschrieben `/opt/netapp/install_logs/`

Jede Protokolldatei kann maximal 10 MB groß sein. Wenn dieser Grenzwert erreicht wird, wird eine neue Protokolldatei gestartet. Die Log-Dateien werden mit „DataSense_Audit.log“, „DataSense_Audit.log.1“, „DataSense_Audit.log.2“ und so weiter benannt. Es werden maximal 100 Protokolldateien im System gespeichert. Ältere Protokolldateien werden automatisch gelöscht, sobald die maximale Anzahl erreicht wurde.

Greifen Sie auf die Protokolldateien zu

Sie müssen sich beim BlueXP Klassifizierungssystem anmelden, um auf die Protokolldateien zugreifen zu können. Informieren Sie sich darüber "Melden Sie sich beim BlueXP Klassifizierungssystem an" Je nachdem, ob Sie die Software manuell auf einem Linux-Rechner installiert haben oder ob Sie die Instanz in der Cloud bereitgestellt haben.

Reduzierung der Scan-Geschwindigkeit der BlueXP Klassifizierung

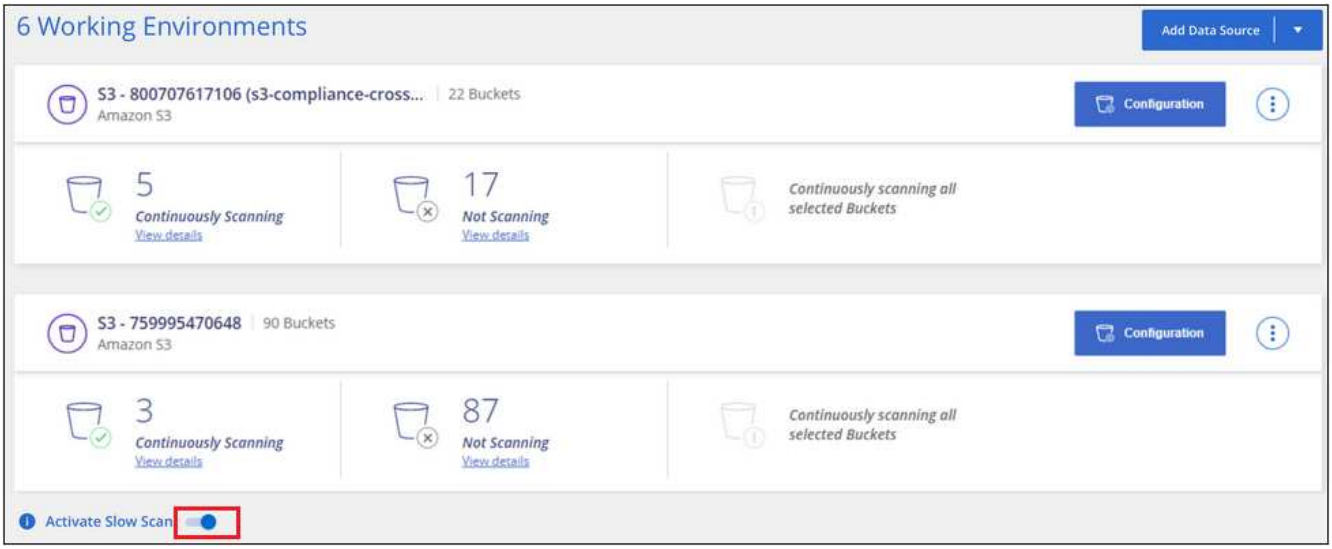
Datenscans haben keine nennenswerten Auswirkungen auf Ihre Storage-Systeme und Ihre Daten. Wenn Sie jedoch auch nur geringe Auswirkungen haben, können Sie die BlueXP-Klassifizierung für „langsame“ Scans konfigurieren.

Wenn diese Option aktiviert ist, wird langsames Scannen auf allen Datenquellen verwendet. Sie können den langsamen Scan nicht für eine einzige Arbeitsumgebung oder Datenquelle konfigurieren.

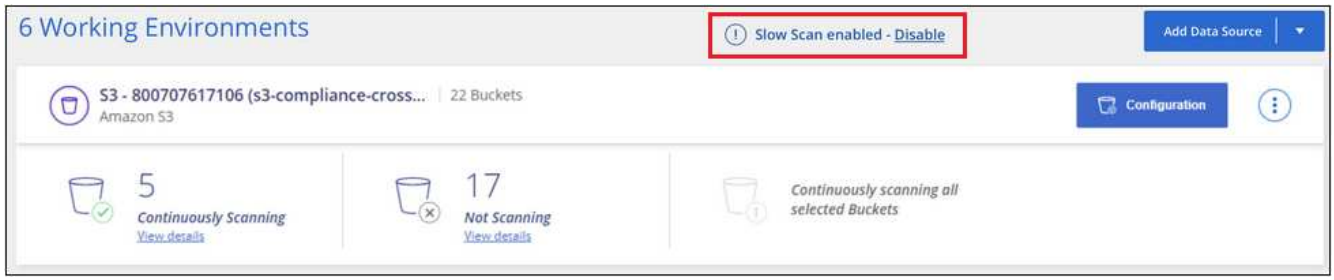
Die Scan-Geschwindigkeit kann beim Scannen von Datenbanken nicht verringert werden.

Schritte

1. Bewegen Sie den Schieberegler von unten auf der Seite *Configuration* nach rechts, um den langsamen Scan zu aktivieren.



Oben auf der Konfigurationsseite wird angezeigt, dass die langsame Messung aktiviert ist.



2. Sie können das langsame Scannen deaktivieren, indem Sie in dieser Meldung auf **Deaktivieren** klicken.

Entfernen von Datenquellen aus der BlueXP Klassifizierung

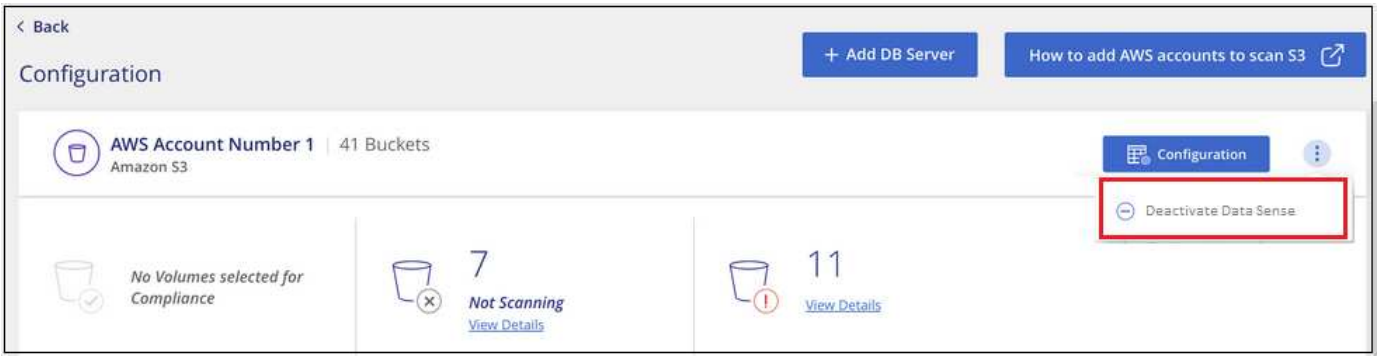
Falls erforderlich können Sie die BlueXP Klassifizierung dadurch beenden, dass sie eine oder mehrere Arbeitsumgebungen, Datenbanken, Dateifreigabegruppen, OneDrive-Konten, Google Drive-Konten scannt. Oder SharePoint-Konten.

