



Veraltete Funktionen

BlueXP classification

NetApp
June 14, 2024

Inhalt

- Veraltete Funktionen 1
 - Veraltete BlueXP Klassifizierungsfunktionen 1
 - Implementieren Sie BlueXP Klassifizierungs-Deprekationen. 3
 - Datenabschreibungen scannen 11
 - Datenabschreibungen verwalten 34

Veraltete Funktionen

Veraltete BlueXP Klassifizierungsfunktionen

Die BlueXP Klassifizierung ist als zentrale Funktion in BlueXP ohne Aufpreis verfügbar. Mit der Klassifizierung von BlueXP als zentrale BlueXP Funktion haben NetApp Sie allen Kunden Zugriff auf maßgeschneidertes Datenmanagement – mit Kernfunktionen.

Es gibt einige Funktionen, die in der BlueXP Kernversion ab Version 1.31 veraltet sind und weiterhin in den älteren Versionen 1.30 und früher unterstützt werden.

Unterstützte Datenquellen

Datenquelle	Ältere Versionen 1.30 und früher	BlueXP Kernversionen 1.31 und höher
Cloud Volumes ONTAP (implementiert in AWS, Azure oder GCP)	Ja.	Ja.
On-Premises ONTAP Cluster	Ja.	Ja.
StorageGRID	Ja.	Nein
Azure NetApp Dateien	Ja.	Ja.
Amazon FSX für ONTAP	Ja.	Ja.
Google Cloud NetApp Volumes	Ja.	Ja.
Cloud Volumes Service für Google Cloud	Ja.	Ja.
Datenbanken	Ja.	Ja.
Amazon S3	Ja.	Nein
Google Cloud Storage	Ja.	Nein
OneDrive	Ja.	Nein
SharePoint Online	Ja.	Nein
SharePoint On-Premises (SharePoint Server)	Ja.	Nein
Google Drive	Ja.	Nein

Compliance-Funktionen

Merkmal	Ältere Versionen 1.30 und früher	BlueXP Kernversionen 1.31 und höher
Ermitteln von personenbezogenen Daten	Ja.	Ja.
Identifizieren Sie sensible personenbezogene Daten	Ja.	Ja.
Reagieren Sie auf DSAR (Data Subject Access Requests).	Ja.	Ja.

Merkmal	Ältere Versionen 1.30 und früher	BlueXP Kernversionen 1.31 und höher
Erstellen Sie eine benutzerdefinierte Liste mit identifizierten „personenbezogenen Daten“	Ja.	Nein
Benachrichtigen Sie Benutzer per E-Mail, wenn Dateien bestimmte personenbezogene Daten enthalten. (Diese Kriterien definieren Sie mit "Richtlinien".)	Ja.	Nein
Verwenden Sie Filter auf Verzeichnisebene	Ja.	Ja.
Verwenden Sie die PII-Analyse auf Verzeichnisebene	Ja.	Nein

Funktionen für das Datenmanagement

Merkmal	Ältere Versionen 1.30 und früher	BlueXP Kernversionen 1.31 und höher
Quelldateien verschieben, kopieren und löschen	Ja.	Nein
Kategorisieren Sie Daten mithilfe von Status-Tags	Ja.	Nein
Kategorisieren Sie Daten mithilfe von AIP-Etiketten	Ja.	Nein
Weisen Sie den Benutzern Dateien zu	Ja.	Nein
Daten nach Bedarf erneut scannen	Ja.	Nein
Erstellen Sie benutzerdefinierte Klassifikatoren	Ja.	Nein
Verzeichnisse vom Scannen ausschließen	Ja.	Ja.
Suche nach Namen in Dateien	Ja.	Ja.
Daten aus der Untersuchung in NFS exportieren	Ja.	Nein
Daten aus der Untersuchung in CSV exportieren	Ja.	Ja.
Unterstützung mehrerer Scanner	Ja.	Nein
Integrieren Sie Active Directory	Ja.	Ja.
Verwenden Sie die Berechtigungsanalyse und Filter	Ja.	Ja.
Verwenden Sie die Speicherkarte	Ja.	Ja.
Verwenden Sie die Heatmap	Ja.	Ja.
Verwenden Sie Aktionen auf Dashboard und Speicherkarte	Ja.	Nein
Verwenden Sie die Audit-Protokollierung für den Dateizugriff	Ja.	Nein
Aktivieren Sie den Dateizugriff über die Konfigurationsseite	Ja.	Nein
Verwenden Sie bestimmte vordefinierte Richtlinien	Ja.	Nein

Implementieren Sie BlueXP Klassifizierungs-Deprekationen

Installieren Sie die BlueXP Klassifizierung auf mehreren Hosts für große Konfigurationen ohne Internetzugang

Führen Sie ein paar Schritte aus, um die BlueXP Klassifizierung auf mehreren Hosts an einem lokalen Standort ohne Internetzugang zu installieren – auch als „*Private Mode*“ bekannt. Diese Art der Installation ist perfekt für Ihre sicheren Standorte.

Bei sehr großen Konfigurationen, bei denen an Standorten ohne Internetzugang Datenmengen im Petabyte-Bereich gescannt werden sollen, können Sie mehrere Hosts einschließen, um zusätzliche Verarbeitungsleistung bereitzustellen. Bei der Verwendung mehrerer Hostsysteme wird das primäre System als *Manager-Node* bezeichnet, und die zusätzlichen Systeme, die zusätzliche Rechenleistung bieten, heißen *Scanner-Nodes*.

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

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

Was Sie benötigen

- Überprüfen Sie, ob alle Linux-Systeme für die Knoten Manager und Scanner die Host-Anforderungen erfüllen.
- 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.
- Stellen Sie sicher, dass Ihre Offline-Umgebung die erforderlichen Berechtigungen und Konnektivität erfüllt.
- 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.

Fügen Sie Scannerknoten zu einer vorhandenen Implementierung hinzu

Sie können Scannerknoten zu einer bestehenden Bereitstellung auf einem Linux-Host mit Internetzugang hinzufügen.

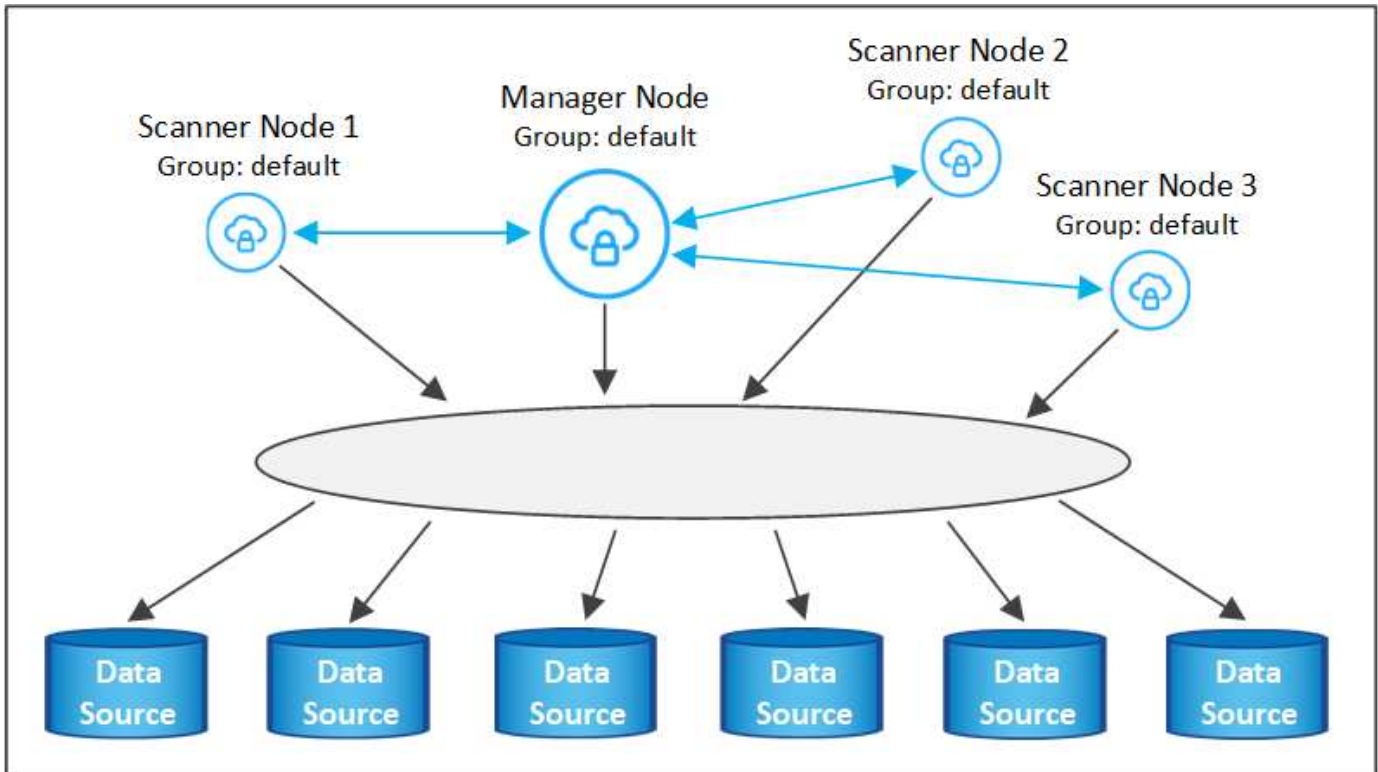
Sie können weitere Scanner-Knoten hinzufügen, wenn Sie feststellen, dass Sie mehr Scanleistung benötigen, um Ihre Datenquellen zu scannen. Sie können die Scanner-Knoten unmittelbar nach der Installation des Manager-Knotens hinzufügen oder später einen Scanner-Knoten hinzufügen. Wenn Sie beispielsweise 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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

Es gibt zwei Möglichkeiten, weitere Scanner-Knoten hinzuzufügen:

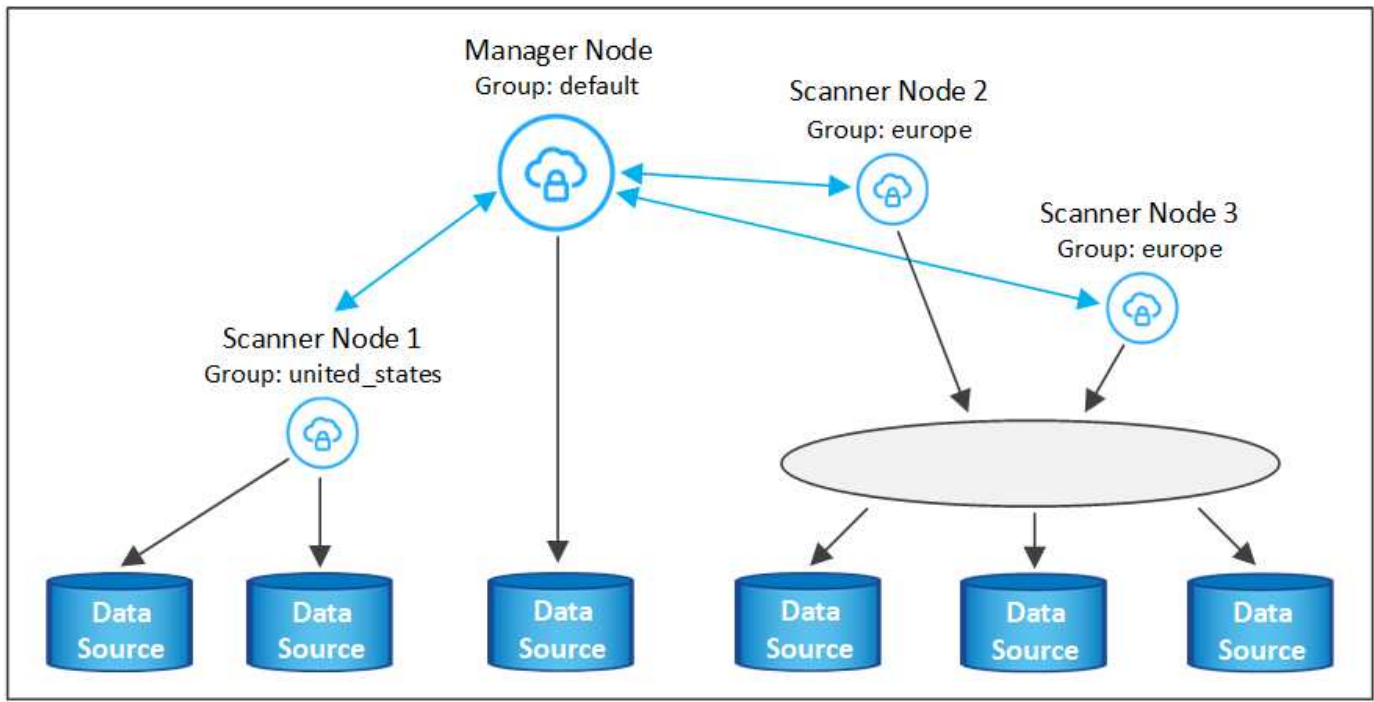
- Fügen Sie einen Knoten hinzu, um das Scannen aller Datenquellen zu unterstützen
- Fügen Sie einen Knoten hinzu, um das Scannen einer bestimmten Datenquelle oder einer bestimmten Gruppe von Datenquellen zu unterstützen (typischerweise basierend auf dem Speicherort).

