BlueXP Klassifizierung managen

BlueXP classification

NetApp
April 03, 2024

Inhalt

BlueXP Klassifizierung managen . . . 1
Ergänzen Sie Ihre BlueXP Klassifizierungs-Scans um persönliche Daten-IDs . . . 1
Ausschließen bestimmter Verzeichnisse von den Klassifikationsscans von BlueXP . . . 16
Anzeigen des Status Ihrer Compliance-Aktionen . . . 19
Definieren Sie zusätzliche Gruppen-IDs als für die Organisation offen . . . 20
Audit der Historie der BlueXP Klassifizierungsaktionen . . . 22
Reduzierung der Scan-Geschwindigkeit der BlueXP Klassifizierung . . . 23
Entfernen von Datenquellen aus der BlueXP Klassifizierung . . . 24
BlueXP Klassifizierung wird deinstalliert . . . 26

BlueXP Klassifizierung managen

Ergänzen Sie Ihre BlueXP Klassifizierungs-Scans um persönliche Daten-IDs

Die BlueXP Klassifizierung bietet Ihnen viele Möglichkeiten, eine benutzerdefinierte Liste mit „personenbezogenen Daten“ hinzuzufügen, die durch die BlueXP Klassifizierung bei zukünftigen Scans identifiziert werden. So haben Sie alle Informationen darüber, wo sich möglicherweise sensible Daten in den Dateien Ihrer Unternehmen befinden.

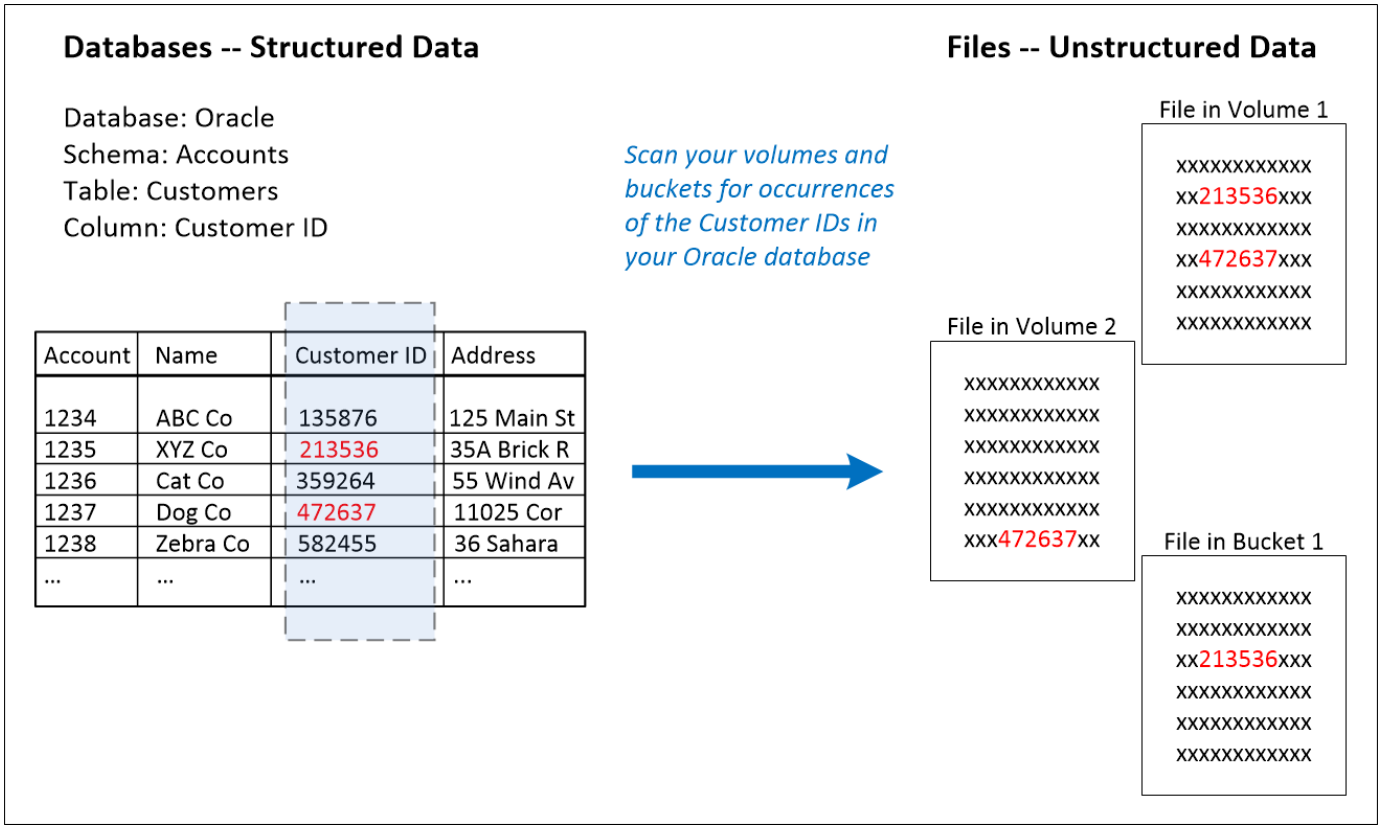
- Sie können eindeutige Kennungen basierend auf bestimmten Spalten in Datenbanken hinzufügen, die Sie scannen.
- Sie können benutzerdefinierte Schlüsselwörter aus einer Textdatei hinzufügen - diese Wörter werden in Ihren Daten identifiziert.
- Sie können ein persönliches Muster mit einem regulären Ausdruck (regex) hinzufügen — der Regex wird den bestehenden vordefinierten Mustern hinzugefügt.
- Sie können benutzerdefinierte Kategorien hinzufügen, um zu ermitteln, wo bestimmte Informationskategorien in Ihren Daten gefunden werden.

Alle diese Mechanismen zum Hinzufügen benutzerdefinierter Scankriterien werden in allen Sprachen unterstützt.

> Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.

Fügen Sie benutzerdefinierte ID-Daten aus Ihren Datenbanken hinzu

Eine Funktion, die wir *Data Fusion* nennen, ermöglicht Ihnen, die Daten Ihres Unternehmens zu überprüfen, um zu ermitteln, ob eindeutige IDs aus Ihren Datenbanken in einer Ihrer anderen Datenquellen gefunden werden. Sie können die zusätzlichen Identifikatoren auswählen, nach denen die BlueXP Klassifizierung in ihren Scans suchen soll, indem Sie eine bestimmte Spalte oder Spalte in einer Datenbanktabelle auswählen. Das folgende Diagramm zeigt beispielsweise, wie Daten-Fusion zur Überprüfung von Volumes, Buckets und Datenbanken eingesetzt wird, um vor allen Kunden-IDs aus der Oracle Datenbank zu kommen.



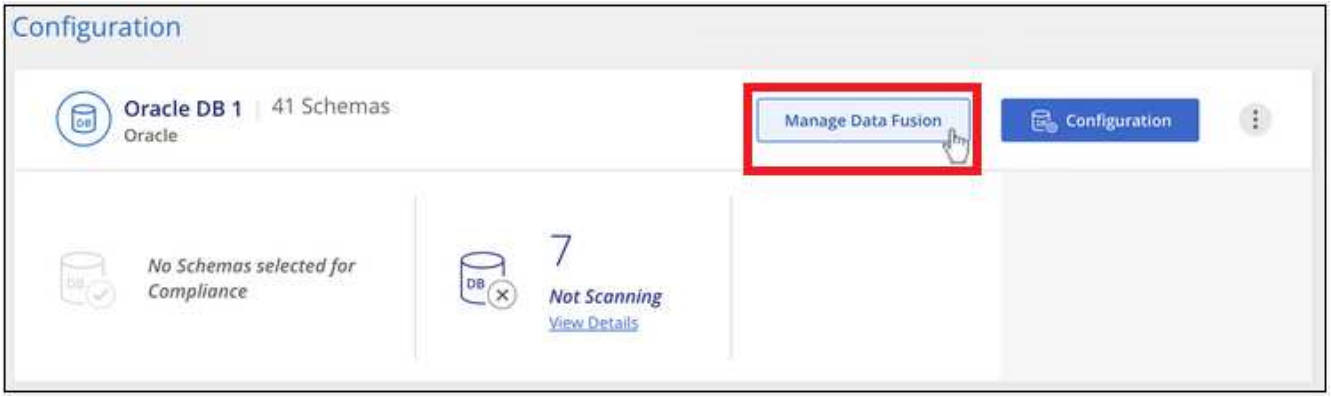
Wie Sie sehen, wurden in zwei Volumes und in einem S3-Bucket zwei eindeutige Kunden-IDs gefunden. Alle Übereinstimmungen in Datenbanktabellen werden ebenfalls identifiziert.

Da Sie Ihre eigenen Datenbanken scannen, können Sie mit jeder Sprache, in der Ihre Daten gespeichert sind, Daten bei zukünftigen BlueXP Klassifizierungs-Scans erkennen.

Schritte

Dieser muss unbedingt vorhanden sein "Hat mindestens einen Datenbankserver hinzugefügt" Bis zur BlueXP Klassifizierung vor dem Hinzufügen von Fusion-Datenquellen

1. Klicken Sie auf der Konfigurationsseite in der Datenbank, in der sich die Quelldaten befinden, auf **Daten-Fusion verwalten**.



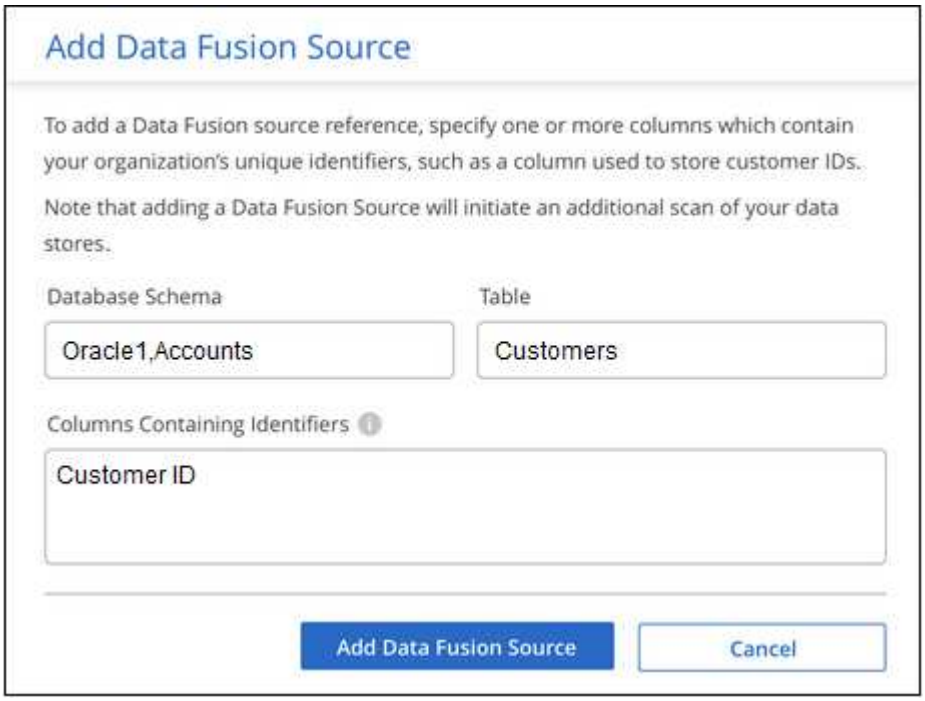
2. Klicken Sie auf der nächsten Seite auf **Data Fusion Source hinzufügen**.
3. Klicken Sie auf der Seite „ Fusion-Quelle hinzufügen “ auf die Seite „

a. Wählen Sie das Datenbankschema aus dem Dropdown-Menü aus.

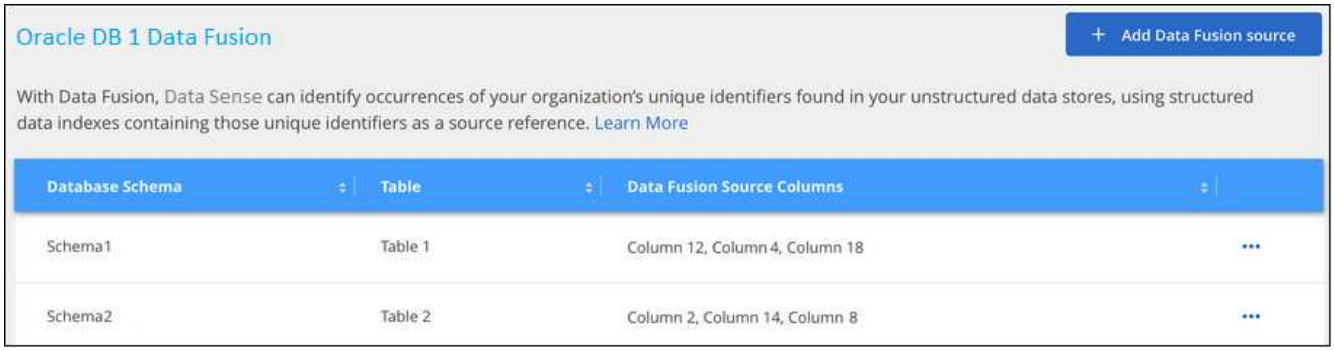
b. Geben Sie den Tabellennamen in dieses Schema ein.

c. Geben Sie die Spalte oder Spalten ein, die die eindeutigen Kennungen enthalten, die Sie verwenden möchten.

