Verwalten der Datenklassifizierung

NetApp Data Classification

NetApp
January 14, 2026

Inhalt

Verwalten der Datenklassifizierung

Schließen Sie bestimmte Verzeichnisse von NetApp Data Classification -Scans aus

Wenn Sie möchten, dass NetApp Data Classification bestimmte Verzeichnisse von Scans ausschließt, können Sie diese Verzeichnisnamen zu einer Konfigurationsdatei hinzufügen. Nachdem Sie diese Änderung angewendet haben, schließt die Datenklassifizierungs-Engine diese Verzeichnisse von Scans aus.

Standardmäßig werden bei Datenklassifizierungsscans Volume-Snapshot-Daten ausgeschlossen, die mit ihrer Quelle im Volume identisch sind.

Unterstützte Datenquellen

Das Ausschließen bestimmter Verzeichnisse von Datenklassifizierungsscans wird für NFS- und CIFS-Freigaben in den folgenden Datenquellen unterstützt:

- On-Premises- ONTAP
- Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Allgemeine Dateifreigaben

Definieren Sie die Verzeichnisse, die vom Scan ausgeschlossen werden sollen

Bevor Sie Verzeichnisse vom Klassifizierungsscan ausschließen können, müssen Sie sich beim Datenklassifizierungssystem anmelden, damit Sie eine Konfigurationsdatei bearbeiten und ein Skript ausführen können. Erfahren Sie, wie Sie"Melden Sie sich beim Datenklassifizierungssystem an" abhängig davon, ob Sie die Software manuell auf einem Linux-Rechner installiert oder die Instanz in der Cloud bereitgestellt haben.

Überlegungen

- Sie können maximal 50 Verzeichnispfade pro Datenklassifizierungssystem ausschließen.
- Das Ausschließen von Verzeichnispfaden kann die Scanzeiten beeinträchtigen.

Schritte

1. Gehen Sie im Datenklassifizierungssystem zu "/opt/netapp/config/custom_configuration" und öffnen Sie die Datei `data_provider.yaml` .
2. Geben Sie im Abschnitt „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 an der Datei.
4. Gehen Sie zu „/opt/netapp/Datasense/tools/customer_configuration/data_providers“ und führen Sie das folgende Skript aus:

```
update_data_providers_from_config_file.sh
```

+ Dieser Befehl übergibt die vom Scannen auszuschließenden Verzeichnisse an die Klassifizierungs-Engine.

Ergebnis

Bei allen nachfolgenden Scans Ihrer Daten werden die angegebenen Verzeichnisse nicht gescannt.

Mit denselben Schritten können Sie Elemente zur Ausschlussliste hinzufügen, bearbeiten oder daraus löschen. Die überarbeitete Ausschlussliste wird aktualisiert, nachdem Sie das Skript ausgeführt haben, um Ihre Änderungen zu bestätigen.

Beispiele

Konfiguration 1:

Jeder Ordner, der irgendwo im Namen „folder1“ enthält, wird von allen Datenquellen ausgeschlossen.

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

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO1/Ordner1
- /CVO1/Ordner1name
- /CVO1/Ordner10
- /CVO1/*Ordner1
- /CVO1/+Ordner1name
- /CVO1/notfolder10
- /CVO22/Ordner1
- /CVO22/Ordner1name
- /CVO22/Ordner10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO1/*Ordner
- /CVO1/Ordnername
- /CVO22/*Ordner20

Konfiguration 2:

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

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

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO/*Ordner1
- /CVO/*Ordner1name
- /CVO/*Ordner10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO/Ordner1
- /CVO/Ordner1name
- /CVO/nicht*Ordner10

Konfiguration 3:
Jeder Ordner in der Datenquelle „CVO22“, der irgendwo im Namen „folder1“ enthält, wird ausgeschlossen.