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

- Überprüfen Sie, ob alle Linux-Systeme für Scanner-Knoten die Host-Anforderungen erfüllen.
- 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.
- Überprüfen Sie, ob Ihre Umgebung die erforderlichen Berechtigungen und Konnektivität erfüllt.

- 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)
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:

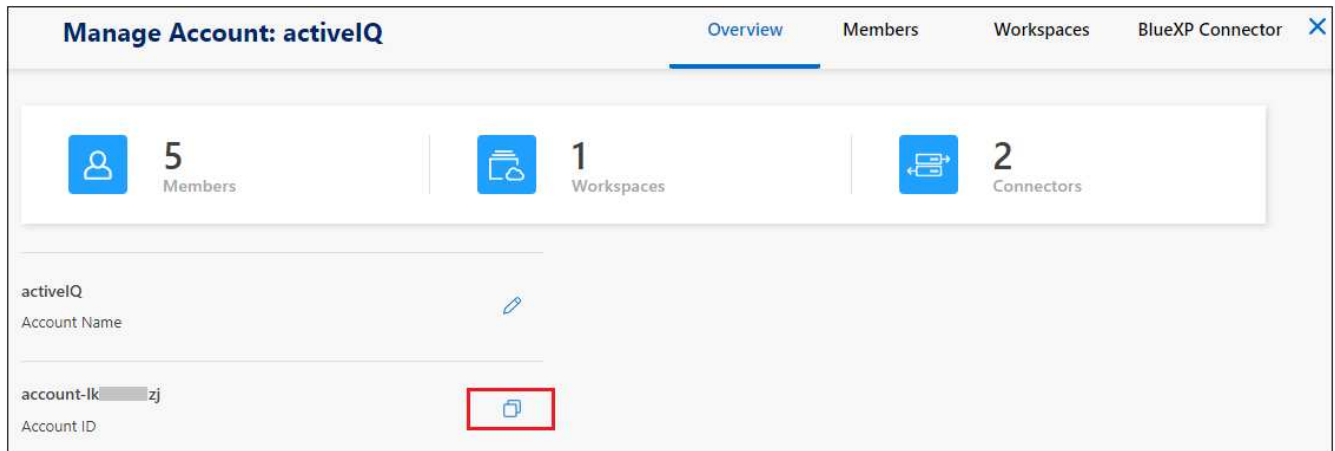
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp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

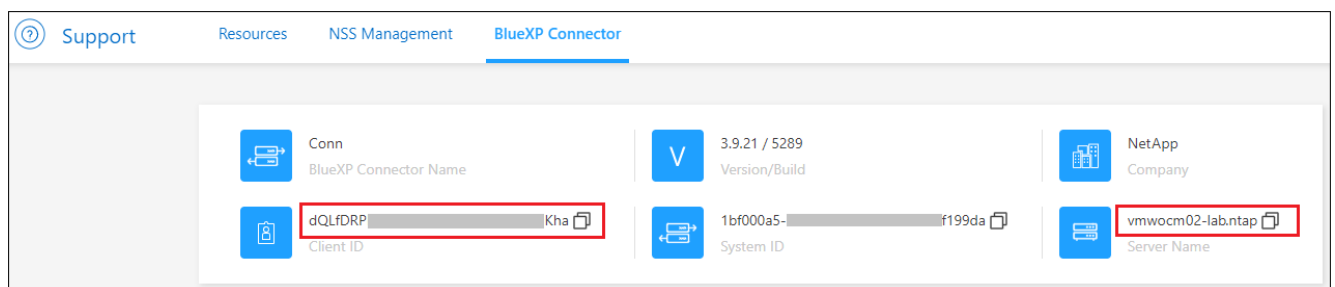
Erforderliche Schritte

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.

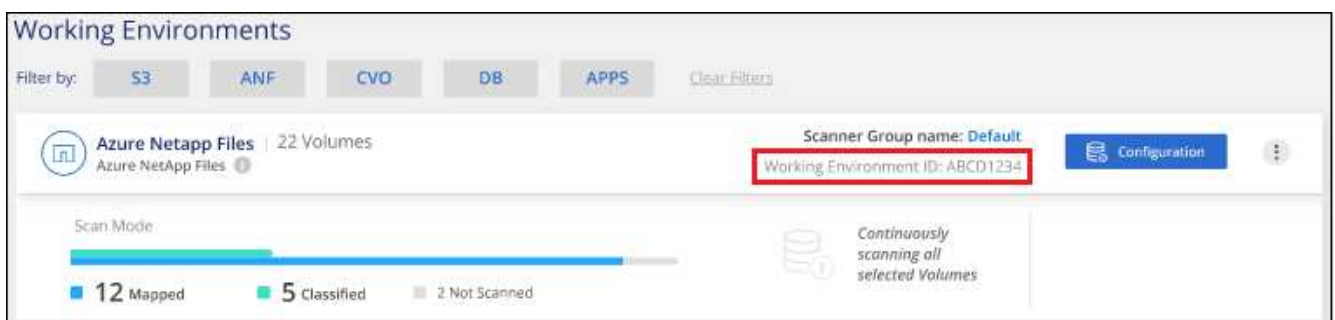
1. Klicken Sie in der Menüleiste von BlueXP auf **Konto > Konten verwalten**.



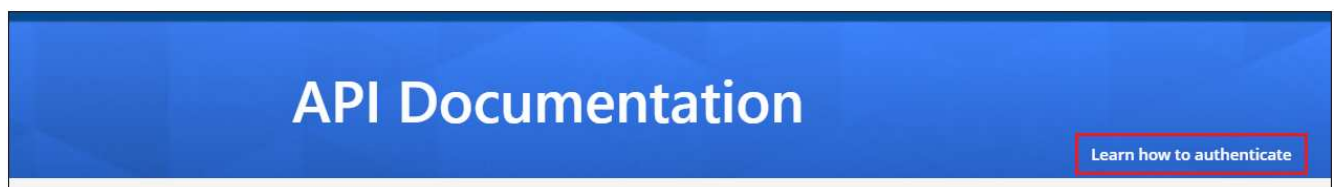
2. Kopieren Sie die *Konto-ID*.
3. Klicken Sie in der Menüleiste von BlueXP auf **Hilfe > Support > BlueXP Connector**.



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.

Scanner Groups Search 

Scanner Group: **Default**  Scanner nodes


2 Scanner nodes

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

Scanner Group: **United_States**  Scanner nodes

2 Scanner nodes

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

Scanner Group: **Europe**  Scanner nodes

Datenabschreibungen scannen

Scannen von Amazon S3 Buckets

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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

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

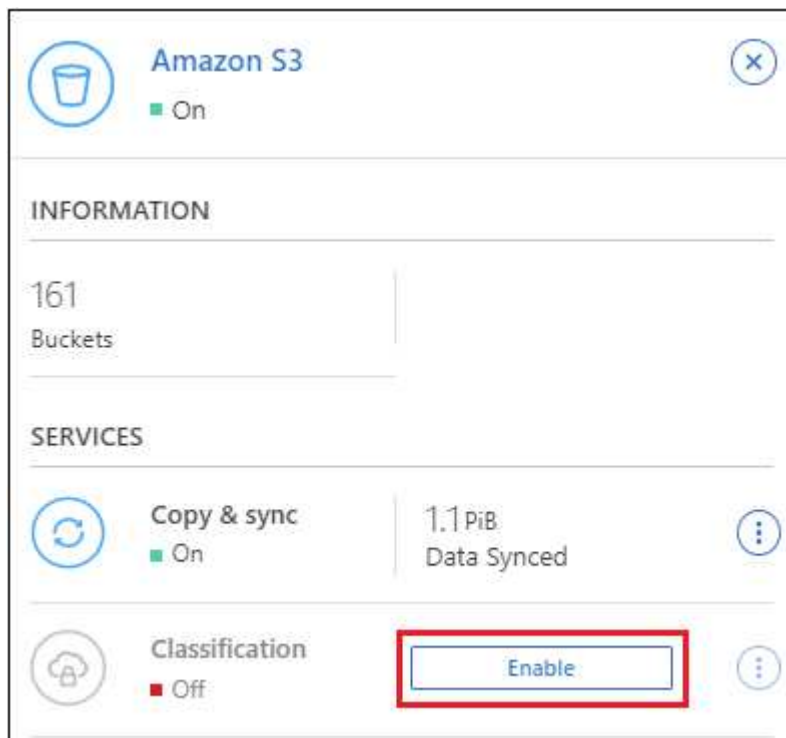
Aktivieren Sie die BlueXP Klassifizierung für Amazon S3, nachdem Sie die Voraussetzungen überprüft haben.

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](#).

Assign an AWS IAM Role for Data Sense & Compliance

To enable Data Sense & Compliance on Amazon S3 buckets, select an existing IAM Role. Make sure that your AWS IAM Role has the permission defined in the [Policy Requirements](#).

Select IAM Role

Select a Role


VPC Endpoint for Amazon S3 Required
 A VPC endpoint to the Amazon S3 service is required so Data Sense & Compliance can securely scan the data. Alternatively, ensure that the Data Sense & Compliance instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Free for the 1st TB
 Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable **Cancel**

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.

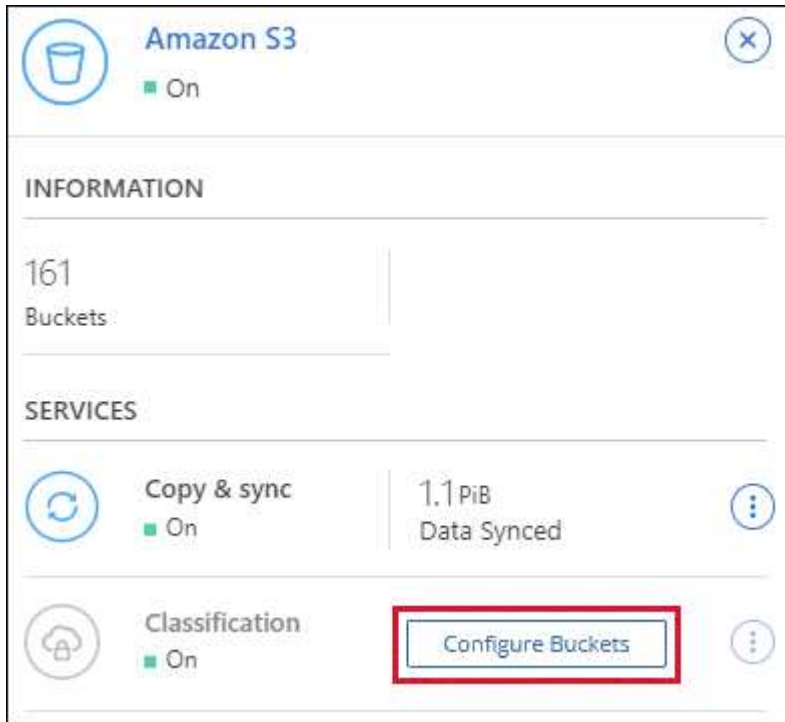
Wenn BlueXP im AWS Konto ausgeführt wird, das über die S3-Buckets verfügt, die Sie scannen möchten, erkennt es diese Buckets und zeigt sie in einer Amazon S3-Arbeitsumgebung an.

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.

Amazon S3 Configuration			
15/28 Buckets in Scan Scope.			
Scan	Bucket Name	Status	Required Action
Off Map Map & Classify	BucketName1	● Not Scanning	Add Credentials
Off Map Map & Classify	BucketName2	● Continuously Scanning	
Off Map Map & Classify	BucketName3	● Not Scanning	

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.

Create role



Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* ⓘ

- Options
- Require external ID (Best practice when a third party will assume this role)
 - Require MFA ⓘ

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.

