CA GREEN BOOK

CA IT Client Manager r12.5

Backup and Restore Procedures for DSM Managers on Microsoft® SQL Server® MDB

- BACKUP AND RESTORE PROCEDURE FOR r12, r12 SP1, AND r12.5 DSM MANAGERS
- BACKUP AND RESTORE PROCEDURE FOR CA ASSET INTELLIGENCE AND CA PATCH MANAGER

LEGAL NOTICE

This publication is based on current information and resource allocations as of its date of publication and is subject to change or withdrawal by CA at any time without notice. The information in this publication could include typographical errors or technical inaccuracies. CA may make modifications to any CA product, software program, method or procedure described in this publication at any time without notice.

Any reference in this publication to non-CA products and non-CA websites are provided for convenience only and shall not serve as CA's endorsement of such products or websites. Your use of such products, websites, and any information regarding such products or any materials provided with such products or at such websites shall be at your own risk.

Notwithstanding anything in this publication to the contrary, this publication shall not (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this publication remain at CA's sole discretion.

The information in this publication is based upon CA's experiences with the referenced software products in a variety of development and customer environments. Past performance of the software products in such development and customer environments is not indicative of the future performance of such software products in identical, similar or different environments. CA does not warrant that the software products will operate as specifically set forth in this publication. CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product.

Certain information in this publication may outline CA's general product direction. All information in this publication is for your informational purposes only and may not be incorporated into any contract. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "AS IS" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised of the possibility of such damages.

COPYRIGHT LICENSE AND NOTICE:

This publication may contain sample application programming code and/or language which illustrate programming techniques on various operating systems. Notwithstanding anything to the contrary contained in this publication, such sample code does not constitute licensed products or software under any CA license or services agreement. You may copy, modify and use this sample code for the purposes of performing the installation methods and routines described in this document. These samples have not been tested. CA does not make, and you may not rely on, any promise, express or implied, of reliability, serviceability or function of the sample code.

TITLE AND PUBLICATION DATE:

CA IT Client Manager r12.5 Green Book Backup and Restore Procedures for DSM Managers on Microsoft SQL Server MDB
Publication Date: May 02, 2011

ACKNOWLEDGEMENTS

Principal Authors

Sreekanth Bathalapalli

Madiraju Naresh

Gerhard Scholand

Steven Parker

The principal authors and CA would like to thank the following contributors:

Omkar Avasarala

Srinivas Choudavarapu

Arun Vellanki

CA Services

Development

Marketing

QA

Support

Engineering Services

Technical Sales

Technical Information

Third-Party Acknowledgements

Microsoft product shots reprinted with permission from Microsoft Corporation. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.

CA PRODUCT REFERENCES

This document references the following CA products:

- CA IT Client Manager (CA ITCM)

PREFACE

CA IT Client Manager combines the following former products into one fully functional solution:

- CA Asset Management
- CA Asset Intelligence
- CA Software Delivery
- CA Remote Control
- CA Patch Manager
- CA Desktop Migration Manager

This document focuses on various components of CA IT Client Manager Release 12.5 solution, and therefore has used the old product names when addressing these functional areas.

FEEDBACK

Please email us at greenbooks@ca.com to share your feedback on this CA Green Publication. Please include the title of this Green Publication in the subject of your email response. For technical assistance with a CA product, please contact CA Technical Support at http://ca.com/support.

Contents

Chapter 1: Preparing for the Backup

This section contains the following topics:

Planning for MDB Backup

Before you create a backup policy for your enterprise, you must take into consideration the following factors:

- The backup and restore tool you want to use

  The backup and restore procedures differ depending on the backup and restore tool that you use. This Green Book covers the full, differential, and transactional log backup procedures.

- The frequency of backups

  Depending on how actively you use CA ITCM especially with regard to software delivery jobs, you must decide the frequency of the backups. Although the asset management data changes frequently, collecting this data from DSM agent is fairly simple. However, software delivery job history is difficult to recreate.

- Scalability server backup

  The data on the scalability server is transient and can be recovered by the reinstallation of the server and redistribution of packages from the domain manager. Scalability server backups are optional unless the recovery time or bandwidth to the domain manager is restricted.

Recommended Backup Policy

We recommend that you devise a backup policy that comprises of the following backups for your enterprise and domain managers:

- Weekly full system backup
- Daily differential backups
- Hourly transactional backups

Also, we recommend that you perform at least two tests yearly to verify the recovery procedures.