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

Erwartete Ergebnisse für Pfade, die ausgeschlossen werden:

- /CVO22/Ordner1
- /CVO22/Ordner1name
- /CVO22/Ordner10

Beispiele für Pfade, die nicht ausgeschlossen werden:

- /CVO1/Ordner1
- /CVO1/Ordner1name
- /CVO1/Ordner10

Escapezeichen für Sonderzeichen in Ordnernamen

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

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

Pfad in der Quelle: `/project/*not_to_scan`

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

Aktuelle Ausschlussliste anzeigen

Es ist möglich, dass der Inhalt der `data_provider.yaml` Konfigurationsdatei anders sein als das, was tatsächlich nach dem Ausführen des `update_data_providers_from_config_file.sh` Skript. Um die aktuelle Liste der Verzeichnisse anzuzeigen, die Sie vom Datenklassifizierungsscan ausgeschlossen haben, führen Sie den folgenden Befehl von „/opt/netapp/Datasense/tools/customer_configuration/data_providers“ aus:

```
get_data_providers_configuration.sh
```

Definieren Sie zusätzliche Gruppen-IDs als offen für die Organisation in NetApp Data Classification

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

Nachdem Sie diese Änderung vorgenommen haben und NetApp Data Classification Ihre Dateien und Ordner erneut scannt, wird diese Berechtigung für alle Dateien und Ordner mit diesen Gruppen-IDs auf der Seite „Untersuchungsdetails“ angezeigt. Außerdem werden sie in Berichten angezeigt, in denen Sie Dateiberechtigungen anzeigen.

Um diese Funktion zu aktivieren, müssen Sie sich beim Datenklassifizierungssystem anmelden, damit Sie eine Konfigurationsdatei bearbeiten und ein Skript ausführen können. Erfahren Sie, wie Sie"Melden Sie sich beim Datenklassifizierungssystem an" abhängig davon, ob Sie die Software manuell auf einem Linux-Rechner installiert oder die Instanz in der Cloud bereitgestellt haben.

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

Sie müssen über die Gruppen-ID-Nummern (GIDs) verfügen, bevor Sie mit dieser Aufgabe beginnen.

Schritte

1. Gehen Sie im Datenklassifizierungssystem zu "/opt/netapp/config/custom_configuration" und öffnen Sie die Datei `data_provider.yaml` .
2. Fügen Sie in der Zeile „organization_group_ids: []“ die Gruppen-IDs hinzu. Beispiel:

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

   Ändern Sie sonst nichts in dieser Datei.
3. Speichern Sie die Änderungen an der Datei.
4. Gehen Sie zu „/opt/netapp/Datasense/tools/customer_configuration/data_providers“ und führen Sie das folgende Skript aus:

```
update_data_providers_from_config_file.sh
```

Dieser Befehl übergibt die überarbeiteten Gruppen-ID-Berechtigungen an die Klassifizierungs-Engine.

Ergebnis

Bei allen nachfolgenden Scans Ihrer Daten werden Dateien oder Ordner mit diesen Gruppen-IDs als „für die Organisation offen“ gekennzeichnet.

Mit denselben 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.

Aktuelle Liste der Gruppen-IDs anzeigen

Es ist möglich, dass der Inhalt der `data_provider.yaml` Konfigurationsdatei von dem abweicht, was nach dem Ausführen des `update_data_providers_from_config_file.sh` Skript. Um die aktuelle Liste der Gruppen-IDs anzuzeigen, die Sie zur Datenklassifizierung hinzugefügt haben, führen Sie den folgenden Befehl von „/opt/netapp/Datasense/tools/customer_configuration/data_providers“ aus:

```
get_data_providers_configuration.sh
```

