Cloud Data Sense Managen

Cloud Data Sense

NetApp
November 28, 2022

This PDF was generated from https://docs.netapp.com/de-de/cloud-manager-data-sense/task-managing-data-fusion.html on November 28, 2022. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

Cloud Data Sense Managen

Hinzufügen persönlicher Daten Kennungen zu Ihren Daten Sense-Scans

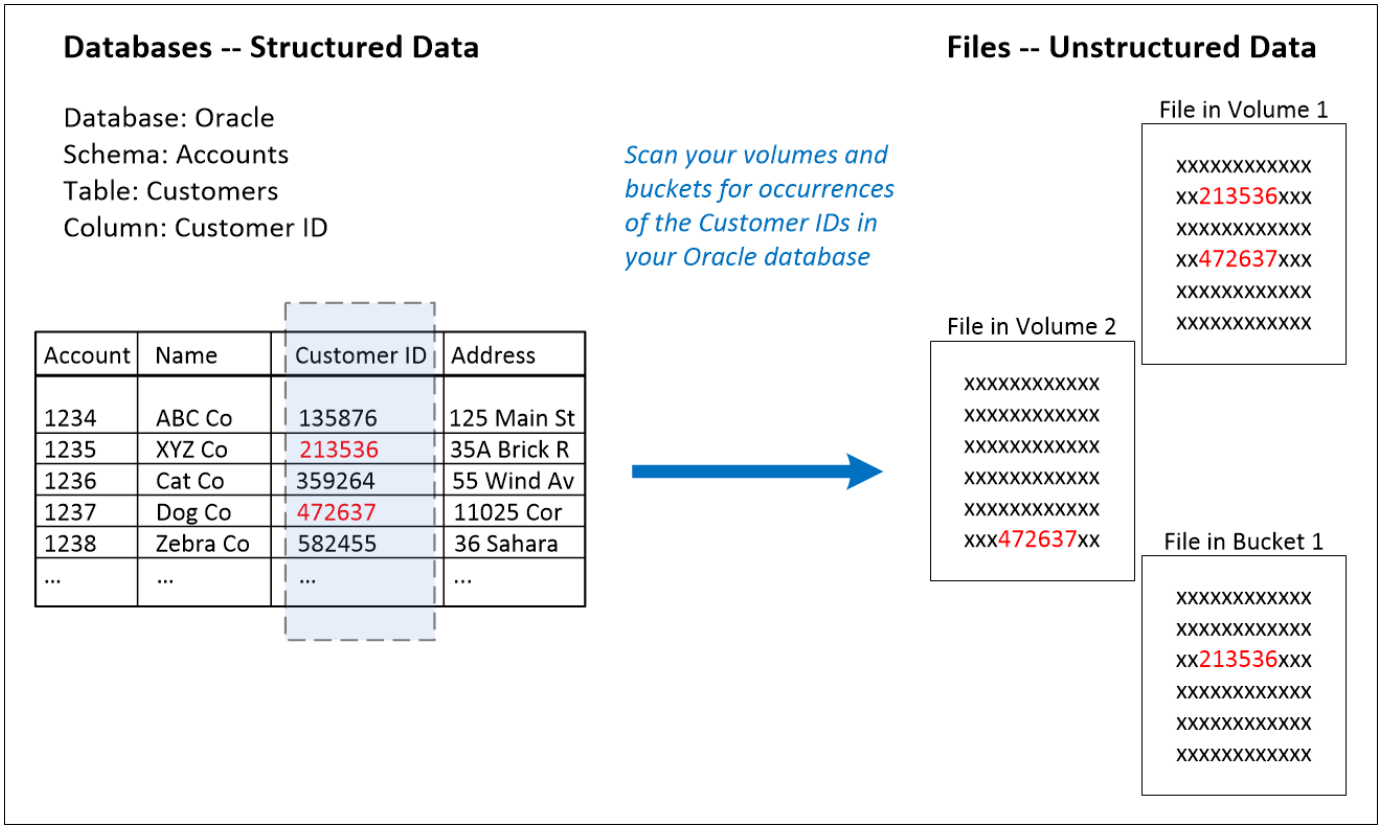
„Data Sense“ bietet Ihnen viele Möglichkeiten, eine benutzerdefinierte Liste „personenbezogener Daten“ hinzuzufügen, die Data Sense bei zukünftigen Scans erkennen kann. So erhalten Sie ein vollständiges Bild darüber, wo sich möglicherweise vertrauliche Daten in Dateien *all* Ihrer Unternehmen befinden.

- 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.

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 Kennungen auswählen, nach denen Data Sense in seinen Scans sucht, indem Sie eine bestimmte Spalte oder Spalten 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.