Der Ladevorgang zum Scannen der Daten wird angehalten, wenn die Datenquelle entfernt wird.

Deaktivieren von Compliance-Scans für eine Arbeitsumgebung

Wenn Sie Scans deaktivieren, scannt die BlueXP Klassifizierung die Daten nicht mehr in der Arbeitsumgebung und entfernt die indizierten Compliance-Einblicke aus der BlueXP Klassifizierungsinstanz (die Daten aus der Arbeitsumgebung werden nicht gelöscht).

1. Klicken Sie auf der Seite *Configuration* auf ⋮ Klicken Sie in der Zeile für die Arbeitsumgebung auf **Data Sense deaktivieren**.



Sie können bei der Auswahl der Arbeitsumgebung auch die Compliance-Scans für eine Arbeitsumgebung im Fenster „Services“ deaktivieren.

Entfernen einer Datenbank aus der BlueXP Klassifizierung

Wenn Sie eine bestimmte Datenbank nicht mehr scannen möchten, können Sie sie aus der BlueXP Klassifizierungs-Schnittstelle löschen und alle Scans anhalten.

1. Klicken Sie auf der Seite *Configuration* auf ⋮ Klicken Sie in der Zeile der Datenbank auf **DB Server entfernen**.

Entfernen eines OneDrive-, SharePoint- oder Google Drive-Kontos aus der BlueXP Klassifizierung

Wenn Sie Benutzerdateien nicht mehr von einem bestimmten OneDrive-Konto, von einem bestimmten SharePoint-Konto oder von einem Google Drive-Konto scannen möchten, können Sie das Konto von der BlueXP Klassifizierungsschnittstelle löschen und alle Scans beenden.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf ⋮ Klicken Sie in der Zeile für das OneDrive-, SharePoint- oder Google-Drive-Konto auf **OneDrive-Konto entfernen**, **SharePoint-Konto entfernen** oder **Google-Laufwerkskonto entfernen**.

2. Klicken Sie im Bestätigungsdialogfeld auf **Konto löschen**.

Entfernen einer Gruppe von Dateifreigaben aus der BlueXP Klassifizierung

Wenn Sie Benutzerdateien nicht mehr aus einer Dateifreigaben-Gruppe scannen möchten, können Sie die File Shares Group aus der BlueXP Klassifizierungs-Schnittstelle löschen und alle Scans anhalten.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf ⋮ Klicken Sie in der Zeile für die Datei-Shares-Gruppe und dann auf **Datei-Shares-Gruppe entfernen**.

2. Klicken Sie im Bestätigungsdialogfeld auf **Gruppe von Freigaben löschen**.

BlueXP Klassifizierung wird deinstalliert

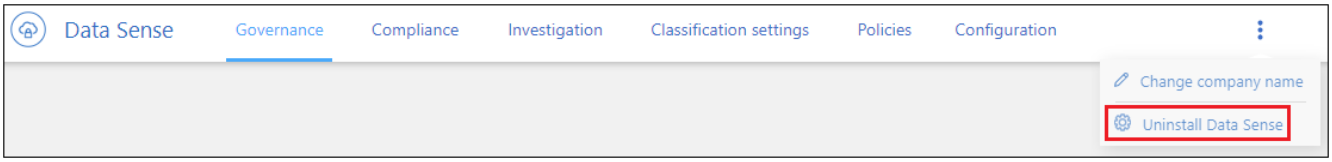
Sie können die BlueXP Klassifizierungssoftware deinstallieren, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen. Wenn Sie die Instanz löschen, werden auch die zugehörigen Festplatten gelöscht, auf denen sich die indizierten Daten befinden. Alle Informationen, die die BlueXP Klassifizierung gescannt hat, werden dauerhaft gelöscht.

Die erforderlichen Schritte hängen davon ab, ob Sie die BlueXP Klassifizierung in der Cloud oder auf einem lokalen Host implementiert haben.

Deinstallieren der BlueXP Klassifizierung aus einer Cloud-Implementierung

Wenn Sie die BlueXP Klassifizierungsinstanz nicht mehr verwenden möchten, können Sie sie deinstallieren oder aus der Cloud-Provider-Umgebung löschen.

1. Klicken Sie oben auf der BlueXP Klassifizierungsseite auf ⋮ Und klicken Sie dann auf **Data Sense deinstallieren**.



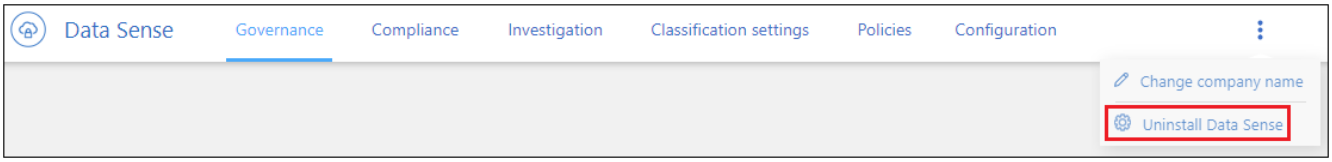
2. Geben Sie im Dialogfeld *Uninstall Data Sense* **uninstall** ein, um zu bestätigen, dass Sie die BlueXP-Klassifikationsinstanz vom BlueXP Connector trennen möchten, und klicken Sie dann auf **Uninstall**.
3. Rufen Sie die Konsole Ihres Cloud-Providers auf und löschen Sie die BlueXP Klassifizierungsinstanz. Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

   Damit werden die Instanz und alle zugehörigen Daten, die durch die BlueXP Klassifizierung erfasst wurden, gelöscht.

Deinstallieren der BlueXP Klassifizierung aus einer lokalen Implementierung

Sie können die BlueXP Klassifizierung von einem Host deinstallieren, wenn Sie nicht mehr die BlueXP Klassifizierung verwenden möchten oder wenn ein Problem aufgetreten ist, das eine Neuinstallation erfordert.

1. Klicken Sie oben auf der BlueXP Klassifizierungsseite auf ⋮ Und klicken Sie dann auf **Data Sense deinstallieren**.



2. Geben Sie im Dialogfeld *Uninstall Data Sense* **uninstall** ein, um zu bestätigen, dass Sie die BlueXP-

Klassifikationsinstanz vom BlueXP Connector trennen möchten, und klicken Sie dann auf **Uninstall**.

3. Um die Software vom Host zu deinstallieren, führen Sie den aus `cleanup.sh` Skript auf dem Host-Rechner, z. B.:

```
cleanup.sh
```

Informieren Sie sich darüber "Melden Sie sich bei der BlueXP Klassifizierungs-Host-Maschine an".

Referenz

Unterstützte BlueXP Klassifizierungs-Instanztypen

Die BlueXP Klassifizierungssoftware muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Software-Anforderungen usw. erfüllt. Bei der Implementierung der BlueXP Klassifizierung in der Cloud empfehlen wir, ein System mit den „großen“ Merkmalen zu verwenden, um den vollen Funktionsumfang zu erhalten.

Sie können die BlueXP Klassifizierung auf einem System mit weniger CPUs und weniger RAM implementieren. Bei der Nutzung dieser weniger leistungsstarken Systeme bestehen jedoch einige Einschränkungen. "Informieren Sie sich über diese Einschränkungen".

Wenn in den folgenden Tabellen das als „Standard“ markierte System in der Region, in der Sie die BlueXP-Klassifizierung installieren, nicht verfügbar ist, wird das nächste System in der Tabelle bereitgestellt.