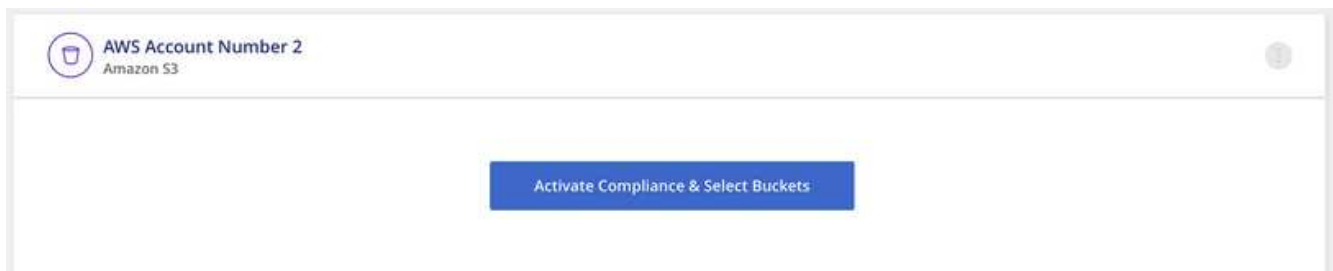
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

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.

Scannen Sie OneDrive-Konten

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

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

Schnellstart

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

1

Alle Voraussetzungen für OneDrive prüfen

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

2

Implementieren der BlueXP Klassifizierungsinstanz

["Implementieren Sie die BlueXP Klassifizierung"](#) Falls noch keine Instanz implementiert wurde.

3

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.

4

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".

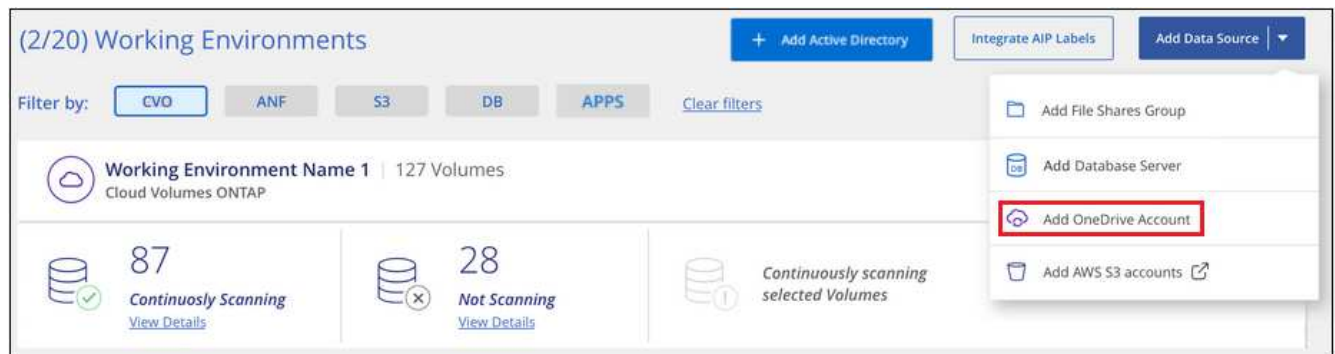
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

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.

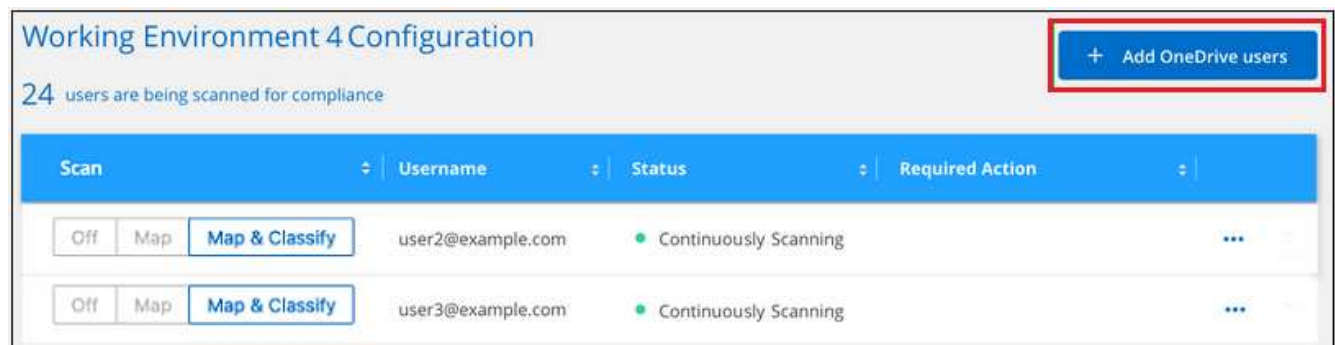


2. Wenn dies das erste Mal ist, Benutzer für dieses OneDrive-Konto hinzuzufügen, klicken Sie auf **Fügen Sie**

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.

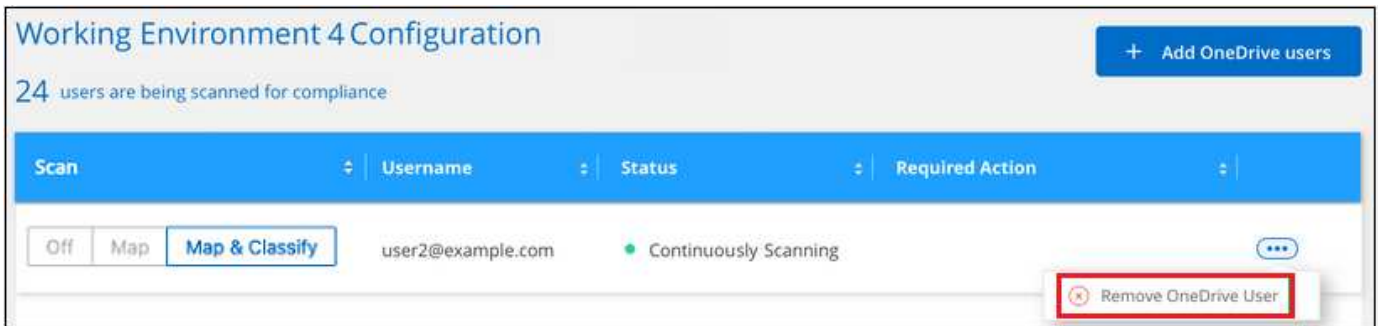
An:	Tun Sie dies:
Aktivieren Sie mappingonly Scans von Benutzerdateien	Klicken Sie Auf Karte
Aktivieren Sie vollständige Scans von Benutzerdateien	Klicken Sie Auf Karte & Klassieren
Deaktivieren Sie das Scannen von Benutzerdateien	Klicken Sie Auf Aus

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.



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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

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.

SharePoint-Anforderungen prüfen

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 ."](#)

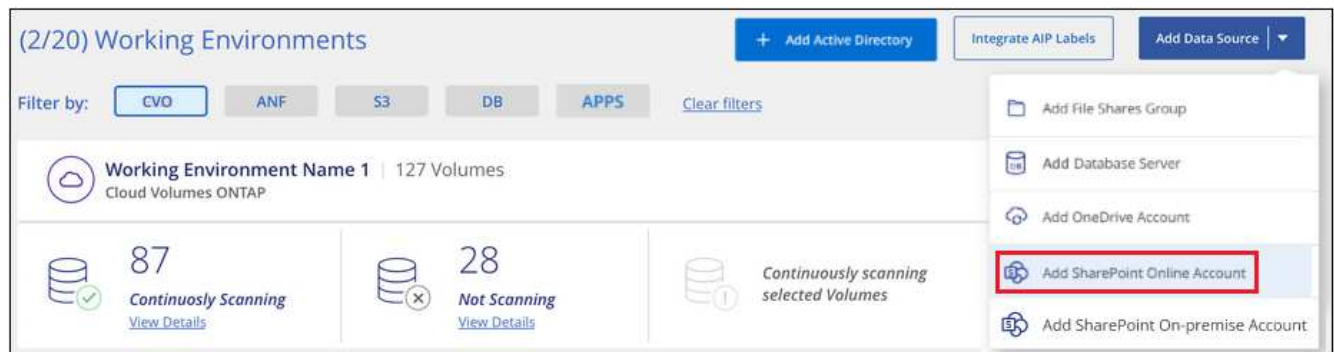
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Fügen Sie ein SharePoint Online-Konto hinzu

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.

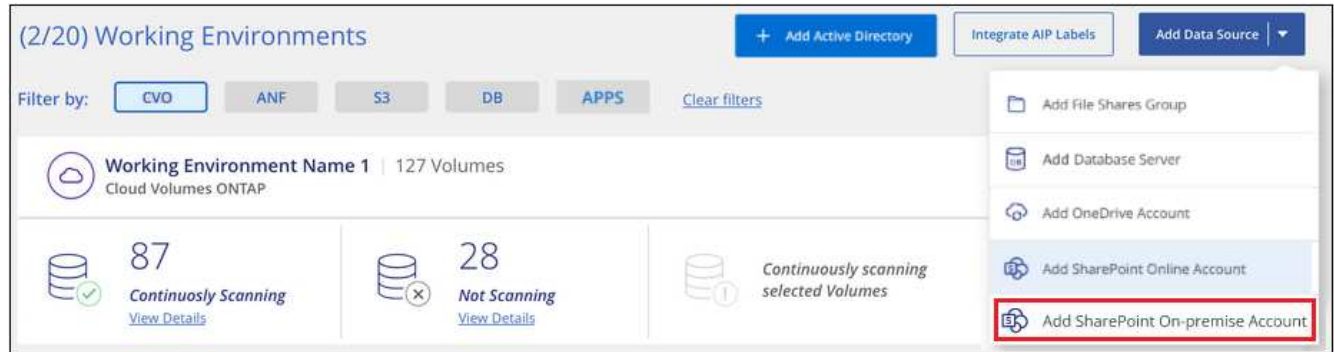
Das SharePoint Online-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

Fügen Sie ein SharePoint On-Premise-Konto hinzu

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

Log into the SharePoint On-Premises Server

To activate Data Sense on your SharePoint business account, sign in to SharePoint with an Admin user.

Username	Password
<input type="text" value="domain/user or user@domain"/>	<input type="password" value="Password"/>

URL

3. Klicken Sie Auf **Verbinden**.

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

Fügen Sie SharePoint-Sites zu Compliance-Scans hinzu

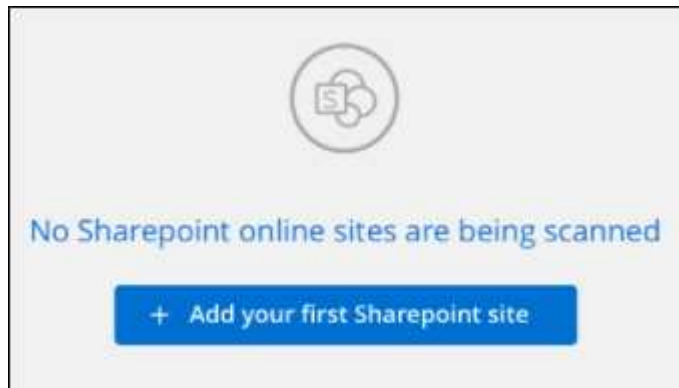
Sie können dem Konto einzelne SharePoint Sites oder bis zu 1,000 SharePoint Sites hinzufügen, sodass die zugehörigen Dateien durch die BlueXP Klassifizierung gescannt werden. Unabhängig davon, ob Sie SharePoint Online oder SharePoint On-Premise-Websites hinzufügen, sind die Schritte gleich.

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 Bestätigungsdiaologfeld 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 Sie eine 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.

Scan	Site URL	Status	Required Action
Off Map Map & Classify	Site URL	Continuously Scanning	Remove SharePoint Site
Off Map Map & Classify	Site URL	Continuously Scanning	

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.

Scannen Sie Google Drive-Konten

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

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

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 Sie die Google Drive-Anforderungen

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 Sie die 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"](#).

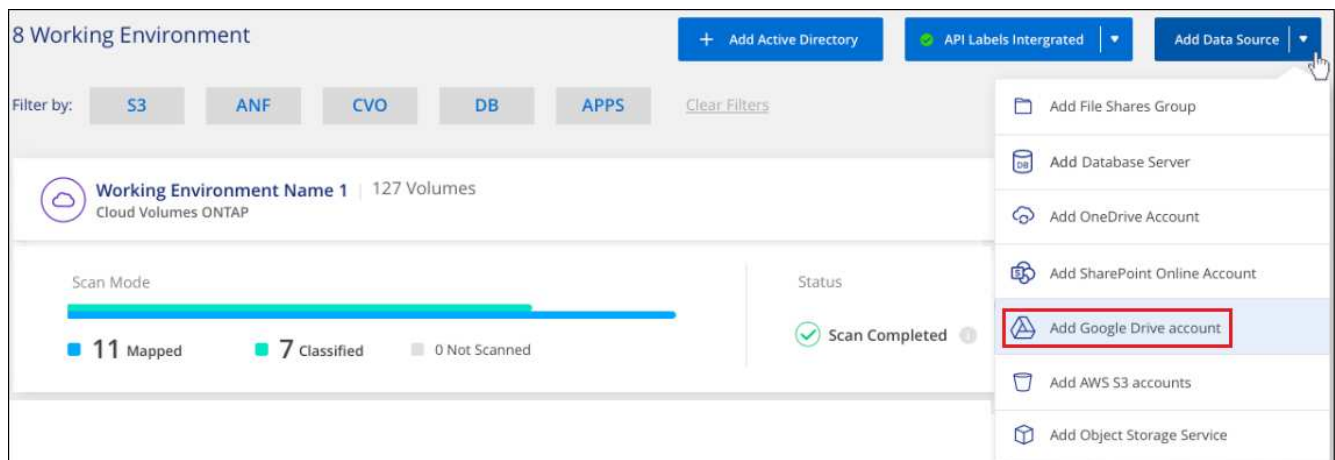
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Fügen Sie das Google Drive-Konto hinzu

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.