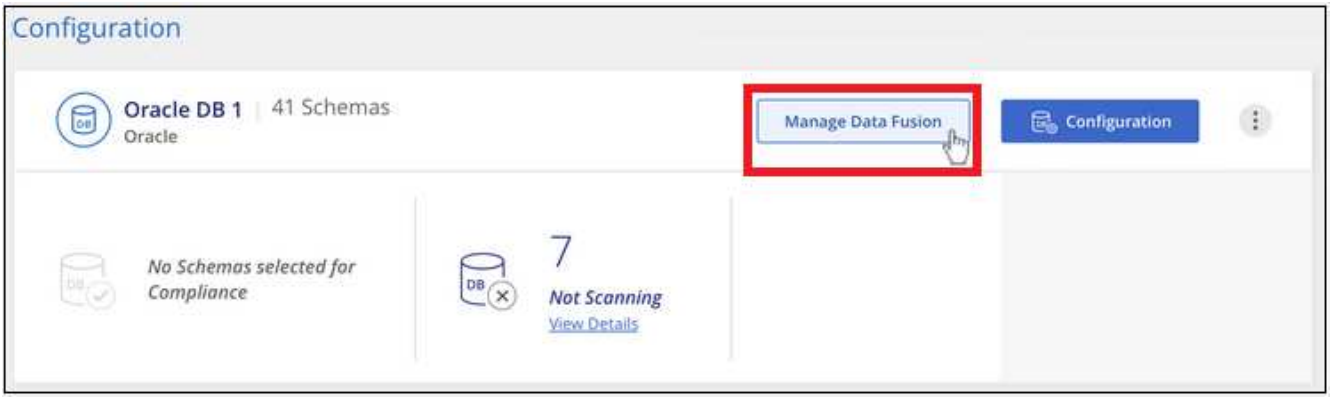


Wie Sie sehen, wurden in zwei Volumes und in einem S3-Bucket zwei eindeutige Kunden-IDs gefunden. Alle Übereinstimmungen in Datenbanktabellen werden ebenfalls identifiziert.

Beachten Sie, dass Sie Ihre eigenen Datenbanken scannen, in welcher Sprache Ihre Daten gespeichert sind, zur Identifizierung von Daten in zukünftigen Daten-Sense-Scans verwendet werden.

Dieser muss unbedingt vorhanden sein "Hat mindestens einen Datenbankserver hinzugefügt" Zu Data Sense, bevor Sie Daten-Fusion-Quellen hinzufügen können.

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



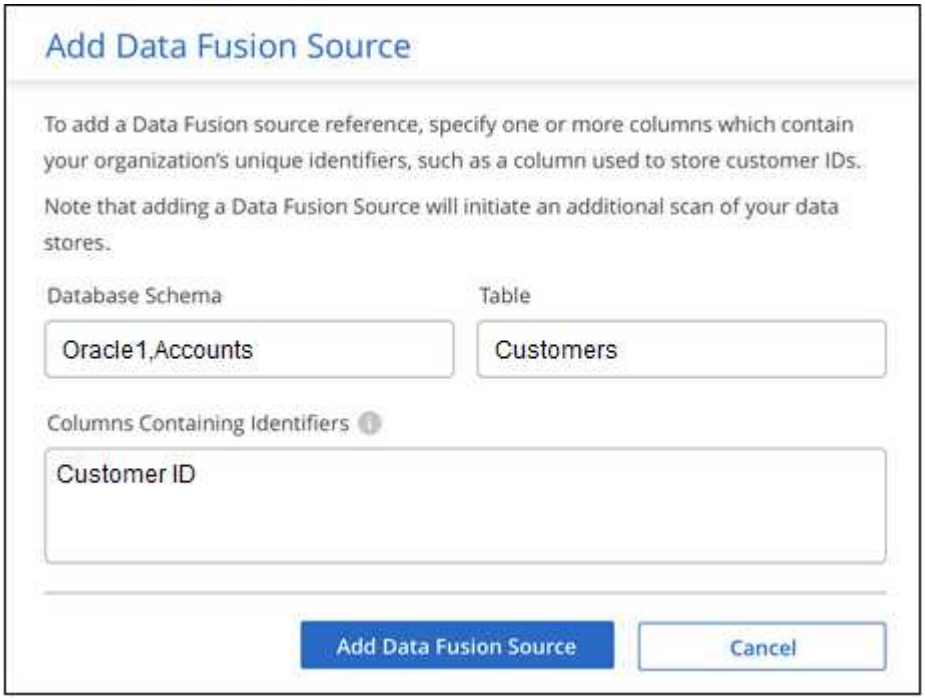
2. Klicken Sie auf der nächsten Seite auf **Data Fusion Source hinzufügen**.
3. Klicken Sie auf der Seite „ Fusion-Quelle hinzufügen “ auf die Seite „

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

b. Geben Sie den Tabellennamen in dieses Schema ein.