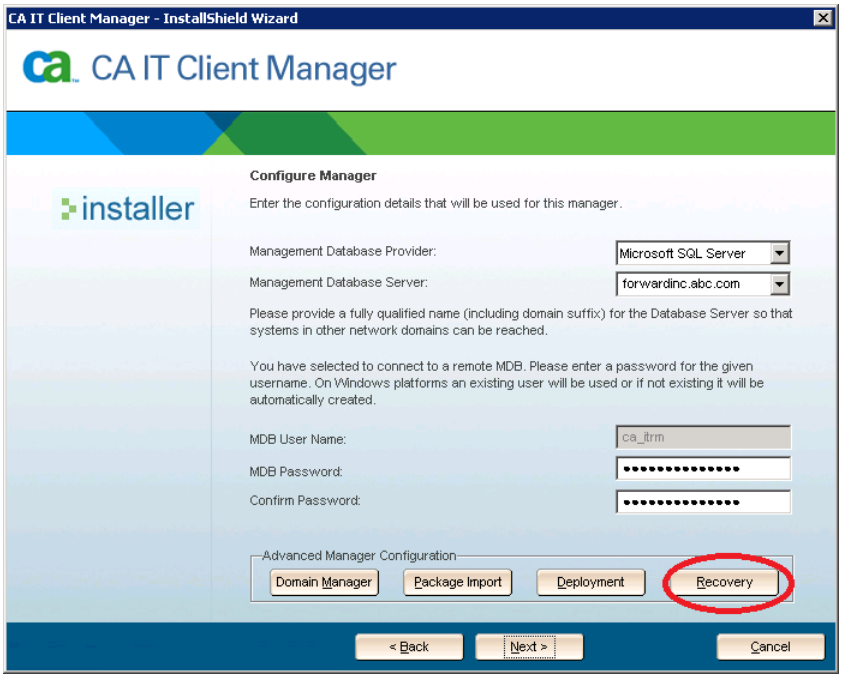
Configure Backup during CA ITCM Installation

You must configure the backup settings when you install the DSM manager. The backup configuration creates a DSMRecovery.ini file that is used in the event of recovering a failed DSM manager.

Note: By default, the backup configurations are enabled during CA ITCM installation. If you have already installed the product, you must only be aware of the default file locations specified in Step 3 and 4 in the following procedure. You specify the file location information in the file backup procedure.

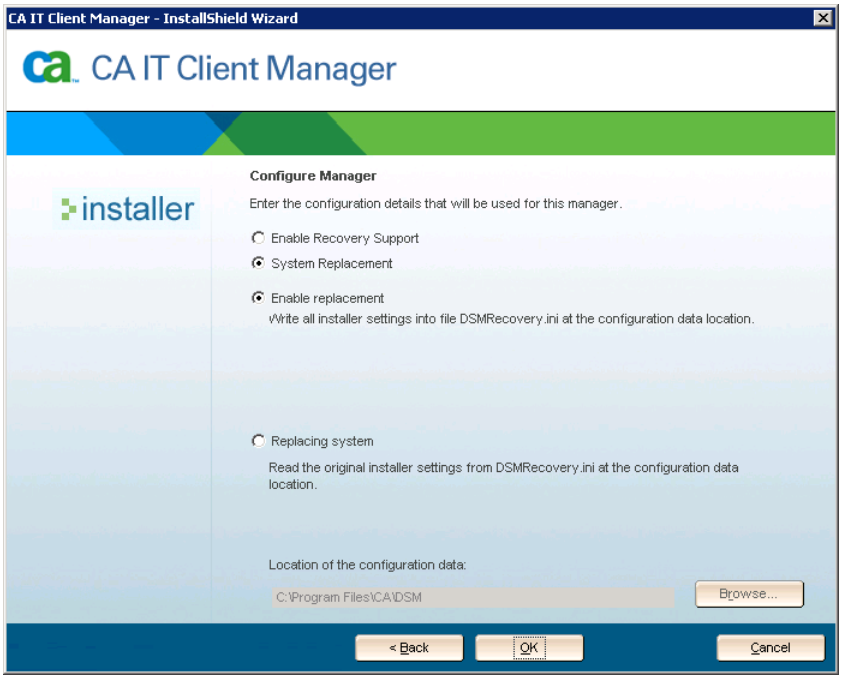
To configure backup during CA ITCM Installation

1. Click Recovery in the Configure Manager page of the CA ITCM installation wizard.

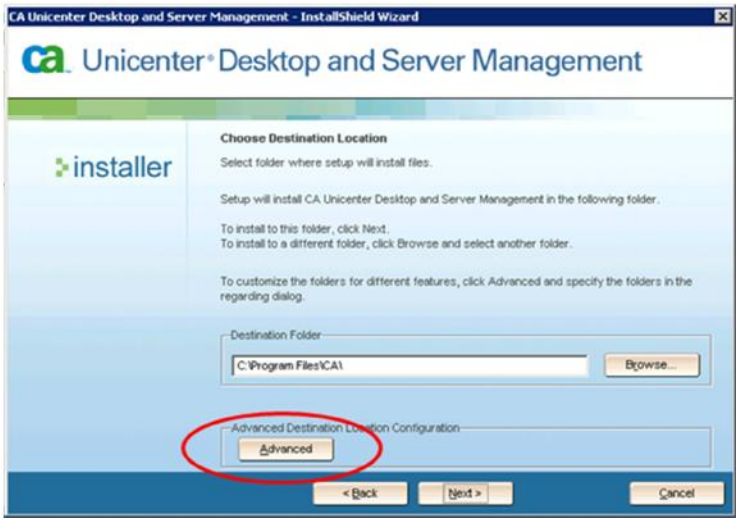


The Configure Manager page opens.

2. Select the System Replacement and Enable Replacement options if they are not already selected and click OK.



3. Proceed with the installation. In the Choose Destination Location page, click Advanced.



4. Modify the destination locations in the pages shown below, if required, to comply with your site-specific standards.

5. Store the location information in the above wizard pages for reference, because you will specify this information in the file backup procedure.