   Wenn Sie mehrere Spalten hinzufügen, geben Sie jeden Spaltennamen oder Namen der Tabellenansicht in einer separaten Zeile ein.

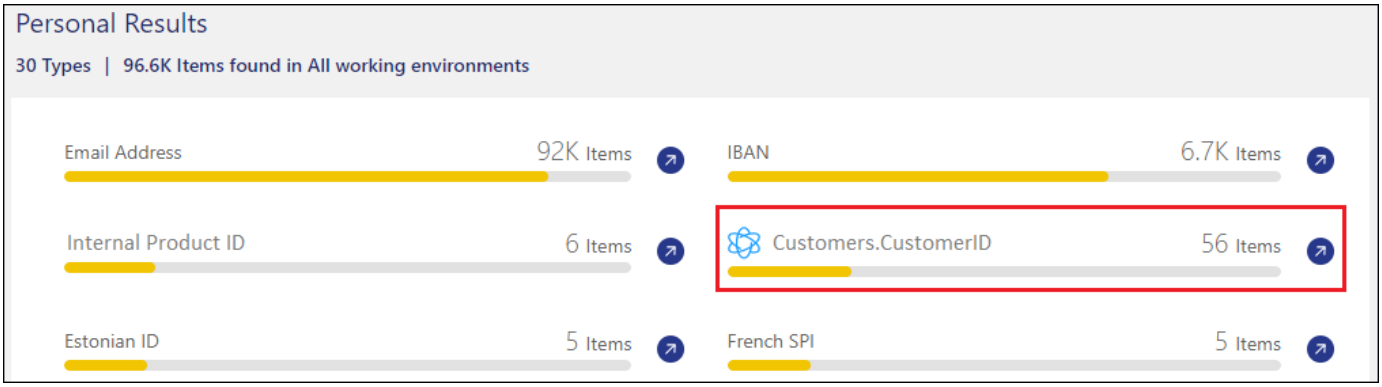


4. Klicken Sie Auf **Data Fusion-Quelle Hinzufügen**.



Ergebnisse

Nach dem nächsten Scan werden diese neuen Informationen im Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Untersuchungsseite im Filter „Persönliche Daten“ angezeigt. Der Name, den Sie für den Klassifikator verwendet haben, wird z. B. in der Filterliste angezeigt `Customers.CustomerID`.



Löschen Sie eine Data Fusion-Quelle

Wenn Sie sich irgendwann entscheiden, Ihre Dateien nicht mit einer bestimmten Data Fusion Quelle zu scannen, können Sie die Quellzeile auf der Seite Data Fusion Inventory auswählen und auf **Daten löschen Fusion Source** klicken.

Fügen Sie benutzerdefinierte Schlüsselwörter aus einer Wortliste hinzu

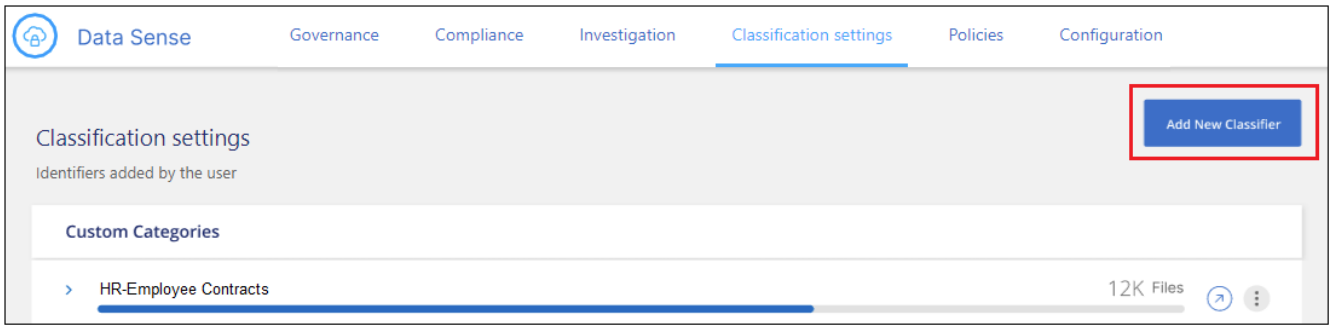
Sie können der BlueXP Klassifizierung benutzerdefinierte Schlüsselwörter hinzufügen, um den Speicherort der Daten bestimmen zu können. Fügen Sie die Schlüsselwörter einfach ein, indem Sie jedes Wort eingeben, das die BlueXP Klassifizierung wiedererkennen soll. Die Schlüsselwörter werden zu den vorhandenen vordefinierten Schlüsselwörtern hinzugefügt, die bereits von der BlueXP-Klassifizierung verwendet werden, und die Ergebnisse werden im Abschnitt „Persönliche Muster“ angezeigt.

Sie können z. B. sehen, wo interne Produktnamen in allen Dateien erwähnt werden, um sicherzustellen, dass diese Namen nicht an Orten zugänglich sind, die nicht sicher sind.

Nach der Aktualisierung der benutzerdefinierten Schlüsselwörter wird die BlueXP Klassifizierung neu gestartet und alle Datenquellen werden gescannt. Nach Abschluss des Scans werden die neuen Ergebnisse im BlueXP Classification Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Untersuchungsseite im Filter „Persönliche Daten“ angezeigt.

Schritte

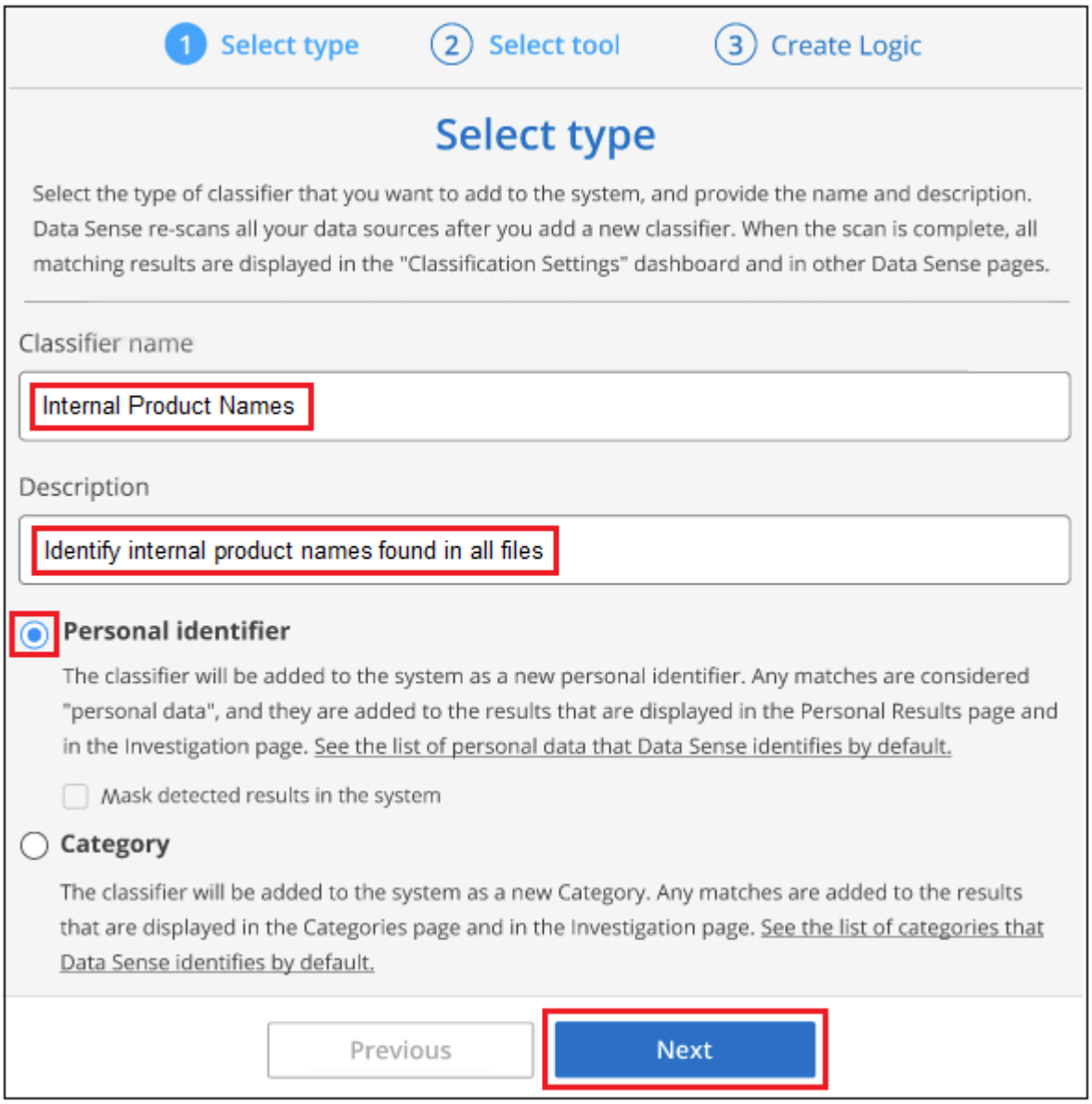
1. Klicken Sie auf der Registerkarte *Classification settings* auf **Add New Classifier**, um den Assistenten *Add Custom Classifier* zu starten.



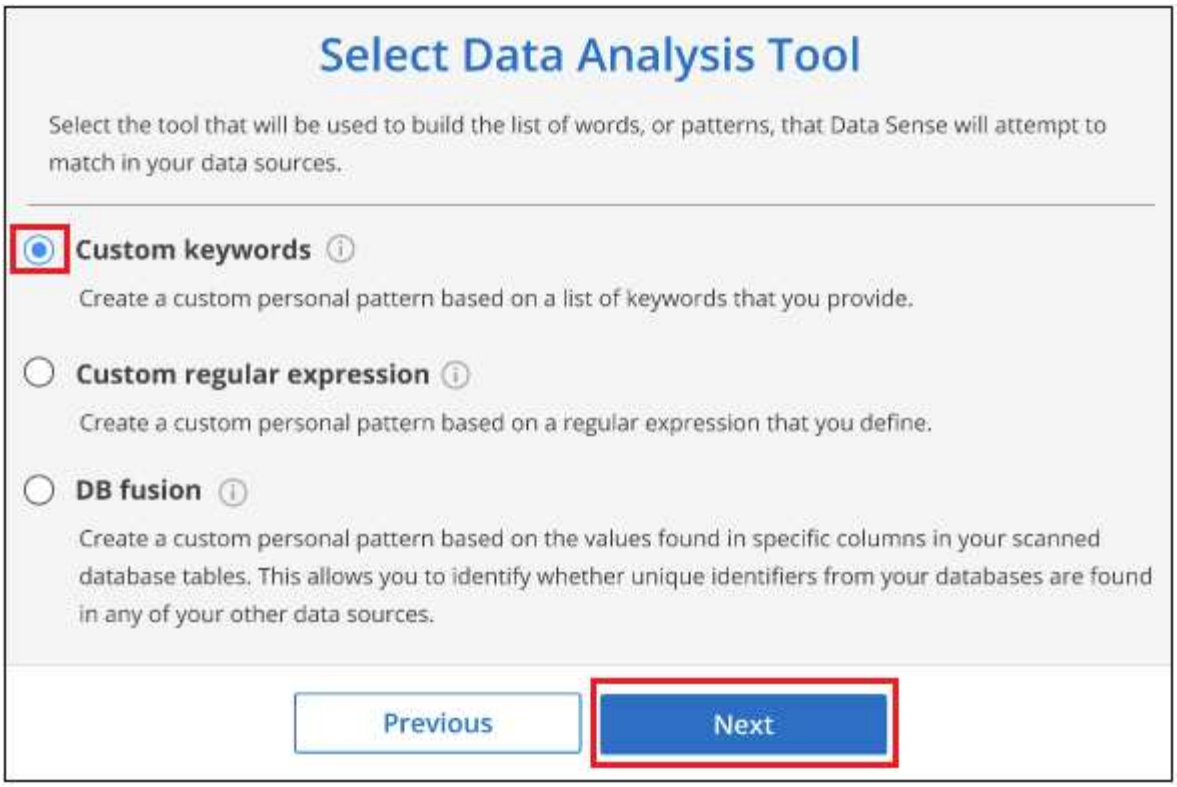
2. Geben Sie auf der Seite *Typ auswählen* den Namen des Klassifikators ein, geben Sie eine kurze Beschreibung ein, wählen Sie **Persönliche Kennung** aus und klicken Sie dann auf **Weiter**.

   Der eingegebene Name wird in der BlueXP-Klassifizierungs-UI als Überschrift für gescannte Dateien angezeigt, die den Anforderungen des Klassifikators entsprechen, und als Name des Filters auf der Seite Untersuchung.

   Sie können das Kontrollkästchen auch aktivieren, um „erkannte Ergebnisse im System maskieren“ zu aktivieren, damit das vollständige Ergebnis nicht in der Benutzeroberfläche angezeigt wird. So können Sie beispielsweise vollständige Kreditkartennummern oder ähnliche persönliche Daten ausblenden (die Maske erscheint in der Benutzeroberfläche wie folgt: "Pass:[***] Pass:[] Pass:[] Pass:[***]" 3434).