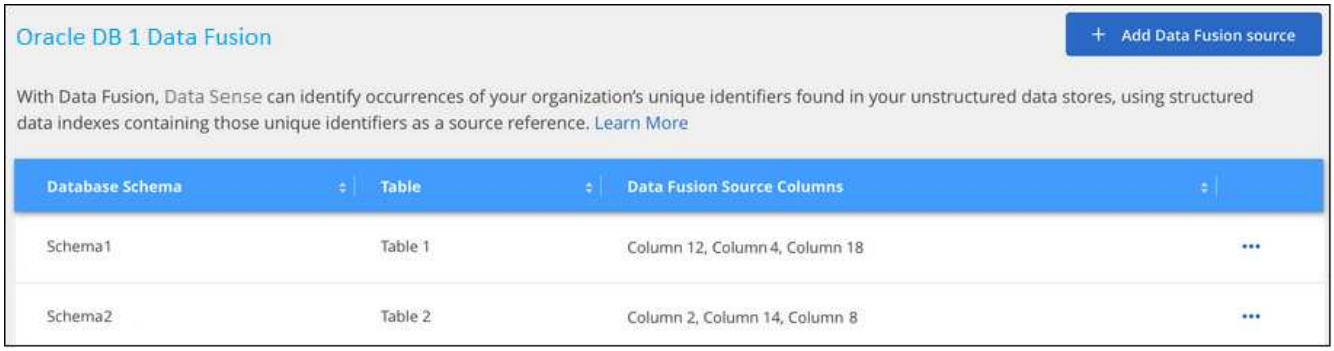
c. Geben Sie die Spalte oder Spalten ein, die die eindeutigen Kennungen enthalten, die Sie verwenden möchten.

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

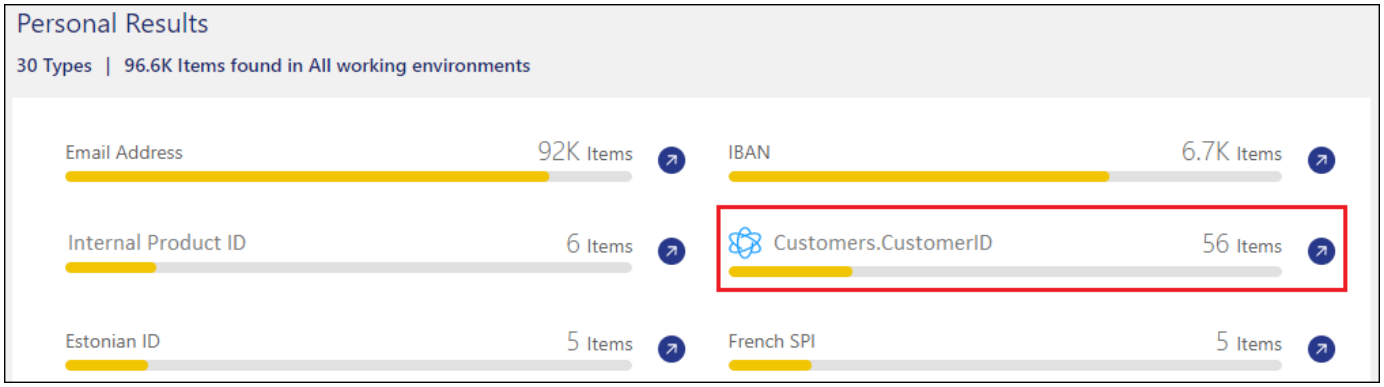


4. Klicken Sie Auf **Data Fusion-Quelle Hinzufügen**.

   Auf der Seite Data Fusion Inventory werden die Spalten für die Datenbankquelle angezeigt, die Sie für das Scannen von Daten Sense konfiguriert haben.



Nach dem nächsten Scan werden diese neuen Informationen im Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Untersuchungsseite im Filter „Persönliche Daten“ angezeigt. Jede von Ihnen hinzugefügte Quellspalte wird beispielsweise im Format „Tabelle.Spalte“ 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 Textdatei hinzu

Sie können dem Data Sense benutzerdefinierte Schlüsselwörter hinzufügen, damit es bestimmte Informationen in Ihren Daten identifiziert. Sie fügen die Schlüsselwörter aus einer von Ihnen definierten Textdatei hinzu. Die Schlüsselwörter werden den bereits vorhandenen vordefinierten Schlüsselwörtern hinzugefügt, die Data Sense verwendet, 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 dem Aktualisieren der benutzerdefinierten Schlüsselwörter startet Data Sense das Scannen aller Datenquellen neu – die neuen Ergebnisse werden nach Abschluss des Scans in Data Sense angezeigt.

Sie müssen die Textdateien, die die benutzerdefinierten Schlüsselwörter in der folgenden Position im Datensense-System enthalten, hinzufügen oder erstellen:

```
 /opt/netapp/Datasense/tools/datascience/custom_keywords/keywords_sets
Sie können eine einzelne Datei mit mehreren Schlüsselwörtern erstellen
oder viele Dateien hinzufügen, die jeweils bestimmte Schlüsselwörter
enthalten. Das Format für die Datei ist ein Wort in jeder Zeile, zum
Beispiel interne Produktnamen, die Arten von Eulen sind, werden unten
aufgelistet:
```

Internal_Product_Names.txt

```
barred
barn
horned
snowy
screech
```

Die Suche nach den gewünschten Daten-Sense nach diesen Elementen ist nicht zwischen Groß- und Kleinschreibung zu wählen.

Beachten Sie die folgenden Anforderungen:

- Der Dateiname darf keine Ziffern enthalten.
- Jede Datei kann maximal 100,000 Wörter enthalten. Wenn es mehr Wörter gibt, werden nur die ersten 100,000 hinzugefügt.
- Jedes Wort muss mindestens 3 Zeichen lang sein. Kürzere Wörter werden ignoriert.
- Doppelte Wörter werden nur einmal hinzugefügt.