Wählen Sie den Typ der Suche nach Benutzerdaten aus

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 Sie ein Google Drive-Konto 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 Objekt-Storage mithilfe des S3-Protokolls

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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

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.

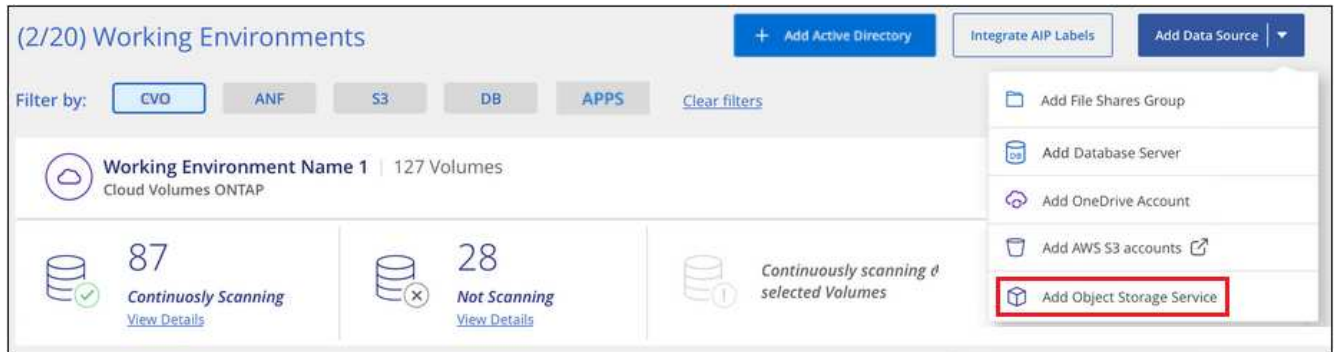
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

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.

Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKDO574NDJG86795"/>	<input type="password" value="....."/>

Ergebnis

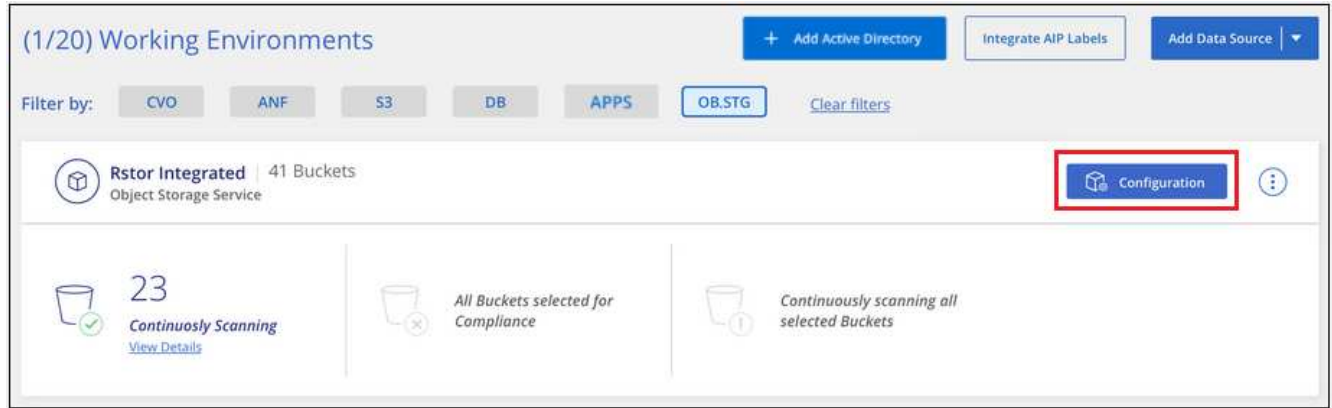
Der neue Objekt-Speicherdienst wird der Liste der Arbeitsumgebungen hinzugefügt.

Aktivieren und Deaktivieren von Compliance-Scans an Objekt-Storage-Buckets

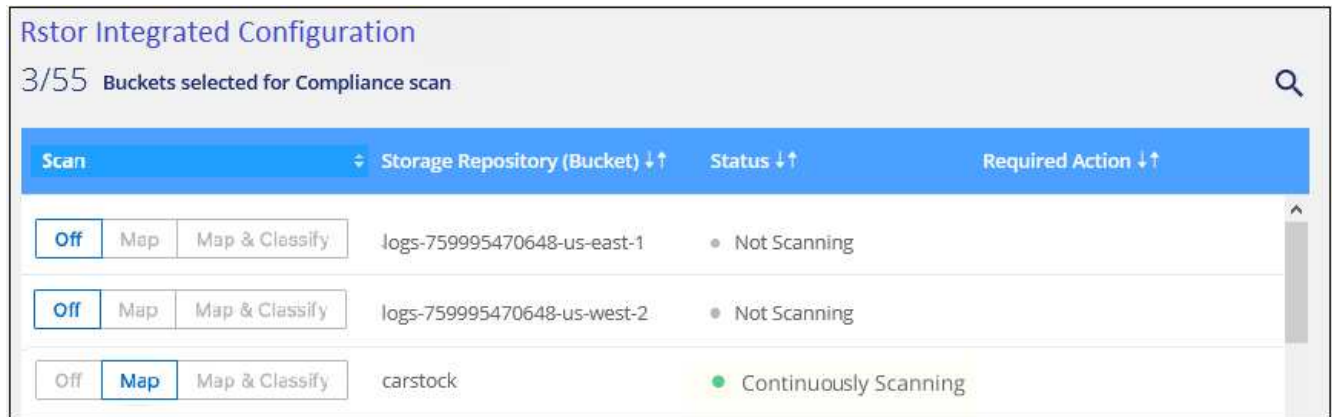
Nachdem Sie die BlueXP Klassifizierung für Ihren Objekt-Storage-Service aktiviert haben, müssen Sie im nächsten Schritt die Buckets konfigurieren, die Sie scannen möchten. Die BlueXP Klassifizierung erkennt diese Buckets und zeigt sie in der von Ihnen erstellten Arbeitsumgebung an.

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.

Datenabschreibungen verwalten

Zeigen Sie Governance-Details zu Ihren Daten über das Governance-Dashboard 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 zudem Daten von lokalen Speicherorten in die Cloud migrieren möchten, können Sie die Größe der Daten und auch prüfen, ob sensible Daten vor dem Verschieben enthalten sind.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

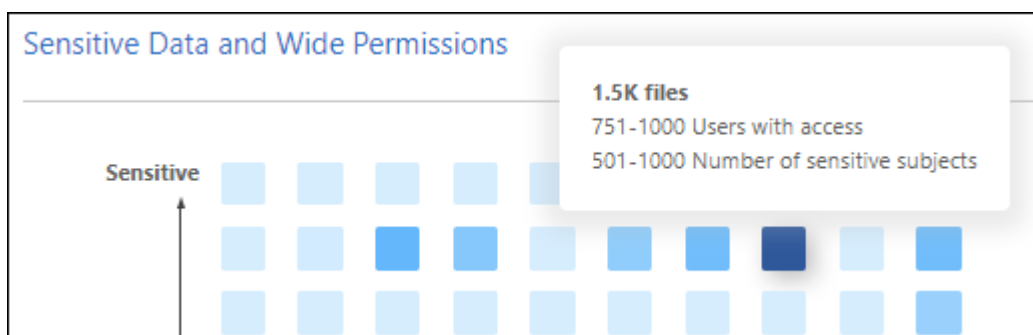
Daten, die im Governance-Dashboard nach Sensitivität und weiten Berechtigungen aufgelistet sind

Der Bereich *sensible Daten und weite Berechtigungen* auf dem Governance-Dashboard bietet eine Heatmap von Dateien, die sensible Daten (einschließlich sensibler und sensibler personenbezogener Daten) enthalten und übermäßig permissiv sind. So erkennen Sie, wo Sie möglicherweise Risiken mit sensiblen Daten haben.



Dies gilt für die BlueXP Klassifizierungsversionen 1.30 und früher.

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 QuickInfo-Text für den dunkelblauen Block angezeigt. Es zeigt, dass Sie 1,500 Dateien haben, auf die 751-1000 Benutzer zugreifen können und wo es 501-1000 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.

Klassifizierungsbereich auf dem Armaturenbrett mit AIP-Etiketten

Der Bereich *Classification* auf dem Dashboard enthält eine Liste der am häufigsten identifizierten AIP-Labels (Azure Information Protection) in Ihren gescannten Daten.

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.

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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant. Mit der Version Dezember 2023 (v1.26.6) wurde die Option zur Integration von Daten mit AIP-Labels (Azure Information Protection) aufgehoben.

- 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.
- 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

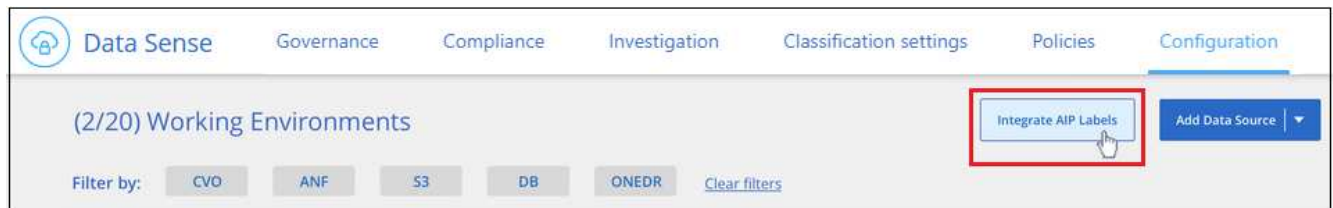
Bevor Sie AIP-Labels managen können, müssen Sie die AIP-Label-Funktionalität in die BlueXP Klassifizierung integrieren, indem Sie sich in Ihr bestehendes Azure Konto anmelden. Nach der Aktivierung können Sie AIP-Beschriftungen in Dateien für alle verwalten ["Datenquellen"](#) In Ihrem BlueXP Workspace.

Anforderungen

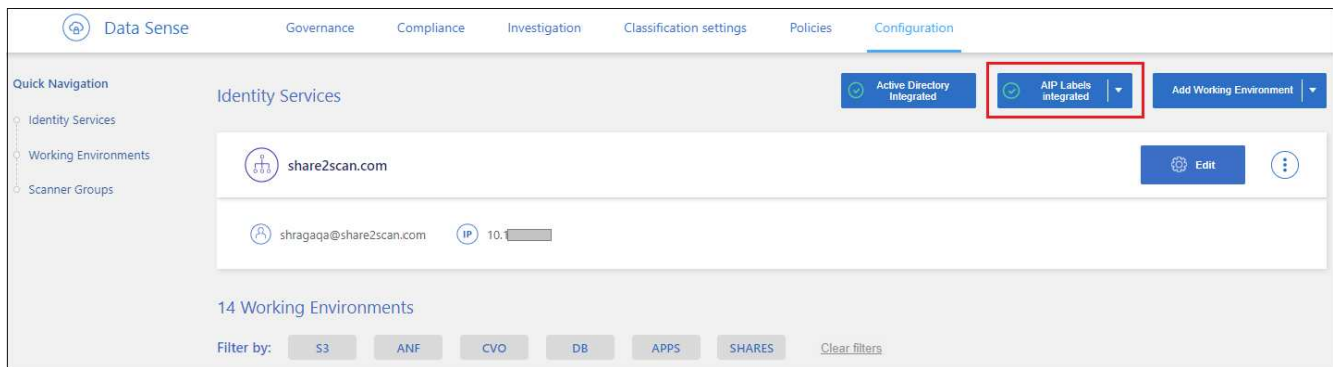
- Sie benötigen ein Konto und eine Azure Information Protection-Lizenz.
- Sie müssen die Anmeldedaten für das Azure-Konto besitzen.
- Wenn Sie Etiketten in Dateien ändern möchten, die in Amazon S3 Buckets gespeichert sind, stellen Sie die Berechtigung sicher `s3:PutObject` Ist in der IAM-Rolle enthalten. 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.