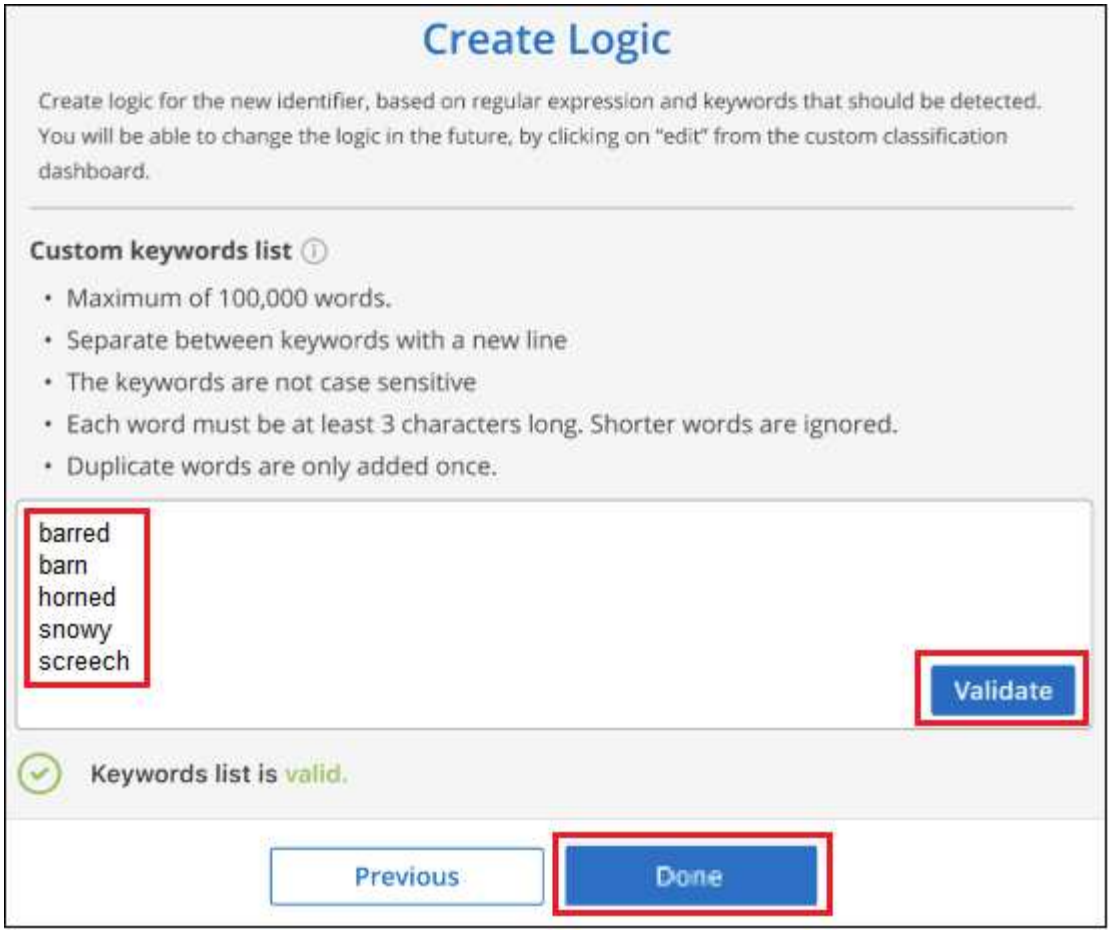


3. Wählen Sie auf der *Select Data Analysis Tool* -Seite **Custom Keywords** als Methode aus, mit der Sie den Klassifikator definieren möchten, und klicken Sie dann auf **Next**.



4. Geben Sie auf der Seite *Create Logic* die Schlüsselwörter ein, die Sie erkennen möchten - jedes Wort in einer separaten Zeile - und klicken Sie auf **Validate**.

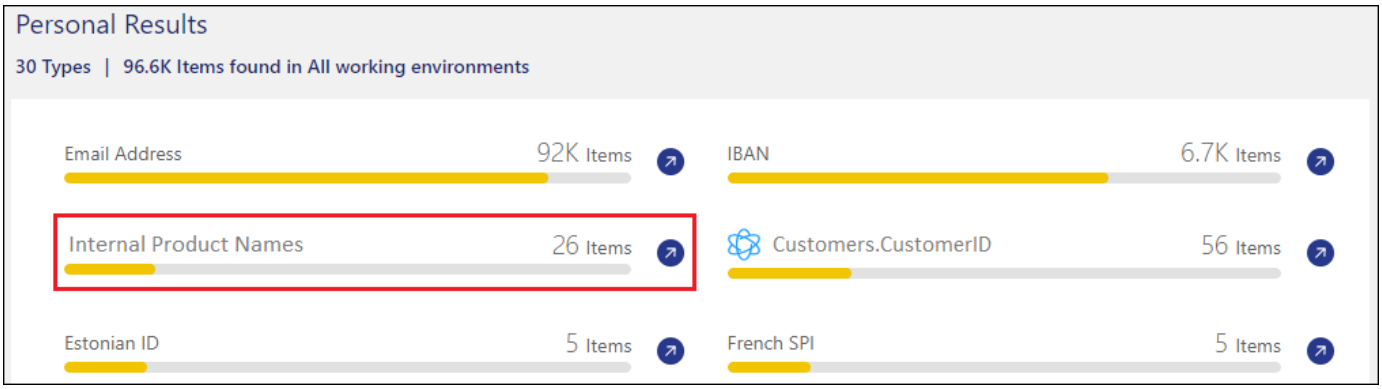
   Die Abbildung unten zeigt interne Produktnamen (verschiedene Arten von Eulen). Bei der BlueXP Klassifizierungssuche für diese Elemente wird die Groß-/Kleinschreibung nicht berücksichtigt.



5. Klicken Sie auf **done** und die BlueXP Klassifizierung beginnt mit der erneuten Überprüfung Ihrer Daten.

Ergebnisse

Nach Abschluss des Scans werden diese neuen Informationen im Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Seite „Untersuchung“ im Filter „Persönliche Daten“ angezeigt.



Wie Sie sehen, wird der Name des Klassifikators als Name im Fenster „Persönliche Ergebnisse“ verwendet. Auf diese Weise können Sie viele verschiedene Gruppen von Schlüsselwörtern aktivieren und die Ergebnisse für jede Gruppe anzeigen.

Fügen Sie mithilfe eines Regex benutzerdefinierte Kennungen für persönliche Daten hinzu

Mit einem benutzerdefinierten regulären Ausdruck (regex) können Sie ein persönliches Muster hinzufügen, um bestimmte Informationen in Ihren Daten zu identifizieren. Auf diese Weise können Sie ein neues benutzerdefiniertes Regex erstellen, um neue persönliche Informationselemente zu identifizieren, die noch nicht im System vorhanden sind. Der regex wird zu den vorhandenen vordefinierten Mustern hinzugefügt, die die BlueXP-Klassifizierung bereits verwendet, und die Ergebnisse werden im Abschnitt „Persönliche Muster“ angezeigt.

Sie können beispielsweise sehen, wo Ihre internen Produkt-IDs in allen Dateien erwähnt werden. Wenn die Produkt-ID z. B. eine klare Struktur hat, ist es eine 12-stellige Nummer, die mit 201 beginnt, können Sie die benutzerdefinierte regex-Funktion verwenden, um sie in Ihren Dateien zu suchen. Der reguläre Ausdruck für dieses Beispiel lautet **\b201\d{9}\b**.

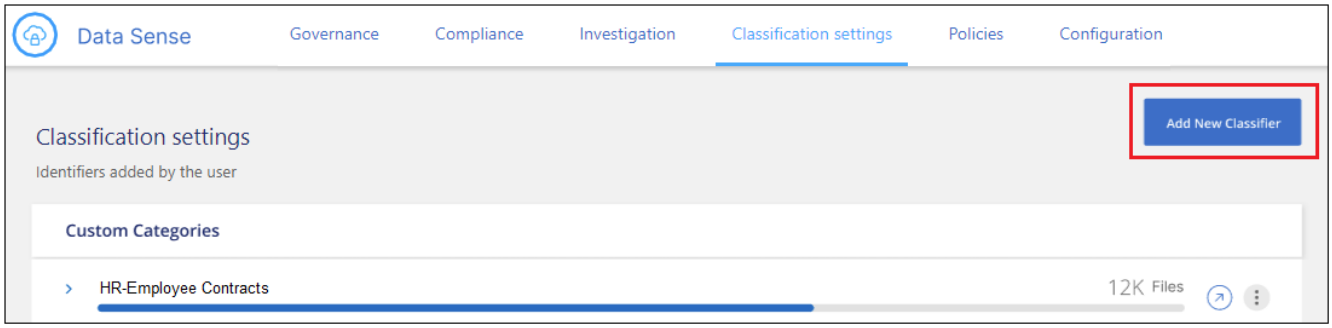
Nach Hinzufügen des regex wird die BlueXP Klassifizierung neu gestartet und scannt alle Datenquellen. Nach Abschluss des Scans werden die neuen Ergebnisse im BlueXP Classification Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Untersuchungsseite im Filter „Persönliche Daten“ angezeigt.

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

> Derzeit erlauben wir die Verwendung von Pattern Flags beim Erstellen eines Regex nicht - das bedeutet, dass Sie "/" nicht verwenden sollten.

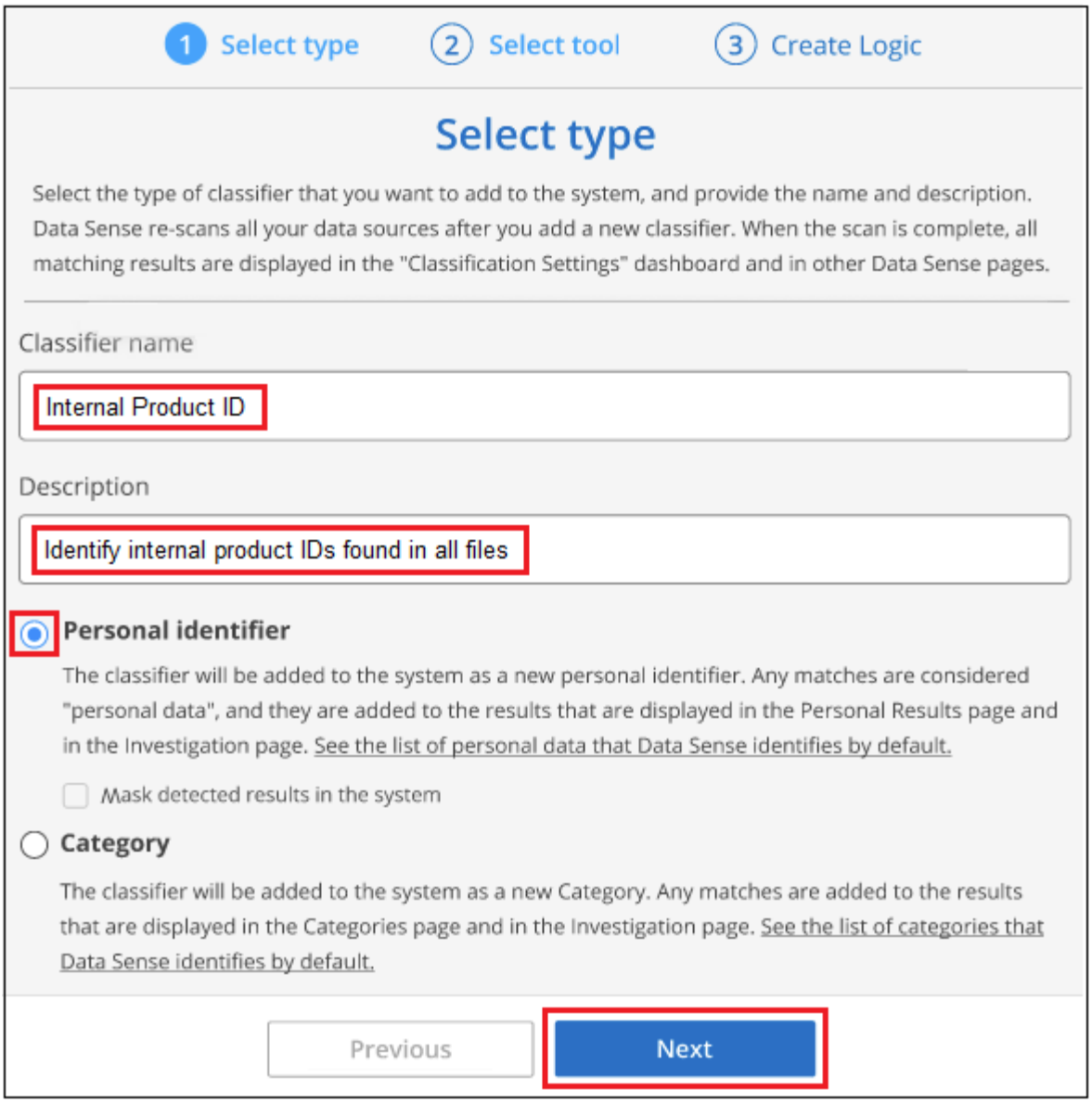
Schritte

1. Klicken Sie auf der Registerkarte *Classification settings* auf **Add New Classifier**, um den Assistenten *Add Custom Classifier* zu starten.