Zugriff auf die Befehlszeile

Sie müssen auf das Data Sense System zugreifen, um den Befehl zum Hinzufügen benutzerdefinierter Schlüsselwörter zu starten.

Wenn Data Sense an Ihrem Standort installiert ist, können Sie direkt auf die Befehlszeile zugreifen.

Wenn Data Sense in der Cloud implementiert wird, muss SSH in der Data Sense Instanz verwendet werden. Sie können SSH auf dem System verwenden, indem Sie den Benutzer und das Kennwort eingeben oder den SSH-Schlüssel verwenden, den Sie während der Installation des BlueXP Connectors angegeben haben. Der SSH-Befehl lautet:

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = Speicherort der ssh-Authentifizierungsschlüssel
* <machine_user>:
```

+
Für AWS: Verwenden Sie <ec2-user>
Für Azure: Verwenden Sie den für die BlueXP-Instanz erstellten Benutzer
** Für GCP: Verwenden Sie den für die BlueXP-Instanz erstellten Benutzer

- <dataense_ip> = IP-Adresse der virtuellen Maschineninstanz

Beachten Sie, dass Sie die Inbound-Regeln der Sicherheitsgruppe ändern müssen, um auf das System in der Cloud zuzugreifen. Weitere Informationen finden Sie unter:

- "Sicherheitsgruppenregeln in AWS"
- "Für Sicherheitsgruppen gibt es in Azure Regeln"
- "Firewall-Regeln in Google Cloud"

Befehlssyntax zum Hinzufügen benutzerdefinierter Schlüsselwörter

Die Befehlssyntax zum Hinzufügen benutzerdefinierter Schlüsselwörter aus einer Datei lautet:

```
 sudo bash tools/datascience/custom_keywords/upload_custom_keywords.sh -s
activate -f <file_name>.txt
* <file_Name> = Dies ist der Name der Datei, die die Schlüsselwörter
enthält.
```

Sie führen den Befehl über den Pfad **/opt/netapp/Datacense/** aus.

Wenn Sie viele Dateien erstellt haben, die benutzerdefinierte Schlüsselwörter enthalten, können Sie die Schlüsselwörter aus allen Dateien gleichzeitig mit diesem Befehl hinzufügen:

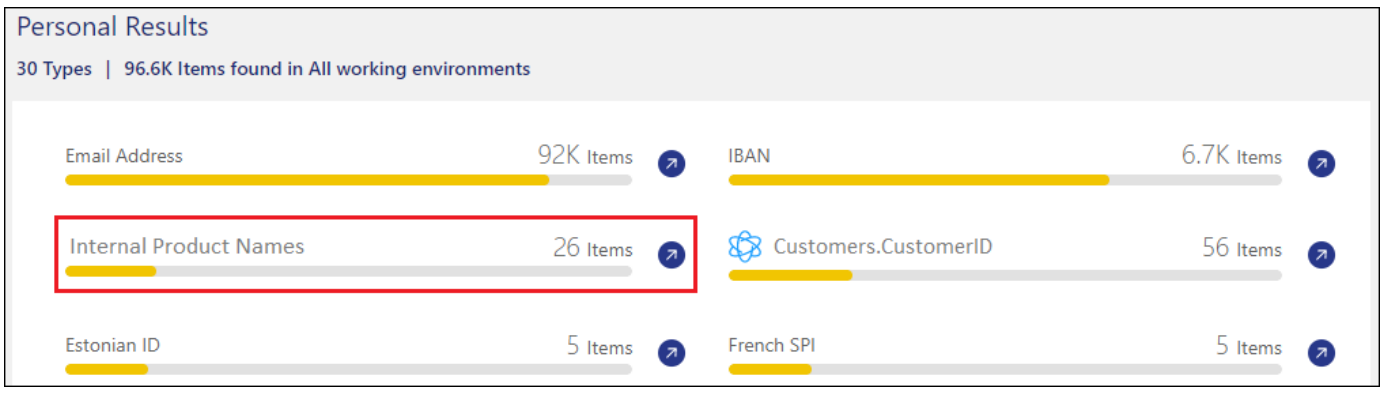
```
sudo bash tools/datascience/custom_keywords/upload_custom_keywords.sh -s
activate
```

Beispiel

Geben Sie den folgenden Befehl ein, um zu sehen, wo Ihre internen Produktnamen in allen Dateien erwähnt werden.

