Datenabschreibungen scannen

BlueXP classification

NetApp
June 14, 2024

This PDF was generated from https://docs.netapp.com/de-de/bluexp-classification/task-scanning-s3.html on June 14, 2024. Always check docs.netapp.com for the latest.

Inhalt

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.

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.

Implementieren der BlueXP Klassifizierungsinstanz

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

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.

Wählen Sie die zu scannenden Buckets aus

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

Überprüfen der S3-Voraussetzungen

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

Richten Sie eine IAM-Rolle für die BlueXP Klassifizierungsinstanz ein

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

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

Konnektivität von der BlueXP Klassifizierung bis zu Amazon S3

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

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

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

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

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

Implementieren der BlueXP Klassifizierungsinstanz

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

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

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

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

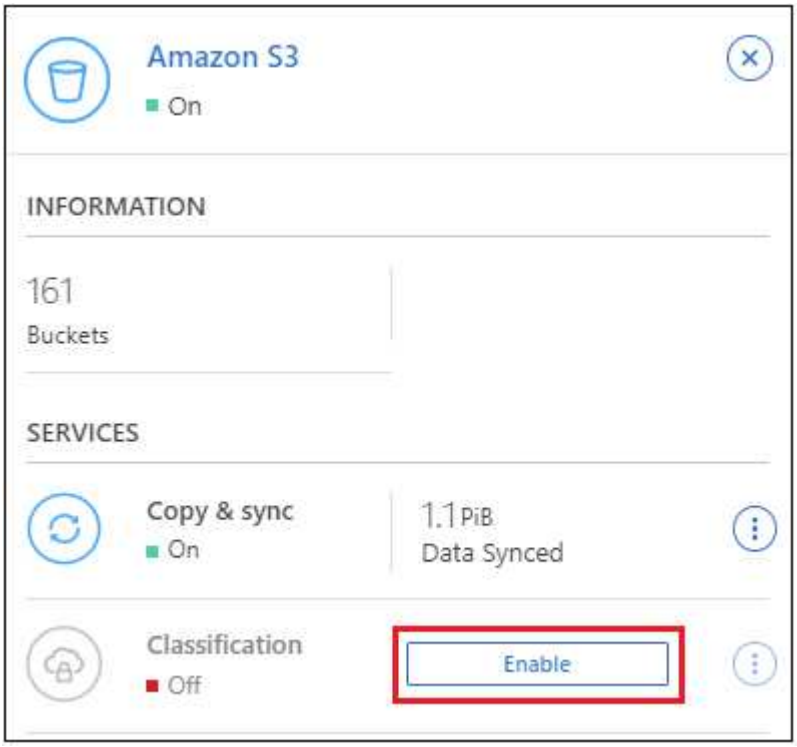
Aktivierung der BlueXP Klassifizierung in Ihrer S3-Arbeitsumgebung

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

Schritte

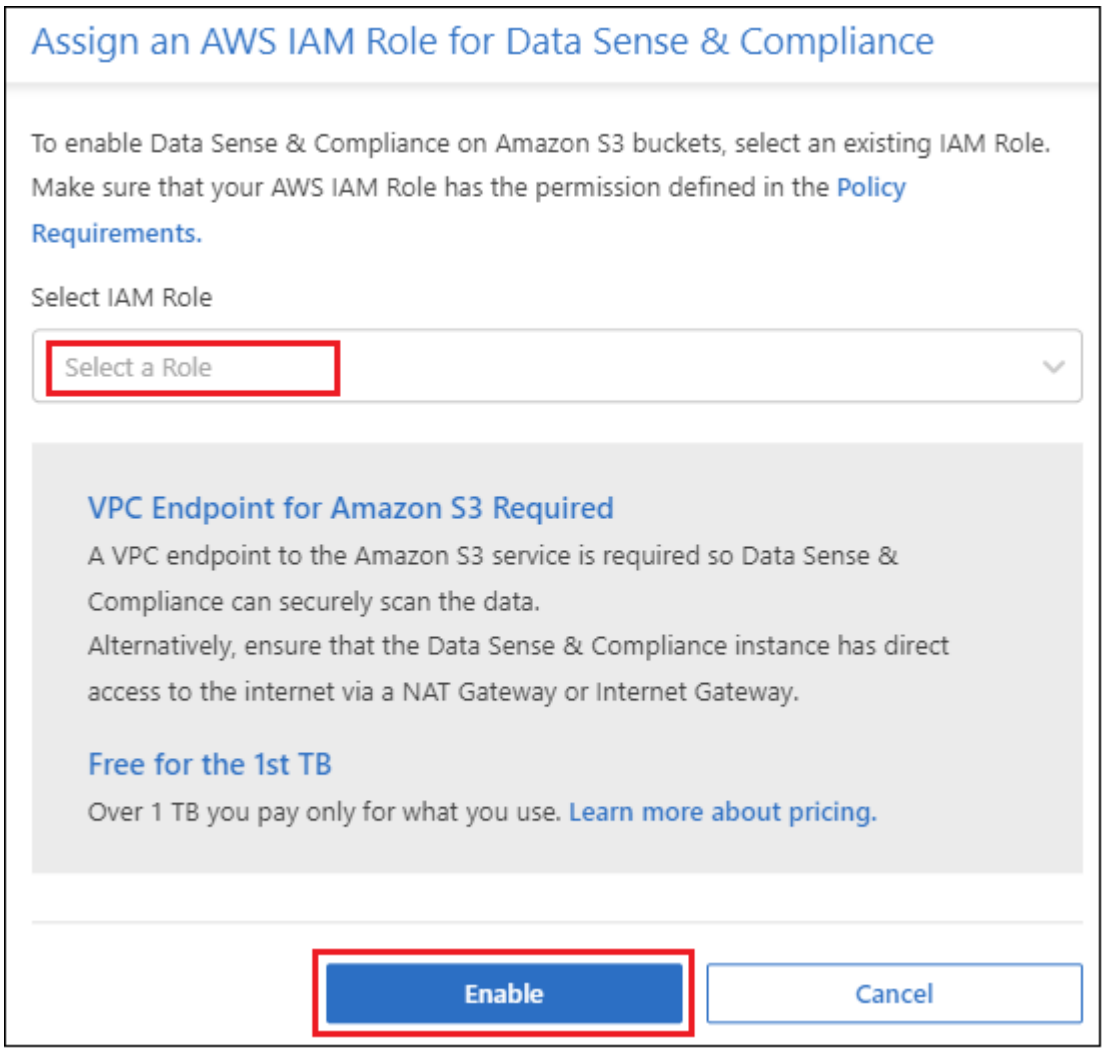
1. Klicken Sie im Navigationsmenü von BlueXP links auf **Speicherung > Leinwand**.
2. Wählen Sie die Amazon S3-Arbeitsumgebung aus.