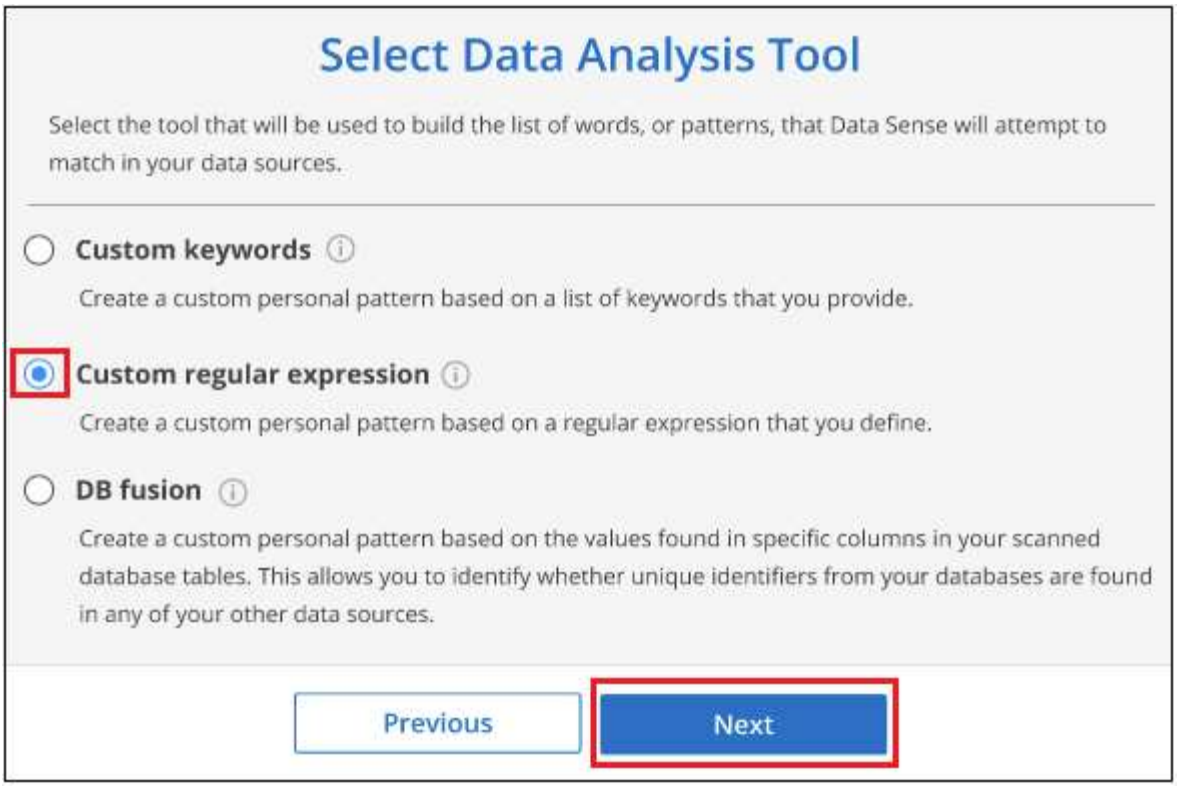


2. Geben Sie auf der Seite *Typ auswählen* den Namen des Klassifikators ein, geben Sie eine kurze Beschreibung ein, wählen Sie **Persönliche Kennung** aus und klicken Sie dann auf **Weiter**.

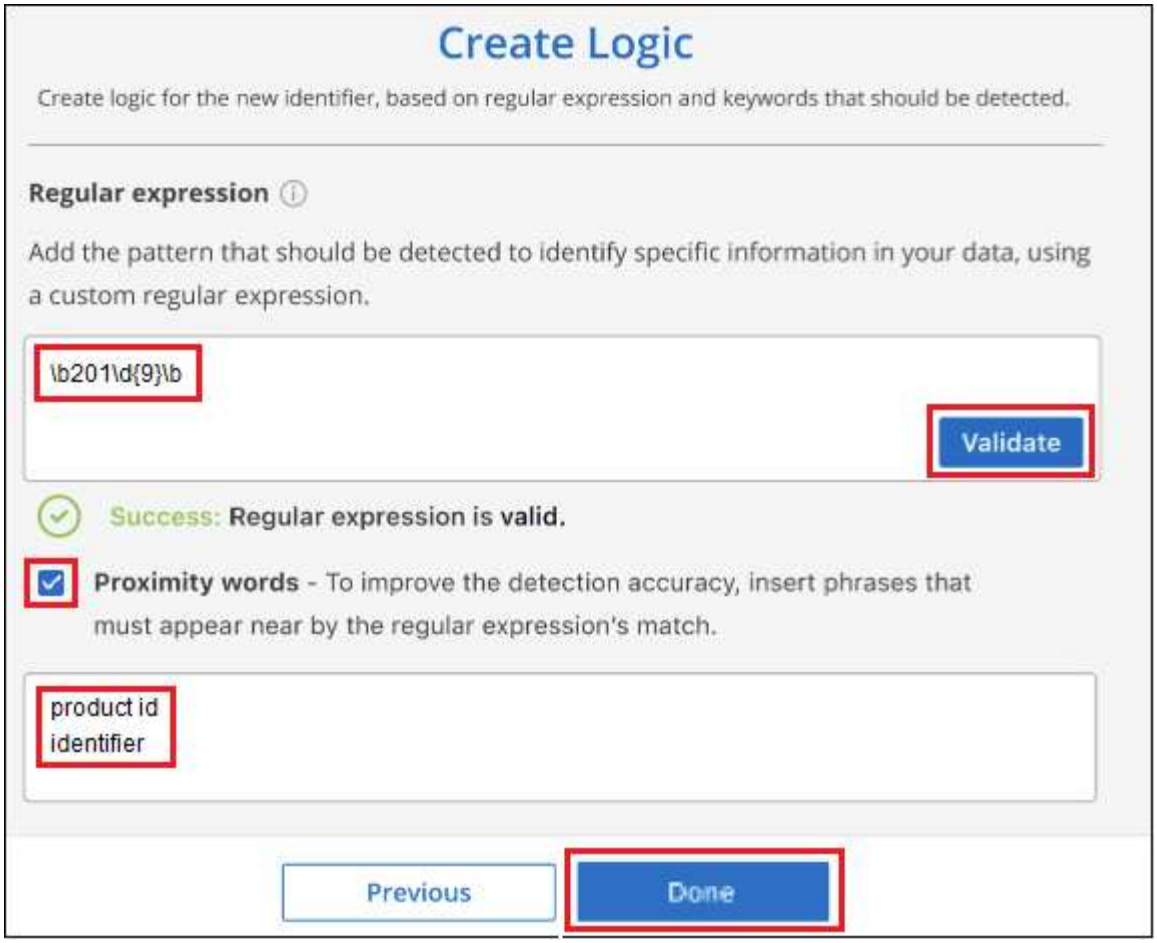
   Der eingegebene Name wird in der BlueXP-Klassifizierungs-UI als Überschrift für gescannte Dateien angezeigt, die den Anforderungen des Klassifikators entsprechen, und als Name des Filters auf der Seite Untersuchung. Sie können das Kontrollkästchen auch aktivieren, um „erkannte Ergebnisse im System maskieren“ zu aktivieren, damit das vollständige Ergebnis nicht in der Benutzeroberfläche angezeigt wird. Sie können dies beispielsweise tun, um vollständige Kreditkartennummern oder ähnliche persönliche Daten zu verbergen.



3. Wählen Sie auf der Seite Datenanalyse-Tool_ **Benutzerdefinierter regulärer Ausdruck** als Methode, mit der Sie den Klassifikator definieren möchten, und klicken Sie dann auf **Weiter**.

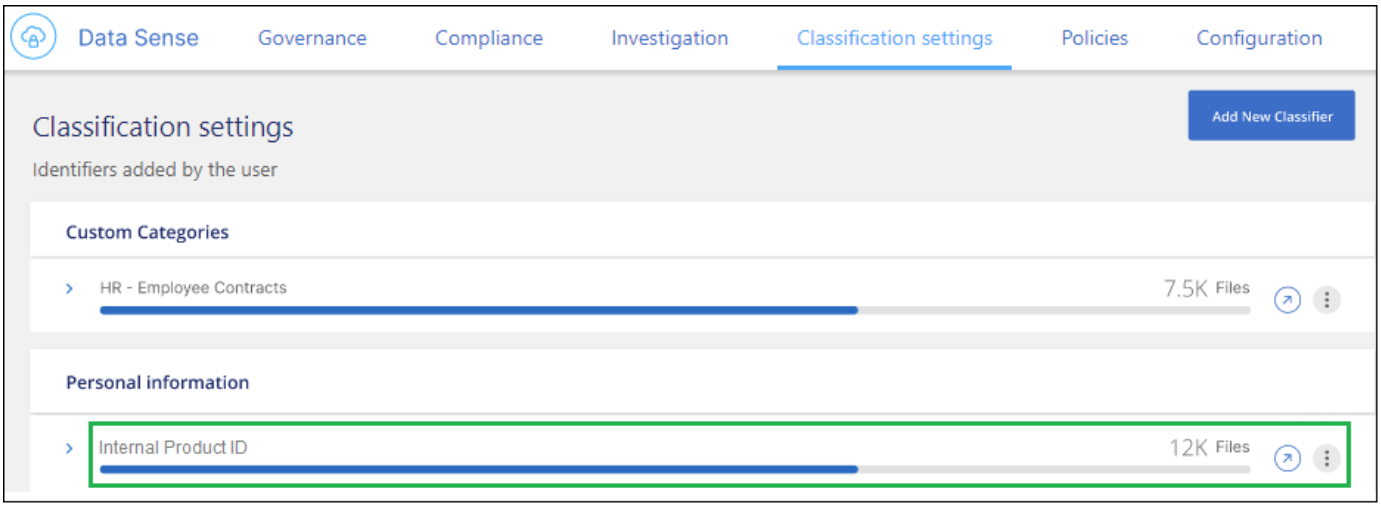


4. Geben Sie auf der Seite *Create Logic* den regulären Ausdruck und beliebige Annäherungswörter ein, und klicken Sie auf **Fertig**.
   a. Sie können jeden beliebigen regulären Ausdruck eingeben. Klicken Sie auf die Schaltfläche **Validieren**, um die BlueXP-Klassifizierung zu überprüfen, ob der reguläre Ausdruck gültig ist und nicht zu breit ist — das bedeutet, dass zu viele Ergebnisse zurückgegeben werden.
   b. Optional können Sie einige Annäherungsworte eingeben, um die Genauigkeit der Ergebnisse zu verbessern. Das sind Wörter, die in der Regel innerhalb von 300 Zeichen des Musters gefunden werden, nach dem Sie suchen (entweder vor oder nach dem gefundenen Muster). Geben Sie jedes Wort oder jede Phrase in eine separate Zeile ein.



Ergebnisse

Der Klassifikator wird hinzugefügt, und die BlueXP Klassifizierung beginnt, alle Datenquellen erneut zu scannen. Sie gelangen zurück zur Seite Benutzerdefinierte Klassifizierungsmerkmale, auf der Sie die Anzahl der Dateien anzeigen können, die Ihrem neuen Klassifikator entsprechen. Die Ergebnisse aus dem Scannen aller Ihrer Datenquellen werden je nach Anzahl der zu scannenden Dateien einige Zeit in Anspruch nehmen.



Benutzerdefinierte Kategorien hinzufügen

Die BlueXP Klassifizierung unterteilt die gescannten Daten in unterschiedliche Kategorien. Kategorien sind Themenbereiche, die auf der künstlichen Intelligenz Analyse der Inhalte und Metadaten der einzelnen Dateien

basieren. "Sehen Sie sich die Liste der vordefinierten Kategorien an".

Kategorien können Ihnen dabei helfen zu verstehen, was mit Ihren Daten passiert, indem Sie die Arten von Informationen anzeigen, die Sie haben. Beispielsweise kann eine Kategorie wie *Lebensläufe* oder *Mitarbeiterverträge* sensible Daten enthalten. Wenn Sie die Ergebnisse untersuchen, können Sie feststellen, dass Mitarbeiterverträge an einem unsicheren Ort gespeichert sind. Sie können das Problem dann beheben.

Sie können der BlueXP Klassifizierung benutzerdefinierte Kategorien hinzufügen, damit Sie erkennen können, in welchen Kategorien von Informationen Sie Ihre Daten finden, die speziell für Ihren Datenbestand sind. Jede Kategorie fügen Sie hinzu, indem Sie „Trainingsdateien“ erstellen, die die Datenkategorien enthalten, die Sie identifizieren möchten. Anschließend lässt die BlueXP Klassifizierung diese Dateien scannen, um sie über KI zu „lernen“, damit die Daten in Ihren Datenquellen identifiziert werden können. Die Kategorien werden zu den vorhandenen vordefinierten Kategorien hinzugefügt, die durch die BlueXP Klassifizierung bereits identifiziert werden. Die Ergebnisse sind im Abschnitt „Kategorien“ sichtbar.