6. Click OK.

   The destination location for various files is updated.

7. Continue with the installation and click Finish to complete the installation.

   Note: For more information about CA ITCM installation, refer the *CA IT Client Manager Implementation Guide*.

Chapter 2: Backing up DSM Manager

This section contains the following topics:

Offline Backup

The DSM manager has data located in the MDB, registry, and in data files on the manager. To help ensure consistency between these data stores in the event of a restore, you must perform CA ITCM application offline backup.

Stop the CA ITCM Processes

To perform an offline backup, you must stop all the running CA ITCM processes.

To stop the CA ITCM processes

1. Execute the following commands on the DSM managers that you are planning to back up:

   Note: If you have installed the DSM engine on separate servers, you must execute the following commands on those servers also to stop them from accessing the DSM managers and the MDB.

   ```
   cfsystray stop
   caf stop
   unicntrl stop all
   cam stop
   ```

   On successful execution of these commands, all the CA ITCM running processes on the servers are stopped.

2. Verify that all the additional CCS services are stopped.

3. Verify that none of the processes are using the MDB.

4. Stop the replication job from domain manager to enterprise manager when you are about to back up the enterprise manager. We recommend that you run the data replication job from the domain manager engine instance. This approach helps ensure that the specific engine instance of the manager can be stopped remotely without impacting other domain manager processes. If the engine instance is running on the domain manager, execute the following command to stop a remote engine instance:

   `caf stop Engine_Name host DM_Name`

   The engine instance on the specified manager is stopped.

Back Up the Registry and Data Files

Data files include critical information such as local configuration settings, certificates, and the software delivery packages. Configuration settings and certificates are typically static information, but software delivery packages are added and removed several times during the day depending on the activity of the administrators.

To back up the registry and data files

1. Back up the following data:

   Note: The exact procedures for performing a backup of data in the registry and files on the hard disk may vary depending on the backup solution used in your organization. Consult your backup administrator for the exact steps to back up the data.