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



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

erforderlichen Berechtigungen.



5. Klicken Sie Auf **Aktivieren**.

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

Ergebnis

BlueXP weist der Instanz die IAM-Rolle zu.

Aktivieren und Deaktivieren von Compliance-Scans auf S3-Buckets

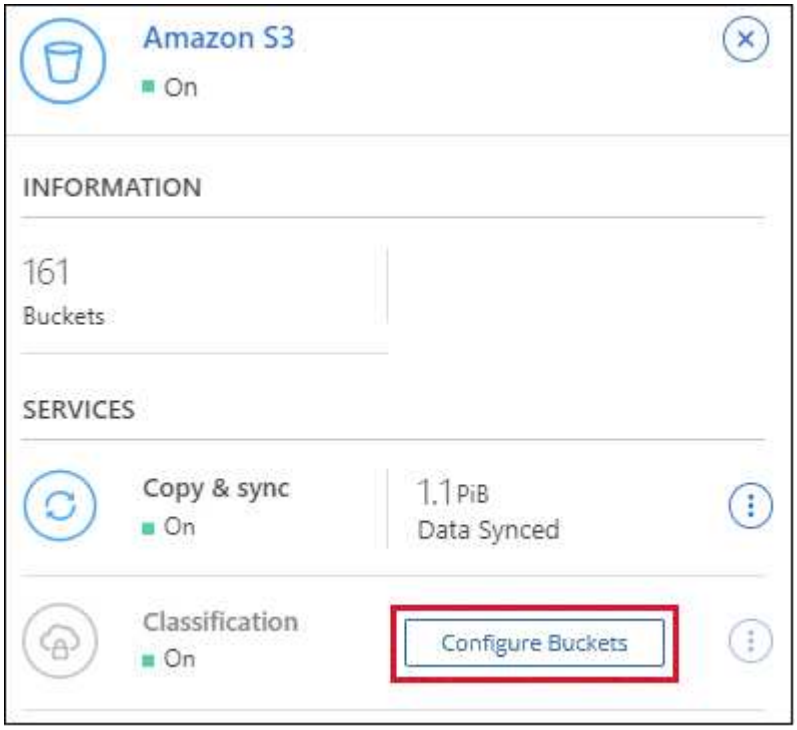
Nachdem BlueXP die BlueXP Klassifizierung für Amazon S3 aktiviert hat, müssen die zu scannenden Buckets konfiguriert werden.

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

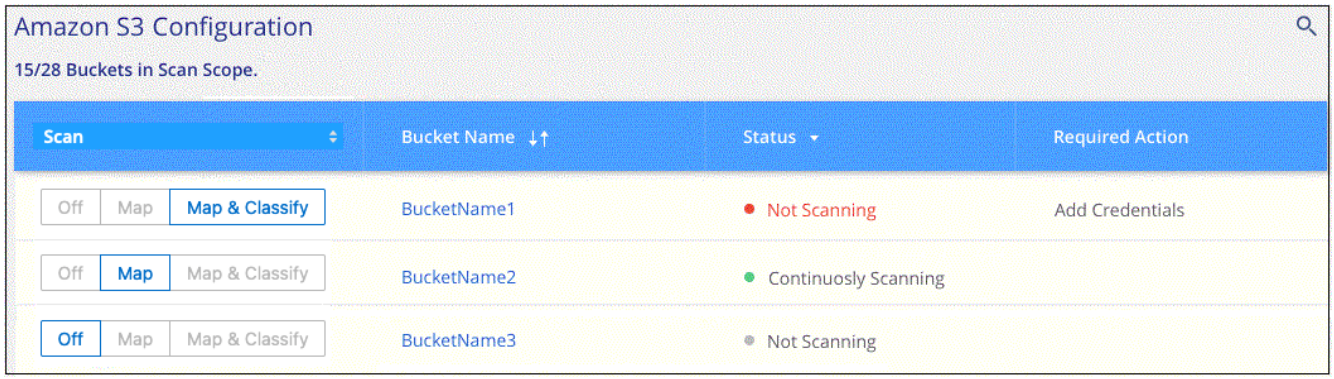
Die BlueXP Klassifizierung kann Sie ebenfalls Scannen von S3-Buckets, die in unterschiedlichen AWS Konten vorhanden sind.

Schritte

1. Wählen Sie die Amazon S3-Arbeitsumgebung aus.
2. Klicken Sie im Bereich Dienste auf der rechten Seite auf **Buckets konfigurieren**.