AWS-Instanztypen

Systemgröße	Spezifikationen	Instanztyp
Extra Groß	32 CPUs, 128 GB RAM, 1 tib gp3-SSD	"M6i.8xlarge" (Standard)
Groß	16 CPUs, 64 GB RAM, 500 gib SSD	"M6i.4xlarge" (Standard) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Mittel	8 CPUs, 32 GB RAM, 200 gib SSD	"M6i.2xlarge" (Standard) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Klein	8 CPUs, 16 GB RAM, 100 gib SSD	"c6a.2xlarge" (Standard) c5a.2xlarge c5.2xlarge c4.2xlarge

Azure Instanztypen

Systemgröße	Spezifikationen	Instanztyp
Extra Groß	32 CPUs, 128 GB RAM, BS-Festplatte (2,048 gib, min. 250 MB/s Durchsatz) und Datenfestplatte (1 tib SSD, min. 750 MB/s Durchsatz)	"Standard_D32_v3" (Standard)
Groß	16 CPUs, 64 GB RAM, 500 gib SSD	"Standard_D16s_v3" (Standard)

GCP-Instanztypen

Systemgröße	Spezifikationen	Instanztyp
Groß	16 CPUs, 64 GB RAM, 500 gib SSD	"n2-Standard-16" (Standard) n2d-Standard-16 n1-Standard-16

Metadaten, die aus Datenquellen erhoben werden

Die BlueXP Klassifizierung erfasst bestimmte Metadaten, wenn Klassifizierungs-Scans für Daten aus Datenquellen und Arbeitsumgebungen durchgeführt werden. Die BlueXP Klassifizierung kann auf die meisten Metadaten zugreifen, die wir für die Klassifizierung Ihrer Daten benötigen. Es gibt jedoch einige Quellen, aus denen wir nicht auf die von uns benötigten Daten zugreifen können.

	Metadaten	CIFS	NFS
Zeitstempel	*Erstellungszeit*	Verfügbar	Nicht verfügbar (nicht unterstützt in Linux)
	Zeitpunkt des letzten Zugriffs	Verfügbar	Verfügbar
	Letzte Änderungszeit	Verfügbar	Verfügbar
Berechtigungen	*Berechtigungen öffnen*	Wenn die Gruppe „ALLE“ Zugriff auf die Datei hat, gilt sie als „für Organisation geöffnet“.	Wenn „andere“ Zugriff auf die Datei haben, gilt sie als „für Organisation geöffnet“.
	Benutzer/Gruppenzugriff	Benutzer- und Gruppeninformationen werden aus LDAP übernommen	Nicht verfügbar (NFS-Benutzer werden in der Regel lokal auf dem Server verwaltet, daher kann dieselbe Person eine andere UID auf jedem Server haben)

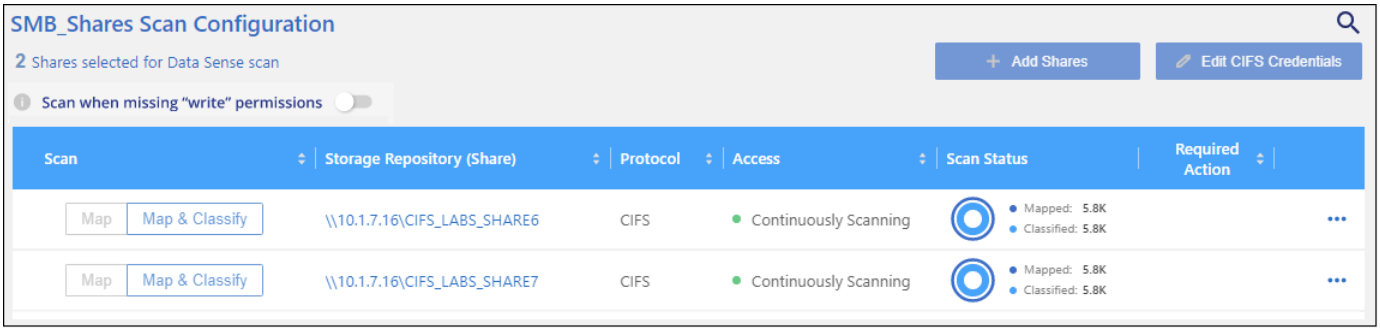
- Die BlueXP Klassifizierung extrahiert nicht den „Zeitpunkt des letzten Zugriffs“ aus den folgenden Datenquellen: SharePoint Online, SharePoint On-Premises (SharePoint Server), OneDrive, Google Drive und Amazon S3 sowie Datenbanken.
- Ältere Versionen des Windows-Betriebssystems (z. B. Windows 7 und Windows 8) deaktivieren standardmäßig die Sammlung des Attributs „Zeit des letzten Zugriffs“, da dies die Systemleistung beeinträchtigen kann. Wenn dieses Attribut nicht erfasst wird, ist die BlueXP Klassifizierungsanalyse, die auf dem Zeitpunkt des letzten Zugriffs basiert, betroffen. Bei Bedarf können Sie die Erfassung der letzten Zugriffszeit auf diesen älteren Windows-Systemen aktivieren.

Zeitstempel der letzten Zugriffszeit

Wenn die BlueXP Klassifizierung Daten aus File Shares extrahiert, berücksichtigt das Betriebssystem sie als Zugriff auf die Daten und ändert entsprechend den Zeitpunkt des letzten Zugriffs. Nach dem Scannen versucht die BlueXP Klassifizierung, die letzte Zugriffszeit auf den ursprünglichen Zeitstempel zurückzusetzen. Wenn die BlueXP Klassifizierung keine Schreibattributberechtigungen in CIFS oder Schreibberechtigungen in NFS hat, kann das System die letzte Zugriffszeit nicht auf den ursprünglichen Zeitstempel zurücksetzen. ONTAP Volumes, die mit SnapLock konfiguriert sind, haben schreibgeschützte Berechtigungen und können auch die letzte Zugriffszeit nicht auf den ursprünglichen Zeitstempel zurücksetzen.

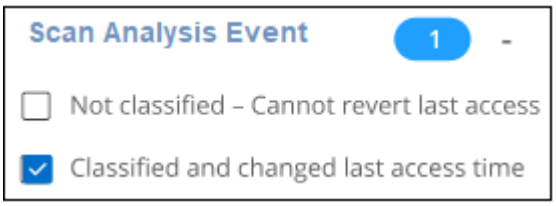
Wenn die BlueXP Klassifizierung diese Berechtigungen nicht besitzt, scannt das System standardmäßig diese Dateien in Ihren Volumes nicht, da die BlueXP Klassifizierung die „letzte Zugriffszeit“ nicht auf den ursprünglichen Zeitstempel zurücksetzen kann. Wenn es Ihnen jedoch egal ist, ob die letzte Zugriffszeit in Ihren Dateien auf die ursprüngliche Zeit zurückgesetzt wird, können Sie unten auf der Konfigurationsseite auf

den Schalter **Scan bei fehlenden Berechtigungen für "Schreibattribute"** klicken, damit die BlueXP-Klassifizierung die Volumes unabhängig von den Berechtigungen scannt.



Diese Funktionalität ist anwendbar auf On-Premises-ONTAP-Systeme, Cloud Volumes ONTAP, Azure NetApp Files, FSX for ONTAP und nicht-NetApp File Shares.