```
[user ~]$ cd /opt/netapp/Datasense/
[user Datasense]$ sudo bash
tools/datascience/custom_keywords/upload_custom_keywords.sh -s activate -f
internal_product_names.txt
```

```
 log v1.0 | 2022-08-24 08:16:25,332 | INFO | ds_logger |
upload_custom_keywords | 126 | 1 | None | upload_custom_keywords_126 | All
legal keywords were successfully inserted
Nach dem nächsten Scan werden diese neuen Informationen im Compliance
Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der
Untersuchungsseite im Filter „Persönliche Daten“ angezeigt.
```



Wie Sie sehen, wird der Name der Textdatei als Name im Bereich Persönliche Ergebnisse verwendet. Auf diese Weise können Sie Schlüsselwörter aus verschiedenen Textdateien aktivieren und die Ergebnisse für jeden Schlüsselworttyp anzeigen.

Benutzerdefinierte Schlüsselwörter deaktivieren

Wenn Sie zu einem späteren Zeitpunkt entscheiden, dass Sie Data Sense nicht benötigen, um bestimmte benutzerdefinierte Schlüsselwörter zu identifizieren, die Sie zuvor hinzugefügt haben, verwenden Sie die Option **deactivate** im Befehl, um die in der Textdatei definierten Schlüsselwörter zu entfernen.

```
 sudo bash tools/datascience/custom_keywords/upload_custom_keywords.sh -s
deactivate -f <file_name>.txt
Zum Beispiel, um die in der Datei *internal_Product_Names.txt definierten
Schlüsselwörter zu entfernen:
```

```
[user ~]$ cd /opt/netapp/Datasense/
[user Datasense]$ sudo bash
tools/datascience/custom_keywords/upload_custom_keywords.sh -s deactivate
-f internal_product_names.txt
```

```
log v1.0 | 2022-08-24 08:16:25,332 | INFO | ds_logger |
upload_custom_keywords | 87 | 1 | None | upload_custom_keywords_87 |
Deactivated keyword pattern from internal_product_names.txt successfully
```

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. Das Regex wird den bereits vorhandenen vordefinierten Mustern hinzugefügt, die Data Sense bereits verwendet, und die Ergebnisse werden im Abschnitt „Persönliche Muster“ sichtbar sein.

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.

Nach dem Hinzufügen des Regex startet Data Sense das Scannen aller Datenquellen neu - die neuen Ergebnisse erscheinen in Data Sense, nachdem der Scan abgeschlossen ist.

Befehlssyntax zum Hinzufügen des Regex

Sie müssen auf das Data Sense System zugreifen, um die Datei hinzuzufügen, die die benutzerdefinierten Schlüsselwortmuster enthält, und um den Befehl zu initiieren, um die benutzerdefinierten Schlüsselwörter hinzuzufügen. the command line,Erfahren Sie, wie Sie auf die Befehlszeile zugreifen Unabhängig davon, ob sich Daten für Ihre lokale Umgebung eignen oder in der Cloud implementiert haben.

Die Befehlssyntax zum Hinzufügen eines benutzerdefinierten Regex ist:

```
 sudo bash tools/datascience/custom_regex/custom_regex.sh -s activate -n
"<pattern_name>" -r "<regular_expression>"
* <pattern_Name> = Dies ist der Name, der in der Datensense-
Benutzeroberfläche angezeigt wird. Stellen Sie sicher, dass der Name
identifiziert, was der Regex entworfen wurde, um zu finden. Der Name muss
mindestens einen Buchstaben enthalten und darf bis zu 70 Zeichen lang
sein.
* <Regular_Expression> = Dies kann jeder legale reguläre Ausdruck sein.
```

Sie führen den Befehl über den Pfad **/opt/netapp/Datacense/** aus.

Beachten Sie, dass wir jeden neuen Regex testen, um zu überprüfen, ob er zu breit ist und es würde zu viele Spiele zurückkehren. Wenn das der Fall ist, wird die folgende Protokollmeldung angezeigt:

```
 log v1.0 | 2022-08-17 07:24:19,585 | ERROR | ds_logger | custom_regex |
119 | 1 | None | custom_regex_119 | The regex has high risk to identify
false positives. Please narrow the regular expression and try again. To
add it anyway, use the force flag (-f) at the end
Sie können die Option *-f* am Ende der Befehlszeile verwenden, wenn Sie
den Regex nachdrücklich zu Data Sense hinzufügen möchten - auch wenn wir
der Meinung sind, dass er zu breit ist.
```

Beispiel

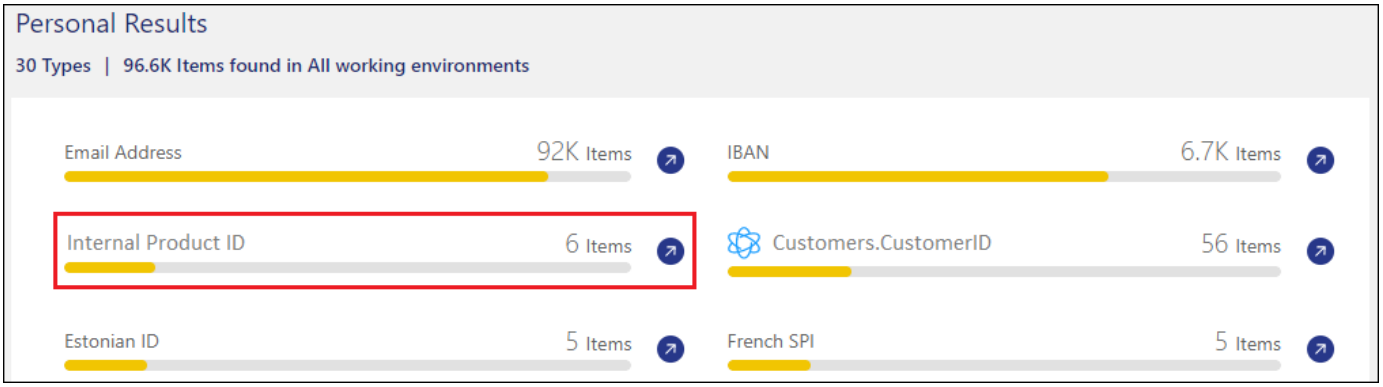
Die Produkt-ID ist eine 12-stellige Nummer, die mit 201 beginnt; der reguläre Ausdruck ist also **\b201\d{9}\b**. Und Sie möchten den Text in der Data Sense-Benutzeroberfläche nutzen, um dieses Muster als **interne Produkt-ID** zu identifizieren.

Geben Sie die folgenden Befehle ein, um zu sehen, wo Ihre internen Produkt-IDs in Ihren Dateien erwähnt werden.