   Registry key

   32-bit:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\HostUUID\HOSTUUID

   64-bit:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\HostUUID

   User Data

   %USERPROFILE%\Application Data\CA\UnicenterDSM

   %USERPROFILE%\Application Data\UnicenterRemoteControl

2. Back up all the directories that contain CA ITCM data. These are the directories you have specified during installation. For more information, see Configure Backup during CA ITCM Installation (see page 8). If you have used default directory names, the directory names differ for CA ITCM r12 manager and CA ITCM Release 12.5 manager. If you are not sure of the directory names specified during installation, find this information in the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Unicenter ITRM\InstallDir*
   ```

   As the CA ITCM data files are required for a successful recovery, it is recommended that you implement the Operating System backup and restore methodologies that best suits your requirements.

Back Up Software Delivery Library

Backing up the activate area of the software delivery library can sometimes be problematic due to the use of junction points. The side effect of junction points is that, when you delete the subdirectories under "activate", the files under the item are automatically deleted from the library.

Select *one* of the following workarounds for this problem:

- Exclude the activate directory from the backup or restore procedure.
- Verify that there are no active jobs during backup.
- Back up to a non-NTFS local drive or to a network share.

Back Up Plan for MDB

If you have single MDB that is shared among multiple CA products such as, CA ITCM, CA Service Desk Manager, CA CMDB, and so on, you must perform frequent differential MDB backups and transaction log backups. The following are the best practices for MDB backups:

- A combination of database, differential database, and transaction log backups minimize the time required to recover from a failure.
- Database backup must be done at the same time as the file backup.
- Differential database backups reduce the number of transaction logs that must be applied to recover the database. This is typically faster than creating a full database backup.

Based on the above best practices, we suggest the following backup plan:

- Use database, differential and transaction log backups.
- Create a full backup at least once a week with the CAF service stopped.
- Create differential backups daily.
- Create transaction log backups every hour.

For information about backup and restore procedures for Microsoft SQL Server, go to http://www.microsoft.com/technet/prodtechnol/sql/2005/maintain/sqlbackuprest.mspx

Back Up the MDB

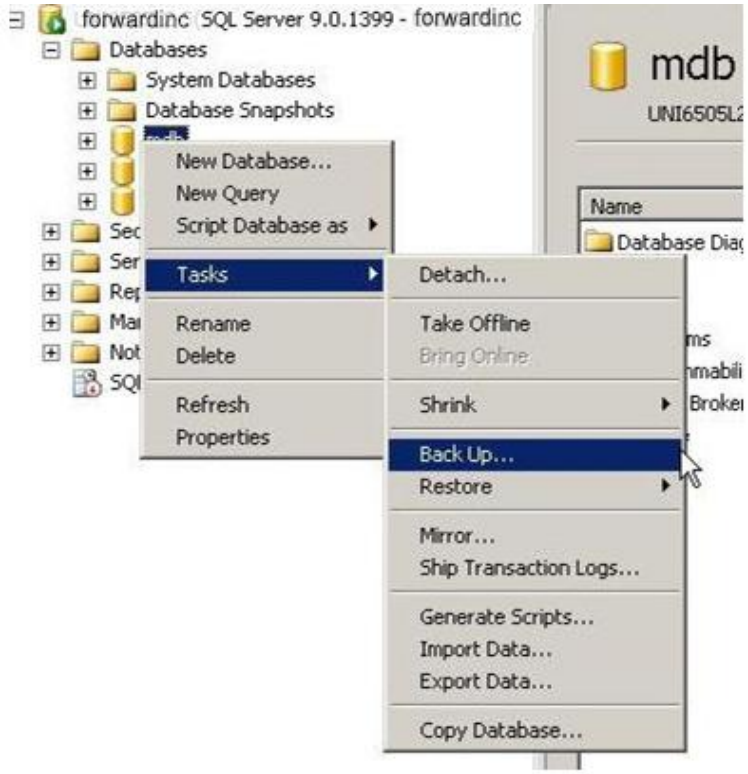
There are different methods for setting full, differential, and transaction log backup procedures depending on the production schedule and size of the database. The following procedure describes a simple backup procedure for the full, differential, and transaction log backups for Microsoft SQL Server 2005 and Microsoft SQL Server 2008 MDBs.

Important! Stop all the CA applications that are using the MDB.

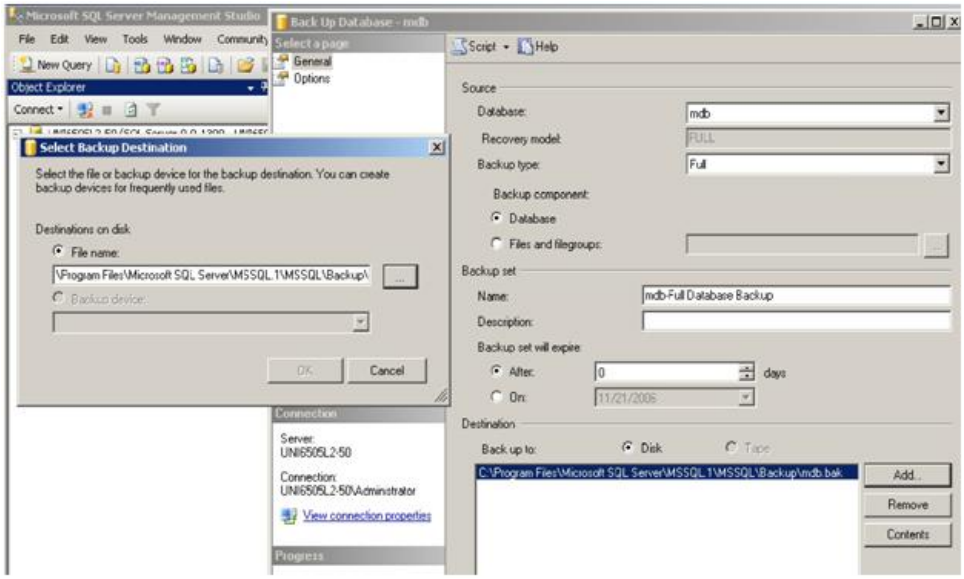
To create a full, differential, or transaction log backup

1. Open Microsoft SQL Server Management Studio, right-click the MDB node, and select Tasks, Backup.

   The Back Up Database window appears.