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



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

Ergebnis

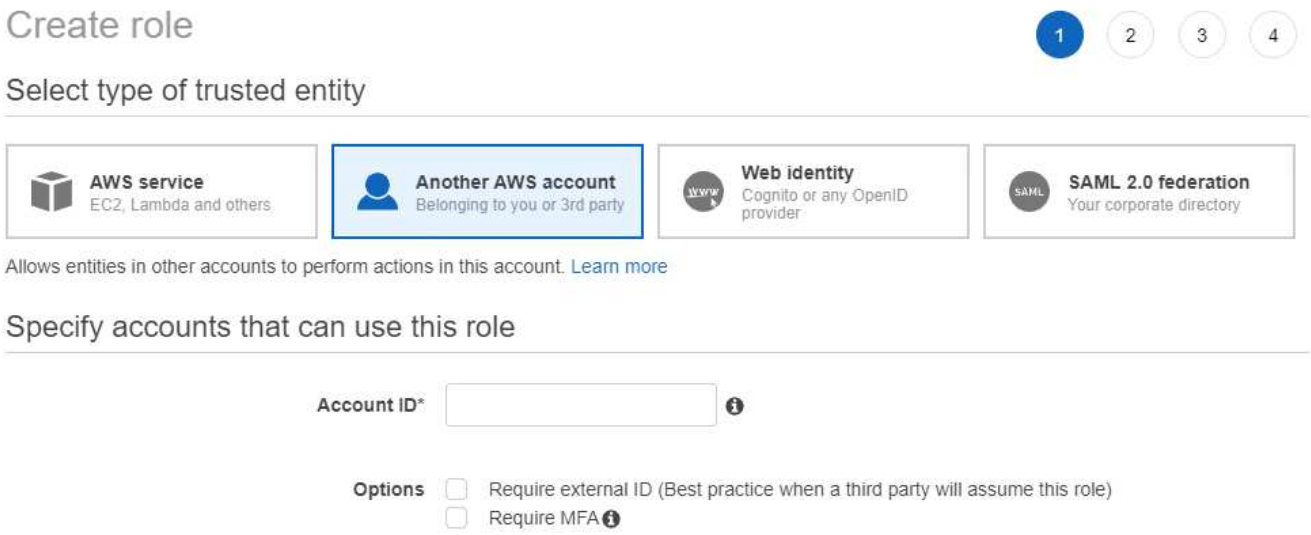
Die BlueXP Klassifizierung beginnt mit dem Scannen der von Ihnen aktivierten S3-Buckets. Wenn Fehler auftreten, werden sie neben der erforderlichen Aktion zur Behebung des Fehlers in der Spalte Status angezeigt.

Scannen von Buckets für weitere AWS Konten

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

Schritte

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



Gehen Sie wie folgt vor:

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

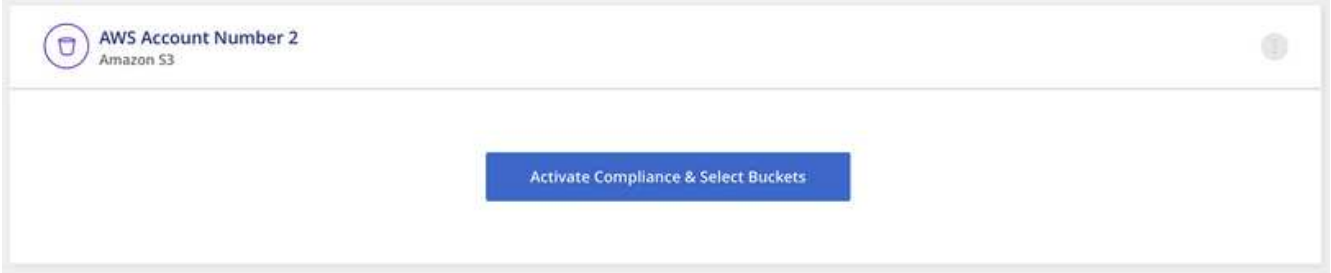
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
  ]
}
```

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

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

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

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



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

Ergebnis

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

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.

Alle Voraussetzungen für OneDrive prüfen

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

Implementieren der BlueXP Klassifizierungsinstanz

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

Fügen Sie das OneDrive Konto hinzu

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

Fügen Sie die Benutzer hinzu und wählen Sie den Scantyp aus

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

OneDrive Anforderungen können Sie überprüfen

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

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

Implementieren der BlueXP Klassifizierungsinstanz

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

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

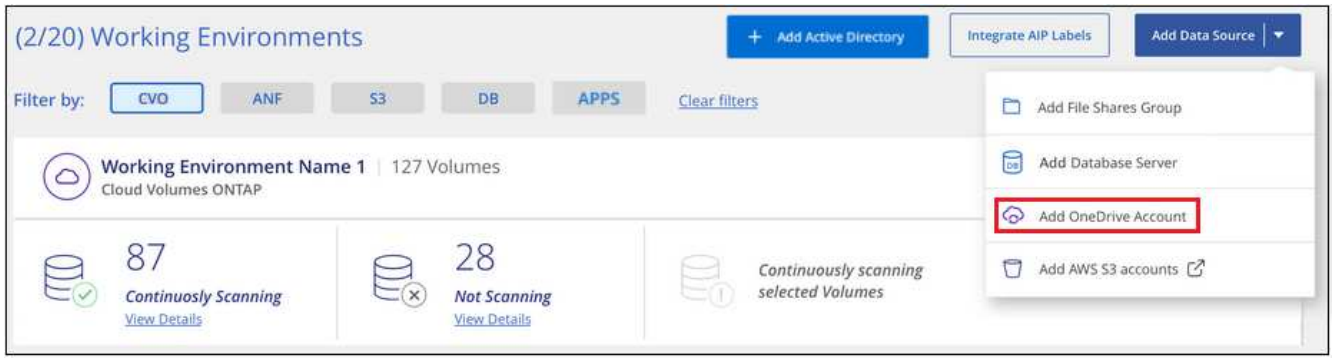
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des OneDrive Kontos