Sie können beispielsweise sehen, wo sich komprimierte Installationsdateien im .gz-Format in Ihren Dateien befinden, damit Sie sie bei Bedarf entfernen können.

Nach der Aktualisierung der benutzerdefinierten Kategorien wird die BlueXP Klassifizierung alle Datenquellen neu gescannt. Nach Abschluss des Scans werden die neuen Ergebnisse im BlueXP Klassifizierungs-Compliance-Dashboard im Abschnitt „Kategorien“ und auf der Untersuchungsseite im Filter „Kategorie“ angezeigt. "Lesen Sie, wie Sie Dateien nach Kategorien anzeigen".

Was Sie benötigen

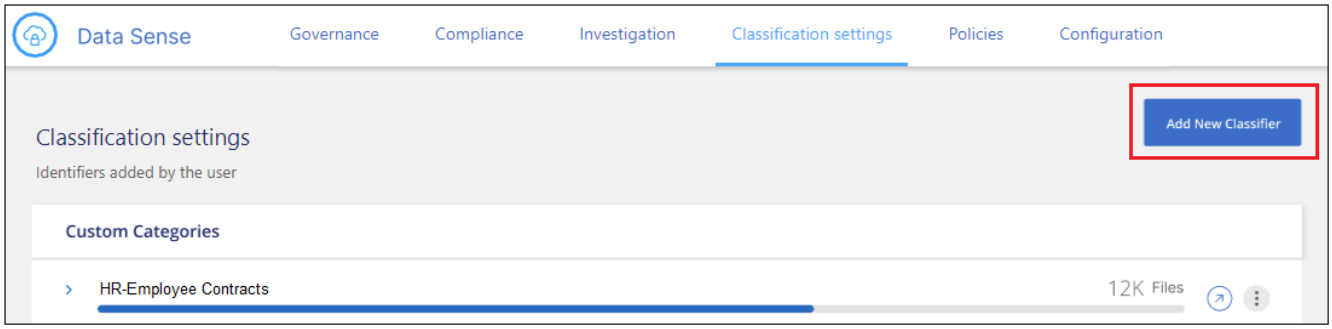
Sie müssen mindestens 25 Trainingsdateien erstellen, die Beispiele für die Datenkategorien enthalten, die von der BlueXP Klassifizierung erkannt werden sollen. Die folgenden Dateitypen werden unterstützt:

```
.CSV, .DOC, .DOCX, .GZ, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs,
Sheets, and Slides
```

Die Dateien müssen mindestens 100 Byte groß sein und sich in einem Ordner befinden, auf den BlueXP Zugriff bietet.

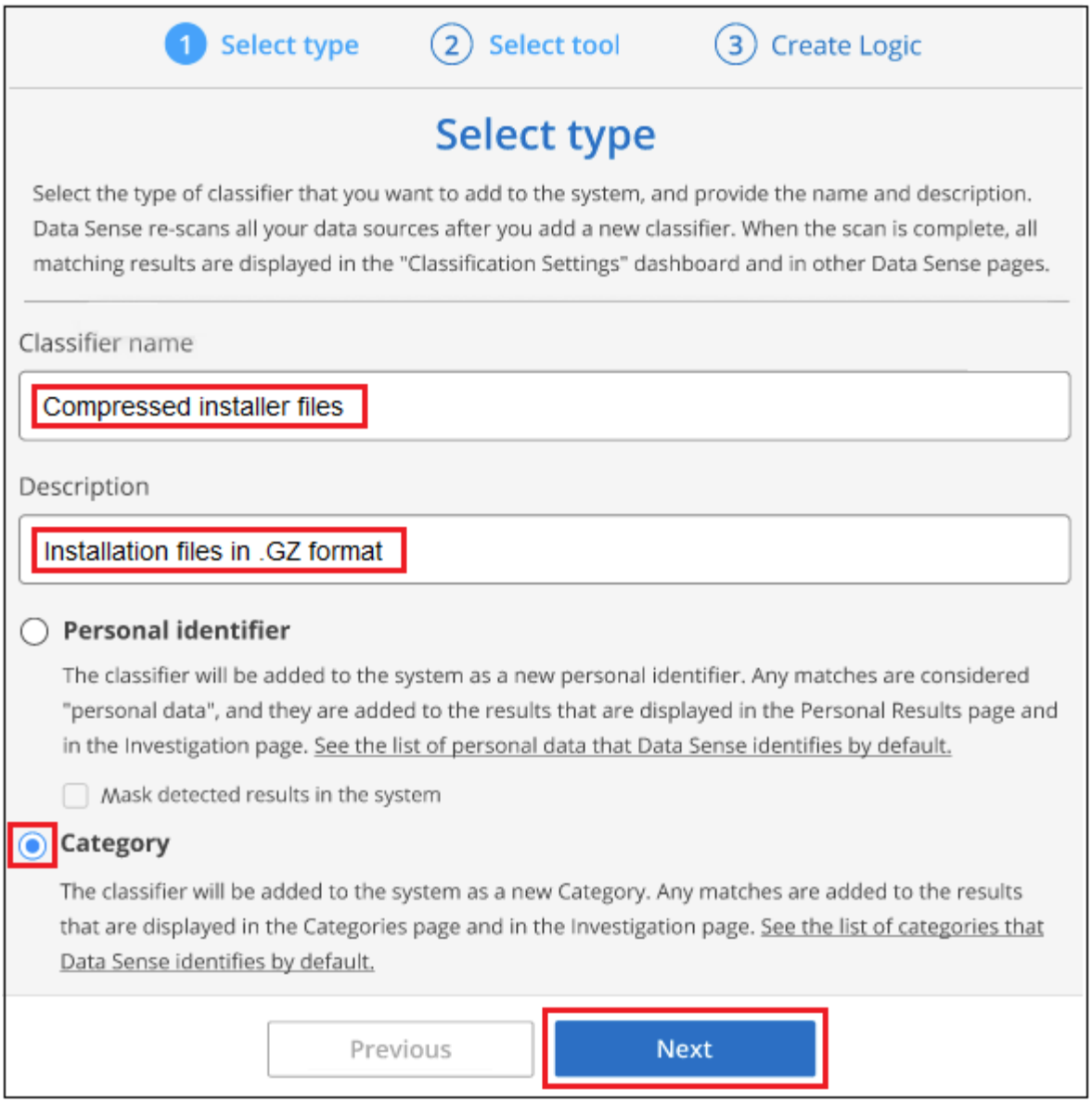
Schritte

1. Klicken Sie auf der Registerkarte *Classification settings* auf **Add New Classifier**, um den Assistenten *Add Custom Classifier* zu starten.

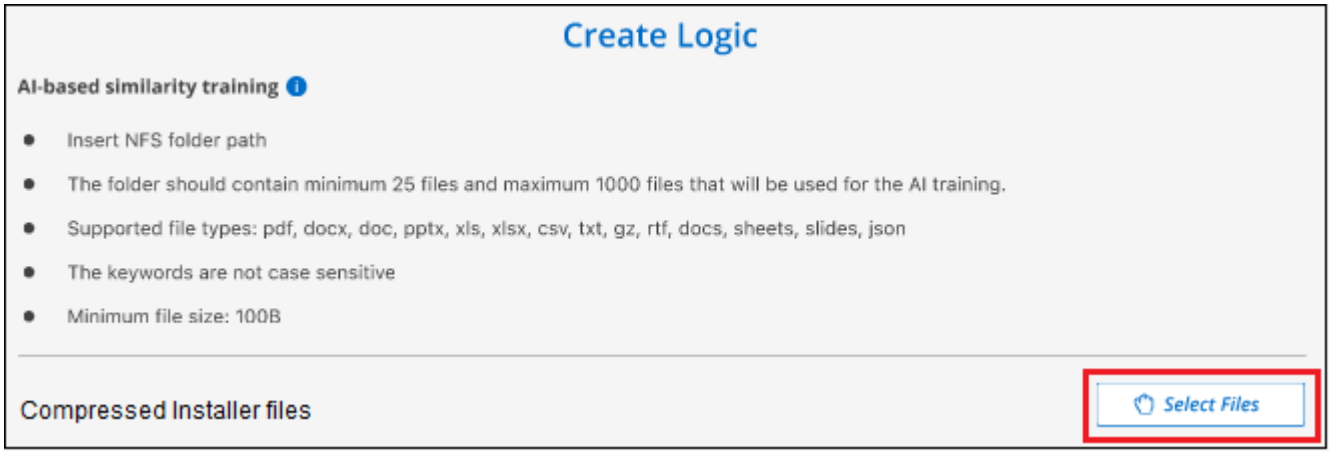


2. Geben Sie auf der Seite *Select type* den Namen des Klassifikators ein, geben Sie eine kurze Beschreibung ein, wählen Sie **Category** aus und klicken Sie dann auf **Next**.

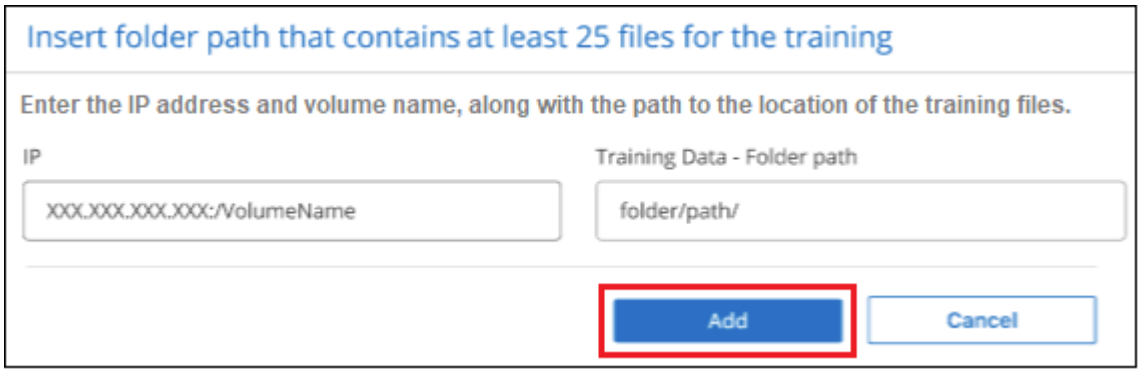
   Der eingegebene Name wird in der BlueXP Klassifizierungs-UI als Überschrift für gescannte Dateien angezeigt, die der von Ihnen definierten Datenkategorie entsprechen, und als Name des Filters auf der Seite Untersuchung.



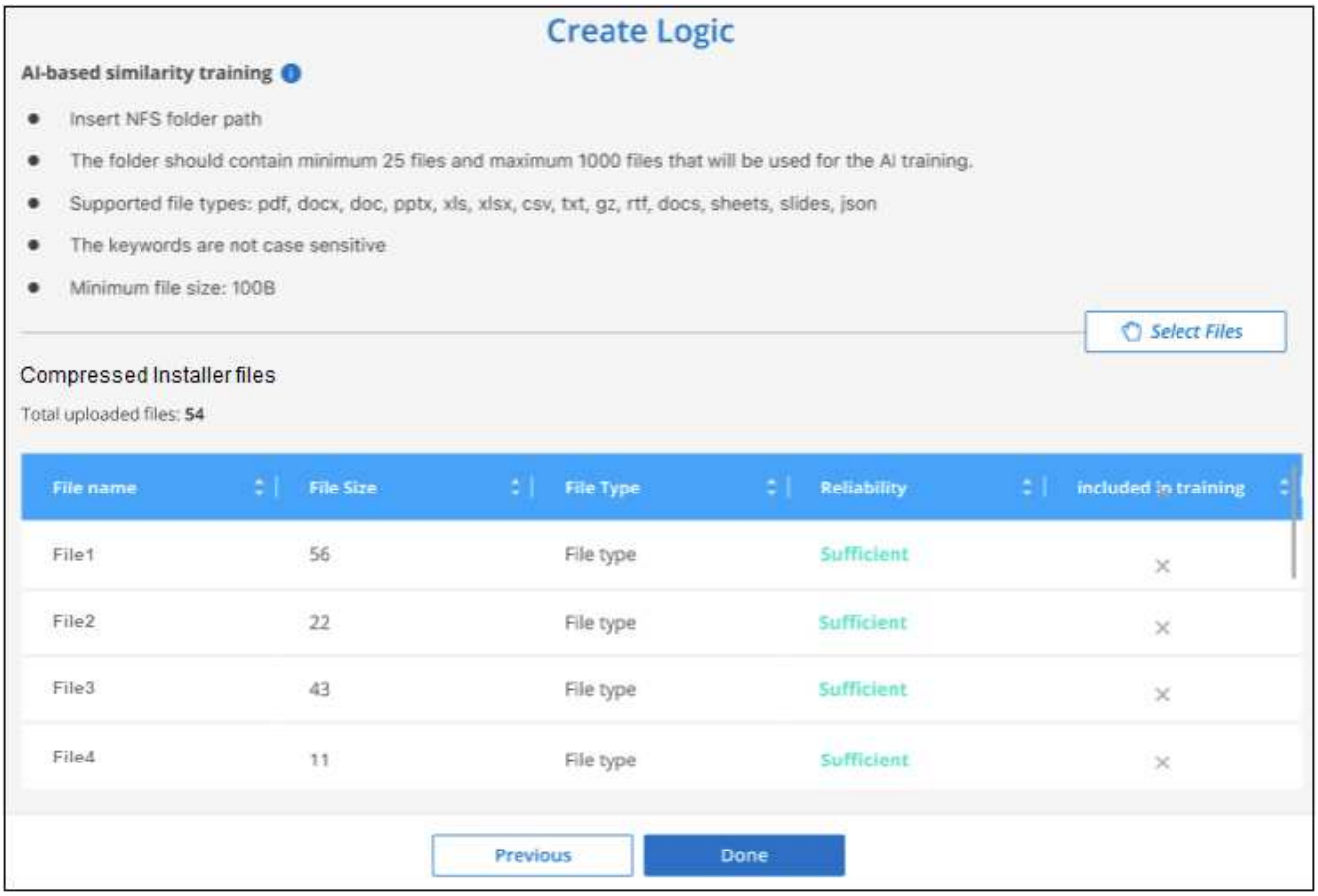
3. Stellen Sie auf der Seite *Create Logic* sicher, dass Sie die Lerndateien vorbereitet haben, und klicken Sie dann auf **Select files**.