2. Click the General node and select Full, Differential, or Transaction Log from the Backup Type drop-down list, depending on the type of backup you want to perform. The following screenshot illustrates the full backup options:



3. Click Add in the Destination section.

   The Select Backup Destination dialog appears.

4. Select the File name option, and specify the directory and a new file name for the MDB backup. Click OK.

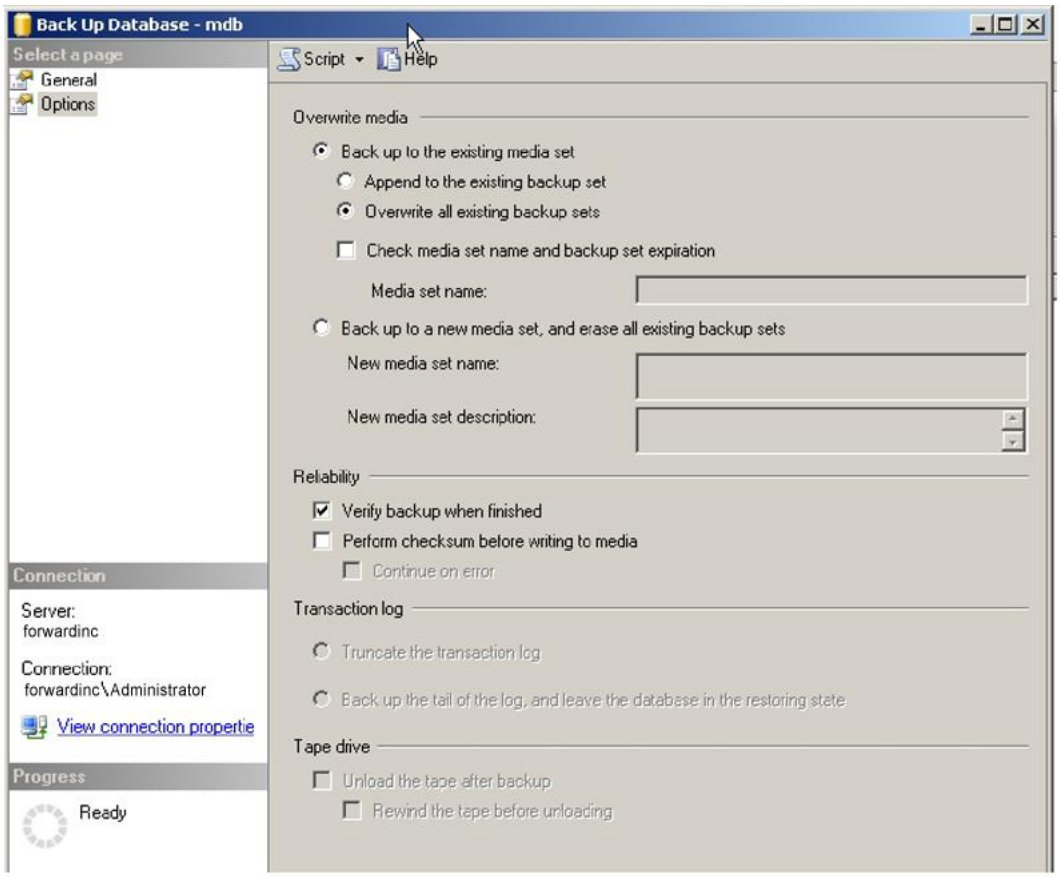
   Important! It is strongly recommended that you specify the backup file on a different drive for safety and performance reasons.

   You are returned to the Back Up Database window

5. Click the Options node and select the following options depending on the backup type that you want to perform:

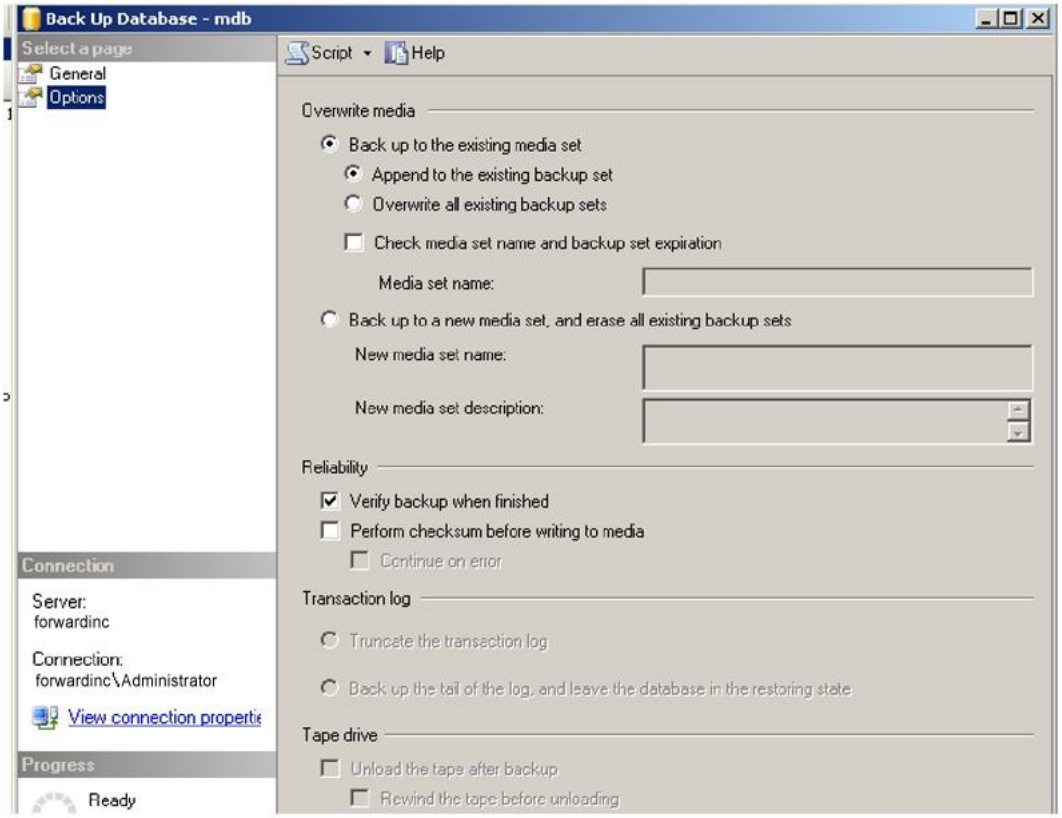
Full Backup

- Select Back up to the existing media set, Overwrite all existing backup sets, and Verify backup when finished options as shown in the following screenshot:



Differential and Transaction Log Backup

- Select the Back up to the existing media set, Append to the existing backup set, and Verify backup when finished options as shown in the following screenshot:



6. Click OK.

   Depending on the backup type you selected, the full, differential, or transaction log backup of the MDB starts.

Chapter 3: Backing Up Patch Manager

Back Up Patch Manager Data Files

You must back up the following patch manager-specific data files on the server where you have installed Patch Manager:

- C:\Program Files\CA\Unicenter Patch Management\conf\Config.properties
- C:\Program Files\CA\Unicenter Patch Management\conf\UPMReports.properties
- C:\Program Files\CA\Unicenter Patch Management\conf\UserReports.properties
- C:\Program Files\CA\Unicenter Patch Management\reports*.*

The exact location of the files depends on the drive and path entered during the Patch Manager installation.

Chapter 4: Backing Up Asset Intelligence

Asset Intelligence MDB Backup

Asset Intelligence Release 12.5 can be installed either on a DSM enterprise manager or on DSM domain managers or on a standalone computer with a local or remote MDB. As the Asset Intelligence MDB schema is installed as part of the CA ITCM MDB installation, no separate backup for Asset Intelligence MDB data is required. The Asset Intelligence data is backed up as part of the CA ITCM MDB backup.

Back up Asset Intelligence Configuration Files

You must back up the Asset Intelligence configuration files separately to preserve the Asset Intelligence configuration settings and restore them after a crash.

Back up the configuration files listed in the following table and save the files on a different drive or on a different folder.

Setting to Preserve	Save from Directory	Files to be Saved
LDAP import configuration	\admin\xxx\cache\	aig_ldap.dat
Customized Global Views	\admin\xxx\GlobalView\	All .dat files (*.DAT)
Links in L1 Views (Customized Global Views)	\public\xxx\linklist\	All files
Charts in L1 Views (Customized Global Views)	\public\xxx\charts\	All files
Saved Reports	\public\xxx\views\	All files
User-defined Hardware and Software Categories	\public\common\inc\	aic_dataArray.inc, aic_hwcat.inc, aic_QueryArray.inc
Roles and Additional (Customized) Roles	\public\common\role\YYYYY\	All role.inc files from the directory of each role (YYYY) in the system
Organization Browser	\public\common\inc\	aiOrgMenuTree.inc