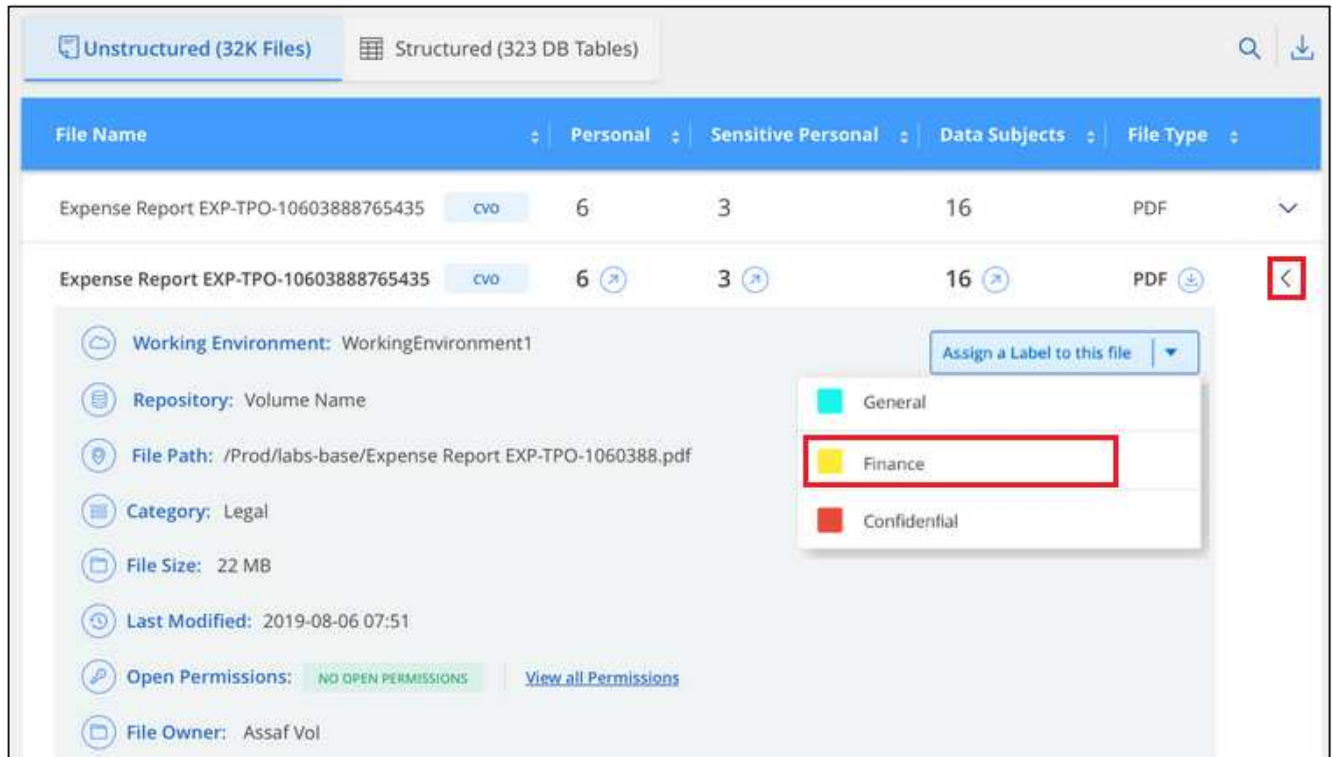
Weisen Sie AIP-Beschriftungen manuell zu

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 erweiteren 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.

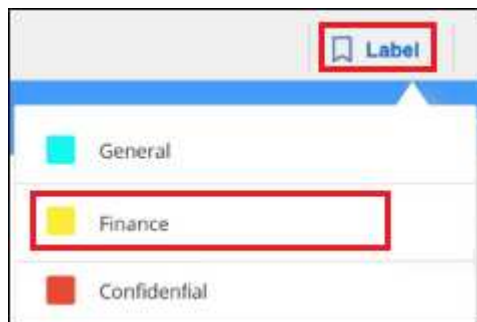
Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie beschriften möchten.

255 items 1.2 GB 2 Selected 3 MB							Tags	Assign to	Label	Copy	Move	Delete
<input type="checkbox"/> File Name	Personal	Sensitive Personal	Data Subjects	File Type								
<input checked="" type="checkbox"/> Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF							
<input checked="" type="checkbox"/> Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF							
<input type="checkbox"/> Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF							
<input type="checkbox"/> Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF							

- 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.

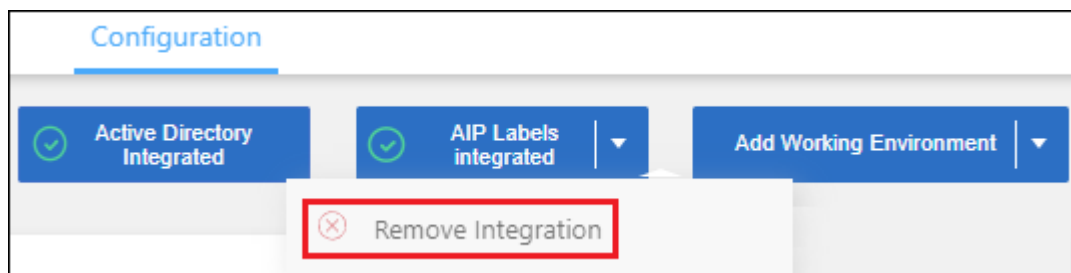
Entfernen Sie die AIP-Integration

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.

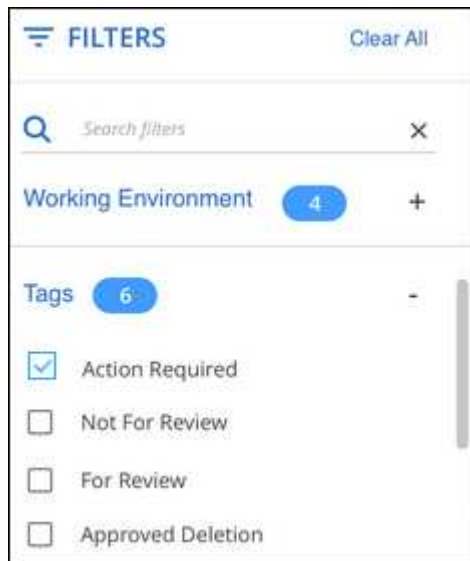


Die Tags, die Dateien in der BlueXP Klassifizierung zugewiesen sind, stehen nicht mit den Tags zusammen, die Sie zu Ressourcen wie Volumes oder Instanzen von Virtual Machines hinzufügen können. BlueXP Klassifizierungs-Tags werden auf Dateiebene angewendet.

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.

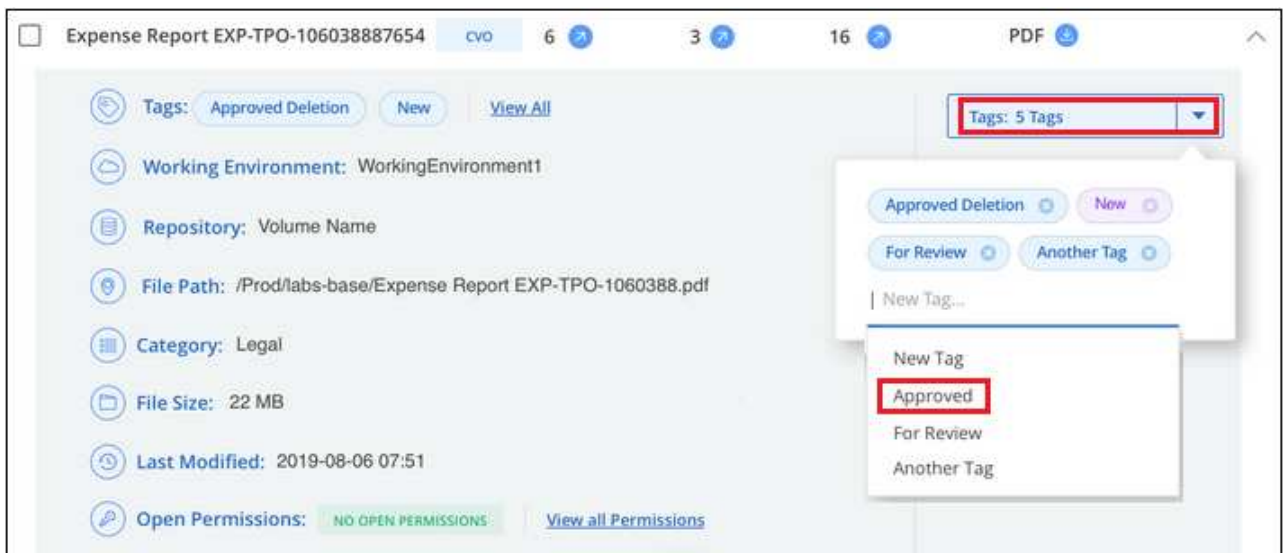
Weisen Sie Dateien Tags zu

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 erweiteren 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.

255 items 1.2 GB 2 Selected 3 MB							Tags	Assign to	Label	Copy	Move	Delete
<input type="checkbox"/>	File Name	Personal	Sensitive Personal	Data Subjects	File Type							
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF						
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF						
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF						
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF						

- 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).

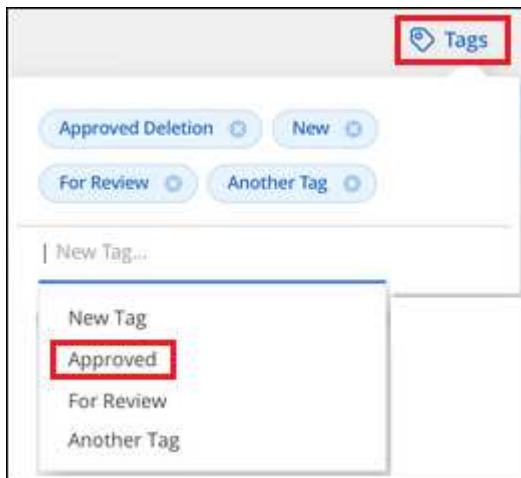
- Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (**File Name**), und dann in der Pop-up-Nachricht **All 20 Items on this page selected** [Select all Items in list \(63K Items\)](#) Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.

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 Bestätigungsdialegfeld, 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.

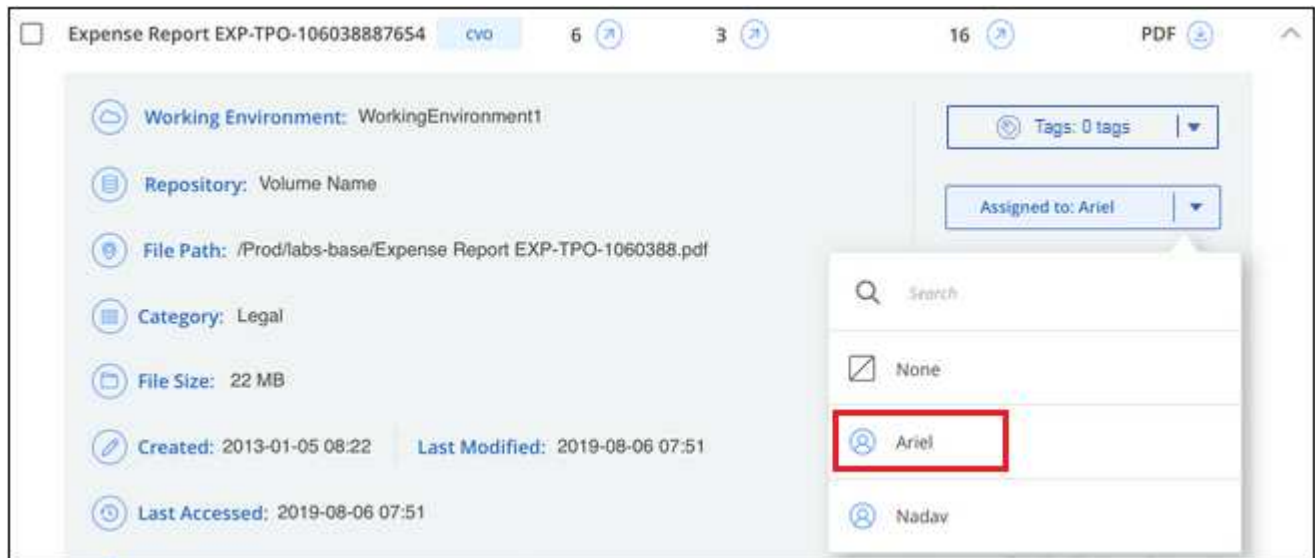
Beachten Sie, dass der Benutzername nicht als Teil der Datei-Metadaten zur Datei hinzugefügt wird. Er wird gerade von BlueXP Benutzern bei der Nutzung der BlueXP Klassifizierung gesehen.

