



# **OnCommand Insight wird aktualisiert**

## **OnCommand Insight**

NetApp  
April 01, 2024

This PDF was generated from <https://docs.netapp.com/de-de/oncommand-insight/install-windows/upgrading-insight-to-version-7-3-12-or-later-windows.html> on April 01, 2024. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Inhalt

- OnCommand Insight wird aktualisiert. . . . . 1
  - Aktualisieren von Insight auf Version 7.3.12 oder höher - Windows . . . . . 1
  - Überblick über den OnCommand Insight Upgrade-Prozess . . . . . 5
  - Herunterladen der OnCommand Insight-Installationspakete . . . . . 10
  - Sichern der Datenbanken. . . . . 11
  - Sichern der Sicherheitskonfiguration . . . . . 14
  - Erstellen von benutzerdefinierten Data Warehouse-Berichten . . . . . 15
  - Durchführen des Software-Upgrades. . . . . 15
  - Aufgaben nach dem Upgrade werden ausgeführt . . . . . 18
  - Fehlerbehebung bei einem Upgrade . . . . . 25

# OnCommand Insight wird aktualisiert

Normalerweise muss ein Upgrade auf allen Insight Servern (Insight Server, Data Warehouse Server, Remote Acquisition Unit) durchgeführt werden. Die Upgrade-Anforderungen für eine neue Version von OnCommand Insight sollten immer in den Versionshinweisen nachschlagen.

Sofern nicht anders angegeben, gelten die Anforderungen und Verfahren für das Upgrade von Insight 7.x auf die aktuelle Version von Insight. Wenn Sie ein Upgrade von einer Version vor 7.0 durchführen, wenden Sie sich an Ihren Kundenbetreuer.

## Aktualisieren von Insight auf Version 7.3.12 oder höher - Windows

Vor dem Upgrade von OnCommand Insight 7.3.10 auf 7.3.11 Version 7.3.12 oder höher müssen Sie das OCI Datenmigrationstool ausführen.

### Hintergrund

OnCommand Insight Version 7.3.12 und höher verwenden zugrunde liegende Software, die möglicherweise mit früheren Versionen nicht kompatibel ist. Insight Version 7.3.12 und höher enthalten ein **Data Migration Tool** zur Unterstützung beim Upgrade.



OnCommand Insight Versionen 7.3.9 und früher werden nicht mehr unterstützt. Wenn Sie eine dieser Versionen ausführen, müssen Sie vor dem Upgrade auf 7.3.12 oder höher auf Insight Version 7.3.10 oder höher (7.3.11 wird dringend empfohlen) aktualisieren.

### Welche Funktionen Bietet Das Datenmigrationstool?

Das Migrationstool führt zunächst eine Kompatibilitätsprüfung durch und folgt dann einem von drei verschiedenen Upgrade-Pfaden. Der ausgewählte Pfad basiert auf der Datenkompatibilität Ihrer aktuellen Version.



Vor dem Upgrade müssen Sie das Data Migration Tool ausführen und die empfohlenen Schritte ausführen.

### Bevor Sie beginnen

- Es wird dringend empfohlen, das OnCommand Insight-System vor dem Ausführen des Datenmigrationstools zu sichern.
- Der Elasticsearch-Service auf dem Server muss betriebsbereit sein.
- Das Data Migration Tool *must* muss für die Datenbank und alle Performance-Archive ausgeführt werden, bevor Sie Insight aktualisieren.

### Ausführen des Data Migration Tools

1. Laden Sie die aktuelle Version des Data Migration Tools (z. B. *SANScreenDataMigrationTool-x86-7.3.12-97.zip*) sowie die entsprechende Insight Installer-Datei auf Ihren Insight Server herunter. Entpacken Sie die

ZIP-Datei in einen Arbeitsordner. Downloads finden Sie auf der ["NetApp Support Website"](#).

2. Öffnen Sie ein Befehlsfenster, und navigieren Sie zu Ihrem Arbeitsordner.
  - Öffnen Sie PowerShell als Administrator.
3. Führen Sie das Datenmigrationstool über den folgenden Befehl aus:
  - `.\SANSscreenDataMigrationTool.ps1``
4. Befolgen Sie bei Bedarf die Anweisungen. Im Folgenden ein Beispiel.

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-121

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory: C:\Program Files\SANSscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
    the most recent of which is for 2021-05-13

Verifying migration component is present...
SANSscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

Das Data Migration Tool überprüft, ob veraltete Indizes auf Ihrem System vorhanden sind, und meldet, ob sie gefunden wurden. Wenn keine vorhanden sind, wird das Werkzeug beendet.

Einige Indizes können migriert werden, während der SANSscreen-Serverdienst ausgeführt wird. Andere können nur migriert werden, wenn der Server angehalten wird. Wenn keine Indizes vorhanden sind, die migriert werden können, wird das Tool beendet. Befolgen Sie andernfalls die Anweisungen, wie Sie dazu aufgefordert werden.

Wenn das Data Migration Tool abgeschlossen ist, wird es erneut auf veraltete Indizes überprüft. Wenn alle Indizes migriert wurden, informiert Sie das Tool darüber, dass ein Upgrade auf OnCommand Insight 7.3.12 unterstützt wird. Sie können jetzt mit dem Upgrade der Insight fortfahren.

```
.\SANScreenDataMigrationTool.ps1
```

```
NetApp SANScreen Data Migration Tool 7.3.12-127
```

```
Checking OnCommand Insight Installation...
```

```
OnCommand Insight 7.3.10 (139) is installed
```

```
Getting installation parameters...
```

```
Installation Directory: D:\SANscreen\
```

```
Elasticsearch Rest Port: 9200
```

```
Checking Elasticsearch service...
```

```
Elasticsearch service is up
```

```
Checking for obsolete (version 5) indexes...
```

```
Found 5 obsolete indexes. Of these,
```

```
    5 indexes need to be migrated with OCI server stopped
```

```
Verifying migration component is present...
```

```
SANscreen Server service is Stopped
```

```
Proceed with offline migration of 5 indexes (y or [n])?: y
```

```
Preparing to perform migration...
```

```
Preparing to migrate ociint-inventory-snmp_win2012_host: copied; backup;  
delete old; restore new; cleanup; done.
```

```
Preparing to migrate ociint-inventory-snmp_win2012_interface: copied;  
backup; delete old; restore new; cleanup; done.
```

```
Preparing to migrate ociint-inventory-snmp_win2012_load_average: copied;  
backup; delete old; restore new; cleanup; done.
```

```
Preparing to migrate ociint-inventory-snmp_win2012_storage: copied;  
backup; delete old; restore new; cleanup; done.
```

```
Preparing to migrate ociint-inventory-snmp_win2012_tcp_connection: copied;  
backup; delete old; restore new; cleanup; done.
```

```
Execution time 0:00:15
```

```
Checking for obsolete (version 5) indexes...
```

```
No obsolete indexes found. Upgrade to 7.3.12+ is supported.
```

```
C:\Users\root\Desktop\SANScreenDataMigrationTool-x64-7.3.12-127>
```

Wenn Sie aufgefordert wurden, den SANscreen-Dienst zu beenden, starten Sie ihn vor dem Upgrade von Insight neu.

## Validierungsfehler

Falls die Indexvalidierung fehlschlägt, informiert Sie das Migrationstool vor dem Beenden über das Problem.

### OnCommand Insight ist nicht vorhanden:

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

### Ungültige Insight-Version:

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

### Elasticsearch-Dienst läuft nicht:

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Installation Directory: C:\Program Files\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

## Befehlszeilenoptionen

Das Datenmigrationstool enthält einige optionale Parameter, die sich auf den Betrieb auswirken.