Asset Management Hardware and Software Data Collection Information	%UAI_ENGINE_HOME%\config	ai_attribute_sets.xml ai_software_filters.xml

Chapter 5: Restoring DSM Manager

The restore procedure slightly differs depending on the CA ITCM architecture implemented and the recovery scenario. The recovery procedure detailed in this chapter covers the following scenarios:

- Restoring the DSM manager on the same or new hardware
- Restoring a remote MDB

This section contains the following topics:

How to Recover a DSM Manager

The recover procedure involves the following basic steps:

1. Prepare the computer for restore.
2. Verify that the computer has the same FQDN.
3. Restore the CA ITCM data files and registry.
4. Restore the MDB database.
5. Reinstall the DSM manager using the System Replacement option.
6. Perform any post procedures depending on site-specific architecture.

Prepare the Computer for Restore

After you have decided to restore the DSM manager on the same hardware or on a new hardware, you must prepare the computer before you restore any data on it.

To prepare the computer for restore

1. Verify that the host name of the computer that you are preparing for restore is the same as that of the old DSM Manager.
2. Disconnect the old computer from the network if you are restoring the DSM manager on a new hardware.
3. Install the operating system, Microsoft SQL Server, and any associated service packs, and perform site-specific server configurations per your server build procedures.

   Important! When you rebuild the server, ensure to configure the drive partitions with the same identifiers as used by the old DSM Manager computer.
4. Verify that the base server is operational.

Restore the Registry and Data Files

To restore the registry and data files

1. Restore the following CA ITCM registry setting from the backup data:

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\HostUUID\HOSTUUID`

   If you are restoring a 32-bit backup on a 64-bit environment, perform the following steps:

   a. Edit the HOSTUUID registry entry on backup device. The path of HOSTUUID contains the following:

      ```
      [HKEY_LOCAL_MACHINE\SOFTWARE\Computer
      Associates\HostUUID]
      ```

   b. Change the HOSTUUID to the following path:

      ```
      [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Com
      puterAssociates\HostUUID
      ```

2. Copy the CA ITCM data files from the backup and restore them on the target computer. Ensure that the files are copied to the exact path from which you backed up the data. For example, if you backed up the files from C:\Documents and Settings\user01\ Application Data\CA\UnicenterRemoteControl, you must restore the files on the exact path in the target computer, which is C:\Documents and Settings\user01\ Application Data\CA\UnicenterRemoteControl.

   Note: For Windows Vista-based operating systems (code named "Long Horn"), the above path is changed to C:\Users*Account ID*\Appdata\CA\UnicenterRemoteControl.

Restore the MDB

Remote MDB

If you have a remote MDB, you need not restore the MDB. However, you must consider the following factors to synchronize the MDB data:

- Synchronize the MDB with the DSM data files using "Point in time restore" to restore the MDB just to the time the DSM directory was backed up.
- Select the nightly backup that was taken at the same time as the file backup while CAF was stopped.
