



Panoramica del processo di aggiornamento di OnCommand Insight

OnCommand Insight

NetApp
October 24, 2024

Sommario

Panoramica del processo di aggiornamento di OnCommand Insight	1
Checklist per l'upgrade di OnCommand Insight	2

Panoramica del processo di aggiornamento di OnCommand Insight

Prima di iniziare l'aggiornamento di Insight, è importante comprendere il processo di aggiornamento. Il processo di aggiornamento è lo stesso per la maggior parte delle versioni di Insight.

 **È necessario eseguire il backup del vault** prima di aggiornare OnCommand Insight.

Per ulteriori informazioni, vedere le "[Strumento securityadmin](#)" istruzioni.

Il processo di aggiornamento di Insight include le seguenti attività di alto livello:

- Scaricare i pacchetti di installazione
- Backup del database Data Warehouse

Per evitare la possibilità di generare report errati dei dati, è necessario eseguire il backup del database Data Warehouse prima di eseguire il backup del database Insight.

- Backup del database Insight

Il backup del database Insight viene eseguito automaticamente quando si esegue l'aggiornamento in-place. È consigliabile eseguire il backup del database prima dell'aggiornamento e collocarlo in una posizione diversa da quella del server Insight. Durante il processo di aggiornamento, Insight non raccoglie nuovi dati. Per ridurre al minimo la quantità di dati non raccolti, è necessario avviare il backup del database entro un'ora o due del tempo di aggiornamento pianificato.

- Eseguire il backup della configurazione di sicurezza Data Warehouse e Remote Acquisition Unit se la configurazione è stata modificata dalla configurazione predefinita.

La configurazione di sicurezza non predefinita deve essere ripristinata nel Data Warehouse e nel server RAU al termine dell'aggiornamento e prima che il database Data Warehouse venga ripristinato nel sistema.

- Backup di report personalizzati di Data Warehouse

Quando si esegue il backup del database Data Warehouse, vengono inclusi report personalizzati. Il file di backup viene creato sul server Data Warehouse. Si consiglia di eseguire il backup dei report personalizzati in una posizione diversa dal server Data Warehouse.

- Disinstallazione del software Data Warehouse e dell'unità di acquisizione remota, se applicabile

Il server Insight dispone di un aggiornamento in-place; non è necessario disinstallare il software. L'aggiornamento in-place esegue il backup del database, disinstalla il software, installa la nuova versione e ripristina il database.

- Aggiornamento del software sul server Insight, sul data warehouse e sulle unità di acquisizione remota

Tutte le licenze applicate in precedenza rimangono nel registro; non è necessario riapplicarle.

- Completamento delle attività di post-aggiornamento

Checklist per l'upgrade di OnCommand Insight

È possibile utilizzare gli elenchi di controllo forniti per registrare i progressi durante la preparazione all'aggiornamento. Queste attività hanno lo scopo di ridurre il rischio di errori di upgrade e accelerare le attività di recovery e ripristino.

Checklist per la preparazione all'aggiornamento (obbligatorio)



È necessario eseguire il backup del vault prima di aggiornare OnCommand Insight.

Per ulteriori informazioni, vedere le "[Strumento securityadmin](#)" istruzioni.

Condizione	Completato?
Assicurarsi di disporre delle autorizzazioni di amministratore locale di Windows, necessarie per eseguire il processo di aggiornamento, su tutti i server Insight.	
Se i server Insight, Data Warehouse o Remote Acquisition Unit risiedono su piattaforme a 32 bit, è necessario aggiornare i server alle piattaforme a 64 bit. A partire da Insight 7.x, gli aggiornamenti sono disponibili solo per le piattaforme a 64 bit.	
Assicurarsi di disporre delle autorizzazioni necessarie per modificare o disattivare il software antivirus su tutti i server dell'ambiente. Per evitare un errore di aggiornamento dovuto a un software di scansione virus attivo, è necessario escludere la directory di installazione Insight (disk drive:\install directory\sanscreen dall'accesso alla scansione antivirus durante l'aggiornamento. Dopo aver aggiornato tutti i componenti, è possibile riattivare il software antivirus in modo sicuro; tuttavia, assicurarsi di configurare la scansione in modo da escludere tutti i componenti presenti nella directory di installazione di Insight. Inoltre, è necessario escludere la cartella IBM/DB2 (ad esempio C: Programmi IBM DB2) dalla scansione antivirus dopo l'installazione.	