Option (Windows)	Funktion
-S	Alle Eingabeaufforderungen unterdrücken
-Perf_Archive	<p>Wenn angegeben, werden vorhandene Archiveinträge für alle Daten ersetzt, deren Index(e) migriert werden. Der Pfad sollte auf das Verzeichnis verweisen, das die ZIP-Dateien für den Archiveintrag enthält.</p> <p>Ein Argument von '-' kann angegeben werden, um anzuzeigen, dass kein Performance-Archiv aktualisiert werden muss.</p> <p>Wenn dieses Argument vorhanden ist, wird die Eingabeaufforderung für den Archivspeicherort unterdrückt.</p>
-Check	Falls vorhanden, wird das Skript sofort nach der Meldung der Indexzahlen beendet.
-Dryrun	Falls vorhanden, meldet die ausführbare Migrationsdatei die Aktionen, die ausgeführt werden würden (zum Migrieren von Daten und Aktualisieren von Archiveinträgen), führt die Vorgänge jedoch nicht aus.

## Überblick über den OnCommand Insight Upgrade-Prozess

Bevor Sie mit dem Upgrade von Insight beginnen, sollten Sie sich unbedingt über den Upgrade-Prozess informieren. Der Upgrade-Prozess ist für die meisten Versionen von Insight gleich.

Der Upgrade-Prozess für Insight umfasst die folgenden grundlegenden Aufgaben:

- Herunterladen der Installationspakete
- Sichern der Data Warehouse-Datenbank

Um die Möglichkeit falscher Berichte zu vermeiden, müssen Sie die Data Warehouse-Datenbank sichern, bevor Sie die Insight-Datenbank sichern.

- Sichern der Insight-Datenbank

Die Insight Datenbank wird automatisch gesichert, wenn Sie das Upgrade durchführen. Es empfiehlt sich, vor dem Upgrade ein Backup der Datenbank zu erstellen und das Backup an einem anderen Ort als auf dem Insight Server abzulegen. Während des Upgrade-Prozesses erfasst Insight keine neuen Daten. Um die Menge der nicht erfassten Daten zu minimieren, müssen Sie das Datenbank-Backup innerhalb von ein oder zwei Stunden Ihrer geplanten Upgrade-Zeit starten.

- Sichern Sie die Sicherheitskonfiguration für Data Warehouse und Remote Acquisition Unit, wenn die Konfiguration von der Standardkonfiguration geändert wurde.

Die nicht standardmäßige Sicherheitskonfiguration muss nach Abschluss des Upgrades auf dem Data Warehouse und dem rau-Server wiederhergestellt werden, bevor die Data Warehouse-Datenbank auf dem System wiederhergestellt wird.

- Erstellen von Backups benutzerdefinierter Data Warehouse-Berichte

Wenn Sie die Data Warehouse-Datenbank sichern, werden benutzerdefinierte Berichte eingeschlossen. Die Sicherungsdatei wird auf dem Data Warehouse-Server erstellt. Es wird empfohlen, die benutzerdefinierten Berichte an einem anderen Speicherort als dem Data Warehouse-Server zu sichern.

- Deinstallieren des Data Warehouse und der Remote Acquisition Unit-Software, falls zutreffend

Der Insight-Server verfügt über ein in-Place-Upgrade. Sie müssen die Software nicht deinstallieren. Mit dem in-Place-Upgrade wird die Datenbank gesichert, die Software deinstalliert, die neue Version installiert und die Datenbank dann wiederhergestellt.

- Aktualisieren der Software auf dem Insight-Server, dem Data Warehouse und den Remote Acquisition Units

Alle zuvor angewendeten Lizenzen verbleiben in der Registrierung; Sie müssen diese Lizenzen nicht erneut anwenden.

- Ausführen der Aufgaben nach dem Upgrade

## OnCommand Insight Upgrade-Checkliste

Sie können die bereitgestellten Checklisten verwenden, um Ihren Fortschritt bei der Vorbereitung des Upgrades zu erfassen. Diese Aufgaben sollen dazu beitragen, das Risiko von Upgrade-Fehlern zu mindern und den Recovery- und Wiederherstellungsaufwand zu beschleunigen.

### Checkliste zur Vorbereitung des Upgrades (erforderlich)

Zustand	Abgeschlossen?
Stellen Sie sicher, dass Sie auf allen Insight-Servern über lokale Windows-Administratorberechtigungen verfügen, die für die Durchführung des Upgrade-Prozesses erforderlich sind.	
Wenn sich Ihre Insight-, Data Warehouse- oder Remote Acquisition Unit-Server auf 32-Bit-Plattformen befinden, müssen Sie Ihre Server auf 64-Bit-Plattformen aktualisieren. Ab Insight 7.x sind Upgrades nur für 64-Bit-Plattformen verfügbar.	



<p>Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, um die Antivirensoftware auf allen Servern in Ihrer Umgebung zu ändern oder zu deaktivieren. Um einen Aktualisierungsfehler aufgrund einer aktiven Virensan-Software zu verhindern, müssen Sie das Insight-Installationsverzeichnis ausschließen (disk drive:\install directory\sanscreen Vom Zugriff auf Virenschutzprüfungen während des Upgrades. Nachdem Sie alle Komponenten aktualisiert haben, können Sie die Antivirensoftware sicher wieder aktivieren. Stellen Sie jedoch sicher, dass Sie den Scan so konfigurieren, dass er im Insight-Installationsverzeichnis weiterhin alle Komponenten ausschließt.</p> <p>Außerdem müssen Sie den IBM/DB2-Ordner (z. B. C:\Program Files\IBM\DB2) nach der Installation von der Virenprüfung ausschließen.</p>	
--	--

### Checkliste zur Vorbereitung des Upgrades (Best Practice)

Zustand	Abgeschlossen?
Planen Sie ein Upgrade ein, und berücksichtigen Sie dabei, dass die meisten Upgrades mindestens 4 bis 8 Stunden dauern. Größere Unternehmen benötigen länger. Die Upgrade-Zeiten hängen von den verfügbaren Ressourcen (Architektur, CPU und Arbeitsspeicher), der Größe der Datenbanken und der Anzahl der in Ihrer Umgebung überwachten Objekte ab.	
Wenden Sie sich bezüglich Ihrer Upgrade-Pläne an Ihren Ansprechpartner, informieren Sie sich über die installierte Insight Version und welche Version Sie aktualisieren möchten.	
Stellen Sie sicher, dass Ihre aktuellen Ressourcen, die den Insight, Data Warehouse und Remote Acquisition Units zugewiesen sind, weiterhin die empfohlenen Spezifikationen erfüllen. Weitere Informationen finden Sie in den Richtlinien zur Dimensionierung für alle Server. Alternativ können Sie sich an Ihren Ansprechpartner wenden, um die Richtlinien zur Dimensionierung zu besprechen.	