Beachten Sie, dass es einen Filter auf der Seite Untersuchung mit dem Namen *Scan Analysis Event* gibt, mit dem Sie entweder die Dateien anzeigen können, die nicht klassifiziert wurden, da die BlueXP-Klassifikation die letzte Zugriffszeit nicht rückgängig machen konnte. Oder die klassifizierten Dateien, auch wenn die BlueXP Klassifizierung den Zeitpunkt des letzten Zugriffs nicht zurücksetzen konnte.



Folgende Filteroptionen stehen zur Auswahl:

- „Nicht klassifiziert — kann letzte Zugriffszeit nicht rückgängig machen“ – zeigt die Dateien an, die aufgrund fehlender Schreibberechtigungen nicht klassifiziert wurden.
- „Zeitpunkt des letzten Zugriffs klassifiziert und aktualisiert“ – Hier werden die Dateien angezeigt, die klassifiziert wurden und die BlueXP-Klassifizierung konnte den Zeitpunkt des letzten Zugriffs nicht auf das ursprüngliche Datum zurücksetzen. Dieser Filter ist nur für Umgebungen relevant, in denen Sie **Scan bei fehlenden Berechtigungen für "Schreibattribute"** AKTIVIERT haben.

Bei Bedarf können Sie diese Ergebnisse in einen Bericht exportieren, damit Sie sehen können, welche Dateien aufgrund von Berechtigungen gescannt werden oder nicht. "Erfahren Sie mehr über den Untersuchungsbericht".

Melden Sie sich beim BlueXP Klassifizierungssystem an

Gelegentlich müssen Sie sich möglicherweise beim BlueXP Klassifizierungssystem anmelden, damit Sie auf Protokolldateien zugreifen oder Konfigurationsdateien bearbeiten können.

Wenn die BlueXP Klassifizierung auf einer lokalen Linux-Maschine oder auf einer in der Cloud implementierten Linux-Maschine installiert wird, können Sie direkt auf die Konfigurationsdatei und das Skript zugreifen.

Wenn die BlueXP Klassifizierung in der Cloud implementiert wird, müssen Sie SSH zur BlueXP Klassifizierungsinstanz verwenden. Sie können SSH auf dem System verwenden, indem Sie den Benutzer und das Kennwort eingeben oder den SSH-Schlüssel verwenden, den Sie während der Installation des BlueXP

Connectors angegeben haben. Der SSH-Befehl lautet:

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = Speicherort der ssh-Authentifizierungsschlüssel
* <machine_user>:
```

+
Für AWS: Verwenden Sie <ec2-user>
Für Azure: Verwenden Sie den für die BlueXP-Instanz erstellten Benutzer
** Für GCP: Verwenden Sie den für die BlueXP-Instanz erstellten Benutzer

- <dataense_ip> = IP-Adresse der virtuellen Maschineninstanz

Beachten Sie, dass Sie die Inbound-Regeln der Sicherheitsgruppe ändern müssen, um auf das System in der Cloud zuzugreifen. Weitere Informationen finden Sie unter:

- "Sicherheitsgruppenregeln in AWS"
- "Für Sicherheitsgruppen gibt es in Azure Regeln"
- "Firewall-Regeln in Google Cloud"

BlueXP Klassifizierungs-APIs

Die über die Web-UI verfügbaren BlueXP Klassifizierungsfunktionen sind auch über die Swagger-API verfügbar.

Die BlueXP Klassifizierung umfasst vier Kategorien, die den Registerkarten in der UI entsprechen:

- Untersuchung
- Compliance
- Governance
- Konfiguration

Die APIs in der Dokumentation von Swagger ermöglichen Ihnen, Daten zu durchsuchen, zu aggregieren, Ihre Scans zu verfolgen und Aktionen wie Kopieren, Verschieben und vieles mehr zu erstellen.

Überblick

Mit der API können Sie die folgenden Funktionen ausführen:

- Informationen exportieren
  - Alles, was in der Benutzeroberfläche verfügbar ist, kann über die API exportiert werden (mit Ausnahme von Berichten)
  - Daten werden in einem JSON-Format exportiert (Analyse und Verschiebung auf Applikationen von Drittanbietern wie Splunk ist einfach).
- Erstellen Sie Abfragen mit „UND“- und „ODER“-Anweisungen, schließen Sie Informationen ein und aus und vieles mehr.

  Beispielsweise können Sie Dateien *ohne* spezifische personenbezogene Daten (PII) suchen (Funktionalität

in der Benutzeroberfläche nicht verfügbar). Sie können auch bestimmte Felder für den Exportvorgang ausschließen.

- Führen Sie Aktionen aus
  - Aktualisieren Sie die CIFS-Anmeldeinformationen
  - Aktionen anzeigen und abbrechen
  - Verzeichnisse erneut scannen
  - Löschen, Kopieren, Beschriften und Zuweisen von Benutzern zu Daten
  - Dateien klonen und kopieren
  - Daten exportieren

Die API ist sicher und verwendet die gleiche Authentifizierungsmethode wie die UI. Informationen zur Authentifizierung finden Sie unter: https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html

Zugriff auf die Swagger-API-Referenz

Um in Swagger zu kommen, benötigen Sie die IP-Adresse der BlueXP Klassifizierungsinstanz. Bei einer Cloud-Bereitstellung verwenden Sie die öffentliche IP-Adresse. Dann müssen Sie zu diesem Endpunkt gelangen:

\Https://<classification_ip>/Dokumentation

Beispiel mit den APIs

Das folgende Beispiel zeigt einen API-Aufruf zum Kopieren von Dateien.

API-Anfrage

Sie müssen zunächst alle relevanten Felder und Optionen für eine Arbeitsumgebung abrufen, um alle Filter auf der Registerkarte Untersuchung anzuzeigen.

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… " -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients"
```

Antwort

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
      "name": "string",
      "operators": [
```

```
        "EQUALS"
      ],
      "optional_values": [
        {}
      ],
      "secondary": {},
      "server_data": false,
      "type": "TEXT"
    }
  ]
}
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "POLICIES",
      "name": "Policies",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "EXTRACTION_STATUS_RANGE",
      "name": "Scan Analysis Status",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "SCAN_ANALYSIS_ERROR",
      "name": "Scan Analysis Event",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
```

```
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "PUBLIC_ACCESS",
      "name": "Open Permissions",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USERS_PERMISSIONS_COUNT_RANGE",
      "name": "Number of Users with Access",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USER_GROUP_PERMISSIONS",
      "name": "User / Group Permissions",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_OWNER",
      "name": "File Owner",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
```

```
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT_TYPE",
      "name": "Working Environment Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT",
      "name": "Working Environment",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "SCAN_TASK",
      "name": "Storage Repository",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_PATH",
      "name": "File / Directory Path",
      "operators": [
        "MULTI_CONTAINS",
        "MULTI_EXCLUDE"
```

```
      ],
      "server_data": true,
      "type": "MULTI_TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
      "field": "CATEGORY",
      "name": "Category",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVITY_LEVEL",
      "name": "Sensitivity Level",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "NUMBER_OF_IDENTIFIERS",
      "name": "Number of identifiers",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_PERSONAL",
      "name": "Personal Data",
      "operators": [
        "IN",
```

```
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVE",
      "name": "Sensitive Personal Data",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DATA_SUBJECT",
      "name": "Data Subject",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "DIRECTORIES",
      "field": "DIRECTORY_TYPE",
      "name": "Directory Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_TYPE",
      "name": "File Type",
```

```
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_SIZE_RANGE",
      "name": "File Size",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_CREATION_RANGE_RETENTION",
      "name": "Created Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DISCOVERED_TIME_RANGE",
      "name": "Discovered Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_MODIFICATION_RETENTION",
      "name": "Last Modified",
```

```
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
      "name": "Last Accessed",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "IS_DUPLICATE",
      "name": "Duplicates",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "FILE_HASH",
      "name": "File Hash",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "USER_DEFINED_STATUS",
      "name": "Tags",
```

```
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ASSIGNED_TO",
      "name": "Assigned to",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    }
  ]
}
```

Wir werden diese Antwort in unseren Anfrageparametern verwenden, um die gewünschten Dateien zu filtern, die wir kopieren möchten.

Sie können eine Aktion auf mehrere Elemente anwenden. Unterstützte Aktionstypen sind: Verschieben, löschen, kopieren, zuweisen, FlexClone, Daten exportieren, erneut scannen und beschriften.

Wir erstellen die Kopieraktion:

API-Anfrage

Diese nächste API ist die AktionAPI, und es ermöglicht Ihnen, mehrere Aktionen zu erstellen.

