Überblick über den OnCommand Insight Upgrade-Prozess

OnCommand Insight

NetApp
October 24, 2024

Inhalt

Überblick über den OnCommand Insight Upgrade-Prozess 1
OnCommand Insight Upgrade-Checkliste 2

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.

Sie müssen den Tresor sichern, bevor Sie OnCommand Insight aktualisieren.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

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)

Sie müssen den Tresor sichern, bevor Sie OnCommand Insight aktualisieren.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

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.	
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 Virenscan-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. Außerdem müssen Sie den IBM/DB2-Ordner (z. B. *C:\Program Files\IBM\DB2*) nach der Installation von der Virenprüfung ausschließen.	

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 stillgelegten 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: `disk drive:\install directory\SANscreen\wildfly\standalone\configuration` 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: `disk drive:\install directory\SANscreen\wildfly\standalone\deployments\datasources.war`.	
Sichern Sie alle benutzerdefinierten Datenbanktabellen und -Ansichten mithilfe des `mysqldump` 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\sanscreen` Verzeichnis, da der Inhalt dieses Verzeichnisses durch den Upgrade-Prozess gelöscht wird.Stellen Sie sicher, dass Sie diese Dinge aus dem verschieben `\sanscreen` 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 `\sanscreen` Verzeichnis: `\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt`.	