- If multiple CA applications are sharing the same MDB, it may be appropriate to restore a more recent backup taken after the last file backup. In this case, the file and database restore may be out of sync. You must manually verify the changes done between the backup and restore period.
- Considerations to verify in case of "point in time restore:"
  - Configuration changes made to the DSM manager, for example, defining a new engine instance
  - Software Distribution Jobs created and deleted
  - Software packages added to or amended in the Software Library
- If you are convinced that the previous considerations are satisfied, continue with the reinstallation of the DSM manager. Otherwise, read the considerations for restoring a remote MDB and restore the MDB using the restore procedures specified in the chapter Restoring the MDB (see page 41).

Local MDB

If the MDB was located on the DSM manager locally, you must restore the MDB from the backup using the procedures specified in the chapter Restoring the MDB (see page 41).

Reinstall DSM Manager

1. Do one of the following depending on whether you are reinstalling an enterprise manager or a domain manager:

   Enterprise Manager

   - Stop CAF on all the domain managers and remote engines that were connected to the enterprise manager.

   Domain Manager

   - Stop the remote engines that are connected to the domain manager.

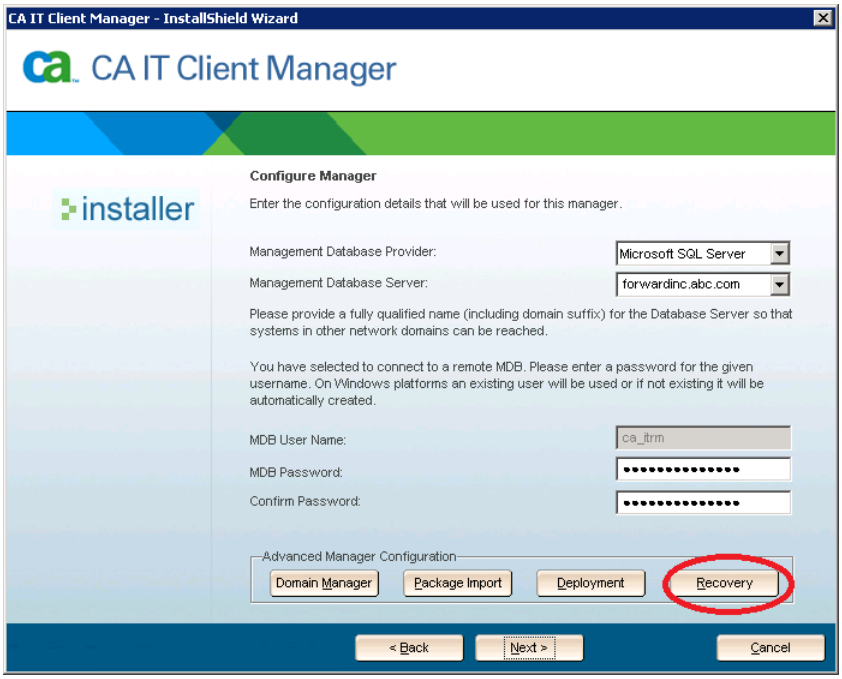
2. Copy the CA ITCM files and directories from your old DSM manager backup.

3. (Optional) Modify the DSMrecovery.ini file, if the installation path and restore path are not the same. For example, you are restoring the manager on a 64-bit operating system and your original manager was on a 32-bit operating system. Do the following steps to modify the DSMrecovery.ini file:

   a. Edit DSMrecovery.ini file in a text editor.

   b. Change the occurrences of "Program Files" to "Program Files(x86)".

4. Start the CA ITCM Release 12.5 installation and follow the instructions in the wizard. Click Recovery in the following wizard page:

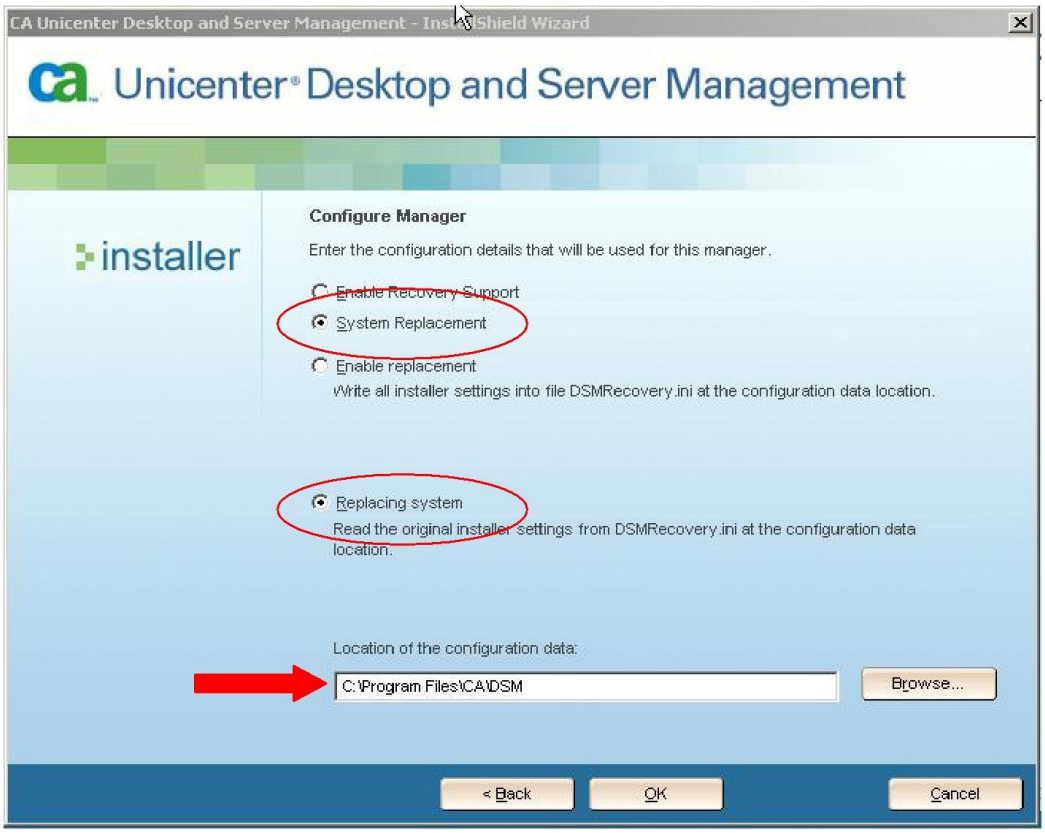


The Configure Manager Wizard page opens.

5. Select System Replacement and Replacing System options, and specify the location of the DSMRecovery.ini file from the old DSM manager backup. By default, the DSMRecovery.ini file is located under one of the following folders in the old DSM manager:

   - C:\Program Files\CA\DSM (in the case of new CA ITCM Release 12.5 installation)
   - C:\Program Files\CA\DSM (in the case of an upgrade from r12)
   - C:\Program Files\CA\Unicenter DSM (in the case of an upgrade from r11.2)

   Note: In an upgraded environment, the DSMRecovery.ini file does not contain the recovery information. Instead, the recovery information is stored in the ITCMrecovery_upgrade.ini file. However, the wizard accepts only the DSMRecovery.ini file. Rename the existing DSMRecovery.ini file to ITCMrecovery_old.ini, and rename the ITCMrecovery_upgrade.ini to DSMRecovery.ini file and continue with the restore process.



The installer reads the data from DSMRecovery.ini file and reinstalls the DSM manager with all the important data from the previous installation.

Important! At the end of the installation, do *not* accept the default option to start CAF or reboot the server as you have to perform certain post-installation steps.

Post-Installation Tasks