```
[user ~]$ cd /opt/netapp/Datasense/
[user Datasense]$ sudo bash tools/datascience/custom_regex/custom_regex.sh
-s activate -n "Internal Product ID" -r "\b201\d{9}\b"
```

```
[+] Adding Custom Regex to Data Sense
log v1.0 | 2022-08-23 13:19:01,476 | INFO | ds_logger | custom_regex | 154
| 1 | None | custom_regex_154 | A pattern named 'Internal Product ID' was
added successfully to Data Sense
```

Nach dem nächsten Scan werden diese neuen Informationen im Compliance Dashboard im Abschnitt „Persönliche Ergebnisse“ und auf der Untersuchungsseite im Filter „Persönliche Daten“ angezeigt.



Deaktivieren eines benutzerdefinierten Regex

Wenn Sie zu einem späteren Zeitpunkt entscheiden, dass Sie Data Sense nicht benötigen, um die benutzerdefinierten Muster zu identifizieren, die Sie als Regex eingegeben haben, verwenden Sie die Option **deactivate** im Befehl, um jeden Regex zu entfernen.

```
 sudo bash tools/datascience/custom_regex/custom_regex.sh -s deactivate -n
"<pattern name>"
So entfernen Sie beispielsweise die *interne Produkt-ID* Regex:
```

```
[user ~]$ cd /opt/netapp/Datasense/
[user Datasense]$ sudo bash tools/datascience/custom_regex/custom_regex.sh
-s deactivate -n "Internal Product ID"
```

```
log v1.0 | 2022-08-17 09:13:15,431 | INFO | ds_logger | custom_regex | 31
| 1 | None | custom_regex_31 | A pattern named 'Internal Product ID' was
deactivated successfully
```

Anzeigen des Status Ihrer Compliance-Aktionen

Wenn Sie eine Aktion aus dem Bereich „Untersuchungsergebnisse“ über viele Dateien ausführen, z. B. das Löschen von 100 Dateien, kann der Prozess einige Zeit in Anspruch nehmen. Sie können den Status dieser asynchronen 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.

Der Status kann lauten:

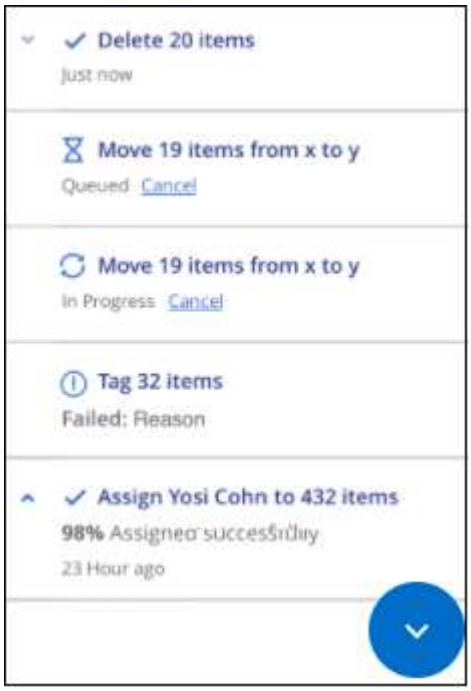
- Fertig
- In Bearbeitung

- Warteschlange
- Storniert
- Fehlgeschlagen

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

Schritte

1. Rechts unten in der Data Sense Benutzeroberfläche 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.

Überprüfung der Historie von „Data Sense“-Aktionen

Data Sense protokolliert Managementaktivitäten, die auf Dateien aus allen Arbeitsumgebungen und Datenquellen, die Data Sense scannt. Sie können den Inhalt der Datensense-Audit-Protokolldateien anzeigen oder herunterladen, um zu sehen, welche Dateiänderungen aufgetreten sind und wann.

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
```

Zugriff auf die Protokolldatei

Die Audit-Log-Dateien befinden sich auf dem Daten-SENSE-Rechner in: `/opt/netapp/audit_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. Maximal 100 Protokolldateien werden auf dem System gespeichert - alte Protokolldateien werden nach Erreichen des Maximalwerts automatisch gelöscht.