Anpassen der Definition veralteter Daten in NetApp Data Classification

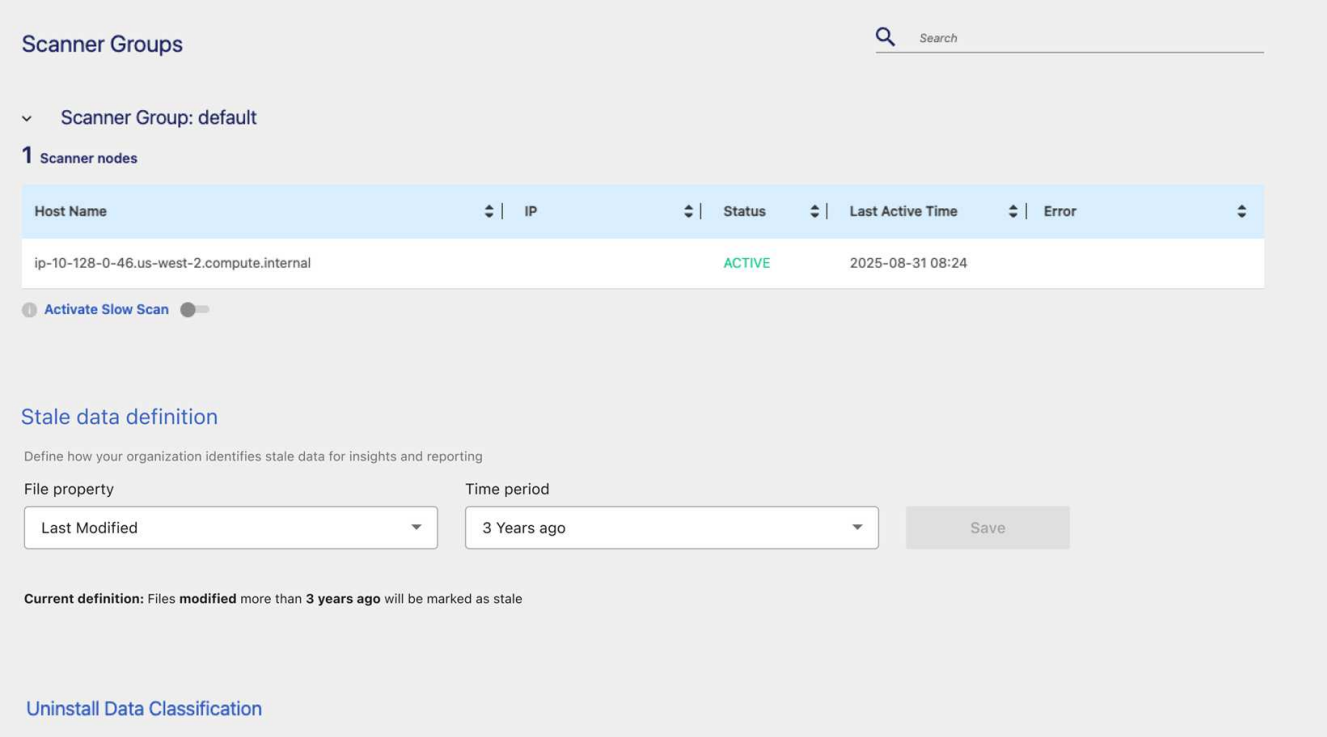
Die NetApp Data Classification identifiziert veraltete Daten, um Ihnen dabei zu helfen, Einsparmöglichkeiten und Governance-Risiken zu erkennen. Da die Definition von veralteten Daten je nach organisatorischem Kontext variieren kann, können Sie anpassen, wie die Datenklassifizierung veraltete Daten definiert.

Veraltete Daten können anhand des Zeitpunkts des letzten Zugriffs oder der letzten Änderung definiert werden. Die wählbaren Zeiträume reichen von vor 6 Monaten bis vor 10 Jahren.

Standardmäßig gelten Daten als veraltet, wenn sie zuletzt vor drei Jahren geändert wurden.

veraltete Daten definieren

1. Wählen Sie unter Ransomware Resilience die Option **Konfiguration**.
2. Scrollen Sie auf der Konfigurationsseite zur Überschrift **Definition veralteter Daten**.
3. Im Dropdown-Menü **Dateieigenschaften** können Sie auswählen, ob veraltete Daten anhand des Zeitpunkts des **zuletzt aufgerufenen** oder des **zuletzt geänderten** Datums definiert werden sollen.
4. Wählen Sie den Zeitraum für die Definition veralteter Daten.