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.

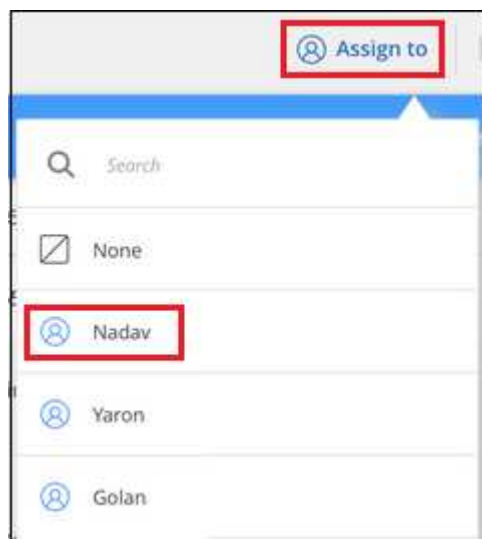
255 items 1.2 GB | 2 Selected 3 MB

Tags Assign to Label Copy Move Delete

<input type="checkbox"/>	File Name	Personal	Sensitive Personal	Data Subjects	File Type	
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF

- 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 Titelseite (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.

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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

- 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.

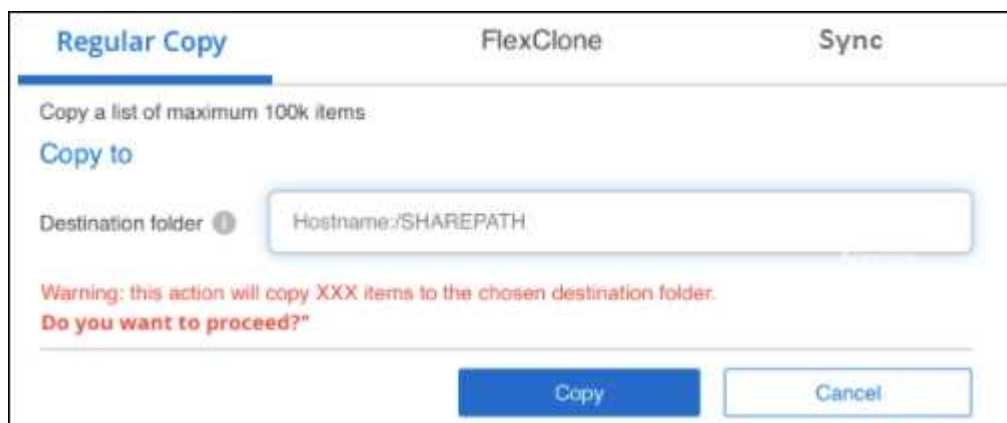
Schritte

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.

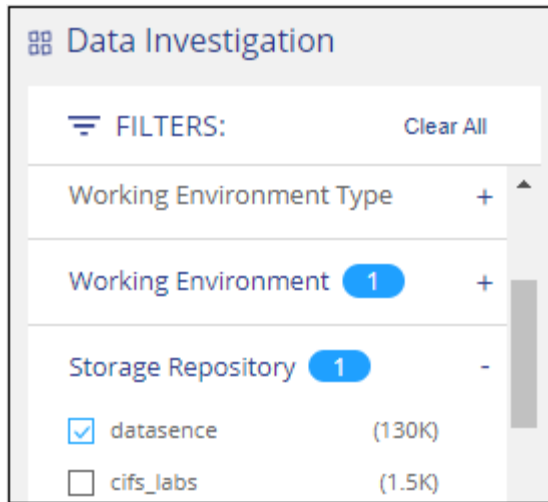
Hinweis: FlexGroup Volumes können nicht geklont werden, da sie nicht von FlexClone unterstützt werden.

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

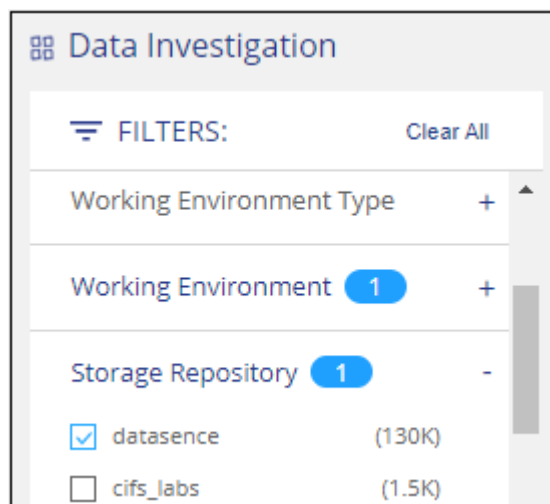
- Zum Kopieren und Synchronisieren von Dateien müssen Sie über die Rolle „Kontoadministrator“ oder „Arbeitsbereichsadministrator“ verfügen.

- 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.

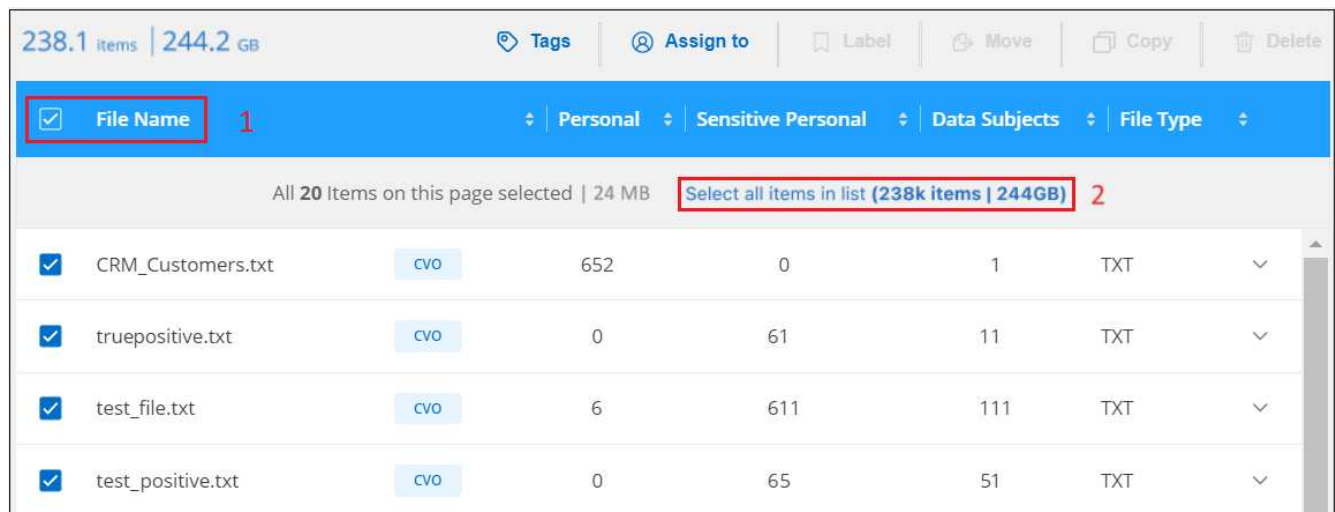
Schritte

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.

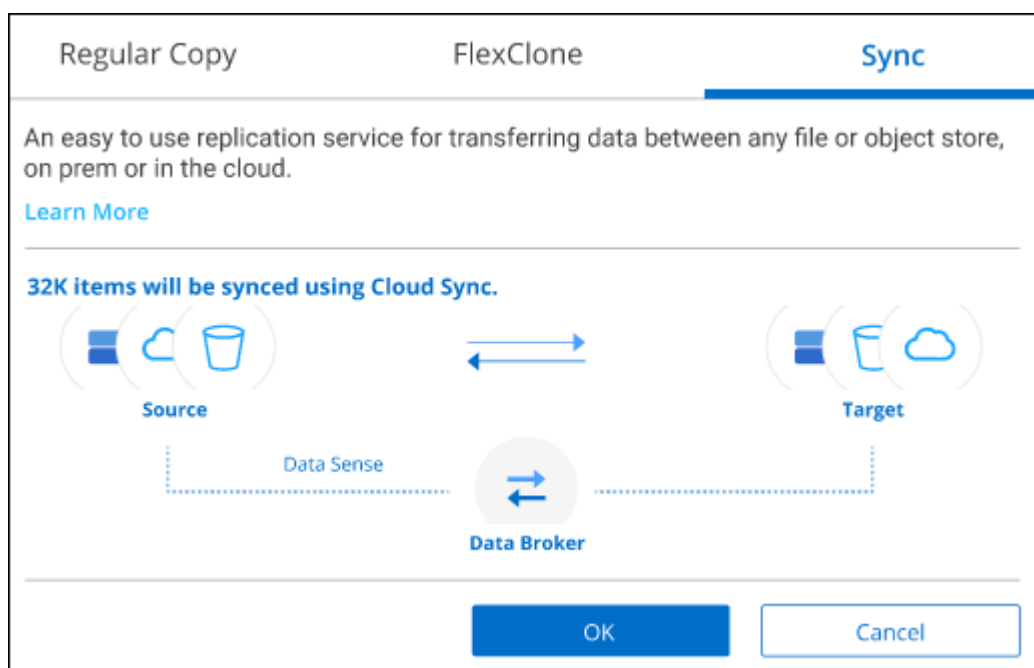


Wenden Sie alle anderen Filter an, sodass nur die Dateien zu sehen sind, die Sie kopieren und mit dem Zielsystem synchronisieren möchten.

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.

255 items 1.2 GB | 2 Selected 3 MB Tags Assign to Label Copy Move Delete

<input type="checkbox"/> File Name	Personal	Sensitive Personal	Data Subjects	File Type
<input checked="" type="checkbox"/> Expense Report EXP-TPO-106038887654 <small>cvo</small>	6	3	16	PDF
<input checked="" type="checkbox"/> Expense Report EXP-TPO-106038887654 <small>cvo</small>	6	3	6	PDF
<input type="checkbox"/> Expense Report EXP-TPO-106038887654 <small>cvo</small>	6	3	6	PDF
<input type="checkbox"/> Expense Report EXP-TPO-106038887654 <small>cvo</small>	6	3	6	PDF

- 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**.

📁 Move Files (63)

The files will be moved to the destination folder you provide and will no longer be available at their current location.

Moving files is supported only to destination folders in NFS Shares. Any NFS Share is supported, no matter where it is hosted, as long as the share's export policy allows access from the data connector instance IP address.

The status of this action will appear in the Action Status.

Enter the NFS destination folder path to continue

Hostname:/SHAREPATH

Leave breadcrumb

A breadcrumb file helps your users understand why a file was moved from its original location. For each moved file, the system creates a breadcrumb file in the source location named `<filename>-breadcrumb-<date>.txt`.

Enter the content of your breadcrumb

📘 Max length should be maximum 400 characters

Move Files

Cancel

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.

255 items 1.2 GB | 2 Selected 3 MB Tags Assign to Label Copy Move Delete

<input type="checkbox"/>	File Name	Personal	Sensitive Personal	Data Subjects	File Type	
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF

- 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**.

Unstructured (32K Files) | Structured (323 DB Tables)

<input type="checkbox"/>	File Name	Personal	Sensitive Personal	Data Subjects	File Type	
<input type="checkbox"/>	Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF

Working Environment: WorkingEnvironment1

Repository: Volume Name

File Path: /Prod/labs-base/Expense Report EXP-TPO-1060388.pdf

Assign a Label to this file

Delete this file

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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

- 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.

Databases -- Structured Data

Database: Oracle
Schema: Accounts
Table: Customers
Column: Customer ID

Account	Name	Customer ID	Address
1234	ABC Co	135876	125 Main St
1235	XYZ Co	213536	35A Brick R
1236	Cat Co	359264	55 Wind Av
1237	Dog Co	472637	11025 Cor
1238	Zebra Co	582455	36 Sahara
...