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

Schritte

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



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

Das OneDrive-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

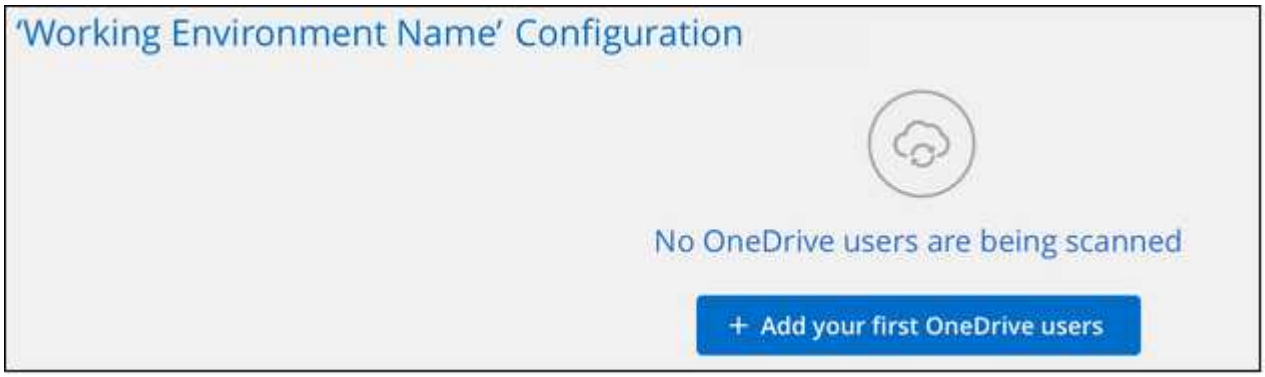
Hinzufügen von OneDrive Benutzern zu Compliance-Scans

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

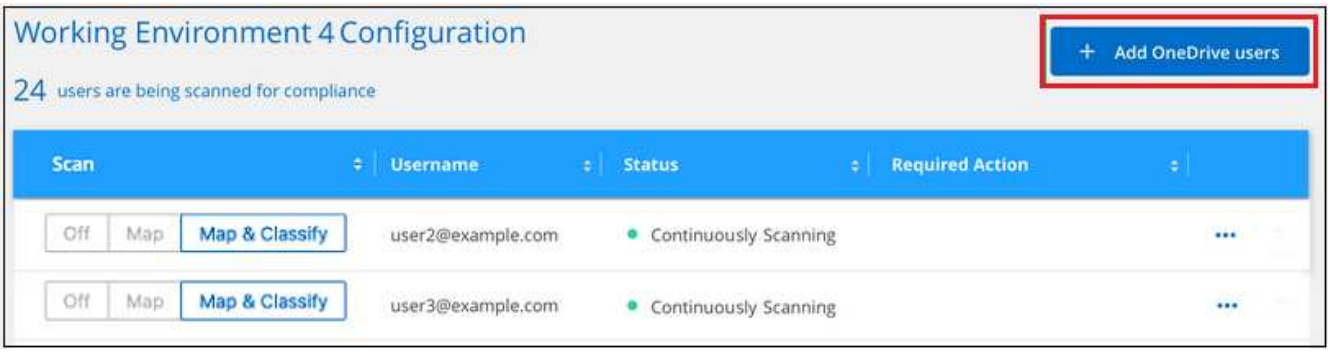
Schritte

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

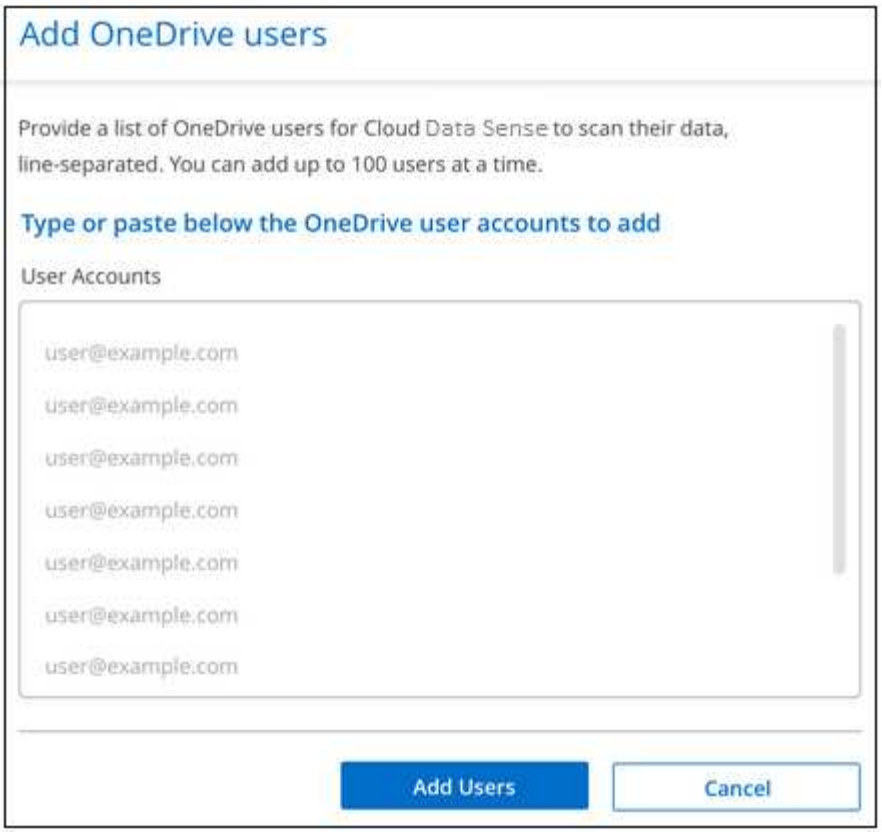
2. Wenn dies das erste Mal ist, Benutzer für dieses OneDrive-Konto hinzuzufügen, klicken Sie auf **Fügen Sie Ihre ersten OneDrive-Benutzer**.



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



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



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

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

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

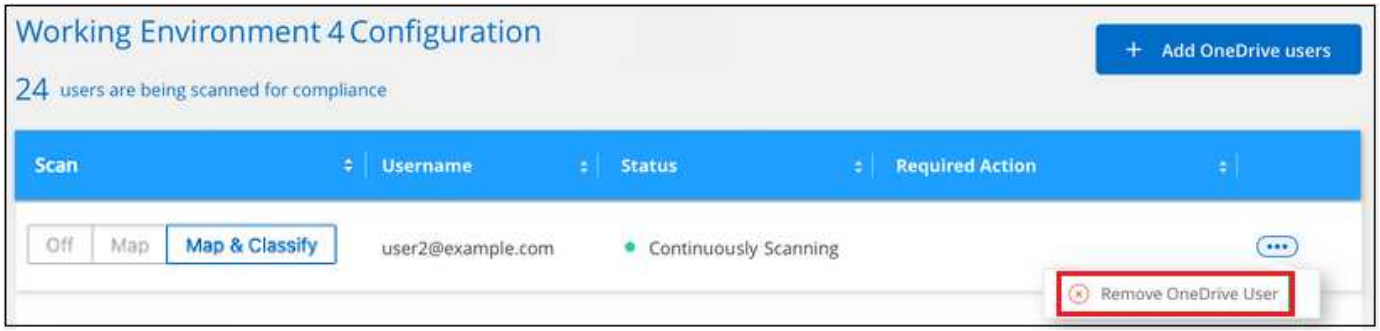
An:	**Tun Sie dies:**
Aktivieren Sie mappingonly Scans von Benutzerdateien	Klicken Sie Auf **Karte**
Aktivieren Sie vollständige Scans von Benutzerdateien	Klicken Sie Auf **Karte & Klassieren**
Deaktivieren Sie das Scannen von Benutzerdateien	Klicken Sie Auf **Aus**

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 .".