5. Wählen Sie **Speichern**.

Datenquellen aus der NetApp Data Classification entfernen

Bei Bedarf können Sie NetApp Data Classification daran hindern, ein oder mehrere Systeme, Datenbanken oder Dateifreigabegruppen zu scannen.

Deaktivieren von Scans für ein System

Wenn Sie Scans deaktivieren, scannt Data Classification die Daten auf dem System nicht mehr und entfernt die indizierten Erkenntnisse aus der Data Classification-Instanz. Die Daten aus dem System selbst werden nicht gelöscht.

1. Wählen Sie auf der Seite *Konfiguration* die Option Klicken Sie in der Zeile für das System auf die Schaltfläche „Datenklassifizierung deaktivieren“ und anschließend auf „Datenklassifizierung deaktivieren“.

Sie können Scans für ein System auch über das Bedienfeld „Dienste“ deaktivieren, wenn Sie das System auswählen.

Entfernen einer Datenbank aus der Datenklassifizierung

Wenn Sie eine bestimmte Datenbank nicht mehr scannen müssen, können Sie sie aus der Datenklassifizierungsschnittstelle löschen und alle Scans stoppen.

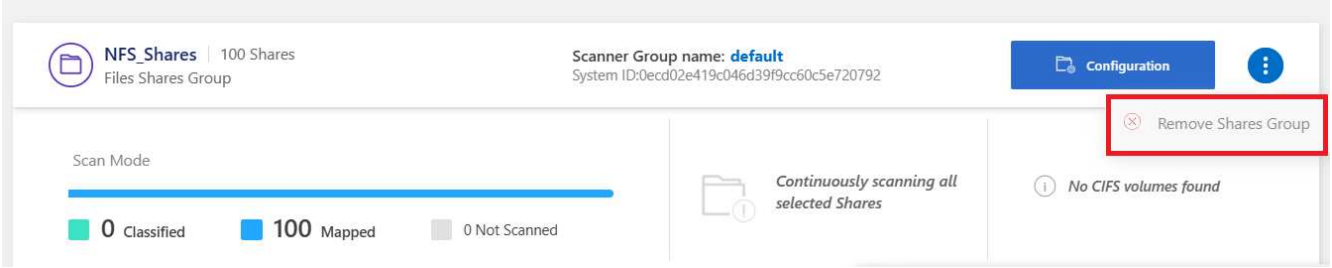
1. Wählen Sie auf der Seite *Konfiguration* die Option Klicken Sie in der Zeile für die Datenbank auf die Schaltfläche „DB-Server entfernen“ und dann auf „DB-Server entfernen“.

Entfernen einer Gruppe von Dateifreigaben aus der Datenklassifizierung

Wenn Sie Benutzerdateien aus einer Dateifreigabegruppe nicht mehr scannen möchten, können Sie die Dateifreigabegruppe aus der Datenklassifizierungsschnittstelle löschen und alle Scans stoppen.

Schritte

1. Wählen Sie auf der Seite *Konfiguration* die Option Klicken Sie in der Zeile für die Dateifreigabegruppe auf die Schaltfläche „Dateifreigabegruppe entfernen“ und dann auf „Dateifreigabegruppe entfernen“.