Scan your volumes and buckets for occurrences of the Customer IDs in your Oracle database

Files -- Unstructured Data

File in Volume 1

```
XXXXXXXXXXXXX  
xx213536xxx  
XXXXXXXXXXXXX  
xx472637xxx  
XXXXXXXXXXXXX  
XXXXXXXXXXXXX
```

File in Volume 2

```
XXXXXXXXXXXXX  
XXXXXXXXXXXXX  
XXXXXXXXXXXXX  
XXXXXXXXXXXXX  
XXXXXXXXXXXXX  
xxx472637xx
```

File in Bucket 1

```
XXXXXXXXXXXXX  
XXXXXXXXXXXXX  
xx213536xxx  
XXXXXXXXXXXXX  
XXXXXXXXXXXXX  
XXXXXXXXXXXXX
```

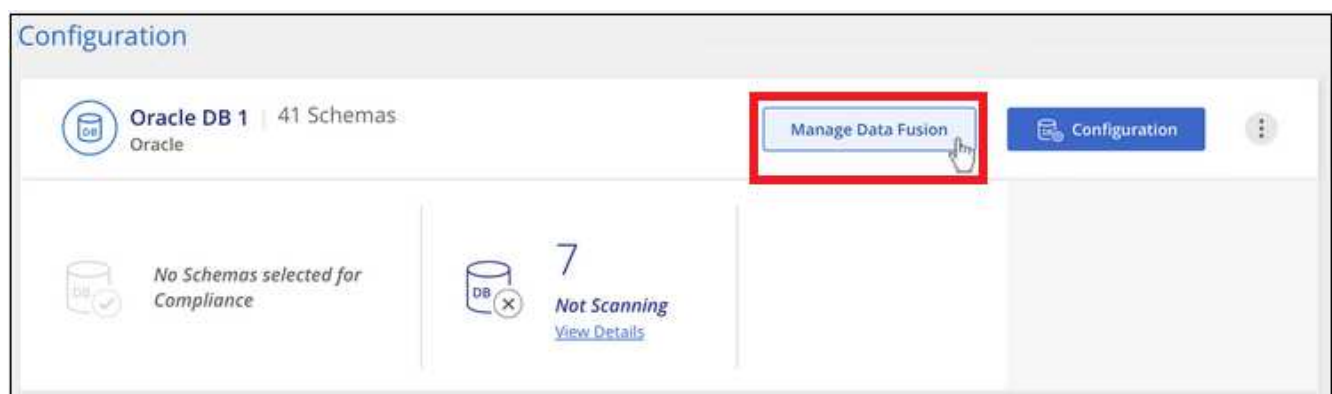
Wie Sie sehen, wurden in zwei Volumes und in einem S3-Bucket zwei eindeutige Kunden-IDs gefunden. Alle Übereinstimmungen in Datenbanktabellen werden ebenfalls identifiziert.

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.

Add Data Fusion Source

To add a Data Fusion source reference, specify one or more columns which contain your organization's unique identifiers, such as a column used to store customer IDs.

Note that adding a Data Fusion Source will initiate an additional scan of your data stores.

Database Schema

Table

Columns Containing Identifiers ⓘ

4. Klicken Sie Auf **Data Fusion-Quelle Hinzufügen**.

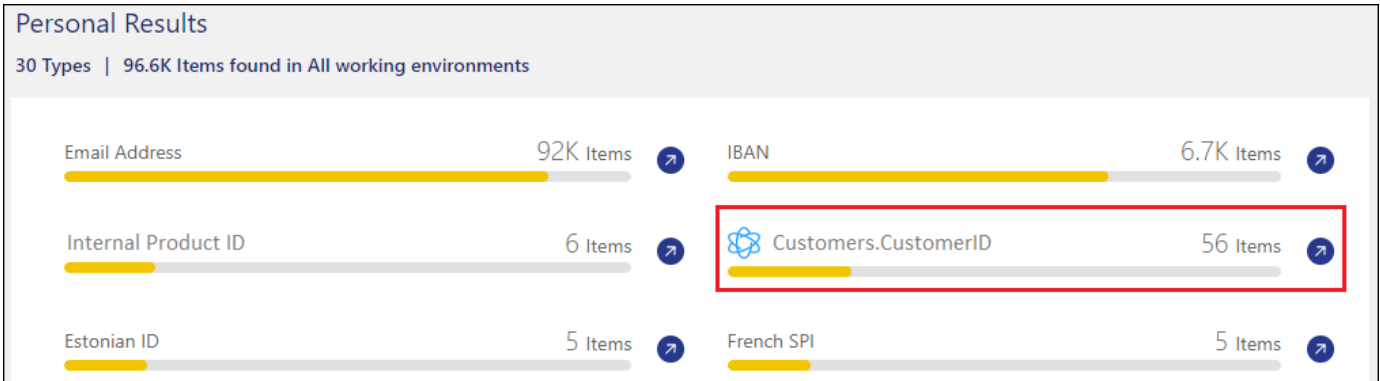
Oracle DB 1 Data Fusion + Add Data Fusion source

With Data Fusion, Data Sense can identify occurrences of your organization's unique identifiers found in your unstructured data stores, using structured data indexes containing those unique identifiers as a source reference. [Learn More](#)

Database Schema	Table	Data Fusion Source Columns	
Schema1	Table 1	Column 12, Column 4, Column 18	⋮
Schema2	Table 2	Column 2, Column 14, Column 8	⋮

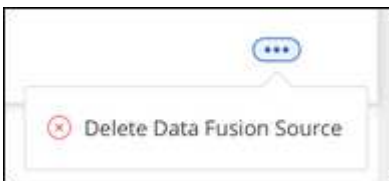
Ergebnisse

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

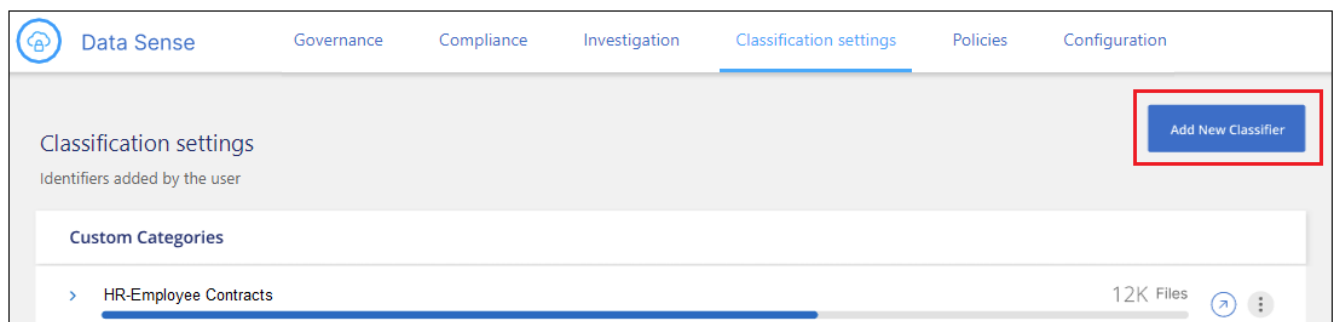
Sie können der BlueXP Klassifizierung benutzerdefinierte Schlüsselwörter hinzufügen, um den Speicherort der Daten bestimmen zu können. Fügen Sie die Schlüsselwörter einfach ein, indem Sie jedes Wort eingeben, das die BlueXP Klassifizierung wiedererkennen soll. Die Schlüsselwörter werden zu den vorhandenen 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).

1 Select type 2 Select tool 3 Create Logic

Select type

Select the type of classifier that you want to add to the system, and provide the name and description. Data Sense re-scans all your data sources after you add a new classifier. When the scan is complete, all matching results are displayed in the "Classification Settings" dashboard and in other Data Sense pages.

Classifier name

Internal Product Names

Description

Identify internal product names found in all files

Personal identifier

The classifier will be added to the system as a new personal identifier. Any matches are considered "personal data", and they are added to the results that are displayed in the Personal Results page and in the Investigation page. [See the list of personal data that Data Sense identifies by default.](#)

Mask detected results in the system

Category

The classifier will be added to the system as a new Category. Any matches are added to the results that are displayed in the Categories page and in the Investigation page. [See the list of categories that Data Sense identifies by default.](#)

Previous Next

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**.

Select Data Analysis Tool

Select the tool that will be used to build the list of words, or patterns, that Data Sense will attempt to match in your data sources.

Custom keywords ⓘ
Create a custom personal pattern based on a list of keywords that you provide.

Custom regular expression ⓘ
Create a custom personal pattern based on a regular expression that you define.

DB fusion ⓘ
Create a custom personal pattern based on the values found in specific columns in your scanned database tables. This allows you to identify whether unique identifiers from your databases are found in any of your other data sources.

[Previous](#) [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.

Create Logic

Create logic for the new identifier, based on regular expression and keywords that should be detected. You will be able to change the logic in the future, by clicking on "edit" from the custom classification dashboard.

Custom keywords list ⓘ

- Maximum of 100,000 words.
- Separate between keywords with a new line
- The keywords are not case sensitive
- Each word must be at least 3 characters long. Shorter words are ignored.
- Duplicate words are only added once.

barred
barn
horned
snowy
screech

Validate

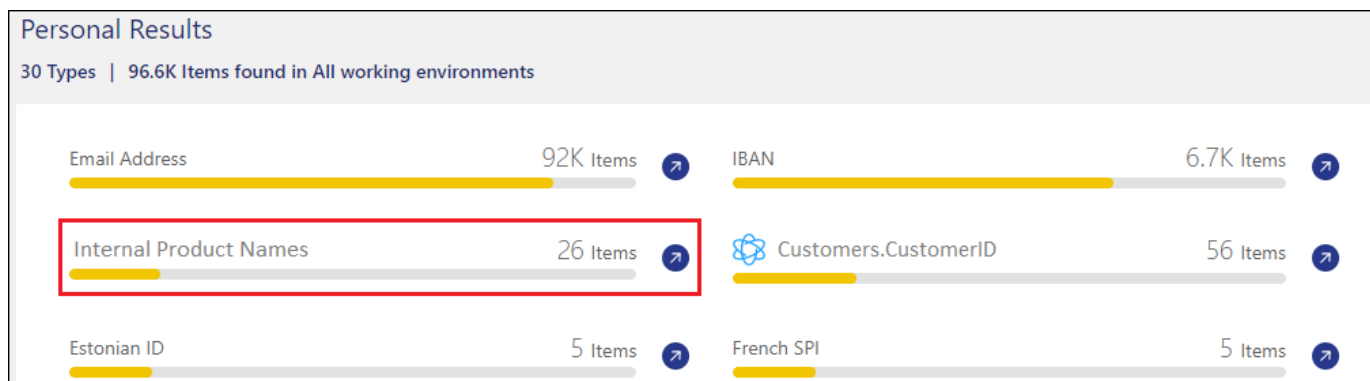
✔ Keywords list is **valid**.

Previous
Done

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 Regexp erstellen, um neue persönliche Informationselemente zu identifizieren, die noch nicht im System vorhanden sind. Der Regexp 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 Regexp-Funktion verwenden, um sie in Ihren Dateien zu suchen. Der reguläre Ausdruck für dieses Beispiel lautet `\b201\d{9}\b`.

Nach Hinzufügen des Regexp 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.

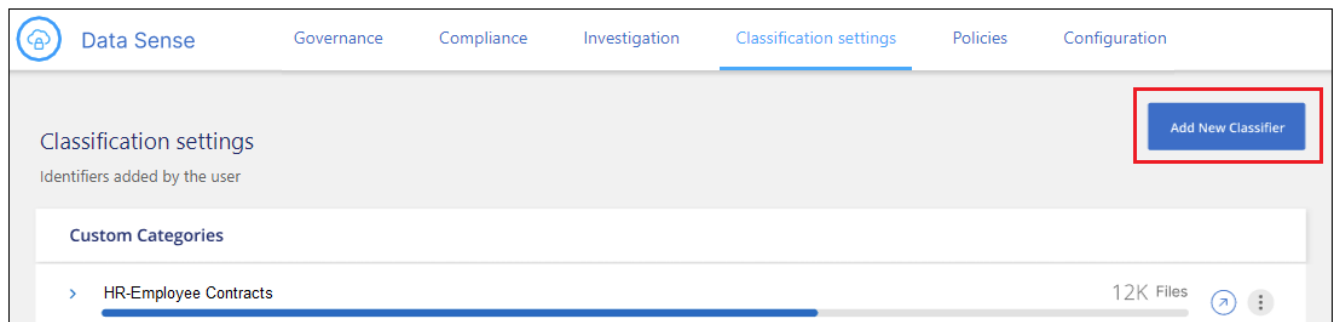
Wenn Sie beim Erstellen des regulären Ausdrucks Hilfe benötigen, lesen Sie ["Reguläre Ausdrücke 101"](#). Wählen Sie **Python** für den Geschmack, um zu sehen, welche Arten von Ergebnissen die BlueXP-Klassifikation vom regulären Ausdruck entspricht. Der ["Seite „Python Regexp Tester“"](#) ist auch nützlich, indem Sie eine grafische Darstellung Ihrer Muster anzeigen.



Derzeit erlauben wir die Verwendung von Pattern Flags beim Erstellen eines Regexp 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.

1 Select type 2 Select tool 3 Create Logic

Select type

Select the type of classifier that you want to add to the system, and provide the name and description. Data Sense re-scans all your data sources after you add a new classifier. When the scan is complete, all matching results are displayed in the "Classification Settings" dashboard and in other Data Sense pages.