Stellen Sie sicher, dass genügend Speicherplatz für die Sicherung und Wiederherstellung der Datenbank vorhanden ist. Die Backup- und Restore-Prozesse benötigen etwa das Fünffache des Speicherplatzes, der von der Backup-Datei auf den Insight- und Data Warehouse-Servern belegt wird. Ein 50-GB-Backup benötigt beispielsweise 250 bis 300 GB freien Festplattenspeicher.	
Stellen Sie sicher, dass Sie Zugriff auf Firefox® oder den Chrome™ Browser haben, wenn Sie die Insight- und Data Warehouse-Datenbanken sichern. Internet Explorer wird nicht empfohlen, da beim Hochladen und Herunterladen von Dateien größer als 4 GB Probleme auftreten.	
Löschen Sie die .tmp Dateien auf dem Insight-Server, die Sie an folgendem Speicherort finden: <install directory>\SANscreen\wildfly\standalone \tmp.	
Doppelte Datenquellen und stillgelegte Datenquellen werden vom Insight Client entfernt. Das Entfernen stillgelegter oder doppelter Datenquellen verringert die für die Durchführung des Upgrades benötigte Zeit und verringert die Möglichkeit einer Datenbeschädigung.	
Wenn Sie einen der mit Insight ausgelieferten Standardberichte geändert haben, sollten Sie die Berichte unter einem anderen Namen speichern und anschließend im Ordner „Kundenberichte“ speichern, damit Sie Ihren geänderten Bericht nicht verlieren, wenn Sie das System aktualisieren oder wiederherstellen.	
Wenn Sie benutzerdefinierte oder geänderte Data Warehouse-Berichte von Ihnen oder Professional Services erstellt haben, erstellen Sie ein Backup dieser Berichte, indem Sie sie in XML exportieren und dann in den Ordner Kundenberichte verschieben. Stellen Sie sicher, dass sich das Backup nicht auf dem Data Warehouse-Server befindet. Wenn Sie Ihre Berichte nicht in die empfohlenen Ordner verschieben, werden diese Berichte möglicherweise nicht durch den Upgrade-Prozess gesichert. Bei früheren Versionen von Insight kann das Suchen von Berichten in den entsprechenden Ordnern zum Verlust benutzerdefinierter und geänderter Berichte führen.	

Notieren Sie alle Einstellungen im IBM Cognos-Konfigurationsdienstprogramm, da diese nicht im Data Warehouse-Backup enthalten sind. Sie müssen diese Einstellungen nach dem Upgrade neu konfigurieren. Das Dienstprogramm befindet sich im `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` Verzeichnis auf dem Data Warehouse-Server, und Sie führen es mit `aus cogconfigw` Command.Alternativ können Sie eine vollständige Sicherung von Cognos durchführen und anschließend alle Einstellungen importieren. Weitere Informationen finden Sie in der Dokumentation zu IBM Cognos.

### Checkliste zur Vorbereitung des Upgrades (falls zutreffend)

Zustand	Abgeschlossen?
Wenn Sie die selbstsignierten Zertifikate, die die Insight-Installation aufgrund von Sicherheitswarnungen im Browser erstellt hat, durch von Ihrer internen Zertifizierungsstelle signierte Zertifikate ersetzt haben, sichern Sie die Keystore-Datei an folgendem Speicherort: <code>disk drive:\install directory\SANscreen\wildfly\standalone\configuration</code> Und stellen Sie sie nach dem Upgrade wieder her. Dadurch werden die selbstsignierten Zertifikate ersetzt, die Insight mit Ihren signierten Zertifikaten erstellt.	
Wenn eine Ihrer Datenquellen für Ihre Umgebung geändert wurde und Sie sich nicht sicher sind, ob diese Änderungen in der Insight-Version verfügbar sind, auf die Sie aktualisieren, erstellen Sie eine Kopie des folgenden Verzeichnisses, das Ihnen bei Problemen mit der Wiederherstellung hilft: <code>disk drive:\install directory\SANscreen\wildfly\standalone\deployments\datasources.war</code> .	
Sichern Sie alle benutzerdefinierten Datenbanktabellen und -Ansichten mithilfe des <code>mysqldump</code> Befehlszeilen-Tool.das Wiederherstellen benutzerdefinierter Datenbanktabellen erfordert privilegierten Zugriff auf die Datenbank. Wenden Sie sich an den technischen Support, um Hilfe beim Wiederherstellen dieser Tabellen zu erhalten.	

In ist sichergestellt, dass keine benutzerdefinierten Integrationsskripte, Komponenten von Drittanbietern, die für Insight-Datenquellen, Backups oder andere erforderliche Daten erforderlich sind disk  
drive:\install directory\sansscreen  
Verzeichnis, da der Inhalt dieses Verzeichnisses durch den Upgrade-Prozess gelöscht wird. Stellen Sie sicher, dass Sie diese Dinge aus dem verschieben  
\sansscreen An einen anderen Speicherort. Wenn Ihre Umgebung beispielsweise benutzerdefinierte Integrationsskripte enthält, stellen Sie sicher, dass Sie die folgende Datei in ein anderes Verzeichnis als das kopieren \sansscreen Verzeichnis:

```
\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt.
```

## Herunterladen der OnCommand Insight-Installationspakete

Sie sollten die Installationspakete für Insight, Data Warehouse und die Remote Acquisition Unit (falls zutreffend) vor dem Tag herunterladen, an dem Sie das Upgrade durchführen möchten. Download-Zeiten für die Pakete (.msi Dateien) variieren je nach verfügbarer Bandbreite.

### Über diese Aufgabe

Sie können die Installationspakete über die WebUI von Insight oder über den entsprechenden Link zu OnCommand Insight von herunterladen <http://support.netapp.com/NOW/cgi-bin/software>.

Gehen Sie wie folgt vor, um das Installationspaket vom Insight-Server herunterzuladen:

### Schritte

1. Öffnen Sie die Web-UI von Insight, indem Sie einen Webbrowser öffnen und einen der folgenden eingeben:

- Auf dem Insight-Server: `https://localhost`
- Von jedem Ort: `https://IP Address:port or fqdn:port`

Die Portnummer lautet entweder 443 oder der Port, der bei der Installation des Insight-Servers konfiguriert wurde. Die Portnummer ist standardmäßig 443, wenn Sie die Portnummer nicht in der URL angeben.

2. Melden Sie sich bei Insight an.
3. Klicken Sie auf das Hilfesymbol und wählen Sie **nach Updates suchen**.
4. Wenn eine neuere Version erkannt wird, befolgen Sie die Anweisungen im Meldungsfeld.

Sie werden zur Seite InsightDescription für die neuere Version weitergeleitet.

5. Klicken Sie auf der Seite **Beschreibung** auf **Weiter**.
6. Wenn die Endbenutzer-Lizenzvereinbarung (EULA) angezeigt wird, klicken Sie auf **Accept**.
7. Klicken Sie für jede Komponente (Insight Server, Data Warehouse, Remote Acquisition Unit) auf den Link für das Installationspaket und klicken Sie auf **Speichern unter**, um das Installationspaket zu speichern.

Bevor Sie ein Upgrade durchführen, sollten Sie sicherstellen, dass Sie die Installationspakete für Data Warehouse und Remote Acquisition Unit auf Festplatten kopieren, die auf ihren jeweiligen Servern lokal sind.

8. Klicken Sie auf **CHECKSUM**, und notieren Sie sich die numerischen Werte, die mit jedem Installationspaket verknüpft sind.
9. Überprüfen Sie, ob die Installationspakete vollständig und fehlerfrei sind, nachdem Sie sie heruntergeladen haben.

Unvollständige Dateiübertragungen können Probleme mit dem Upgrade-Prozess verursachen.

Um MD5-Hash-Werte für die Installationspakete zu generieren, können Sie ein Drittanbieter-Dienstprogramm wie Microsoft verwenden "[Dateiüberprüfung der Integrität](#)" Utility:

## Sichern der Datenbanken

Bevor Sie ein Upgrade durchführen, sollten Sie sowohl die Data Warehouse- als auch die OnCommand Insight-Datenbanken sichern. Für die Aktualisierung ist ein Backup der Data Warehouse-Datenbank erforderlich, damit Sie die Datenbank später im Upgrade wiederherstellen können. Mit dem in-Place-Upgrade für Insight wird die Datenbank gesichert. Vor dem Upgrade sollten Sie jedoch als Best Practice eine Sicherung der Datenbank durchführen.