2. Wählen Sie im Bestätigungsdialogfeld **Freigabegruppe löschen** aus.

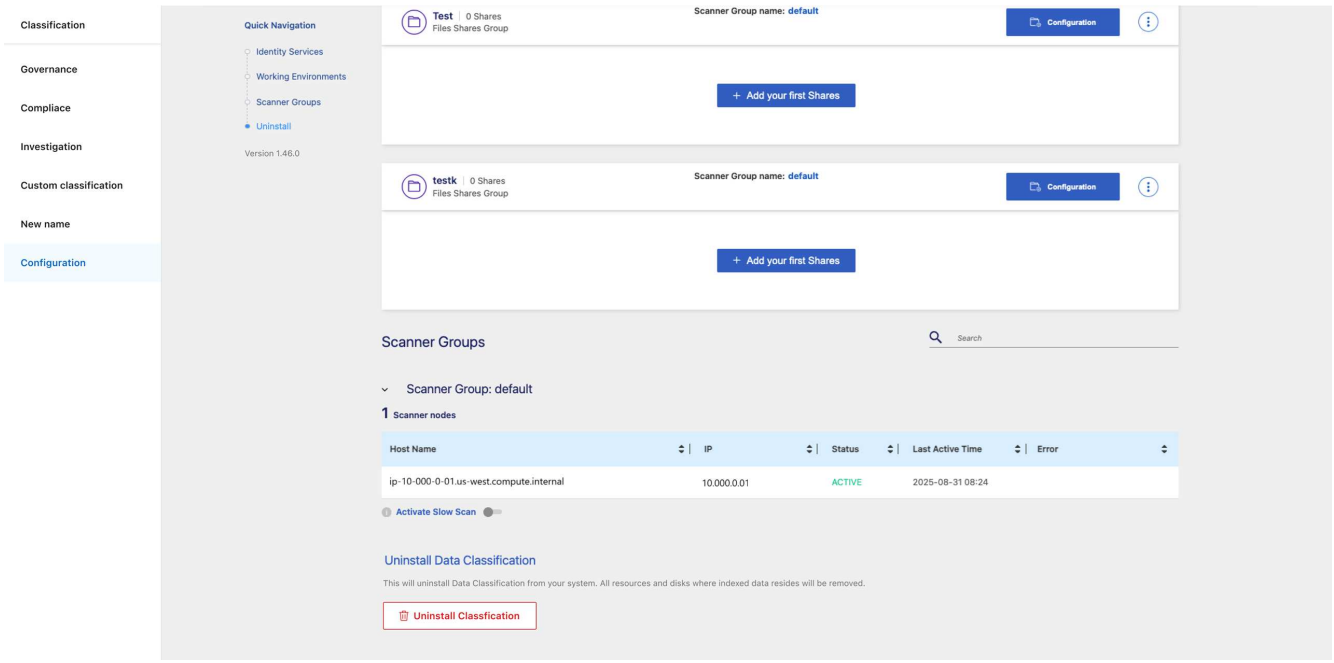
Deinstallieren Sie NetApp Data Classification

Sie können NetApp Data Classification deinstallieren, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen. Durch das Löschen der Instanz werden auch die zugehörigen Datenträger gelöscht, auf denen sich die indizierten Daten befinden. Das bedeutet, dass alle von Data Classification gescannten Informationen dauerhaft gelöscht werden.

