BlueXP Klassifizierung managen

BlueXP classification

NetApp
June 14, 2024

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

Inhalt

BlueXP Klassifizierung managen

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
```

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` Konfigurationsdatei, die sich von dem unterscheidet, was nach der Ausführung des tatsächlich übertragen 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
```

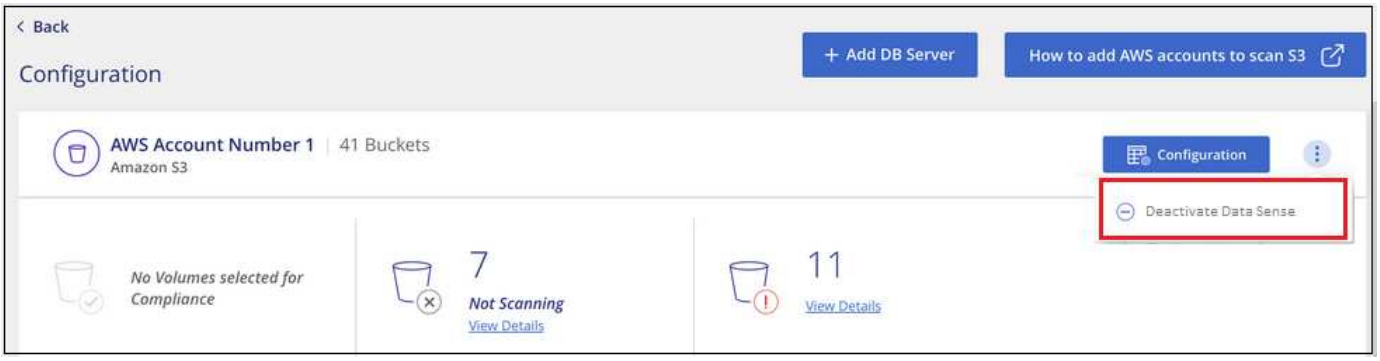
Datenquellen aus der BlueXP Klassifizierung entfernen

Falls erforderlich können Sie die BlueXP Klassifizierung davon abhalten, eine oder mehrere Arbeitsumgebungen, Datenbanken oder Dateifreigabegruppen zu scannen.

Deaktivieren Sie 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**.

Gruppe von Dateifreigaben aus der BlueXP Klassifizierung entfernen

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

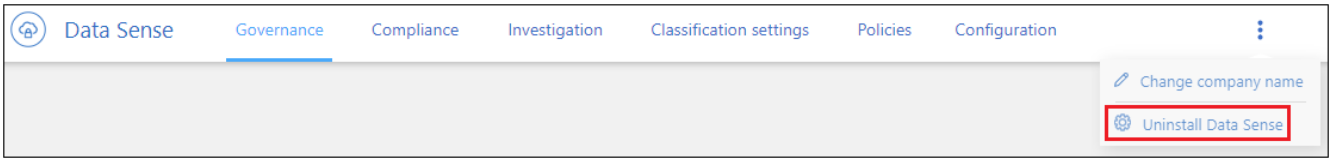
Sie können die BlueXP Klassifizierungssoftware deinstallieren, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen. Wenn Sie die Instanz löschen, werden auch die zugehörigen Festplatten gelöscht, auf denen sich die indizierten Daten befinden. Alle Informationen, die die BlueXP Klassifizierung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



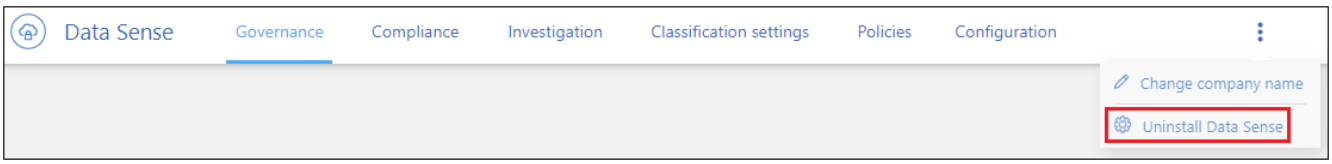
2. Geben Sie im Dialogfeld *Uninstall Data Sense* **uninstall** ein, um zu bestätigen, dass Sie die BlueXP-Klassifikationsinstanz vom BlueXP Connector trennen möchten, und klicken Sie dann auf **Uninstall**.
3. Rufen Sie die Konsole Ihres Cloud-Providers auf und löschen Sie die BlueXP Klassifizierungsinstanz. 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".

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.