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



5. Überprüfen Sie, ob die Trainingsdateien von der BlueXP Klassifizierung erkannt wurden. Klicken Sie auf **x**, um alle Trainingsdateien zu entfernen, die nicht den Anforderungen entsprechen. Klicken Sie dann auf **Fertig**.

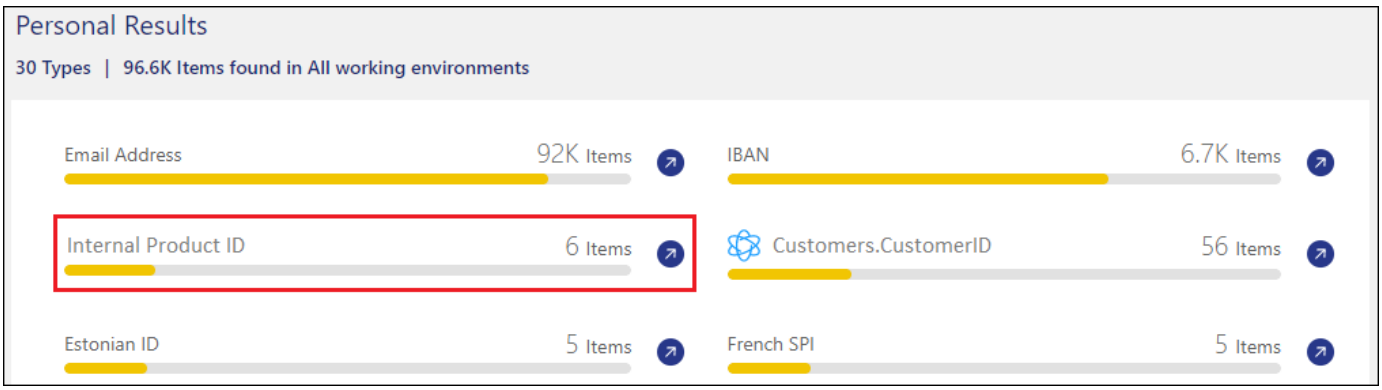


Ergebnisse

Die neue Kategorie wird gemäß den Trainingsdateien erstellt und der BlueXP Klassifizierung hinzugefügt. Die BlueXP Klassifizierung beginnt dann, alle Datenquellen neu zu scannen, um Dateien zu identifizieren, die in diese neue Kategorie passen. Sie kehren zur Seite Benutzerdefinierte Klassifikatoren zurück, auf der Sie die Anzahl der Dateien anzeigen können, die Ihrer neuen Kategorie entsprechen. Die Ergebnisse aus dem Scannen aller Ihrer Datenquellen werden je nach Anzahl der zu scannenden Dateien einige Zeit in Anspruch nehmen.

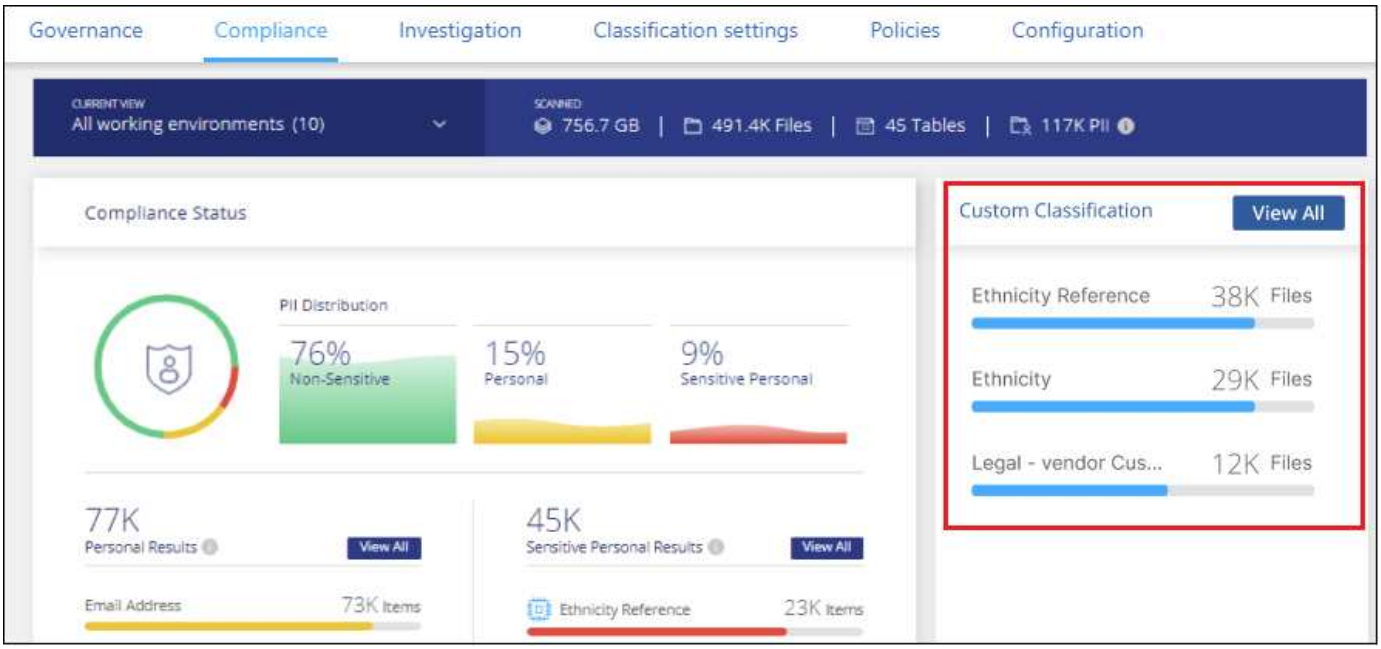
Ergebnisse von Ihren benutzerdefinierten Klassifikatoren anzeigen

Sie können die Ergebnisse von einem Ihrer benutzerdefinierten Klassifikatoren im Compliance Dashboard und auf der Untersuchungsseite anzeigen. In diesem Screenshot werden beispielsweise die übereinstimmenden Informationen im Compliance-Dashboard im Abschnitt „Persönliche Ergebnisse“ angezeigt.



Klicken Sie auf das Um die detaillierten Ergebnisse auf der Untersuchungsseite anzuzeigen.

Darüber hinaus werden alle benutzerdefinierten Klassifikatorergebnisse auf der Registerkarte Benutzerdefinierte Klassifikatoren angezeigt, und die oberen 6 benutzerdefinierten Klassifikatorergebnisse werden wie unten gezeigt im Compliance Dashboard angezeigt.



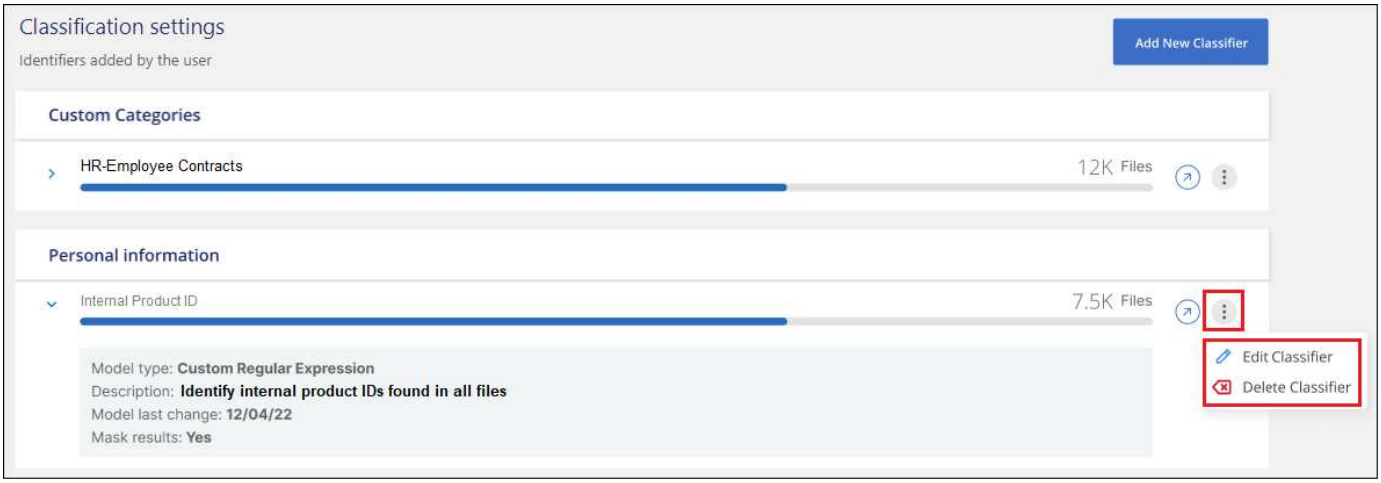
Benutzerdefinierte Klassifikatoren verwalten

Sie können alle benutzerdefinierten Klassifikatoren ändern, die Sie mit der Schaltfläche **Klassifikator bearbeiten** erstellt haben.

Sie können derzeit keine Data Fusion-Klassifikatoren bearbeiten.

Und wenn Sie zu einem späteren Zeitpunkt entscheiden, dass Sie keine BlueXP-Klassifizierung benötigen, um die von Ihnen hinzugefügten benutzerdefinierten Muster zu identifizieren, können Sie die Schaltfläche

Klassifikator löschen verwenden, um jedes Element zu entfernen.



Ausschließen bestimmter Verzeichnisse von den Klassifikationsscans von BlueXP

Wenn die BlueXP Klassifizierung Scandaten in bestimmten Datenquellen-Verzeichnissen ausschließen soll, können Sie diese Verzeichnisnamen zu einer Konfigurationsdatei hinzufügen. Nachdem Sie diese Änderung angewendet haben, schließt die BlueXP Klassifizierungs-Engine Scandaten in diesen Verzeichnissen aus.

Beachten Sie, dass die BlueXP Klassifizierung standardmäßig so konfiguriert ist, dass die Scan-Volume-Snapshot-Daten ausgeschlossen werden, da dieser Inhalt mit dem Inhalt des Volumes identisch ist.

Diese Funktion ist ab Version 1.29 der BlueXP Klassifizierung verfügbar (ab März 2024).

Unterstützte Datenquellen

Der Ausschluss bestimmter Verzeichnisse aus der BlueXP Klassifizierungs-Scans wird für NFS- und CIFS-Freigaben in den folgenden Datenquellen unterstützt:

- On-Premises-ONTAP
- Cloud Volumes ONTAP
- Amazon FSX für NetApp ONTAP
- Azure NetApp Dateien
- Allgemeine Dateifreigaben

Definieren Sie die Verzeichnisse, die vom Scannen ausgeschlossen werden sollen

Bevor Sie Verzeichnisse von der Klassifizierungsüberprüfung ausschließen können, müssen Sie sich beim BlueXP Klassifizierungssystem anmelden, damit Sie eine Konfigurationsdatei bearbeiten und ein Skript ausführen können. Informieren Sie sich darüber "Melden Sie sich beim BlueXP Klassifizierungssystem an" Je nachdem, ob Sie die Software manuell auf einem Linux-Rechner installiert haben oder ob Sie die Instanz in der Cloud bereitgestellt haben.

- Pro BlueXP Klassifizierungssystem können Sie maximal 50 Verzeichnispfade ausschließen.
- Das Ausschließen von Verzeichnispfaden kann sich auf die Scanzeiten auswirken.

Schritte

1. Öffnen Sie auf dem BlueXP Klassifizierungssystem die Datei unter „/opt/netapp/config/Custom_Configuration“ `data_provider.yaml`.
2. Geben Sie im Bereich „Data_Providers“ unter der Zeile „exclude:“ die auszuschließenden Verzeichnispfade ein. Beispiel:

   ```
   exclude:
   - "folder1"
   - "folder2"
   ```

   Ändern Sie nichts anderes in dieser Datei.

3. Speichern Sie die Änderungen in der Datei.
4. Gehen Sie zu „/opt/netapp/Datense/Tools/Customer_Configuration/Data_Providers“ und führen Sie das folgende Skript aus:

   ```
   update_data_providers_from_config_file.sh
   ```

   Mit diesem Befehl werden die Verzeichnisse, die vom Scannen ausgeschlossen werden sollen, an die Klassifizierungs-Engine übergeben.