Um falsche Berichte zu vermeiden, sollten Sie die Data Warehouse-Datenbank vor dem Backup der Insight-Datenbank sichern. Wenn Sie über eine Testumgebung verfügen, sollten Sie außerdem sicherstellen, dass Sie das Backup wiederherstellen können, bevor Sie mit dem Upgrade fortfahren.

### Sichern der Data Warehouse-Datenbank

Sie können die Data Warehouse-Datenbank, die auch ein Cognos-Backup enthält, in einer Datei sichern und später mithilfe des Data Warehouse-Portals wiederherstellen. Mit einem solchen Backup können Sie auf einen anderen Data Warehouse-Server migrieren oder auf eine neue Data Warehouse-Version aktualisieren.

#### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter `https://fqdn/dwh` an.
2. Wählen Sie im Navigationsfenster links **Backup/Restore** aus.
3. Klicken Sie auf **Backup** und wählen Sie Ihre Backup-Konfiguration aus:
  - a. Alle Datamarts außer Performance Datamart
  - b. Alle Datamarts

Dieser Vorgang kann 30 Minuten oder länger dauern.

+ Data Warehouse erstellt eine Sicherungsdatei und zeigt ihren Namen an.

4. Klicken Sie mit der rechten Maustaste auf die Sicherungsdatei, und speichern Sie sie an einem gewünschten Speicherort.

Sie möchten den Dateinamen möglicherweise nicht ändern. Sie sollten die Datei jedoch außerhalb des Installationspfads des Data Warehouse speichern.

Die Data Warehouse Backup-Datei enthält MySQL der DWH-Instanz; benutzerdefinierte Schemas (MySQL DBs) und Tabellen; LDAP-Konfiguration; die Datenquellen, die Cognos mit der MySQL-Datenbank verbinden (nicht die Datenquellen, die den Insight-Server mit Geräten verbinden, um Daten zu erfassen); Importieren und Exportieren von Aufgaben, die Berichte importiert oder exportiert haben; Reporting von Sicherheitsrollen, Gruppen und Namespaces; Benutzerkonten; Alle geänderten Reporting Portal-Berichte sowie alle benutzerdefinierten Berichte, unabhängig davon, wo sie gespeichert sind, selbst im Verzeichnis „Meine Ordner“. Cognos-Systemkonfigurationsparameter wie SMTP-Servereinstellungen und Cognos-Einstellungen für benutzerdefinierten Speicher werden nicht gesichert.

Die Standardschemas, in denen benutzerdefinierte Tabellen gesichert werden, umfassen Folgendes:

dwh_Capacity
dwh_Capacity_Staging
dwh_Bemaßungen
dwh_fs_util
dwh_Inventory
dwh_Inventory_Staging
dwh_Inventory_transient
dwh_Management
dwh_Performance
dwh_Performance_Staging
dwh_Ports
dwh_Reports
dwh_sa_Staging

Schemas, bei denen benutzerdefinierte Tabellen vom Backup ausgeschlossen werden, umfassen

Folgendes:

Information_Schema
Akquisition
Cloud_Modell
Host_Data
innodb
Inventar
Inventory_private
Inventory_Time
Protokolle
Vereinfachtes
mysql
nas
Performance
Performance_Schema
Performance_Views
SANscreen
Schrubben
Servicesicherheit
Test
Tmp
workbench

Bei manuell initiierten Backups wird ein angezeigt .zip Datei wird erstellt, die folgende Dateien enthält:

- Ein tägliches Backup .zip Datei, die Cognos-Berichtsdefinitionen enthält
- Ein meldet Backup .zip Datei, die alle Berichte in Cognos enthält, einschließlich der Berichte im Verzeichnis eigene Ordner
- Eine Data Warehouse-Datenbank-Sicherungsdatei Zusätzlich zu manuellen Backups, die Sie jederzeit durchführen können, erstellt Cognos täglich ein Backup (automatisch jeden Tag in einer Datei mit dem Namen generiert) `DailyBackup.zip`), das die Berichtsdefinitionen enthält. Die tägliche Sicherung umfasst die wichtigsten Ordner und Pakete, die mit dem Produkt geliefert werden. Das Verzeichnis „Meine Ordner“ und alle Verzeichnisse, die Sie außerhalb der obersten Produktordner erstellen, sind nicht im Cognos-Backup enthalten.



Aufgrund der Art und Weise, wie Insight die Dateien benennt .zip Datei, zeigen einige Entpackprogramme, dass die Datei leer ist, wenn sie geöffnet wird. So lange wie die .zip Die Datei hat eine Größe größer als 0 und endet nicht mit einem .bad Erweiterung, die .zip Datei ist gültig. Sie können die Datei mit einem anderen Entpackprogramm wie 7-Zip oder WinZip® öffnen.

## Sichern der OnCommand Insight-Datenbank

Sichern Sie die Insight-Datenbank, um sicherzustellen, dass Sie ein Backup vor kurzem haben, falls nach dem Upgrade ein Problem auftritt. Während der Backup- und Wiederherstellungsphase werden keine Performance-Daten erfasst, daher sollte das Backup so nah wie möglich an der Upgrade-Zeit erfolgen.

### Schritte

1. Öffnen Sie Insight in Ihrem Browser.
2. Klicken Sie Auf **Admin > Fehlerbehebung**.
3. Klicken Sie auf der Seite **Fehlerbehebung** auf **Backup**.

Die Dauer für die Sicherung der Datenbank kann je nach verfügbaren Ressourcen (Architektur, CPU und Arbeitsspeicher), der Größe der Datenbank und der Anzahl der in Ihrer Umgebung überwachten Objekte variieren.

Wenn die Sicherung abgeschlossen ist, werden Sie gefragt, ob Sie die Datei herunterladen möchten.

4. Laden Sie die Sicherungsdatei herunter.

## Sichern der Sicherheitskonfiguration

Wenn Ihre Insight-Komponenten eine nicht standardmäßige Sicherheitskonfiguration verwenden, müssen Sie die Sicherheitskonfiguration sichern und die Konfiguration anschließend auf allen Komponenten wiederherstellen, nachdem die neue Software installiert wurde. Die Sicherheitskonfiguration muss wiederhergestellt werden, bevor das Data Warehouse-Datenbankbackup wiederhergestellt wird.




## Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zum Erstellen einer Sicherungskopie der Konfiguration und zum Wiederherstellen der gespeicherten Konfiguration. Weitere Informationen erhalten Sie, wenn Sie nach suchen `securityadmin` Im OnCommand Insight Dokumentationszentrum: <http://docs.netapp.com/oci-73/index.jsp>

## Erstellen von benutzerdefinierten Data Warehouse-Berichten

Wenn Sie benutzerdefinierte Berichte erstellt haben und nicht über den verfügbaren `.xml` Quelldateien für sie, dann sollten Sie diese Berichte vor dem Upgrade sichern. Sie sollten sie dann auf einen anderen Server als den Data Warehouse-Server kopieren.