Wenn Data Sense auf Ihrem Gelände installiert ist, können Sie direkt zur Protokolldatei navigieren.

Wenn Data Sense in der Cloud implementiert wird, muss SSH in der Data Sense Instanz verwendet werden. Sie können SSH auf dem System verwenden, indem Sie den Benutzer und das Kennwort eingeben oder den SSH-Schlüssel verwenden, den Sie während der Installation des BlueXP Connectors angegeben haben. Der SSH-Befehl lautet:

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = Speicherort der ssh-Authentifizierungsschlüssel
* <machine_user>:
```

+
Für AWS: Verwenden Sie <ec2-user>
Für Azure: Verwenden Sie den für die BlueXP-Instanz erstellten Benutzer
** Für GCP: Verwenden Sie den für die BlueXP-Instanz erstellten Benutzer

- <dataense_ip> = IP-Adresse der virtuellen Maschineninstanz

Beachten Sie, dass Sie die Inbound-Regeln der Sicherheitsgruppe ändern müssen, um auf das System in der Cloud zuzugreifen. Weitere Informationen finden Sie unter:

- "Sicherheitsgruppenregeln in AWS"
- "Für Sicherheitsgruppen gibt es in Azure Regeln"
- "Firewall-Regeln in Google Cloud"

Verringerung der Scangeschgeschwindigkeit des Datensense

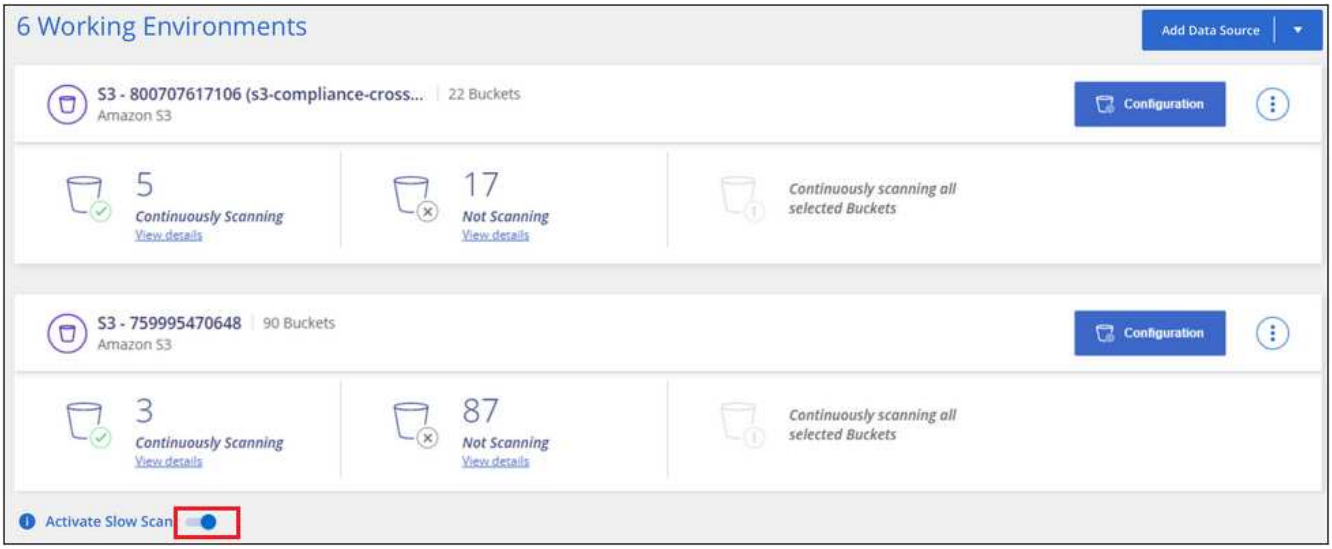
Datenscans haben keine nennenswerten Auswirkungen auf Ihre Storage-Systeme und Ihre Daten. Wenn Sie jedoch auch nur geringe Auswirkungen haben, können Sie Data Sense so konfigurieren, dass Sie „langsame“ Scans durchführen.

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.

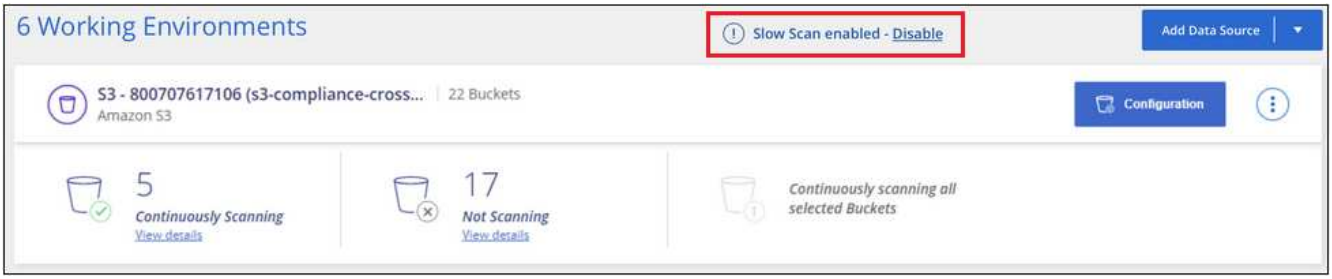
Die Scan-Geschwindigkeit kann beim Scannen von Datenbanken nicht verringert werden.

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.

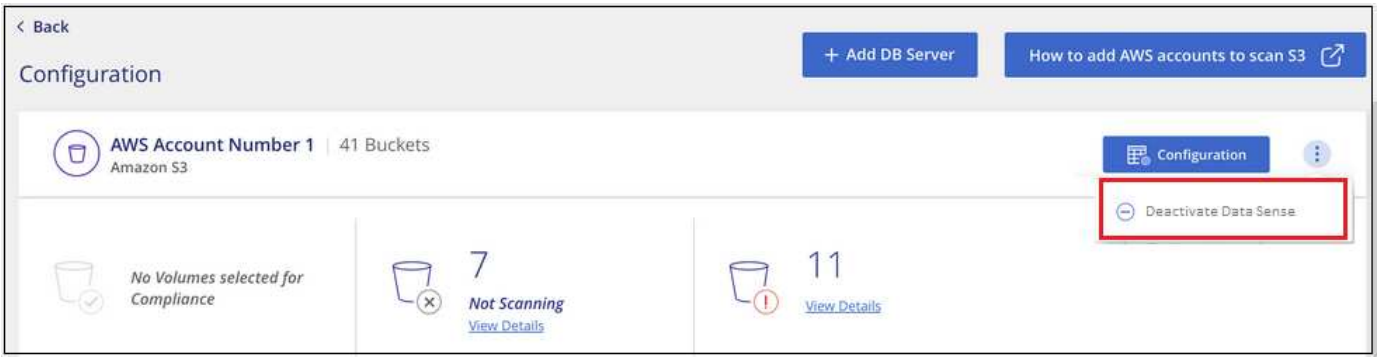
Entfernen von Datenquellen aus Cloud Data Sense

Wenn Sie möchten, können Sie Cloud Data Sense daran hindern, eine oder mehrere Arbeitsumgebungen, Datenbanken, Dateifreigabegruppen, OneDrive-Konten, Google Drive Konten, zu scannen. Oder SharePoint Konten.

Deaktivieren von Compliance-Scans für eine Arbeitsumgebung

Wenn Sie Scans deaktivieren, scannt Cloud Data Sense die Daten nicht mehr in der Arbeitsumgebung und entfernt sie die indizierten Compliance-Erkenntnisse aus der Data Sense Instanz (die Daten aus der Arbeitsumgebung selbst 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 Cloud Data Sense