Ergebnis

Alle nachfolgenden Scans Ihrer Daten schließen das Scannen dieser angegebenen Verzeichnisse aus.

Mit den gleichen Schritten können Sie Elemente aus der Ausschlussliste hinzufügen, bearbeiten oder löschen. Die überarbeitete Ausschlussliste wird aktualisiert, nachdem Sie das Skript ausgeführt haben, um Ihre Änderungen zu übernehmen.

Beispiele

Konfiguration 1:

Jeder Ordner, der an einer beliebigen Stelle im Namen „folder1“ enthält, wird von allen Datenquellen ausgeschlossen.

```
data_providers:
   exclude:
   - "folder1"
```

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO1/folder1
- /CVO1/folder1Name

- /CVO1/folder10
- /CVO1/*folder1
- /CVO1/+folder1Name
- /CVO1/notfolder10
- /CVO22/folder1
- /CVO22/folder1Name
- /CVO22/folder10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO1/*Ordner
- /CVO1/Ordnername
- /CVO22/*folder20

Konfiguration 2:

Jeder Ordner, der "*folder1" nur am Anfang des Namens enthält, wird ausgeschlossen.

```
data_providers:
   exclude:
   - "\\*folder1"
```

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO/*folder1
- /CVO/*folder1Name
- /CVO/*folder10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO/folder1
- /CVO/folder1Name
- /CVO/Not*folder10

Konfiguration 3:

Jeder Ordner in der Datenquelle „CVO22“, der „folder1“ irgendwo im Namen enthält, wird ausgeschlossen.

```
data_providers:
   exclude:
   - "CVO22/folder1"
```

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO22/folder1
- /CVO22/folder1Name
- /CVO22/folder10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO1/folder1
- /CVO1/folder1Name
- /CVO1/folder10

Sonderzeichen in Ordnernamen werden entfernt

Wenn Sie einen Ordnernamen haben, der eines der folgenden Sonderzeichen enthält und Sie Daten in diesem Ordner vom Scannen ausschließen möchten, müssen Sie die Escape-Sequenz \\ vor dem Ordnernamen verwenden.

```
 ., +, *, ?, ^, $, (, ), [, ], {, }, |
Beispiel:
```

Pfad in Quelle: `/project/*not_to_scan`

Syntax in Ausschlussdatei: `"\\*not_to_scan"`

Aktuelle Ausschlussliste anzeigen

Es ist möglich für den Inhalt des `data_provider.yaml` Die Konfigurationsdatei muss sich von der Datei unterscheiden, die nach dem Ausführen des festgelegt wurde `update_data_providers_from_config_file.sh` Skript: Um die aktuelle Liste der Verzeichnisse anzuzeigen, die Sie nicht beim Klassifizierungs-Scan von BlueXP berücksichtigt haben, führen Sie den folgenden Befehl von „/opt/netapp/Datense/Tools/Customer_Configuration/Data_Providers“ aus:

```
get_data_providers_configuration.sh
```

Anzeigen des Status Ihrer Compliance-Aktionen

Wenn Sie eine asynchrone Aktion aus dem Bereich Untersuchungsergebnisse über viele Dateien ausführen, z. B. das Verschieben oder Löschen von 100 Dateien, kann der Prozess einige Zeit in Anspruch nehmen. Sie können den Status dieser Aktionen im Fenster „*Action Status* “ überwachen, sodass Sie wissen, wann sie auf alle Dateien angewendet wurde.

Auf diese Weise können Sie die Aktionen sehen, die erfolgreich abgeschlossen wurden, die derzeit in Bearbeitung sind und die, die nicht erfolgreich waren, damit Sie Probleme diagnostizieren und beheben können. Beachten Sie, dass kurze Vorgänge, die schnell abgeschlossen werden, z. B. das Verschieben einer einzelnen Datei, nicht im Bereich Aktionsstatus angezeigt werden.

Der Status kann lauten:

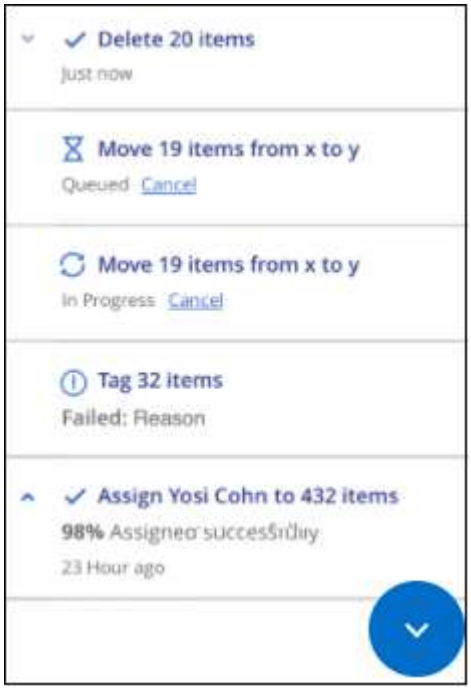
- Erfolg – Eine BlueXP Klassifizierungsaktion wurde abgeschlossen und alle Elemente erfolgreich abgeschlossen.
- Teilweiser Erfolg: Eine BlueXP-Klassifizierungsaktion ist abgeschlossen, einige Elemente sind fehlgeschlagen, einige erfolgreich.

- In Bearbeitung – die Aktion läuft noch.
- Warteschlange: Die Aktion wurde nicht gestartet.
- Storniert: Die Aktion wurde abgebrochen.
- Fehlgeschlagen - die Aktion ist fehlgeschlagen.

Beachten Sie, dass Sie alle Aktionen mit dem Status „in Bearbeitung“ oder „in Bearbeitung“ abbrechen können.

Schritte

1. Rechts unten auf der BlueXP-Klassifikations-UI sehen Sie die Schaltfläche **Actions Status**  .
2. Klicken Sie auf diese Schaltfläche, und die letzten 20 Aktionen werden aufgelistet.



Sie können auf den Namen einer Aktion klicken, um die entsprechenden Details anzuzeigen.

Definieren Sie zusätzliche Gruppen-IDs als für die Organisation offen

Wenn Gruppen-IDs (GIDs) an Dateien oder Ordner in NFS-Dateifreigaben angehängt werden, definieren sie die Berechtigungen für die Datei oder den Ordner, z. B. ob sie „für die Organisation offen“ sind. Wenn einige Gruppen-IDs (GIDs) zunächst nicht mit der Berechtigungsebene „für Organisation öffnen“ eingerichtet wurden, können Sie diese Berechtigung zur GID hinzufügen, sodass alle Dateien und Ordner, die mit dieser GID verknüpft sind, als „für die Organisation offen“ gelten.

Nachdem Sie diese Änderung vorgenommen und die BlueXP-Klassifizierung Ihre Dateien und Ordner erneut scannt, werden alle Dateien und Ordner, denen diese Gruppen-IDs angehängt sind, auf der Seite

„Ermittlungsdetails“ diese Berechtigung angezeigt. Sie werden auch in Berichten angezeigt, in denen Sie Dateiberechtigungen anzeigen.

Um diese Funktion zu aktivieren, müssen Sie sich beim BlueXP Klassifizierungssystem anmelden, damit Sie eine Konfigurationsdatei bearbeiten und ein Skript ausführen können. Informieren Sie sich darüber "Melden Sie sich beim BlueXP Klassifizierungssystem an" Je nachdem, ob Sie die Software manuell auf einem Linux-Rechner installiert haben oder ob Sie die Instanz in der Cloud bereitgestellt haben.

Fügen Sie den Gruppen-IDs die Berechtigung „für Organisation öffnen“ hinzu

Sie müssen die Gruppen-ID-Nummern (GIDs) haben, bevor Sie diese Aufgabe starten.

Schritte

1. Öffnen Sie auf dem BlueXP Klassifizierungssystem die Datei unter „/opt/netapp/config/Custom_Configuration“ `data_provider.yaml`.
2. Fügen Sie in der Zeile "Organisation_Group_ids: []" die Gruppen-IDs hinzu. Beispiel:

   ```
   organization_group_ids: [1014, 1015, 21, 2021, 1013, 2020, 1018, 1019]
   ```

   Ändern Sie nichts anderes in dieser Datei.

3. Speichern Sie die Änderungen in der Datei.
4. Gehen Sie zu „/opt/netapp/Datense/Tools/Customer_Configuration/Data_Providers“ und führen Sie das folgende Skript aus:

   ```
   update_data_providers_from_config_file.sh
   ```

   Mit diesem Befehl werden die überarbeiteten Gruppen-ID-Berechtigungen für die Klassifizierungs-Engine übertragen.

Ergebnis

Bei allen nachfolgenden Scans Ihrer Daten werden Dateien oder Ordner identifiziert, bei denen diese Gruppen-IDs als „für Unternehmen offen“ angehängt sind.

Mit den gleichen Schritten können Sie die Liste der Gruppen-IDs bearbeiten und alle Gruppen-IDs löschen, die Sie in der Vergangenheit hinzugefügt haben. Die überarbeitete Liste der Gruppen-IDs wird aktualisiert, nachdem Sie das Skript ausgeführt haben, um Ihre Änderungen zu übernehmen.

Die aktuelle Liste der Gruppen-IDs anzeigen

Es ist möglich für den Inhalt des `data_provider.yaml` Die Konfigurationsdatei muss sich von der Datei unterscheiden, die nach dem Ausführen des festgelegt wurde `update_data_providers_from_config_file.sh` Skript: Um die aktuelle Liste der Gruppen-IDs anzuzeigen, die Sie der BlueXP Klassifizierung hinzugefügt haben, führen Sie den folgenden Befehl von „/opt/netapp/Datense/Tools/Customer_Configuration/Data_Providers“ aus:

```
get_data_providers_configuration.sh
```

Audit der Historie der BlueXP Klassifizierungsaktionen

Die BlueXP Klassifizierungs-Logs managen-Aktivitäten, die an Dateien aus allen Arbeitsumgebungen und Datenquellen ausgeführt wurden, die von der BlueXP Klassifizierung gescannt werden. Die BlueXP Klassifizierung protokolliert auch die Aktivitäten, wenn Sie eine BlueXP Klassifizierungsinstanz implementieren.

Sie können den Inhalt der BlueXP Klassifizierungs-Audit-Protokolldateien anzeigen oder herunterladen, um festzustellen, welche Dateiänderungen wann vorgenommen wurden. Beispielsweise können Sie sehen, welche Anfrage erstellt wurde, wann die Anfrage gestellt wurde, und Details wie den Quellspeicherort für das Löschen einer Datei oder den Quell- und Zielstandort, falls eine Datei verschoben wurde.

Inhalt der Protokolldatei protokollieren

Jede Zeile im Auditprotokoll enthält Informationen in diesem Format:

```
<full date> | <status> | ds_audit_logger | <module> | 0 | 0 | File <full file
path> deleted from device <device path> - <result>
```

- Datum und Uhrzeit: Vollständiger Zeitstempel für das Ereignis
- Status - INFO, WARNUNG
- Aktionstyp (Löschen, Kopieren, Verschieben, Erstellen einer Richtlinie, Aktualisieren der Richtlinie, Dateien erneut scannen, JSON-Bericht herunterladen usw.)
- Dateiname (wenn die Aktion für eine Datei relevant ist)
- Details zur Aktion - was getan wurde: Hängt von der Aktion ab
  - Name der Richtlinie
  - Für Move - Quelle und Ziel
  - Für Copy - Quelle und Ziel
  - Für Tag - Tag-Name
  - Zum Zuweisen an - Benutzername
  - Für E-Mail Alert - E-Mail-Adresse / Konto

Beispielsweise zeigen die folgenden Zeilen aus der Protokolldatei einen erfolgreichen Kopiervorgang und einen fehlerhaften Kopiervorgang an.

```
2022-06-06 15:23:08,910 | INFO | ds_audit_logger | es_scanned_file | 237 |
49 | Copy file /CIFS_share/data/dop1/random_positives.tsv from device
10.31.133.183 (type: SMB_SHARE) to device 10.31.130.133:/export_reports
(NFS_SHARE) - SUCCESS
2022-06-06 15:23:08,968 | WARNING | ds_audit_logger | es_scanned_file |
239 | 153 | Copy file /CIFS_share/data/compliance-netapp.tar.gz from
device 10.31.133.183 (type: SMB_SHARE) to device
10.31.130.133:/export_reports (NFS_SHARE) - FAILURE
```

Speicherorte der Protokolldateien

Die Management-Audit-Log-Dateien befinden sich auf der BlueXP Klassifizierungs-Maschine in: `/opt/netapp/audit_logs/`

Die Audit-Protokolldateien für die Installation werden in geschrieben `/opt/netapp/install_logs/`

Jede Protokolldatei kann maximal 10 MB groß sein. Wenn dieser Grenzwert erreicht wird, wird eine neue Protokolldatei gestartet. Die Log-Dateien werden mit „DataSense_Audit.log“, „DataSense_Audit.log.1“, „DataSense_Audit.log.2“ und so weiter benannt. Es werden maximal 100 Protokolldateien im System gespeichert. Ältere Protokolldateien werden automatisch gelöscht, sobald die maximale Anzahl erreicht wurde.