### Schritte

1. Melden Sie sich beim Data Warehouse-Portal unter `an https://fqdn/dwh`.
2. Klicken Sie in der Symbolleiste Data Warehouse auf  Um das Reporting Portal zu öffnen und sich anzumelden.
3. Wählen Sie **Datei > Öffnen**.
4. Wählen Sie den Ordner aus, in dem sich der Bericht befindet, wählen Sie den Bericht aus, und klicken Sie dann auf **Öffnen**.
5. Wählen Sie **Extras > Bericht in Zwischenablage kopieren**.
6. Öffnen Sie einen Texteditor, fügen Sie den Inhalt des Berichts ein, und speichern Sie die Datei unter `report_name.txt`, Wo `report _name` Ist der Name des Berichts.
7. Speichern Sie die Berichte auf einem anderen Server als dem Data Warehouse-Server.

## Durchführen des Software-Upgrades

Nachdem Sie alle erforderlichen Aufgaben abgeschlossen haben, können Sie alle Insight-Komponenten auf eine neue Version aktualisieren, indem Sie das entsprechende Installationspaket auf jedem Server herunterladen und ausführen.

### Aktualisieren Von Insight

Nachdem Sie alle erforderlichen Aufgaben abgeschlossen haben, melden Sie sich beim Insight Server an und führen das Installationspaket aus, um das Upgrade abzuschließen. Beim Upgrade wird die vorhandene Software deinstalliert, die neue Software installiert und der Server anschließend neu gestartet.

### Bevor Sie beginnen

Das Insight-Installationspaket muss sich auf dem Server befinden.

### Schritte

1. Melden Sie sich beim Insight-Server mit einem Konto an, das über lokale Windows-

Administratorberechtigungen verfügt.

2. Suchen Sie das Insight Installationspaket (SANscreenServer-x64-version\_number-build\_number.msi) Verwenden Sie Windows Explorer und doppelklicken Sie darauf.

Der OnCommand InsightSetup-Assistent wird angezeigt.

3. Bewegen Sie das Fortschrittsfenster von der Mitte des Bildschirms weg und weg vom **Setup-Wizard**-Fenster, so dass alle generierten Fehler nicht aus der Ansicht ausgeblendet werden.
4. Befolgen Sie die Anweisungen des Setup-Assistenten.

Es empfiehlt sich, alle Standardeinstellungen ausgewählt zu lassen.

### Nachdem Sie fertig sind

Um zu überprüfen, ob das Upgrade erfolgreich war oder Fehler generiert wurden, überprüfen Sie das Upgrade-Protokoll am folgenden Speicherort: <install directory>\SANscreen\wildfly\standalone\log.

## Data Warehouse Wird Aktualisiert

Nachdem Sie alle erforderlichen Aufgaben abgeschlossen haben, können Sie sich beim Data Warehouse-Server anmelden und das Installationspaket ausführen, um das Upgrade abzuschließen.

### Über diese Aufgabe

Inline-Upgrade wird vom Data Warehouse (DWH) nicht unterstützt. Führen Sie die folgenden Schritte aus, um auf die neue Version der DWH-Software zu aktualisieren.



Beim Aktualisieren von DWH wird der Ordner, der das Tresorbackup des *securityadmin*-Tools enthält, gelöscht. Es wird dringend empfohlen, den Tresor vor der Aktualisierung der DWH zu sichern. Als Referenz gelten die Standardordner für Tresorordner wie folgt:

- Vault-Ordner (verwendete Vaults): %SANSCREEN\_HOME%\wildfly\standalone\configuration\vault
- Vault-Backups: %SANSCREEN\_HOME%\backup\vault

Siehe "[Verwaltung der Sicherheit im Data Warehouse](#)" Finden Sie weitere Informationen.

### Schritte

1. Melden Sie sich beim DWH-Server mit einem Konto an, das über lokale Windows-Administratorberechtigungen verfügt.
2. Sichern Sie die DWH-DB und Berichte über die DWH-Portalschnittstelle.
3. Sichern Sie die Sicherheitskonfiguration, wenn der Server eine nicht standardmäßige Sicherheitskonfiguration verwendet.
4. Deinstallieren Sie die DWH-Software vom Server.
5. Starten Sie den Server neu, um Komponenten aus dem Speicher zu entfernen.

6. Installieren Sie die neue Version von DWH auf dem Server.

Die Installation dauert etwa 2 Stunden. Es empfiehlt sich, alle Standardeinstellungen ausgewählt zu lassen.

7. Stellen Sie die nicht standardmäßige Sicherheitskonfiguration auf dem DWH-Server wieder her.

8. Stellen Sie die DWH-Datenbank auf dem Server wieder her.

### **Nachdem Sie fertig sind**

Nach dem Upgrade müssen Sie die Data Warehouse-Datenbank wiederherstellen, die so lange oder länger dauern kann wie das Upgrade.



Während eines OnCommand Insight-Upgrades ist es nicht ungewöhnlich, dass ein Kunde zu einem anderen Insight-Server wechselt. Wenn Sie Ihren Insight-Server geändert haben, zeigen die vorhandenen Konnektoren nach der Wiederherstellung der Data Warehouse-Datenbank auf die vorherige Server-IP-Adresse oder den Hostnamen. Es empfiehlt sich, den Konnektor zu löschen und einen neuen zu erstellen, um mögliche Fehler zu vermeiden.

### **Beibehalten von benutzerdefinierten Cognos-Einstellungen während einer Data Warehouse-Aktualisierung**

Benutzerdefinierte Cognos-Einstellungen, z. B. nicht standardmäßige SMTP-E-Mail-Einstellungen, werden nicht automatisch als Teil eines Data Warehouse-Upgrades gesichert. Sie müssen die benutzerdefinierten Einstellungen nach einem Upgrade manuell dokumentieren und wiederherstellen.

Bevor Sie das Data Warehouse aktualisieren, erstellen Sie eine Checkliste mit allen benutzerdefinierten Cognos-Einstellungen, die Sie beibehalten möchten, und überprüfen Sie die Liste vor dem Upgrade des Systems. Nach Abschluss der Aktualisierung können Sie die Werte manuell wiederherstellen, um sie auf die Einstellungen in der ursprünglichen Konfiguration zurückzusetzen.

### **Sichern der Sicherheitskonfiguration**

Wenn Ihre Insight-Umgebung eine nicht standardmäßige Sicherheitskonfiguration verwendet, müssen Sie die Sicherheitskonfiguration sichern und die Sicherheitskonfiguration nach der Installation der neuen Software wiederherstellen. Die Sicherheitskonfiguration muss wiederhergestellt werden, bevor das Data Warehouse-Datenbankbackup wiederhergestellt wird.

### **Über diese Aufgabe**

Sie verwenden das `securityadmin` Tool zum Erstellen einer Sicherungskopie der Konfiguration und zum Wiederherstellen der gespeicherten Konfiguration. Weitere Informationen erhalten Sie, wenn Sie nach suchen `securityadmin` Im OnCommand Insight Dokumentationszentrum: <http://docs.netapp.com/oci-73/index.jsp>

### **Aktualisierung der Server der Remote-Akquisitionseinheit**

Nachdem Sie alle erforderlichen Aufgaben abgeschlossen haben, können Sie sich beim Server der Remote-Erfassungseinheit anmelden und das Installationspaket ausführen,

um das Upgrade abzuschließen. Sie müssen diese Aufgabe auf allen Remote-Akquisitionsservern in Ihrer Umgebung ausführen.

### Bevor Sie beginnen

- Sie müssen ein Upgrade von OnCommand Insight durchgeführt haben.
- Das OnCommand Insight-Installationspaket muss sich auf dem Server befinden.