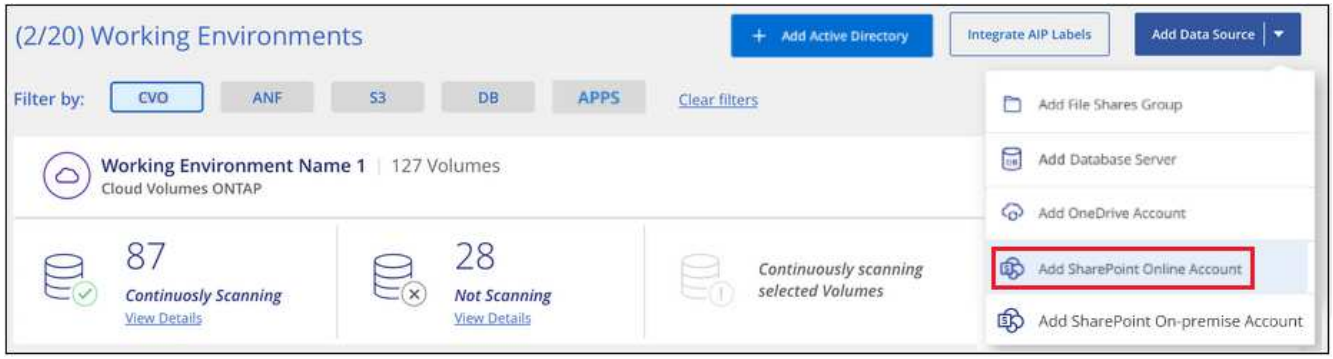
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

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.

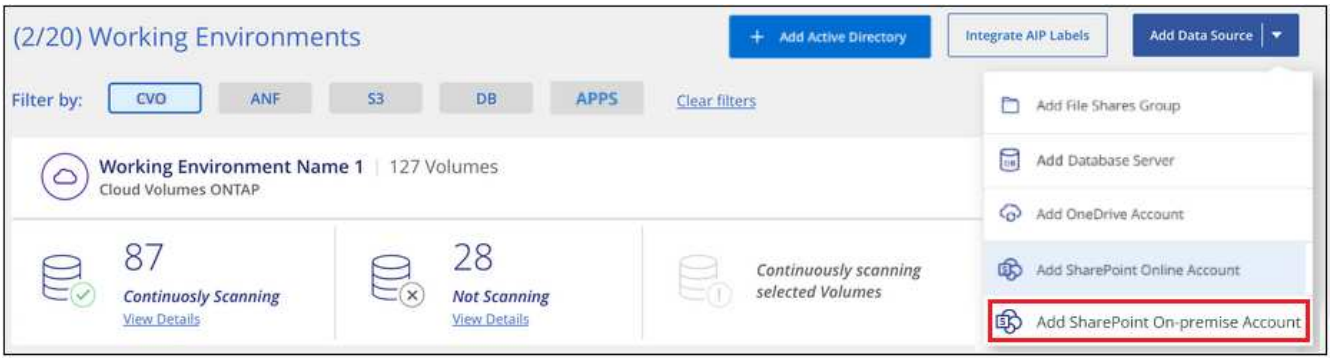
Das SharePoint Online-Konto wird der Liste der Arbeitsumgebungen hinzugefügt.

Fügen Sie ein SharePoint On-Premise-Konto hinzu

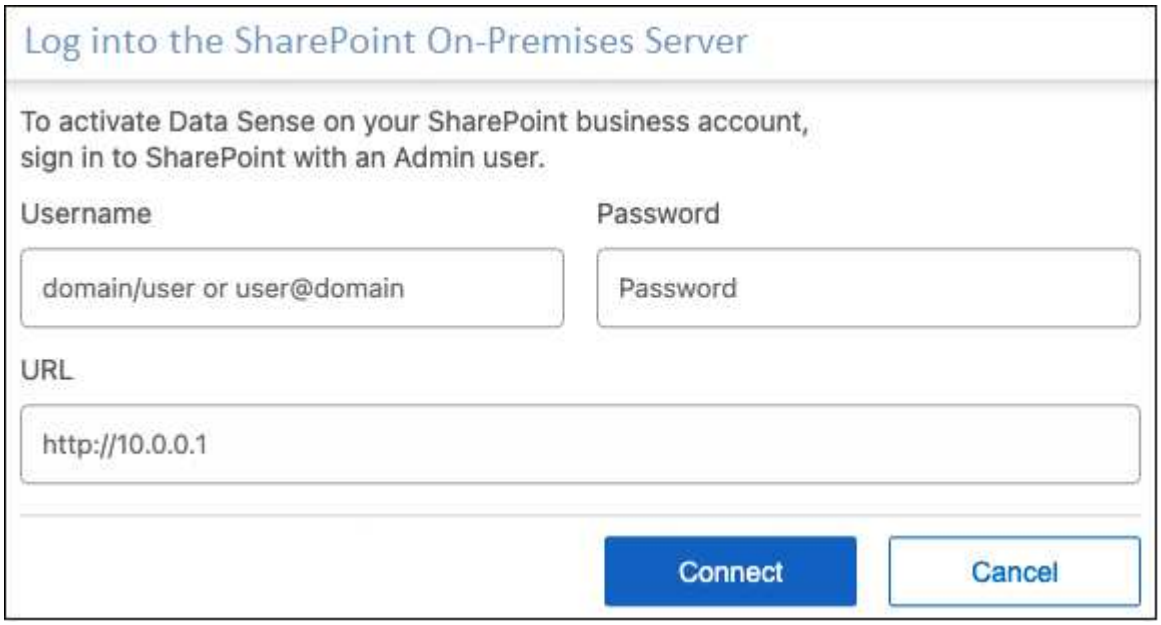
Fügen Sie das SharePoint-On-Premise-Konto hinzu, in dem sich die Benutzerdateien befinden.

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



3. Klicken Sie Auf **Verbinden**.

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

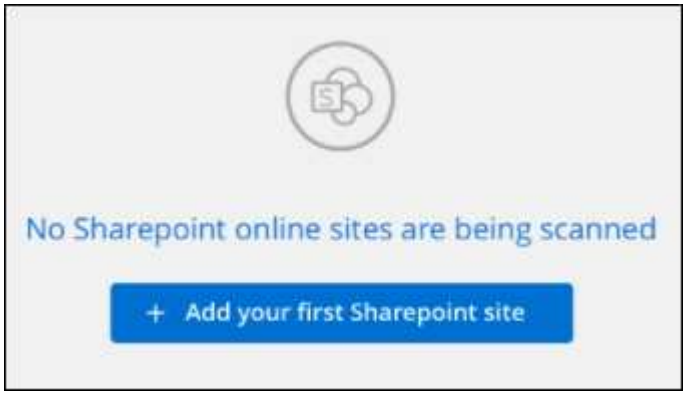
Fügen Sie SharePoint-Sites zu Compliance-Scans hinzu

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

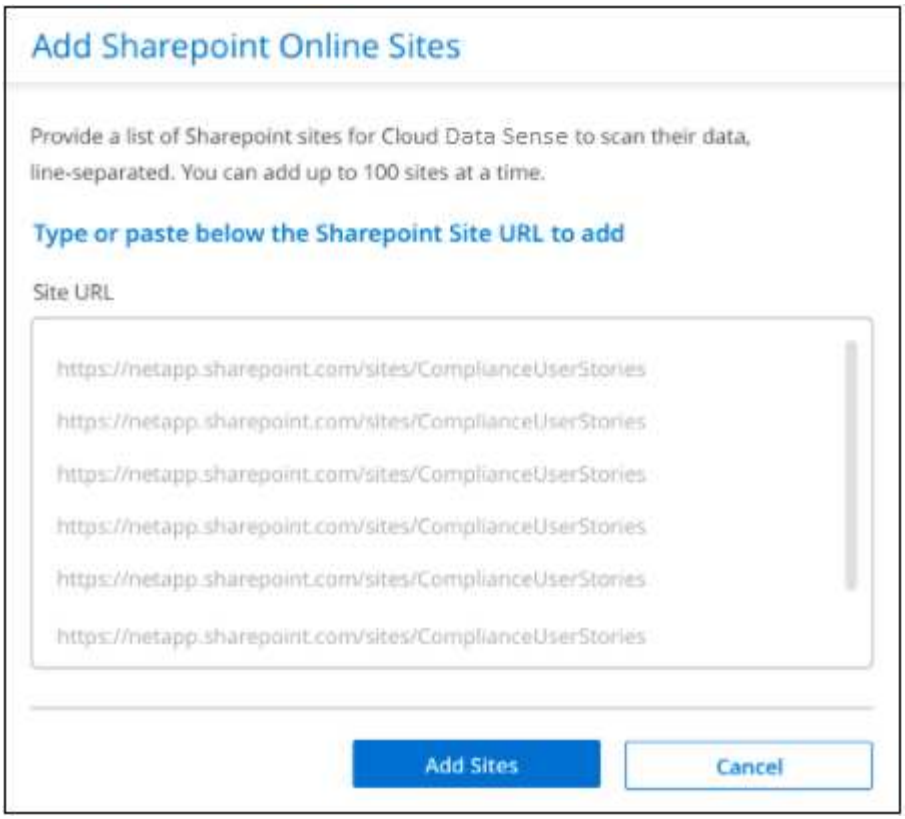
1. Klicken Sie auf der Seite *Configuration* auf die Schaltfläche **Configuration** für das SharePoint-Konto.

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 Bestätigungsdialogfeld wird die Anzahl der hinzugefügten Standorte angezeigt.

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

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

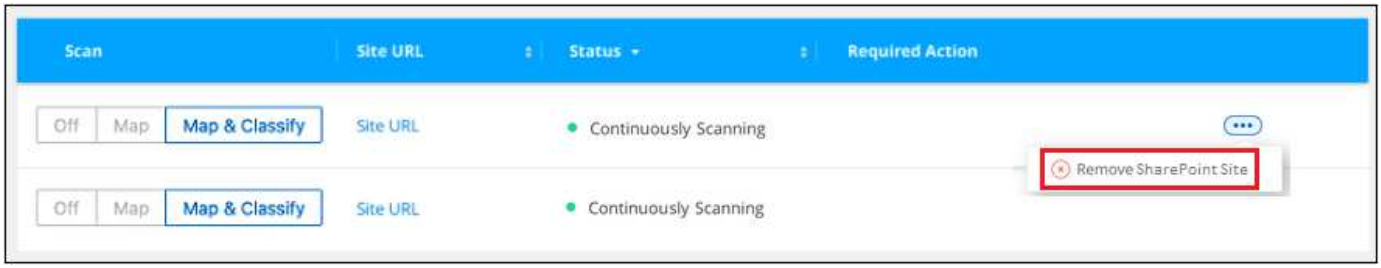
An:	Tun Sie dies:
Aktivieren Sie Mapping-Only-Scans auf Dateien	Klicken Sie Auf **Karte**
Aktivieren Sie vollständige Scans auf Dateien	Klicken Sie Auf **Karte & Klassieren**