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

Deinstallieren Sie Data Classification von einem Cloud-Anbieter

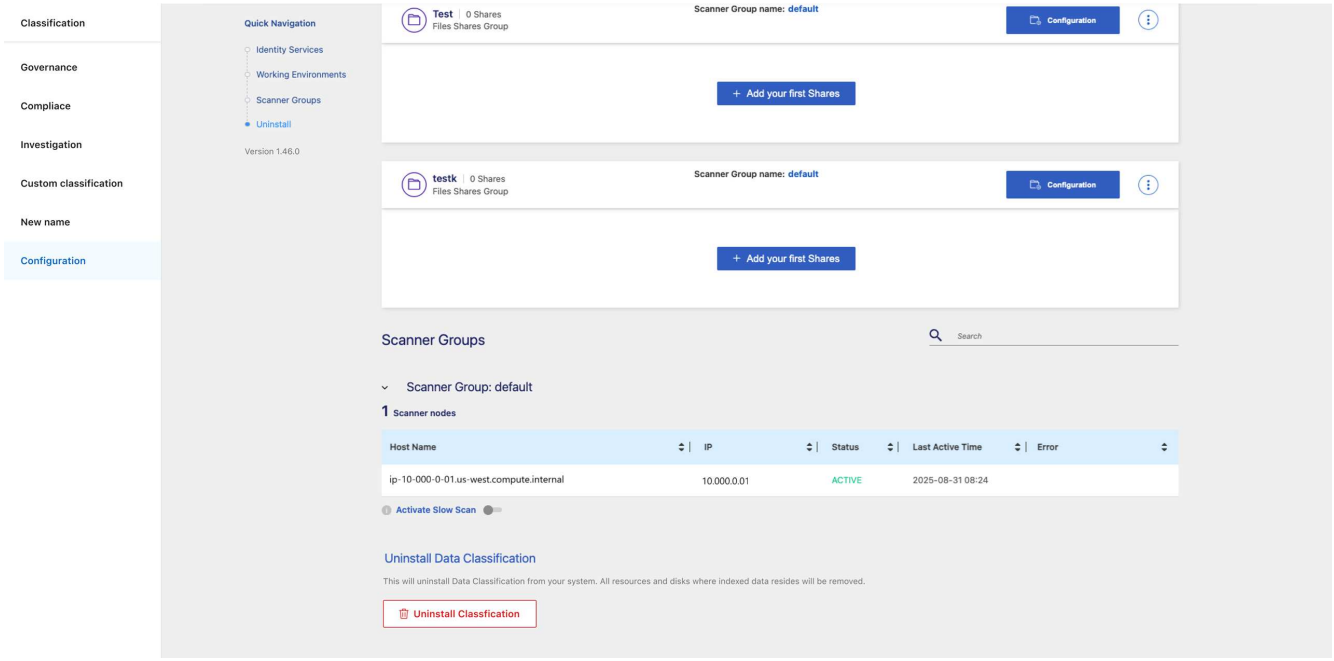
1. Wählen Sie unter „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie unten auf der Konfigurationsseite **Klassifizierung deinstallieren** aus.



3. Geben Sie im Dialogfeld „uninstall“ ein, um mit der Trennung der Data Classification-Instanz vom Konsolenagent fortzufahren. Wählen Sie zur Bestätigung **Deinstallieren**.
4. Geben Sie im Dialogfeld „Klassifizierung deinstallieren“ **deinstallieren** ein, um zu bestätigen, dass Sie die Datenklassifizierungsinstanz vom Konsolenagenten trennen möchten, und wählen Sie dann **Deinstallieren** aus.
5. Um den Deinstallationsvorgang abzuschließen, gehen Sie zur Konsole Ihres Cloud-Anbieters und löschen Sie die Data Classification-Instanz. Die Instanz trägt den Namen *CloudCompliance* und ist mit einem generierten Hash (UUID) verknüpft. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Deinstallieren der Datenklassifizierung aus einer lokalen Bereitstellung

1. Wählen Sie unter „Datenklassifizierung“ die Option „Konfiguration“ aus.
2. Wählen Sie unten auf der Konfigurationsseite **Klassifizierung deinstallieren** aus.



3. Geben Sie im Dialogfeld „uninstall“ ein, um mit der Trennung der Data Classification-Instanz vom Konsolenagent fortzufahren. Wählen Sie zur Bestätigung **Deinstallieren**.
4. Um die Software vom Host zu deinstallieren, führen Sie den `cleanup.sh` Skript auf dem Hostcomputer für die Datenklassifizierung, zum Beispiel:

```
cleanup.sh
```

Das Skript befindet sich im `/install/light_probe/onprem_installer/cleanup.sh` Verzeichnis. Erfahren Sie, wie Sie"Melden Sie sich beim Data Classification-Hostcomputer an" .