### Schritte

1. Melden Sie sich beim Server der Remote-Erfassungseinheit mit einem Konto an, das über lokale Windows-Administratorberechtigungen verfügt.
2. Suchen Sie das Insight Installationspaket (`RAU-x64-version_number-build_number.msi`)  
Verwenden Sie Windows Explorer und doppelklicken Sie darauf.

Der OnCommand Insight-Einrichtungsassistent wird angezeigt.

3. Verschieben Sie das Fenster mit dem Installationsassistenten vom Zentrum des Bildschirms weg und entfernen Sie es aus dem Fenster mit dem Installationsassistenten, sodass generierte Fehler nicht aus der Ansicht ausgeblendet werden.
4. Befolgen Sie die Anweisungen des Setup-Assistenten.

Es empfiehlt sich, alle Standardeinstellungen ausgewählt zu lassen.

### Nachdem Sie fertig sind

- Um zu überprüfen, ob das Upgrade erfolgreich war oder Fehler generiert wurden, überprüfen Sie das Upgrade-Protokoll am folgenden Speicherort: `<install_directory>\SANscreen\bin\log`.
- Verwenden Sie die `securityadmin` Tool zum Wiederherstellen der gespeicherten Sicherheit

Konfiguration. Weitere Informationen finden Sie im OnCommand Insight nach `securityadmin`

Dokumentationscenter: <http://docs.netapp.com/oci-73/index.jsp>

- Löschen Sie den Cache und den Verlauf Ihres Browsers, um sicherzustellen, dass Sie die neuesten Daten vom Server empfangen.

## Aufgaben nach dem Upgrade werden ausgeführt

Nachdem Sie ein Upgrade auf die neueste Version von Insight durchgeführt haben, müssen Sie weitere Aufgaben ausführen.

### Installieren von Patches für Datenquellen

Falls zutreffend, sollten Sie die neuesten Patches installieren, die für Ihre Datenquellen verfügbar sind, um die neuesten Funktionen und Verbesserungen nutzen zu können. Nach dem Hochladen eines Datenquellpatches können Sie ihn auf allen Datenquellen desselben Typs installieren.

## Bevor Sie beginnen

Sie müssen sich an den technischen Support wenden und den erhalten haben .zip Datei, die die neuesten Datenquellpatches enthält, indem sie ihnen die Version bereitstellt, von der Sie ein Upgrade durchführen möchten, und die Version, auf die Sie aktualisieren möchten.

### Schritte

1. Platzieren Sie die Patch-Datei auf dem Insight-Server.
2. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
3. Klicken Sie Auf **Patches**.
4. Wählen Sie über die Schaltfläche Aktionen die Option **Patch anwenden** aus.
5. Klicken Sie im Dialogfeld **Data source Patch anwenden** auf **Browse**, um die hochgeladene Patch-Datei zu finden.
6. Überprüfen Sie die Typen **Patch-Name**, **Beschreibung** und **betroffene Datenquellen**.
7. Wenn der ausgewählte Patch korrekt ist, klicken Sie auf **Patch anwenden**.

Alle Datenquellen des gleichen Typs werden mit diesem Patch aktualisiert. Insight zwingt den Neustart der Erfassung automatisch, sobald eine Datenquelle hinzugefügt wird. Die Erkennung umfasst die Erkennung von Änderungen in der Netzwerktopologie, einschließlich des Hinzufügens oder Löschens von Knoten oder Schnittstellen.

8. Um den Ermittlungsvorgang manuell zu erzwingen, klicken Sie auf **Datenquellen** und klicken Sie neben der Datenquelle auf **erneut abrufen**, um die Datenerhebung sofort zu erzwingen.

Wenn sich die Datenquelle bereits in einem Erfassungsprozess befindet, ignoriert Insight die Abfrage erneut.

## Ersetzen eines Zertifikats nach dem Upgrade von OnCommand Insight

Das Öffnen der OnCommand Insight-Web-Benutzeroberfläche nach einem Upgrade führt zu einer Zertifizierungswarnung. Die Warnmeldung wird angezeigt, weil nach dem Upgrade kein gültiges selbstsigniertes Zertifikat verfügbar ist. Um zu verhindern, dass die Warnmeldung in Zukunft angezeigt wird, können Sie ein gültiges selbstsigniertes Zertifikat installieren, um das ursprüngliche Zertifikat zu ersetzen.

## Bevor Sie beginnen

Ihr System muss die minimale Verschlüsselungsbit-Ebene (1024 Bit) erfüllen.

### Über diese Aufgabe

Die Zertifizierungswarnung hat keinen Einfluss auf die Benutzerfreundlichkeit des Systems. An der Eingabeaufforderung können Sie angeben, dass Sie das Risiko verstanden haben, und dann mit Insight fortfahren.

### Schritte

1. Listen Sie den Inhalt des Keystore auf: `C:\Program Files\SANscreen\java64\bin>keytool.exe -list -v -keystore "c:\Program`

```
Files\SANscreen\wildfly\standalone\configuration\server.keystore"
```

Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie ein `changeit`.

Es sollte mindestens ein Zertifikat im Schlüsselspeicher vorhanden sein, `ssl certificate`.

2. Löschen Sie die `ssl certificate`: `keytool -delete -alias ssl certificate -keystore c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Einen neuen Schlüssel generieren: `keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize 2048 -keystore "c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore"`
  - a. Wenn Sie nach vor- und Nachnamen gefragt werden, geben Sie den vollständig qualifizierten Domännennamen (FQDN) ein, den Sie verwenden möchten.
  - b. Geben Sie die folgenden Informationen zu Ihrer Organisation und Organisationsstruktur an:
    - Land: Zweistellige ISO-Abkürzung für Ihr Land (z. B. USA)
    - Bundesland oder Provinz: Name des Bundesstaates oder der Provinz, in dem sich der Hauptsitz Ihres Unternehmens befindet (z. B. Massachusetts)
    - Ort: Name der Stadt, in der sich der Hauptsitz Ihrer Organisation befindet (z. B. Waltham)
    - Name des Unternehmens: Name des Unternehmens, dem der Domain-Name gehört (z. B. NetApp)
    - Name der Organisationseinheit: Name der Abteilung oder Gruppe, die das Zertifikat verwenden soll (z. B. Support)
    - Domänenname/ Allgemeiner Name: Der FQDN, der für DNS-Suchen Ihres Servers verwendet wird (z. B. `www.example.com`). Das System antwortet mit Informationen wie den folgenden: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
  - c. Eingabe `Yes` Wenn der allgemeine Name (CN) gleich dem FQDN ist.
  - d. Wenn Sie zur Eingabe des Schlüsselpassworts aufgefordert werden, geben Sie das Kennwort ein, oder drücken Sie die Eingabetaste, um das vorhandene Schlüsselspeicher-Passwort zu verwenden.
4. Erstellen Sie eine Zertifikatanforderungsdatei: `keytool -certreq -alias localhost -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

Der `c:\localhost.csr` Die Datei ist die neu generierte Zertifikatanforderungsdatei.

5. Senden Sie die `c:\localhost.csr` Bei der Zertifizierungsstelle zur Genehmigung einreichen.

Nachdem die Zertifikatanforderungsdatei genehmigt wurde, möchten Sie das Zertifikat in zurücksenden .der Formatieren. Die Datei wird möglicherweise als zurückgegeben .der Datei: Das Standarddateiformat ist .cer Für Microsoft CA-Services.

6. Importieren Sie das genehmigte Zertifikat: `keytool -importcert -alias localhost -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
  - a. Wenn Sie zur Eingabe eines Kennworts aufgefordert werden, geben Sie das Passwort für den Keystore ein.