Deaktivieren Sie das Scannen von Dateien	Klicken Sie Auf **Aus**

Ergebnis

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

Entfernen 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.



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".

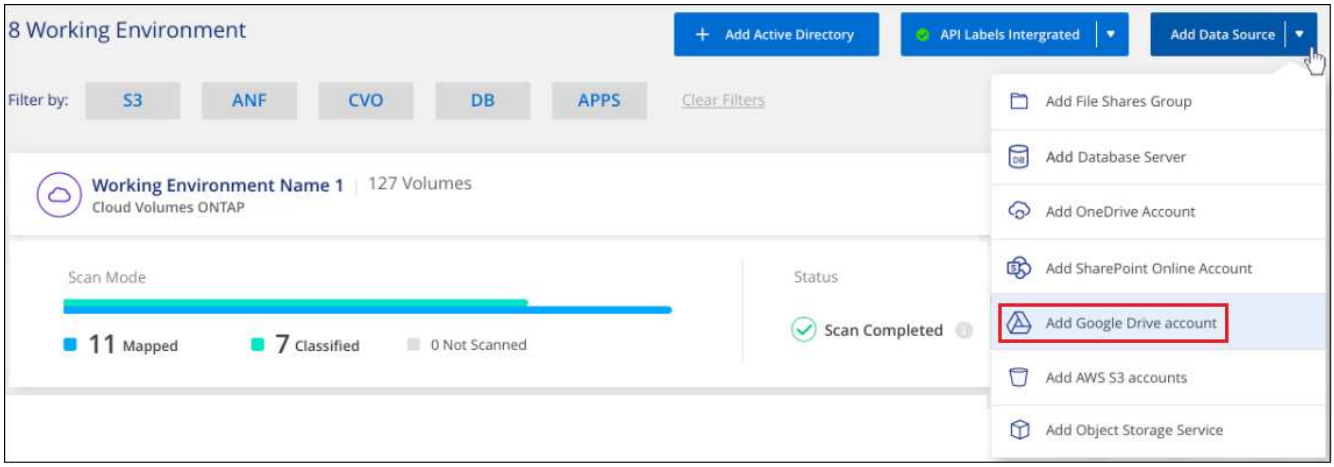
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

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.

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.

Implementieren der BlueXP Klassifizierungsinstanz

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

Fügen Sie den Objekt-Storage-Service hinzu

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

Wählen Sie die zu scannenden Buckets aus

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

Überprüfung der Objekt-Storage-Anforderungen

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

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

Implementieren der BlueXP Klassifizierungsinstanz

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

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

Wenn Sie Daten vom S3 Objekt-Storage scannen, der auf einem dunklen Standort ohne Internetzugang installiert wurde, müssen Sie sie überprüfen "Implementieren Sie die BlueXP Klassifizierung an demselben

lokalen Standort ohne Internetzugang". Dazu ist auch die Implementierung des BlueXP Connectors am selben Standort erforderlich.