```
curl -X POST "http://
{classification_ip}/api//{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
"{ontap_ip}:/{share_name} " },
\"requested_query\":{"condition":"AND","rules":[{"field":"ENVIRONMENT_TYPE
","operator":"IN","value":["ONPREM"]},{"field":"CATEGORY","operator":"IN",
"value":["21"]}]}}"
```

Antwort

Die Antwort gibt das Aktionsobjekt zurück, sodass Sie mit den APIs get and delete den Status der Aktion

abrufen oder abbrechen können.


```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```

Wissen und Support

Für den Support anmelden

Für den Support von BlueXP und seinen Storage-Lösungen und Services ist eine Support-Registrierung erforderlich. Um wichtige Workflows für Cloud Volumes ONTAP Systeme zu ermöglichen, ist außerdem eine Support-Registrierung erforderlich.

Durch die Registrierung für den Support wird die NetApp-Unterstützung für einen Fileservice eines Cloud-Providers nicht aktiviert. Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Cloud Volumes Service für Google Cloud"

Übersicht über die Support-Registrierung

Es gibt zwei Registrierungsformulare, um die Support-Berechtigung zu aktivieren:

- Registrieren Ihres BlueXP-Konto-ID-Support-Abonnements (Ihre 20-stellige Seriennummer 960xxxxxxxxx auf der Seite Support-Ressourcen in BlueXP).

  Dies dient als Ihre einzige Support-Abonnement-ID für jeden Service in BlueXP. Jedes BlueXP-Abonnement für Support auf Kontoebene muss registriert werden.

- Registrieren der Cloud Volumes ONTAP Seriennummern für ein Abonnement auf dem Markt Ihres Cloud-Providers (dies sind 20-stellige Seriennummern von 909201xxxxxx).

  Diese Seriennummern werden als *PAYGO Seriennummern* bezeichnet und werden zum Zeitpunkt der Cloud Volumes ONTAP Implementierung von BlueXP generiert.

Durch das Registrieren beider Arten von Seriennummern können Kunden Funktionen wie das Öffnen von Support-Tickets und die automatische Erstellung von Support-Cases nutzen. Die Registrierung ist abgeschlossen, indem wie unten beschrieben Konten der NetApp Support Website (NSS) zu BlueXP hinzugefügt werden.

Registrieren Sie Ihr BlueXP Konto für NetApp Support

Um sich für den Support zu registrieren und die Supportberechtigung zu aktivieren, muss ein Benutzer in Ihrem BlueXP Konto ein NetApp Support Site Konto mit seinen BlueXP Anmeldedaten verknüpfen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über einen NSS Account (NetApp Support Site) verfügen.

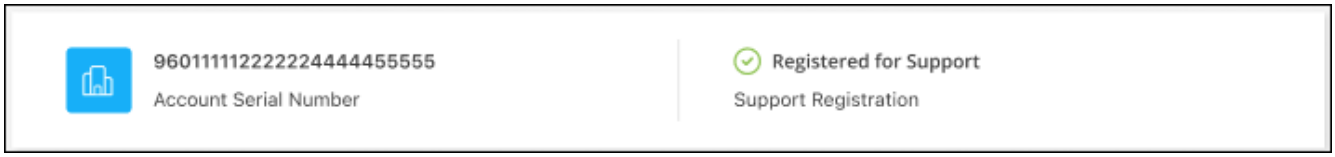
Bestandskunde mit NSS-Konto

Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich für den Support über BlueXP registrieren.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Eingabeaufforderung für die NetApp-Support-Website (NSS)-Authentifizierung.
4. Um zu bestätigen, dass die Registrierung erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Konto für Support registriert ist.

   Beachten Sie, dass andere BlueXP Benutzer diesen Support-Registrierungsstatus nicht sehen, wenn sie ihrem BlueXP Login kein NetApp Support Site Konto zugeordnet haben. Das bedeutet jedoch nicht, dass Ihr BlueXP Konto nicht für den Support registriert ist. Solange ein Benutzer im Konto diese Schritte befolgt hat, wurde Ihr Konto registriert.

Vorhandener Kunde, aber kein NSS-Konto

Wenn Sie bereits NetApp Kunde sind und über vorhandene Lizenzen und Seriennummern sowie *No* NSS Konto verfügen, müssen Sie ein NSS Konto erstellen und es Ihren BlueXP Anmeldedaten zuordnen.

Schritte

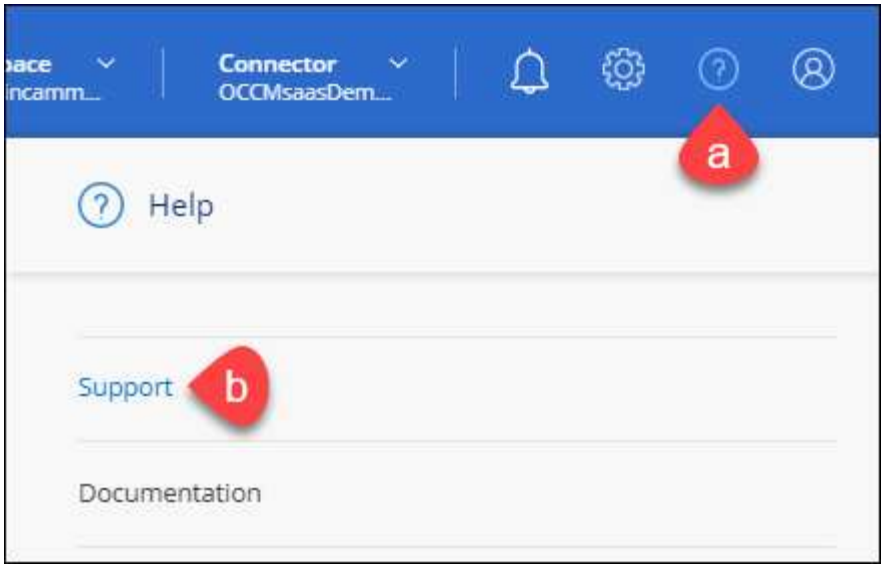
1. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie unbedingt die oben verwendete BlueXP-Kontonummer (960xxxx) für das Feld Seriennummer. Dadurch wird die Kontobearbeitung beschleunigt.
2. Ordnen Sie Ihr neues NSS-Konto Ihrer BlueXP Anmeldung zu, indem Sie die unter aufgeführten Schritte durchführen Bestandskunde mit NSS-Konto.