Wenn Sie eine bestimmte Datenbank nicht mehr scannen möchten, können Sie sie über die Cloud Data Sense 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-Laufwerkkontos aus Cloud Data Sense

Wenn Sie keine Benutzerdateien von einem bestimmten OneDrive-Konto, von einem bestimmten SharePoint-Konto oder von einem Google Drive-Konto scannen möchten, können Sie das Konto über die Cloud Data Sense Schnittstelle 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 Cloud Data Sense

Wenn Sie keine Benutzerdateien aus einer Datei-Shares-Gruppe mehr scannen möchten, können Sie die File Shares-Gruppe über die Cloud Data Sense 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**.

Deinstallieren Von Cloud Data Sense

Sie können die Software Data Sense deinstallieren, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen. Durch das Löschen der Instanz werden auch die zugeordneten Festplatten gelöscht, auf denen sich die indizierten Daten befinden. Alle Informationen, die der Sinn für Daten gescannt hat, werden dauerhaft gelöscht.

Die erforderlichen Schritte hängen davon ab, ob Daten Sense in der Cloud oder auf einem lokalen Host implementiert wurde.

Deinstallieren Sie Data Sense aus einer Cloud-Implementierung

Sie können die Cloud Data Sense Instanz beim Cloud Provider deinstallieren und löschen, wenn Sie Data Sense nicht mehr verwenden möchten.

1. Klicken Sie oben auf der Seite Data Sense 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 Instanz und alle zugehörigen Daten löschen möchten, und klicken Sie dann auf **Uninstall**.

Beachten Sie, dass Sie die Konsole Ihres Cloud-Providers aufrufen und von dort aus die Instanz Cloud Data Sense löschen können. Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Deinstallieren Sie Data Sense aus einer lokalen Implementierung

Sie können Data Sense von einem Host deinstallieren, wenn Sie Data Sense nicht mehr verwenden möchten oder wenn ein Problem auftritt, das eine Neuinstallation erfordert.

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

2. Geben Sie im Dialogfeld *Uninstall Data Sense* die Option **uninstall** ein, um zu bestätigen, dass Sie alle Konfigurationsinformationen löschen möchten, und klicken Sie dann auf **Uninstall**.
3. Um die Deinstallation vom Host abzuschließen, führen Sie das Deinstallationsskript auf dem Hostcomputer aus, zum Beispiel:

```
uninstall.sh
```

Copyright-Informationen

Copyright © 2022 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.