Vom System wird die folgende Meldung angezeigt: `Certificate reply was installed in keystore`

7. Starten Sie den SANscreen-Serverdienst neu.

## Ergebnisse

Der Webbrowser meldet keine Zertifikatwarnungen mehr.

## Cognos-Speicher wird erhöht

Bevor Sie die Data Warehouse-Datenbank wiederherstellen, sollten Sie die Java-Zuweisung für Cognos von 768 MB auf 2048 MB erhöhen, um die Zeit für die Berichterstellung zu verkürzen.


### Schritte

1. Öffnen Sie ein Eingabeaufforderungsfenster als Administrator auf dem Data Warehouse-Server.
2. Navigieren Sie zum `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` Verzeichnis.
3. Geben Sie den folgenden Befehl ein: `cogconfigw`



Das Fenster IBM Cognos Configuration wird angezeigt.



Die Verknüpfung IBM Cognos Configuration verweist auf `disk drive:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat`. Wenn Insight im Verzeichnis Programme (Leerzeichen zwischen) installiert ist, das als Standard anstelle von ProgramFiles (kein Leerzeichen) dient, wird der installiert `.bat` Die Datei funktioniert nicht. Klicken Sie in diesem Fall mit der rechten Maustaste auf die Anwendungsverknüpfung, und ändern Sie sie `cognosconfigw.bat` Bis `cognosconfig.exe` Um die Verknüpfung zu korrigieren.

4. Erweitern Sie im linken Navigationsbereich **Environment**, erweitern Sie **IBM Cognos Services** und klicken Sie dann auf **IBM Cognos**.
5. Wählen Sie **Maximum Memory for Tomcat in MB** und ändern Sie 768 MB auf 2048 MB.
6. Klicken Sie in der Symbolleiste IBM Cognos Configuration auf  (Speichern).

Es wird eine Informationsmeldung angezeigt, die Sie über die Aufgaben informiert, die Cognos ausführt.

7. Klicken Sie Auf **Schließen**.
8. Klicken Sie in der Symbolleiste IBM Cognos Configuration auf  (Stopp).
9. Klicken Sie in der Symbolleiste IBM Cognos Configuration auf  (Start).

## Wiederherstellen der Data Warehouse-Datenbank

Wenn Sie die Data Warehouse-Datenbank sichern, erstellt Data Warehouse einen `.zip` Datei, die Sie später zur Wiederherstellung derselben Datenbank verwenden können.

### Über diese Aufgabe

Wenn Sie die Data Warehouse-Datenbank wiederherstellen, können Sie auch Benutzerkontoinformationen aus dem Backup wiederherstellen. Benutzerverwaltungstabellen werden von der Data Warehouse-Berichtsenge

in einer reinen Data Warehouse-Installation verwendet.

## Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://fqdn/dwh`.
2. Klicken Sie im Navigationsfenster links auf **Backup/Restore**.
3. Klicken Sie im Abschnitt **Datenbank und Berichte wiederherstellen** auf **Durchsuchen**, und suchen Sie den `.zip` Datei, die das Data Warehouse-Backup enthält.
4. Es ist eine Best Practice, beide der folgenden Optionen ausgewählt zu lassen:

- **Datenbank wiederherstellen**

Enthält Data Warehouse-Einstellungen, Data Marts, Verbindungen und Benutzerkontoinformationen.

- **Berichte wiederherstellen**

Umfasst benutzerdefinierte Berichte, vordefinierte Berichte, Änderungen an vordefinierten Berichten, die Sie vorgenommen haben, und Berichtseinstellungen, die Sie in der Berichtsverbindung vorgenommen haben.

5. Klicken Sie Auf **Wiederherstellen**.

Navigieren Sie nicht vom Wiederherstellungsstatus weg. Wenn Sie dies tun, wird der Wiederherstellungsstatus nicht mehr angezeigt und Sie erhalten keine Anzeige mehr, wenn der Wiederherstellungsvorgang abgeschlossen ist.

6. Um den Upgrade-Prozess zu überprüfen, lesen Sie die `dwh_upgrade.log` Datei, die sich am folgenden Speicherort befindet: `<install directory>\SANSscreen\wildfly\standalone\log`.

Nachdem der Wiederherstellungsvorgang abgeschlossen ist, erscheint eine Meldung direkt unter der Schaltfläche **Wiederherstellen**. Wenn die Wiederherstellung erfolgreich war, wird die Meldung erfolgreich angezeigt. Wenn der Wiederherstellungsvorgang fehlschlägt, zeigt die Meldung die spezifische Ausnahme an, die aufgetreten ist, um den Fehler zu verursachen. Wenden Sie sich in diesem Fall an den technischen Support und stellen Sie diese bereit `dwh_upgrade.log` Datei: Wenn eine Ausnahme auftritt und der Wiederherstellungsvorgang fehlschlägt, wird die ursprüngliche Datenbank automatisch zurückgesetzt.



Wenn der Wiederherstellungsvorgang mit der Meldung „Failed upgrading cognos content Store“ fehlschlägt, stellen Sie die Data Warehouse-Datenbank ohne ihre Berichte wieder her (nur Datenbank) und verwenden Sie Ihre XML-Berichtsbackups zum Importieren Ihrer Berichte.


## Benutzerdefinierte Data Warehouse-Berichte werden wiederhergestellt

Falls zutreffend, können Sie alle benutzerdefinierten Berichte, die Sie vor dem Upgrade gesichert haben, manuell wiederherstellen. Sie müssen dies jedoch nur tun, wenn Sie Berichte verlieren, wenn diese beschädigt wurden.

## Schritte

1. Öffnen Sie Ihren Bericht mit einem Texteditor, und wählen Sie den Inhalt aus, und kopieren Sie ihn.
2. Melden Sie sich beim Reporting-Portal unter an `https://fqdn/reporting`.



3. Klicken Sie in der Symbolleiste Data Warehouse auf  Um das Insight Reporting-Portal zu öffnen.
4. Wählen Sie im Menü Start die Option **Report Studio**.
5. Wählen Sie ein beliebiges Paket aus.

Report Studio wird angezeigt.

6. Klicken Sie auf **Create New**.
7. Wählen Sie **Liste**.
8. Wählen Sie im Menü Extras die Option **Bericht aus Zwischenablage öffnen**.

Das Dialogfeld **Bericht aus Zwischenablage öffnen** wird angezeigt.

9. Wählen Sie im Menü Datei die Option **Speichern unter** und speichern Sie den Bericht im Ordner Benutzerdefinierte Berichte.
10. Öffnen Sie den Bericht, um zu überprüfen, ob er importiert wurde.

Wiederholen Sie diese Aufgabe für jeden Bericht.





Beim Laden eines Berichts wird möglicherweise ein „Expression Parsing error“ angezeigt. Das bedeutet, dass die Abfrage einen Verweis auf mindestens ein Objekt enthält, das nicht vorhanden ist, was bedeutet, dass im Fenster Quelle kein Paket ausgewählt ist, um den Bericht zu validieren. Klicken Sie in diesem Fall mit der rechten Maustaste auf eine Data-Mart-Dimension im Fenster Quelle, und wählen Sie Berichtspaket, Wählen Sie dann das dem Bericht zugeordnete Paket aus (z. B. das Bestandspaket, wenn es sich um einen Bestandsbericht handelt, oder eines der Leistungspakete, wenn es sich um einen Leistungsbericht handelt), damit Report Studio es validieren und speichern kann.

## Überprüfung, ob das Data Warehouse historische Daten enthält

Nachdem Sie Ihre benutzerdefinierten Berichte wiederhergestellt haben, sollten Sie überprüfen, ob Data Warehouse historische Daten sammelt, indem Sie Ihre benutzerdefinierten Berichte anzeigen.