Neu bei NetApp

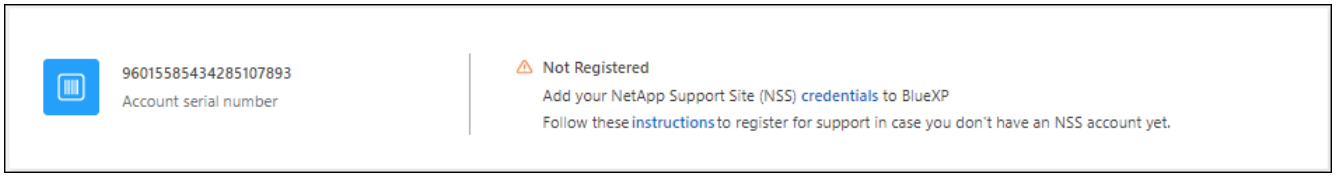
Wenn Sie neu bei NetApp sind und über keinen NSS-Account verfügen, befolgen Sie jeden Schritt unten.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.



2. Suchen Sie auf der Seite für die Support-Registrierung die Seriennummer Ihres Kontos.



3. Navigieren Sie zu "Die Support-Registrierungs-Website von NetApp" Und wählen Sie **Ich bin kein registrierter NetApp Kunde**.
4. Füllen Sie die Pflichtfelder aus (mit roten Sternchen).
5. Wählen Sie im Feld **Product Line** die Option **Cloud Manager** aus, und wählen Sie dann den gewünschten Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer des Kontos von Schritt 2 oben, füllen Sie die Sicherheitsprüfung aus und bestätigen Sie dann, dass Sie die globale Datenschutzrichtlinie von NetApp lesen.

   Zur Fertigstellung dieser sicheren Transaktion wird sofort eine E-Mail an die angegebene Mailbox gesendet. Überprüfen Sie Ihre Spam-Ordner, wenn die Validierungs-E-Mail nicht in wenigen Minuten ankommt.

7. Bestätigen Sie die Aktion in der E-Mail.

   Indem Sie Ihre Anfrage an NetApp senden, wird Ihnen die Erstellung eines NetApp Support Site Kontos empfohlen.

8. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie die oben angegebene Seriennummer (960xxxx) für das Feld „Seriennummer“. Dadurch wird die Kontobearbeitung beschleunigt.

Nachdem Sie fertig sind

NetApp sollte sich bei diesem Prozess mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Wenn Sie über Ihren NetApp Support Site Account verfügen, ordnen Sie das Konto Ihrer BlueXP Anmeldung zu, indem Sie die Schritte unter ausführen Bestandskunde mit NSS-Konto.

Verknüpfen von NSS-Anmeldeinformationen für den Cloud Volumes ONTAP-Support

Um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu ermöglichen, müssen die Zugangsdaten für die NetApp Support Website mit Ihrem BlueXP Konto verknüpft werden:

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen für Support

  Die Bereitstellung Ihres NSS Kontos ist erforderlich, um Support für Ihr System zu aktivieren und Zugang zu den technischen Support-Ressourcen von NetApp zu erhalten.

- Implementierung von Cloud Volumes ONTAP unter Verwendung von BYOL (Bring-Your-Own-License)

  Die Bereitstellung Ihres NSS-Kontos ist erforderlich, damit BlueXP Ihren Lizenzschlüssel hochladen und das Abonnement für den von Ihnen erworbenen Zeitraum aktivieren kann. Dies schließt automatische Updates für Vertragsverlängerungen ein.

- Aktualisieren der Cloud Volumes ONTAP Software auf die neueste Version

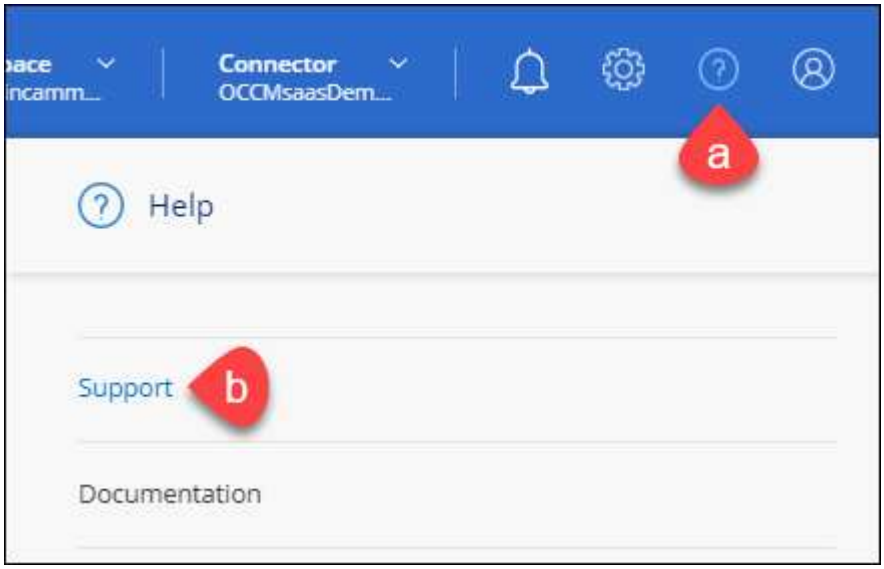
Das Zuordnen der NSS-Anmeldedaten zu Ihrem BlueXP Konto unterscheidet sich von dem NSS-Konto, das mit einer BlueXP Benutzeranmeldung verknüpft ist.

Diese NSS-Zugangsdaten sind mit Ihrer spezifischen BlueXP Konto-ID verknüpft. Benutzer, die zum BlueXP Konto gehören, können über **Support > NSS Management** auf diese Anmeldedaten zugreifen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.
- Wenn Sie einen Partner- oder Reseller-Account haben, können Sie ein oder mehrere NSS-Konten hinzufügen, können aber nicht neben Kunden-Level Accounts hinzugefügt werden.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.



2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite umgeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsservices, die speziell auf Support und Lizenzierung zugeschnitten sind.

4. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

   Mit diesen Aktionen kann BlueXP Ihr NSS-Konto für Dinge wie Lizenzdownloads, Softwareaktualisierungs-Verifizierung und zukünftige Support-Registrierungen verwenden.

   Beachten Sie Folgendes:

   - Das NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder Temporärkonto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto vorhanden sein, wenn es sich bei diesem Konto um ein Partner-Level-Konto handelt. Wenn Sie versuchen, NSS-Konten auf Kundenebene hinzuzufügen und ein Konto auf Partnerebene vorhanden ist, erhalten Sie die folgende Fehlermeldung:

     „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da es bereits NSS-Benutzer unterschiedlichen Typs gibt.“

   Dasselbe gilt, wenn Sie bereits NSS-Konten auf Kundenebene haben und versuchen, ein Konto auf Partnerebene hinzuzufügen.

   - Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern.

     Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet ist. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen ••• Menü.

   - Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option ••• Menü.

     Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Eine Benachrichtigung wird gesendet, um Sie darüber zu informieren.

Holen Sie sich Hilfe

NetApp bietet Unterstützung für BlueXP und seine Cloud-Services auf unterschiedliche Weise. Umfassende kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie etwa Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

Unterstützung für Fileservices von Cloud-Providern

Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Cloud Volumes Service für Google Cloud"

Wenn Sie technischen Support für BlueXP und seine Storage-Lösungen und -Services erhalten möchten, nutzen Sie die unten beschriebenen Support-Optionen.