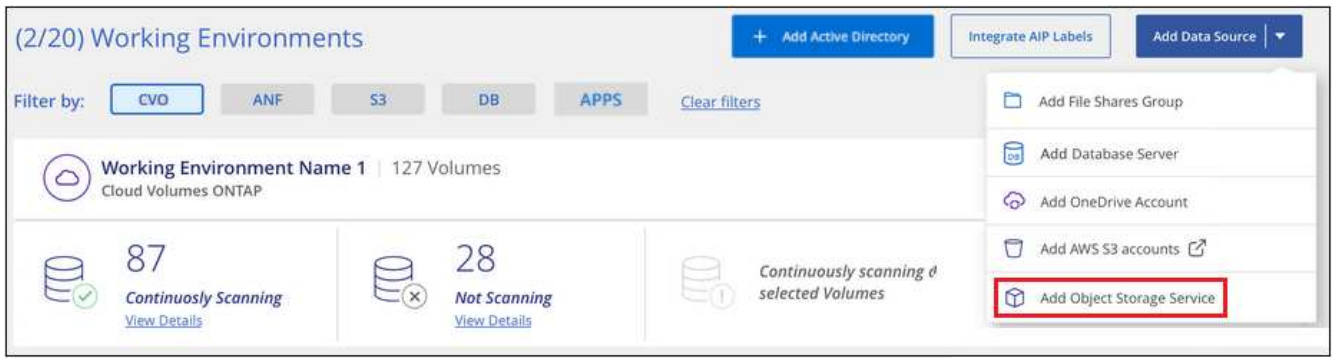
Ein Upgrade auf die BlueXP Klassifizierungssoftware ist automatisiert, solange die Instanz über eine Internetverbindung verfügt.

Hinzufügen des Objekt-Storage-Service zur BlueXP Klassifizierung

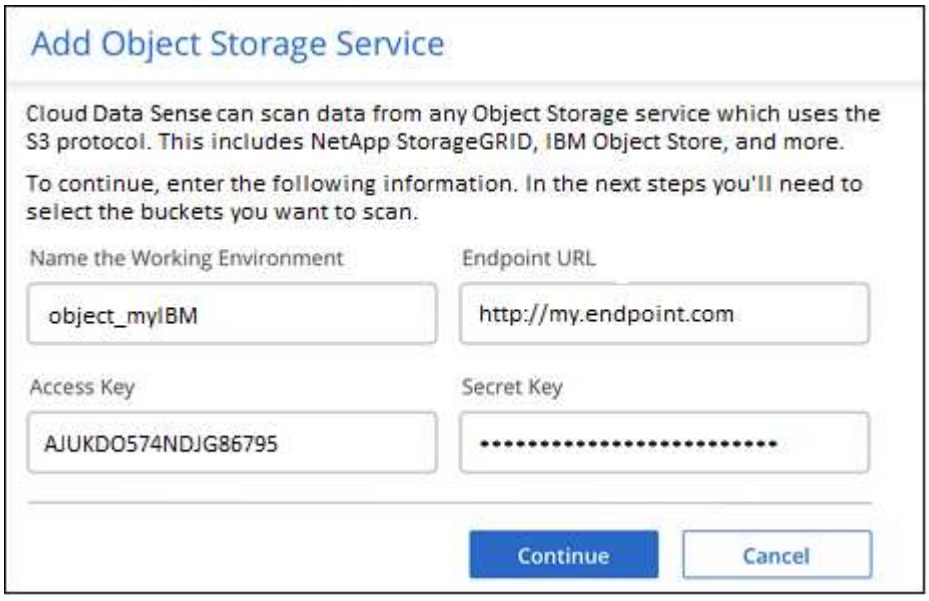
Fügen Sie den Objekt-Storage-Service hinzu.

Schritte

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



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



Ergebnis

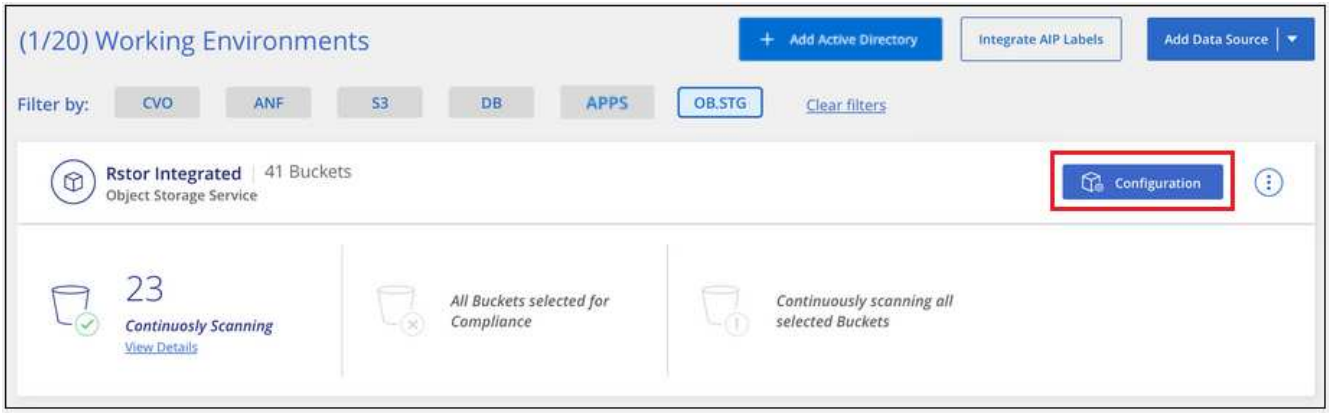
Der neue Objekt-Speicherdienst wird der Liste der Arbeitsumgebungen hinzugefügt.

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

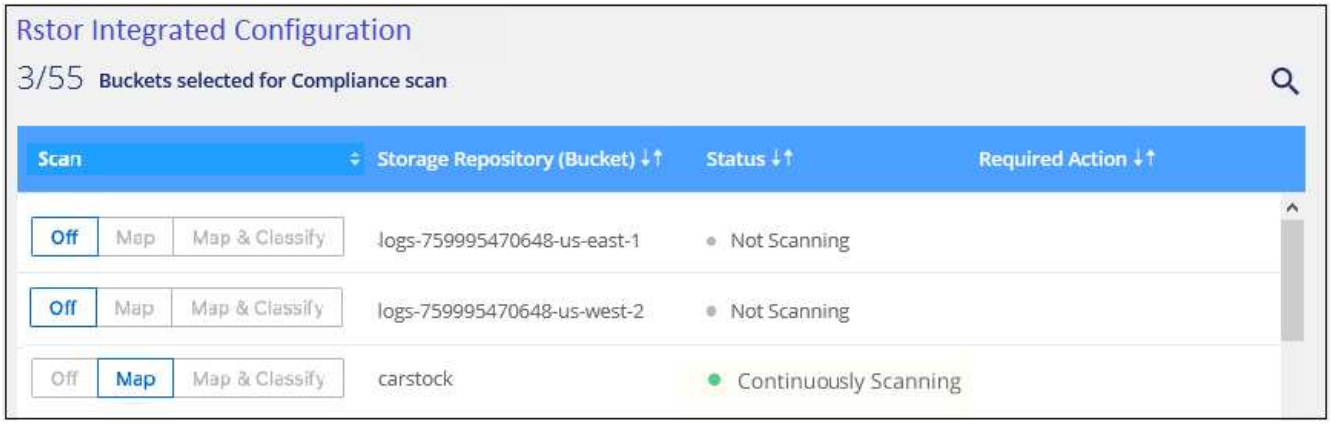
Nachdem Sie die BlueXP Klassifizierung für Ihren Objekt-Storage-Service aktiviert haben, müssen Sie im nächsten Schritt die Buckets konfigurieren, die Sie scannen möchten. Die BlueXP Klassifizierung erkennt diese Buckets und zeigt sie in der von Ihnen erstellten Arbeitsumgebung an.

Schritte

1. Klicken Sie auf der Konfigurationsseite in der Arbeitsumgebung Object Storage Service auf **Konfiguration**.



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



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

Ergebnis

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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.