### Schritte

1. Melden Sie sich beim Data Warehouse-Portal unter an <https://fqdn/dwh>.
2. Klicken Sie in der Symbolleiste Data Warehouse auf  Um das Insight Reporting-Portal zu öffnen und sich anzumelden.
3. Öffnen Sie den Ordner, der Ihre benutzerdefinierten Berichte enthält (z. B. Benutzerdefinierte Berichte).
4. Klicken Sie Auf  Um die Ausgabeformatoptionen für diesen Bericht zu öffnen.
5. Wählen Sie die gewünschten Optionen aus und klicken Sie auf **Ausführen**, um sicherzustellen, dass sie mit Speicher-, Rechen- und Switch-historischen Daten gefüllt sind.

## Wiederherstellung des Performance-Archivs

Bei Systemen, die eine Performance-Archivierung durchführen, werden im Upgrade-Prozess nur Archivdaten von sieben Tagen wiederhergestellt. Sie können die

verbleibenden Archivdaten wiederherstellen, nachdem das Upgrade konkurriert wurde.

## Über diese Aufgabe

Führen Sie die folgenden Schritte aus, um das Performance-Archiv wiederherzustellen.

### Schritte

1. Klicken Sie in der Symbolleiste auf **Admin > Fehlerbehebung**
2. Klicken Sie im Abschnitt Wiederherstellen unter **Load Performance Archive** auf **Load**.

Das Laden des Archivs erfolgt im Hintergrund. Das vollständige Archiv kann sehr lange geladen werden, da die archivierten Performance-Daten der einzelnen Tage in Insight eingetragen sind. Der Status des Archivladens wird im Archiv-Bereich dieser Seite angezeigt.

## Prüfen der Anschlüsse

Nach dem Upgrade möchten Sie die Konnektoren testen, um sicherzustellen, dass eine Verbindung zwischen dem OnCommand Insight Data Warehouse und dem OnCommand Insight-Server besteht.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://fqdn/dwh`.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.
3. Wählen Sie den ersten Anschluss aus.

Die Seite Connector bearbeiten wird angezeigt.

4. Klicken Sie Auf **Test**.
5. Wenn der Test erfolgreich ist, klicken Sie auf **Schließen**; wenn er fehlschlägt, geben Sie den Namen des Insight-Servers in das Feld **Name** und seine IP-Adresse in das Feld **Host** ein und klicken Sie auf **Test**.
6. Wenn eine erfolgreiche Verbindung zwischen dem Data Warehouse und dem Insight-Server besteht, klicken Sie auf **Speichern**.

Wenn dies nicht gelingt, überprüfen Sie die Verbindungskonfiguration und stellen Sie sicher, dass der Insight-Server keine Probleme hat.

7. Klicken Sie Auf **Test**.

Data Warehouse testet die Verbindung.

## Überprüfen der Planung für Extrahieren, Transformieren und Laden

Nach dem Upgrade sollten Sie sicherstellen, dass der ETL-Prozess (Extrahieren, Transformieren und Laden) Daten aus den OnCommand Insight-Datenbanken abrufen, die Daten transformiert und in den Data Marts speichert.

## Schritte

1. Melden Sie sich beim Data Warehouse-Portal unter an `https://fqdn/dwh`.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Zeitplan**.
3. Klicken Sie auf **Zeitplan bearbeiten**.
4. Wählen Sie **Täglich** oder **wöchentlich** aus der Liste **Typ** aus.

Es wird empfohlen, die Ausführung von ETL einmal pro Tag zu planen.

5. Vergewissern Sie sich, dass die ausgewählte Zeit die Zeit ist, zu der der Job ausgeführt werden soll.

Dadurch wird sichergestellt, dass der Build-Job automatisch ausgeführt wird.

6. Klicken Sie Auf **Speichern**.

## Festplattenmodelle werden aktualisiert

Nach der Aktualisierung sollten Sie über aktualisierte Festplattenmodelle verfügen. Wenn Insight jedoch aus irgendeinem Grund neue Laufwerksmodelle nicht erkennen konnte, können Sie sie manuell aktualisieren.

### Bevor Sie beginnen

Sie müssen den technischen Support von erhalten haben .zip Datei, die die neuesten Patches für die Datenquelle enthält.

## Schritte

1. Stoppen Sie den SANscreen Acq-Dienst.
2. Navigieren Sie zum folgenden Verzeichnis: `<install directory>\SANscreen\wildfly\standalone\deployments\datasources.war`.
3. Verschieben Sie den aktuellen `diskmodels.jar` An einem anderen Speicherort ablegen.
4. Kopieren Sie das neue `diskmodels.jar` In die Datei `datasources.war` Verzeichnis.
5. Starten Sie den SANscreen Acq-Dienst.

## Überprüfung der Ausführung von Business Intelligence-Tools

Falls zutreffend, sollten Sie überprüfen, ob Ihre Business Intelligence-Tools ausgeführt werden und Daten nach dem Upgrade abrufen.

Stellen Sie sicher, dass Business Intelligence-Tools wie BMC Atrium und ServiceNow ausgeführt werden und Daten abrufen können. Dazu gehören der BMC-Anschluss und Lösungen, die REST nutzen.

## Fehlerbehebung bei einem Upgrade

Wenn nach einem OnCommand Insight-Upgrade Probleme auftreten, können Sie die Fehlerbehebungsinformationen zu einigen möglichen Problemen prüfen.

## Cognos kann nicht über das Windows-Startmenü gestartet werden

Die Existenz eines Raumes vor \SANSscreen\cognos Im Pfadnamen liegt ein Problem vor. Weitere Informationen finden Sie in der NetApp Customer Success Community unter: <https://forums.netapp.com/thread/62721>.

## Fehlermeldung „Keine gültige win32-Anwendung“

Dies ist ein Problem mit Microsoft Windows. Um dieses Problem zu beheben, müssen Sie Anführungszeichen um den Bildpfad in der Registrierung setzen. Weitere Informationen finden Sie in der folgenden Dokumentation: <https://support.microsoft.com/en-us/kb/812486/en-us>.

## Anmerkungen sind nicht vorhanden

Wenn ein Data Warehouse-ETL-Job Anmerkungen von einer Insight-Instanz abfragt, erhält er manchmal eine leere Antwort (ein 0-Ergebnis) als Fehler. Dieser Fehler führt zu Anmerkungen für bestimmte Objekte, die zwischen dem Status „Present“ und „Not Present“ im Data Warehouse hin und her verschoben werden. Weitere Informationen finden Sie im Folgenden: <https://forums.netapp.com/docs/DOC-44167>

## Unterschiede bei den in Berichten angezeigten Werten

Vor 7.0 waren Berichte ganzzahlig. Sie sind jetzt dezimal-basiert; daher können Sie nach dem Upgrade feststellen, dass die Anzeige der Werte erhöht oder verringert wird.

## Daten werden nicht in Berichten angezeigt

In 7.0 wurden mehrere Modellnamen geändert (z. B. wurde Symmetrix in Symmetrix VMAX geändert). Wenn ein Bericht daher einen Filter für „Symmetrix“ enthält, werden beim Ausführen des Berichts keine Daten angezeigt. Um den Bericht zu ändern, müssen Sie den Bericht mit dem Abfrage-Explorer in Report Studio öffnen, nach dem Modellnamen suchen, ihn durch den neuen Modellnamen ersetzen und den Bericht speichern.

## 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 IRGEND EINER 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.