Checklist per la preparazione all'aggiornamento (Best practice)

Condizione	Completato?
------------	-------------

Pianifica quando intendi eseguire l'upgrade, tenendo conto del fatto che la maggior parte degli aggiornamenti richiede un minimo di 4-8 ore; le aziende più grandi richiederanno più tempo. I tempi di aggiornamento possono variare in base alle risorse disponibili (architettura, CPU e memoria), alle dimensioni dei database e al numero di oggetti monitorati nell'ambiente.	
Contatta il tuo account representative per informazioni sui tuoi piani di aggiornamento e fornisci la versione di Insight installata e a quale versione desideri eseguire l'aggiornamento.	
Assicurarsi che le risorse correnti allocate a Insight, Data Warehouse e Remote Acquisition Unit soddisfino ancora le specifiche consigliate. Consulta le linee guida per il dimensionamento consigliato per tutti i server. In alternativa, puoi contattare il tuo rappresentante commerciale per discutere delle linee guida per il dimensionamento.	
Assicurarsi di disporre di spazio su disco sufficiente per il processo di backup e ripristino del database. I processi di backup e ripristino richiedono circa cinque volte lo spazio su disco utilizzato dal file di backup sui server Insight e Data Warehouse. Ad esempio, un backup da 50 GB richiede da 250 a 300 GB di spazio libero su disco.	
Assicurarsi di avere accesso a Firefox® o al browser Chrome™ quando si esegue il backup dei database Insight e Data Warehouse. Internet Explorer non è consigliato, perché si verificano alcuni problemi durante il caricamento e il download di file di dimensioni superiori a 4 GB.	
Eliminare .tmp File sul server Insight, che si trovano nella seguente posizione: <install directory>\SANscreen\wildfly\standalone\tmp.	
Rimuovere le origini dati duplicate e le origini dati decommissionate dal client Insight. La rimozione di origini dati dismesse o duplicate riduce il tempo necessario per eseguire l'aggiornamento e riduce l'opportunità di corruzione dei dati.	

<p>Se sono stati modificati i report predefiniti forniti con Insight, è necessario salvarli con un nome diverso e salvarli nella cartella Report clienti in modo da non perdere il report modificato durante l'aggiornamento o il ripristino del sistema.</p>	
<p>Se si dispone di report personalizzati o modificati di Data Warehouse creati dall'utente o da servizi professionali, creare un backup di tali report esportandoli in XML e spostandoli nella cartella Report clienti. Assicurarsi che il backup non si trovi sul server Data Warehouse. Se i report non vengono spostati nelle cartelle consigliate, il processo di aggiornamento potrebbe non eseguire il backup di tali report. Per le versioni precedenti di Insight, la mancata individuazione dei report nelle cartelle appropriate può causare la perdita di report personalizzati e modificati.</p>	
<p>Registrare tutte le impostazioni nell'utility di configurazione di IBM Cognos, poiché non sono incluse nel backup di Data Warehouse; è necessario riconfigurare queste impostazioni dopo l'aggiornamento. L'utility si trova in disk drive:\install directory\SANscreen\cognos\c10_64\bin64 Sul server Data Warehouse ed è possibile eseguirlo utilizzando cogconfigw Command.in alternativa, è possibile eseguire un backup completo di Cognos e importare tutte le impostazioni. Per ulteriori informazioni, consultare la documentazione di IBM Cognos.</p>	

Checklist per la preparazione all'aggiornamento (se applicabile)

Condizione	Completato?
<p>Se sono stati sostituiti i certificati autofirmati creati dall'installazione di Insight a causa di avvisi di sicurezza del browser con certificati firmati dall'autorità di certificazione interna, eseguire il backup del file keystore, che si trova nella seguente posizione: disk drive:\install directory\SANscreen\wildfly\standalone\configuration e ripristinarlo dopo l'aggiornamento. Questo sostituisce i certificati autofirmati creati da Insight con i certificati firmati.</p>	

<p>Se una delle origini dati è stata modificata per l'ambiente in uso e non si è certi che queste modifiche siano disponibili nella versione Insight alla quale si sta eseguendo l'aggiornamento, creare una copia della seguente directory, che consente di risolvere eventuali problemi di ripristino: <code>disk drive:\install\directory\SANscreen\wildfly\standalone\deployments\datasources.war</code>.</p>	
<p>Eseguire il backup di tutte le tabelle e le viste del database personalizzate utilizzando <code>mysqldump</code> Tool della riga di comando. Il ripristino di tabelle di database personalizzate richiede un accesso privilegiato al database. Contattare il supporto tecnico per assistenza sul ripristino di queste tabelle.</p>	
<p>Assicurarsi che non siano memorizzati in script di integrazione personalizzati, componenti di terze parti necessari per origini dati Insight, backup o altri dati richiesti <code>disk drive:\install\directory\sanscreen</code>. Poiché il contenuto di questa directory viene cancellato dal processo di aggiornamento, assicurarsi di spostare tali elementi da <code>\sanscreen</code> directory in un'altra posizione. Ad esempio, se l'ambiente contiene script di integrazione personalizzati, assicurarsi di copiare il seguente file in una directory diversa da <code>\sanscreen</code> directory:</p> <pre><code>\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt.</code></pre>	

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.