Nutzen Sie Self-Support-Optionen

Diese Optionen sind kostenlos verfügbar, 24 Stunden am Tag, 7 Tage die Woche:

- Dokumentation

  Die BlueXP-Dokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  Suchen Sie in der BlueXP Knowledge Base nach hilfreichen Artikeln zur Fehlerbehebung.

- "Communitys"

  Treten Sie der BlueXP Community bei, um laufende Diskussionen zu verfolgen oder neue zu erstellen.

Erstellen Sie einen Fall mit dem NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie gemeinsam mit einem NetApp Support-Experten eventuelle Probleme nach der Aktivierung des Supports beheben.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** nutzen zu können, müssen Sie zunächst Ihre Anmeldedaten für die NetApp Support-Website mit Ihren BlueXP Anmeldedaten verknüpfen. "Managen Sie Zugangsdaten für Ihre BlueXP Anmeldung".
- Wenn Sie einen Fall für ein ONTAP System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer des Systems verknüpft sein.

Schritte

1. Wählen Sie in BlueXP **Hilfe > Support** aus.
2. Wählen Sie auf der Seite **Ressourcen** eine der verfügbaren Optionen unter Technischer Support:

   a. Wählen Sie **Rufen Sie uns an**, wenn Sie mit jemandem am Telefon sprechen möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.

   b. Wählen Sie **Fall erstellen**, um ein Ticket mit einem NetApp-Supportspezialisten zu öffnen:

      - **Service**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: BlueXP, wenn es sich um ein Problem des technischen Supports mit Workflows oder Funktionen im Service handelt.
      - **Arbeitsumgebung**: Wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

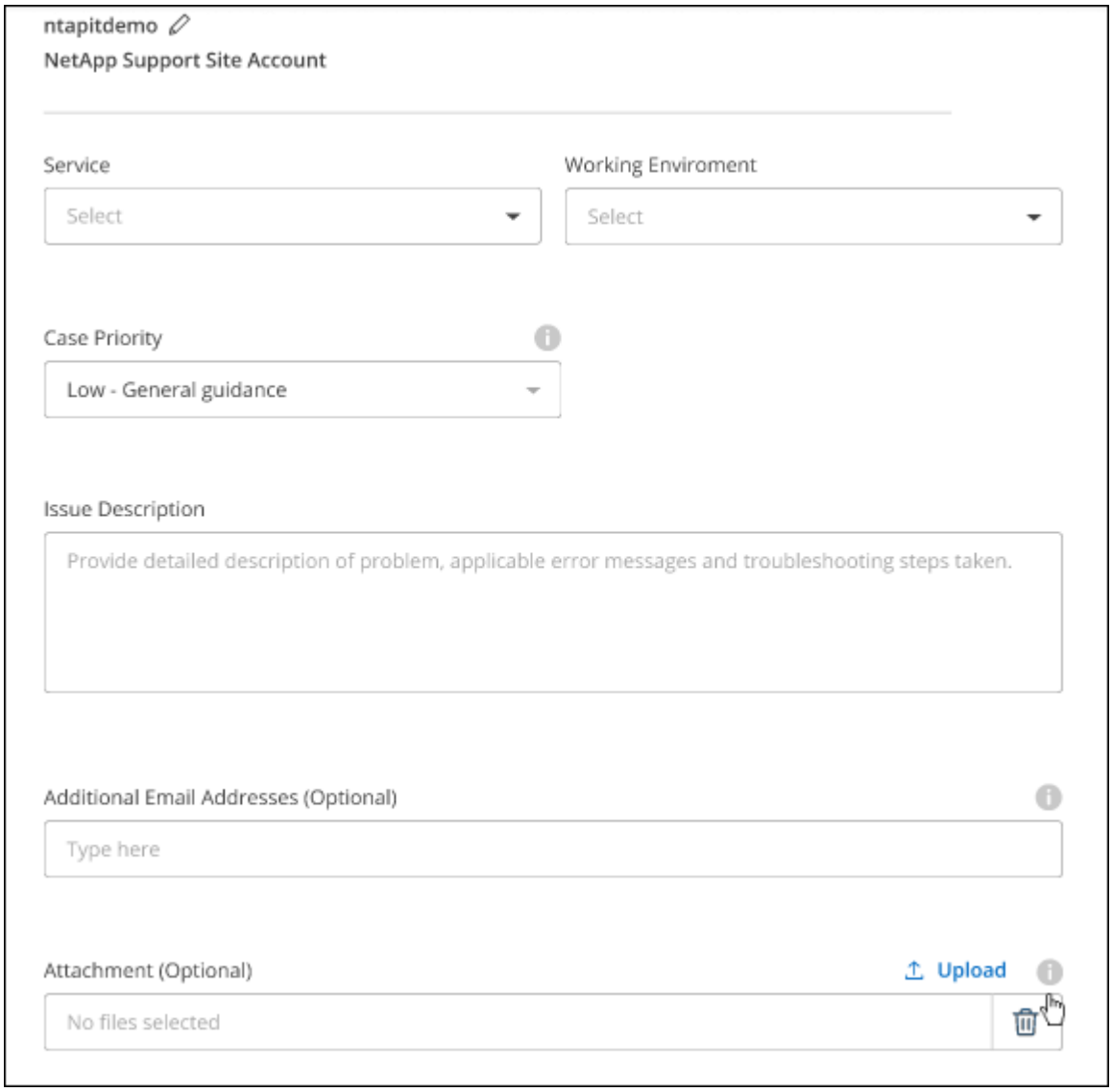
        Die Liste der Arbeitsumgebungen liegt im Bereich des BlueXP-Kontos, des Arbeitsbereichs und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **Case Priority**: Wählen Sie die Priorität für den Fall, der niedrig, Mittel, hoch oder kritisch sein kann.

  Wenn Sie weitere Informationen zu diesen Prioritäten wünschen, bewegen Sie den Mauszeiger über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller anwendbaren Fehlermeldungen oder Fehlerbehebungsschritte, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderes auf dieses Problem aufmerksam machen möchten.
- **Anhang (optional)**: Laden Sie bis zu fünf Anhänge nacheinander hoch.

  Anhänge sind auf 25 MB pro Datei begrenzt. Folgende Dateierweiterungen werden unterstützt: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nachdem Sie fertig sind

Es wird ein Popup-Fenster mit der Support-Fallnummer angezeigt. Ein NetApp Support-Experte prüft Ihren Fall und macht Sie umgehend mit.

Um eine Historie deiner Support-Fälle anzuzeigen, kannst du **Einstellungen > Chronik** auswählen und nach Aktionen mit dem Namen „Support-Case erstellen“ suchen. Mit einer Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, möglicherweise die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Service zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das Unternehmen des Datensatzes, mit dem es verbunden ist, nicht das gleiche Unternehmen des Eintrags für die BlueXP Account Seriennummer (dh 960xxxx) oder Seriennummer der Arbeitsumgebung. Sie können Hilfe mit einer der folgenden Optionen anfordern:

- Verwenden Sie den Chat im Produkt
- Übermitteln eines nicht-technischen Cases unter https://mysupport.netapp.com/site/help

Managen Ihrer Support-Cases (Vorschau)

Sie können aktive und gelöste Support-Cases direkt über BlueXP anzeigen und managen. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verbundenen Fälle verwalten.

Case Management ist als Vorschau verfügbar. Wir planen, diese Erfahrungen weiter zu verbessern und in zukünftigen Versionen Verbesserungen hinzuzufügen. Bitte senden Sie uns Ihr Feedback über den Product-Chat.