Classifier name

Internal Product ID

Description

Identify internal product IDs found in all files

Personal identifier

The classifier will be added to the system as a new personal identifier. Any matches are considered "personal data", and they are added to the results that are displayed in the Personal Results page and in the Investigation page. [See the list of personal data that Data Sense identifies by default.](#)

Mask detected results in the system

Category

The classifier will be added to the system as a new Category. Any matches are added to the results that are displayed in the Categories page and in the Investigation page. [See the list of categories that Data Sense identifies by default.](#)

Previous Next

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**.

Select Data Analysis Tool

Select the tool that will be used to build the list of words, or patterns, that Data Sense will attempt to match in your data sources.

Custom keywords ⓘ
Create a custom personal pattern based on a list of keywords that you provide.

Custom regular expression ⓘ
Create a custom personal pattern based on a regular expression that you define.

DB fusion ⓘ
Create a custom personal pattern based on the values found in specific columns in your scanned database tables. This allows you to identify whether unique identifiers from your databases are found in any of your other data sources.

[Previous](#) [Next](#)

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 Annäherungswörter 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.

Create Logic

Create logic for the new identifier, based on regular expression and keywords that should be detected.

Regular expression ⓘ

Add the pattern that should be detected to identify specific information in your data, using a custom regular expression.

Validate

✓ **Success:** Regular expression is valid.

Proximity words - To improve the detection accuracy, insert phrases that must appear near by the regular expression's match.

Previous
Done

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.

🏠 Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration

Classification settings

Add New Classifier

Identifiers added by the user

Custom Categories

> HR - Employee Contracts
7.5K Files
↗ ⋮

Personal information

> Internal Product ID
12K Files
↗ ⋮

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

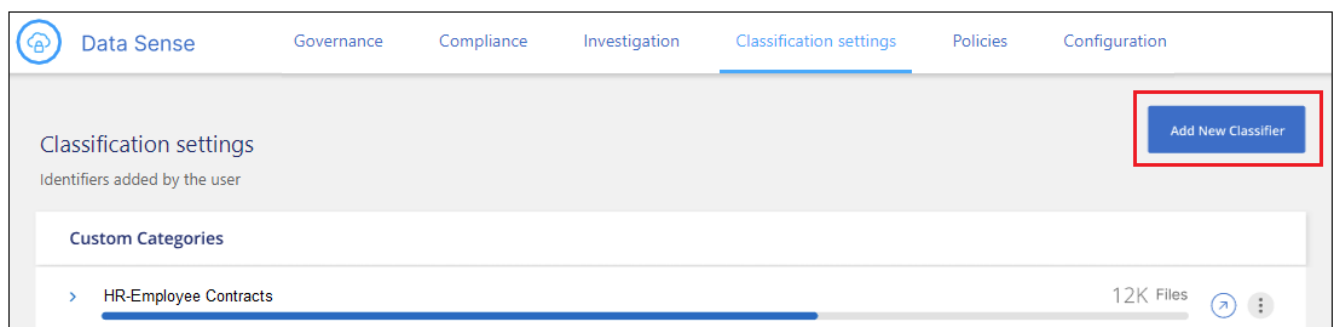
Sie müssen mindestens 25 Trainingsdateien erstellen, die Beispiele für die Datenkategorien enthalten, die von der BlueXP Klassifizierung erkannt werden sollen. Die folgenden Dateitypen werden unterstützt:

.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.

1 Select type 2 Select tool 3 Create Logic

Select type

Select the type of classifier that you want to add to the system, and provide the name and description. Data Sense re-scans all your data sources after you add a new classifier. When the scan is complete, all matching results are displayed in the "Classification Settings" dashboard and in other Data Sense pages.

Classifier name

Description

Personal identifier

The classifier will be added to the system as a new personal identifier. Any matches are considered "personal data", and they are added to the results that are displayed in the Personal Results page and in the Investigation page. [See the list of personal data that Data Sense identifies by default.](#)

Mask detected results in the system

Category

The classifier will be added to the system as a new Category. Any matches are added to the results that are displayed in the Categories page and in the Investigation page. [See the list of categories that Data Sense identifies by default.](#)

3. Stellen Sie auf der Seite *Create Logic* sicher, dass Sie die Lerndateien vorbereitet haben, und klicken Sie dann auf **Select files**.

Create Logic

AI-based similarity training ⓘ

- Insert NFS folder path
- The folder should contain minimum 25 files and maximum 1000 files that will be used for the AI training.
- Supported file types: pdf, docx, doc, pptx, xls,xlsx, csv, txt, gz, rtf, docs, sheets, slides, json
- The keywords are not case sensitive
- Minimum file size: 100B

Compressed Installer files

4. Geben Sie die IP-Adresse des Volumes und den Pfad ein, in dem sich die Trainingsdateien befinden, und klicken Sie auf **Hinzufügen**.

Insert folder path that contains at least 25 files for the training

Enter the IP address and volume name, along with the path to the location of the training files.

IP:

Training Data - Folder path:

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**.

Create Logic

AI-based similarity training

- Insert NFS folder path
- The folder should contain minimum 25 files and maximum 1000 files that will be used for the AI training.
- Supported file types: pdf, docx, doc, pptx, xls, xlsx, csv, txt, gz, rtf, docs, sheets, slides, json
- The keywords are not case sensitive
- Minimum file size: 100B

Compressed Installer files

Total uploaded files: 54

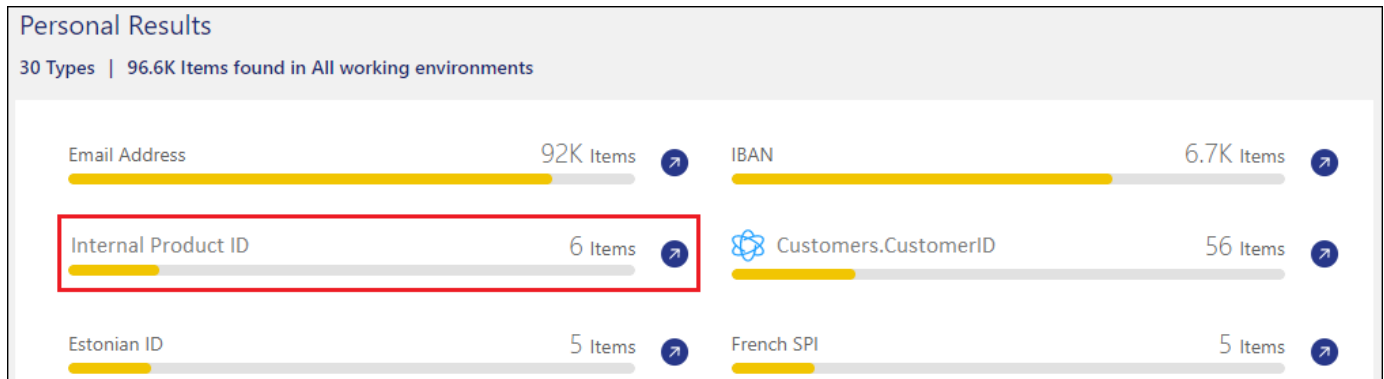
File name	File Size	File Type	Reliability	included in training
File1	56	File type	Sufficient	x
File2	22	File type	Sufficient	x
File3	43	File type	Sufficient	x
File4	11	File type	Sufficient	x


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.

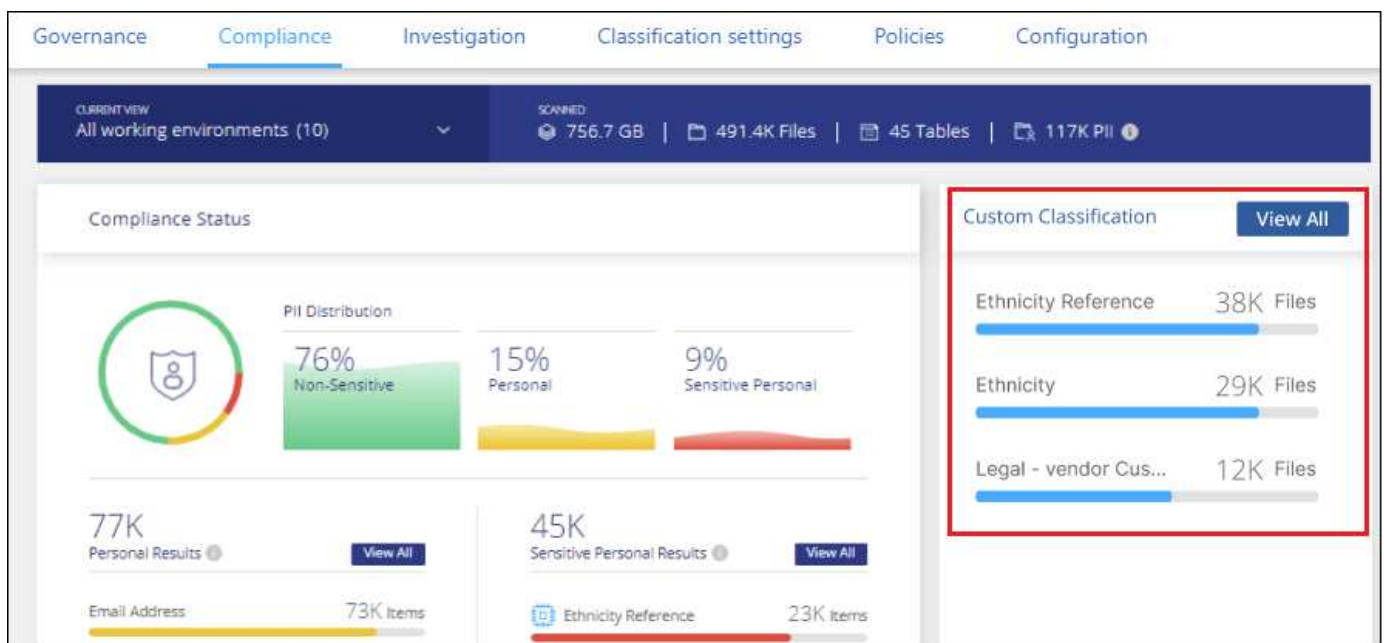
Ergebnisse von Ihren benutzerdefinierten Klassifikatoren anzeigen

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.

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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

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.

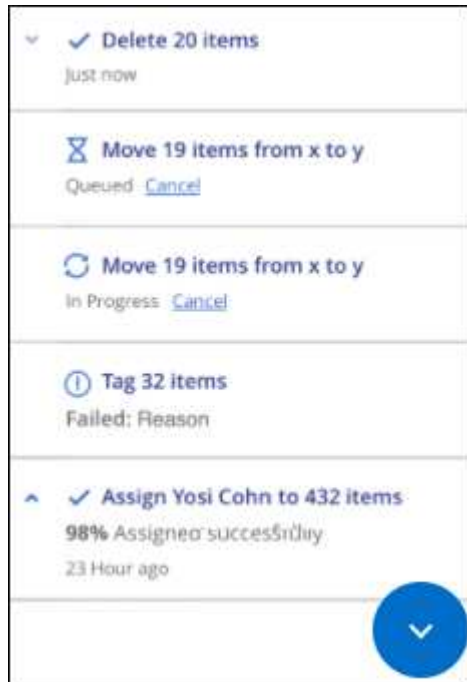
Schritte

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.

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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

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/dopl/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.

HINWEIS Diese Informationen sind nur für die BlueXP-Klassifikation der älteren Versionen 1.30 und früher relevant.

Schritte

1. Bewegen Sie den Schieberegler von unten auf der Seite *Configuration* nach rechts, um den langsamen Scan zu aktivieren.

The screenshot shows the '6 Working Environments' configuration page. At the bottom left, there is a toggle switch labeled 'Activate Slow Scan' which is currently turned on (indicated by a blue circle). The page displays two Amazon S3 buckets with their respective scanning status: 5 buckets are 'Continuously Scanning', 17 are 'Not Scanning', and the status for all selected buckets is 'Continuously scanning all selected Buckets'.

Oben auf der Konfigurationsseite wird angezeigt, dass die langsame Messung aktiviert ist.


The screenshot shows the '6 Working Environments' configuration page. At the top right, a notification banner reads 'Slow Scan enabled - Disable', which is highlighted with a red box. The rest of the page content is identical to the previous screenshot, showing the bucket scanning status and the 'Activate Slow Scan' toggle.

2. Sie können das langsame Scannen deaktivieren, indem Sie in dieser Meldung auf **Deaktivieren** klicken.

Entfernen Sie ein OneDrive-, SharePoint- oder Google Drive-Konto 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 Bestätigungsdiaologfeld auf **Konto löschen**.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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