Greifen Sie auf die Protokolldateien zu

Sie müssen sich beim BlueXP Klassifizierungssystem anmelden, um auf die Protokolldateien zugreifen zu können. Informieren Sie sich darüber "Melden Sie sich beim BlueXP Klassifizierungssystem an" Je nachdem, ob Sie die Software manuell auf einem Linux-Rechner installiert haben oder ob Sie die Instanz in der Cloud bereitgestellt haben.

Reduzierung der Scan-Geschwindigkeit der BlueXP Klassifizierung

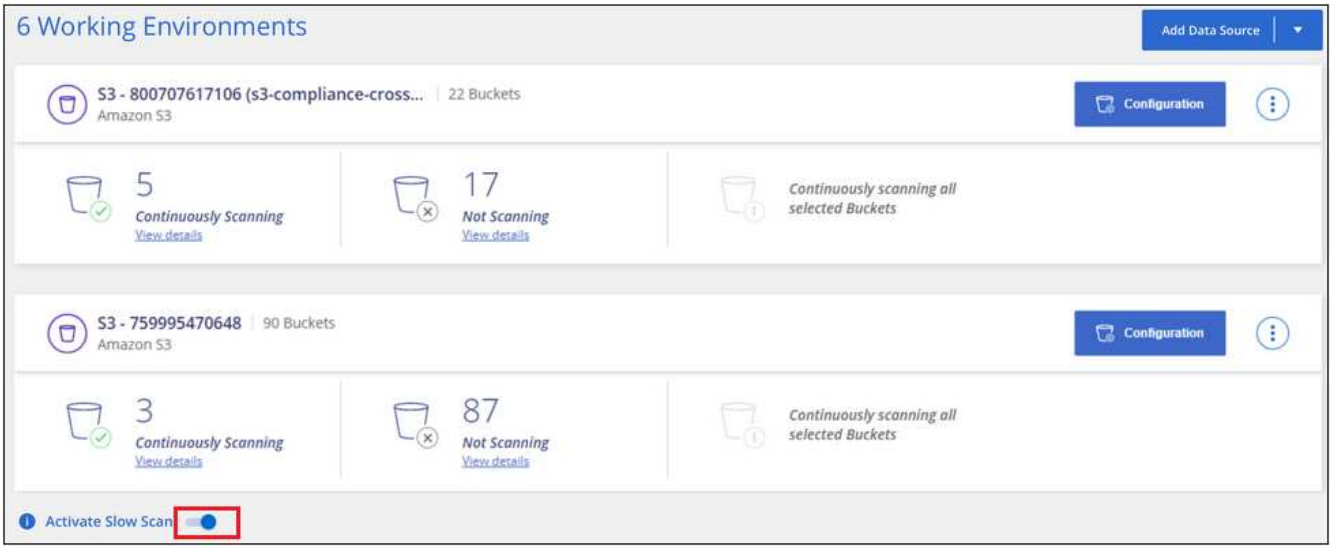
Datenscans haben keine nennenswerten Auswirkungen auf Ihre Storage-Systeme und Ihre Daten. Wenn Sie jedoch auch nur geringe Auswirkungen haben, können Sie die BlueXP-Klassifizierung für „langsame“ Scans konfigurieren.

Wenn diese Option aktiviert ist, wird langsames Scannen auf allen Datenquellen verwendet. Sie können den langsamen Scan nicht für eine einzige Arbeitsumgebung oder Datenquelle konfigurieren.

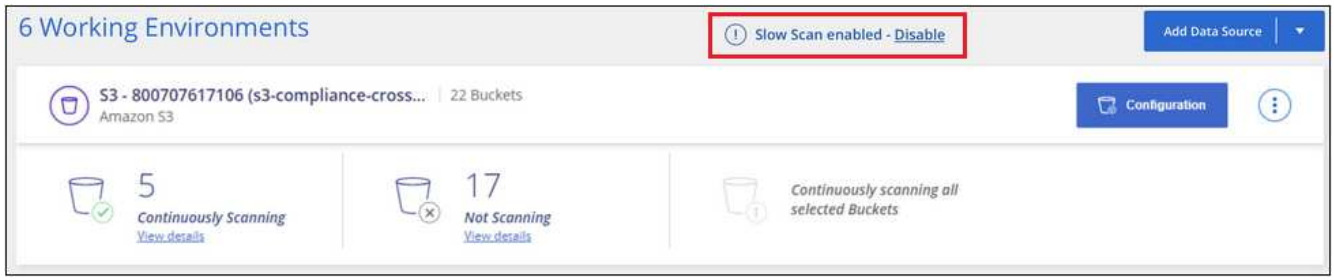
Die Scan-Geschwindigkeit kann beim Scannen von Datenbanken nicht verringert werden.

Schritte

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



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



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

Entfernen von Datenquellen aus der BlueXP Klassifizierung

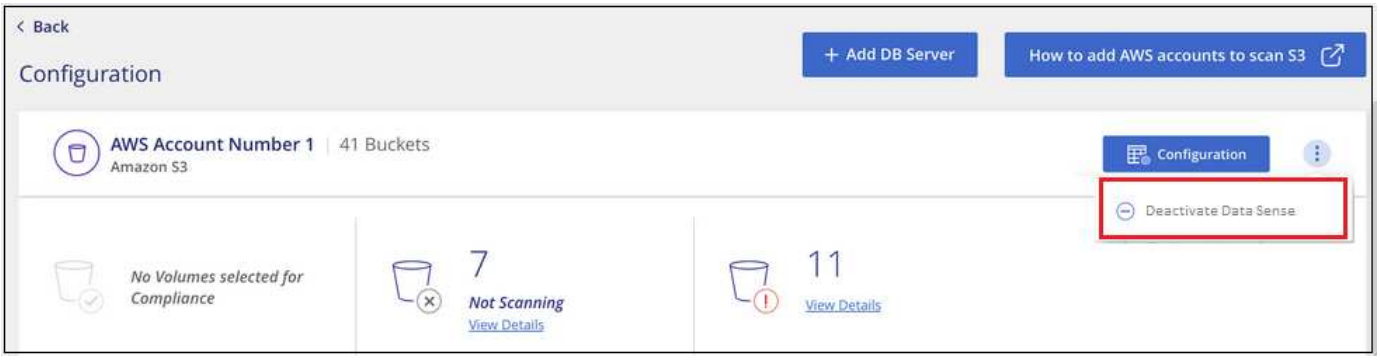
Falls erforderlich können Sie die BlueXP Klassifizierung dadurch beenden, dass sie eine oder mehrere Arbeitsumgebungen, Datenbanken, Dateifreigabegruppen, OneDrive-Konten, Google Drive-Konten scannt. Oder SharePoint-Konten.

Der Ladevorgang zum Scannen der Daten wird angehalten, wenn die Datenquelle entfernt wird.

Deaktivieren von Compliance-Scans für eine Arbeitsumgebung

Wenn Sie Scans deaktivieren, scannt die BlueXP Klassifizierung die Daten nicht mehr in der Arbeitsumgebung und entfernt die indizierten Compliance-Einblicke aus der BlueXP Klassifizierungsinstanz (die Daten aus der Arbeitsumgebung werden nicht gelöscht).

1. Klicken Sie auf der Seite *Configuration* auf ⋮ Klicken Sie in der Zeile für die Arbeitsumgebung auf **Data Sense deaktivieren**.



Sie können bei der Auswahl der Arbeitsumgebung auch die Compliance-Scans für eine Arbeitsumgebung im Fenster „Services“ deaktivieren.

Entfernen einer Datenbank aus der BlueXP Klassifizierung

Wenn Sie eine bestimmte Datenbank nicht mehr scannen möchten, können Sie sie aus der BlueXP Klassifizierungs-Schnittstelle löschen und alle Scans anhalten.

1. Klicken Sie auf der Seite *Configuration* auf ⋮ Klicken Sie in der Zeile der Datenbank auf **DB Server entfernen**.

Entfernen eines OneDrive-, SharePoint- oder Google Drive-Kontos aus der BlueXP Klassifizierung

Wenn Sie Benutzerdateien nicht mehr von einem bestimmten OneDrive-Konto, von einem bestimmten SharePoint-Konto oder von einem Google Drive-Konto scannen möchten, können Sie das Konto von der BlueXP Klassifizierungsschnittstelle löschen und alle Scans beenden.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf ⋮ Klicken Sie in der Zeile für das OneDrive-, SharePoint- oder Google-Drive-Konto auf **OneDrive-Konto entfernen**, **SharePoint-Konto entfernen** oder **Google-Laufwerkskonto entfernen**.

2. Klicken Sie im Bestätigungsdialogfeld auf **Konto löschen**.

Entfernen einer Gruppe von Dateifreigaben aus der BlueXP Klassifizierung

Wenn Sie Benutzerdateien nicht mehr aus einer Dateifreigaben-Gruppe scannen möchten, können Sie die File Shares Group aus der BlueXP Klassifizierungs-Schnittstelle löschen und alle Scans anhalten.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf ⋮ Klicken Sie in der Zeile für die Datei-Shares-Gruppe und dann auf **Datei-Shares-Gruppe entfernen**.

2. Klicken Sie im Bestätigungsdialogfeld auf **Gruppe von Freigaben löschen**.

BlueXP Klassifizierung wird deinstalliert

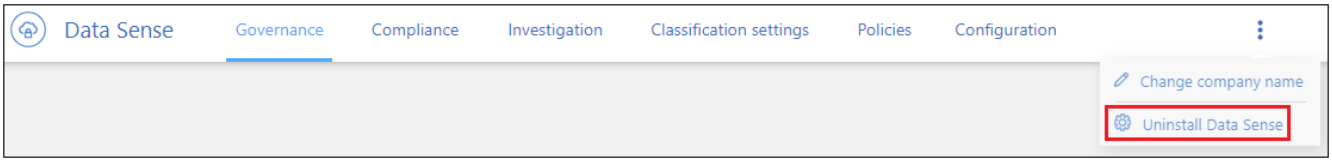
Sie können die BlueXP Klassifizierungssoftware deinstallieren, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen. Wenn Sie die Instanz löschen, werden auch die zugehörigen Festplatten gelöscht, auf denen sich die indizierten Daten befinden. Alle Informationen, die die BlueXP Klassifizierung gescannt hat, werden dauerhaft gelöscht.

Die erforderlichen Schritte hängen davon ab, ob Sie die BlueXP Klassifizierung in der Cloud oder auf einem lokalen Host implementiert haben.

Deinstallieren der BlueXP Klassifizierung aus einer Cloud-Implementierung

Wenn Sie die BlueXP Klassifizierungsinstanz nicht mehr verwenden möchten, können Sie sie deinstallieren oder aus der Cloud-Provider-Umgebung löschen.

1. Klicken Sie oben auf der BlueXP Klassifizierungsseite auf Und klicken Sie dann auf **Data Sense deinstallieren**.



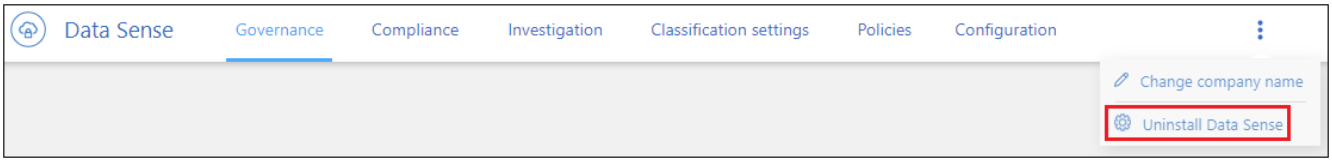
2. Geben Sie im Dialogfeld *Uninstall Data Sense* **uninstall** ein, um zu bestätigen, dass Sie die BlueXP-Klassifikationsinstanz vom BlueXP Connector trennen möchten, und klicken Sie dann auf **Uninstall**.
3. Rufen Sie die Konsole Ihres Cloud-Providers auf und löschen Sie die BlueXP Klassifizierungsinstanz. Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

   Damit werden die Instanz und alle zugehörigen Daten, die durch die BlueXP Klassifizierung erfasst wurden, gelöscht.

Deinstallieren der BlueXP Klassifizierung aus einer lokalen Implementierung

Sie können die BlueXP Klassifizierung von einem Host deinstallieren, wenn Sie nicht mehr die BlueXP Klassifizierung verwenden möchten oder wenn ein Problem aufgetreten ist, das eine Neuinstallation erfordert.

1. Klicken Sie oben auf der BlueXP Klassifizierungsseite auf Und klicken Sie dann auf **Data Sense deinstallieren**.



2. Geben Sie im Dialogfeld *Uninstall Data Sense* **uninstall** ein, um zu bestätigen, dass Sie die BlueXP-

Klassifikationsinstanz vom BlueXP Connector trennen möchten, und klicken Sie dann auf **Uninstall**.

3. Um die Software vom Host zu deinstallieren, führen Sie den aus `cleanup.sh` Skript auf dem Host-Rechner, z. B.:

```
cleanup.sh
```

Informieren Sie sich darüber "Melden Sie sich bei der BlueXP Klassifizierungs-Host-Maschine an".