Beachten Sie Folgendes:

- Das Case-Management-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht auf der linken Seite zeigt die Gesamtzahl der Fälle, die in den letzten 3 Monaten durch das von Ihnen angegebene NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht auf der rechten Seite zeigt die Gesamtzahl der in den letzten 3 Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto an.

  Die Ergebnisse in der Tabelle geben die Fälle in Bezug auf die ausgewählte Ansicht wieder.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie Priorität und Status filtern. Andere Spalten bieten nur Sortierfunktionen.

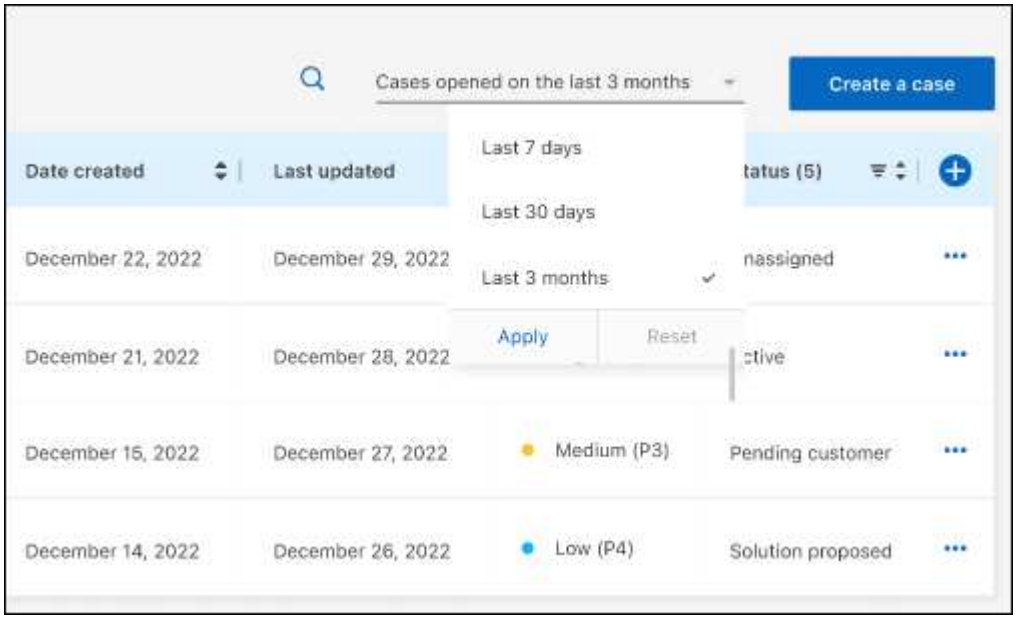
  Weitere Informationen erhalten Sie in den Schritten unten.
- Auf Fallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Geschlossen“ oder „Geschlossen“ befindet.

Schritte

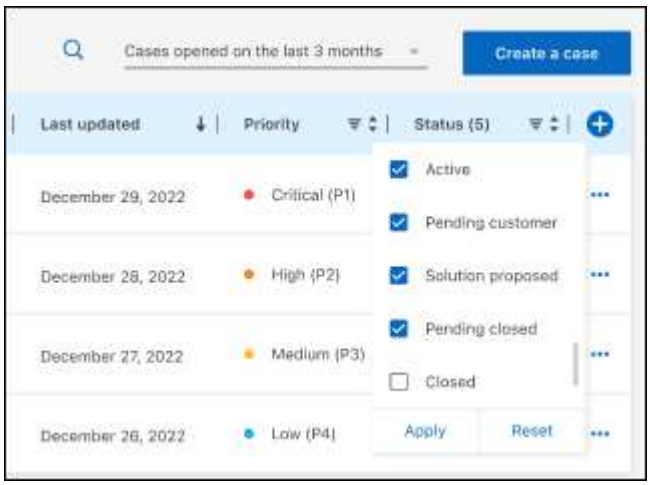
1. Wählen Sie in BlueXP **Hilfe > Support** aus.
2. Wählen Sie **Case Management** aus und fügen Sie bei Aufforderung Ihr NSS-Konto zu BlueXP hinzu.

   Auf der Seite **Case Management** werden offene Fälle im Zusammenhang mit dem NSS-Konto angezeigt, das mit Ihrem BlueXP Benutzerkonto verknüpft ist. Dies ist das gleiche NSS-Konto, das oben auf der Seite **NSS Management** angezeigt wird.
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:

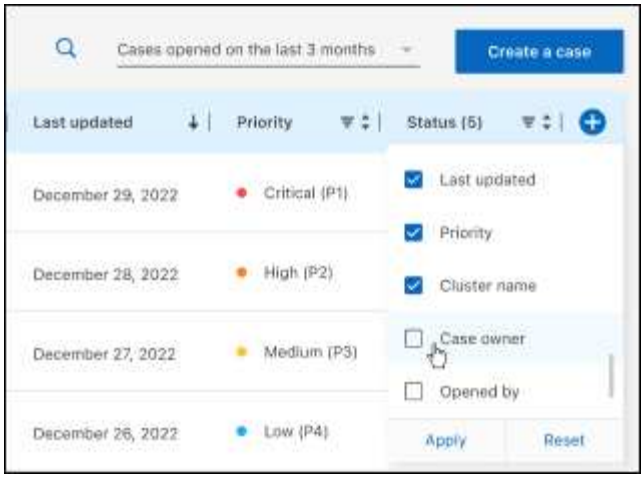
- Wählen Sie unter **Vorgänge der Organisation Ansicht** aus, um alle mit Ihrem Unternehmen verbundenen Fälle anzuzeigen.
- Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.



- Filtern Sie den Inhalt der Spalten.



- Ändern Sie die Spalten, die in der Tabelle angezeigt werden, indem Sie auswählen Und wählen Sie dann die Spalten, die Sie anzeigen möchten.

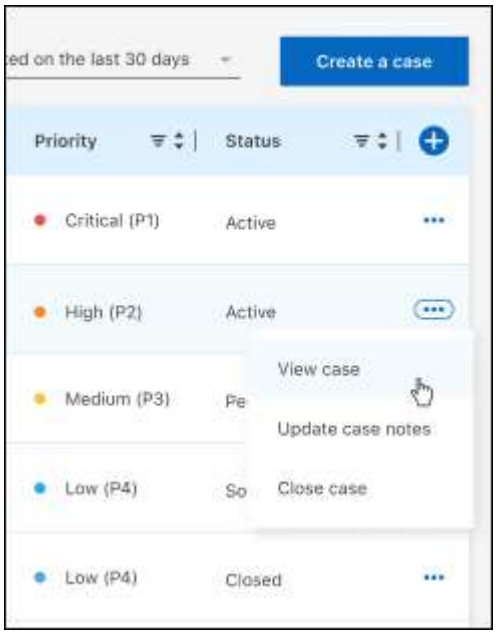


4. Managen Sie einen bestehenden Fall, indem Sie auswählen ••• Und eine der verfügbaren Optionen auswählen:

   - **Fall anzeigen**: Vollständige Details zu einem bestimmten Fall anzeigen.
   - **Aktennotizen aktualisieren**: Geben Sie zusätzliche Details zu Ihrem Problem an oder wählen Sie **Dateien hochladen**, um maximal fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei begrenzt. Folgende Dateierweiterungen werden unterstützt: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

   - **Fall schließen**: Geben Sie Einzelheiten darüber an, warum Sie den Fall schließen und wählen Sie **Fall schließen**.



Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- "Hinweis für BlueXP"
- "Hinweis zur BlueXP Klassifizierung"