(Optional) Modify Comstore and Certstor.dat for 64-bit Operating Systems

Note: The following procedure is applicable only if you are restoring the manager on a 64-bit operating system and the old manager was on a 32-bit operating system.

The restore process does not update the "Program Files" references in some of the parameters in comstore and certstor.dat files. You must modify these files manually to change the parameters to work on 64-bit operating systems.

Note: The following procedure assumes that you had installed the manager in the default location "C:\Program Files." The number of parameters to be modified depends on the CA ITCM components you had installed.

To modify comstore and certstor.dat for 64-bit operating system

1. Execute the following command on the new DSM manager:

   ccnfcmda -cmd -getconfigstore -fi *filename.*xml

   The command writes all the configuration parameters from comstore to the specified file.

2. Open the *filename*.xml in a text editor, Notepad for example.

3. Search for "Program Files" and note down the parameter name for each of the occurrences of "Program Files." For example:

   ```
   <parameter name="repository_id" entity="Client" value="C:\Program Files\CA\DSM\dts\dtm\sos">
   <parameter name="keylocation" entity="Client" value="C:\Program Files\CA\DSM\DMDeploy">
   ```

   In this example, the parameter names are repository_id and keylocation.

4. Modify the parameters to use "Program Files(x86)" using the following command:

   ```
   ccnfcmda -cmd SetParameterValue -ps section_path -pn parameter_name -v new_value
   ```

   To change the value for the parameters given in the example, run the following command:

   ```
   ccnfcmda -cmd SetParameterValue -ps /itrm/dts/dtssos -pn repository_id -v "C:\Program Files (x86)\CA\DSM\dts\dtm\sos"
   ```

   ```
   ccnfcmda -cmd SetParameterValue -ps /itrm/dmdeploy -pn name="keylocation" -v value="C:\Program Files\CA\DSM\DMDeploy"
   ```

   When the command completes, the comstore is updated with Program Files(x86) references as follows:

   ```
   <parameter name="repository_id" entity="Client" value="C:\Program Files(x86)\CA\DSM\dts\dtm\sos">
   <parameter name="keylocation" entity="Client" value="C:\Program Files(x86)\CA\DSM\DMDeploy">
   ```

5. Open the CA\SC\CBB\certstor.dat file in a text editor.

6. Replace the occurrences of Program Files with Program Files(x86).

7. Save the file.

   The certstor.dat file is updated.

Reconfigure the Domain Manager after Restoration

1. Reapply the test fixes, if any, that you had applied on the DSM manager before the rebuild.

2. Verify any special instructions included with the fix to validate whether certain steps are necessary, for example, a fix that modifies properties of the MDB may not need to be reapplied. When in doubt, contact CA Support for advice.

3. Restore data files related to Web Admin Console (WAC), if you are using WAC. The following WAC data files are used for configuring WAC and Patch Manager:

   ```
   Restore \Web Console\conf\server.xml
   ```

   ```
   Restore \Web Console\jakarta\workers.properties
   ```

4. Restore CA Patch Manager and CA Asset Intelligence, if they resided on the DSM manager computer. For more information, see chapters Restoring CA Patch Manager, Restoring CA Asset Intelligence.

5. Re-enable the shares used by software delivery, if the domain manager was configured to use shares for software delivery. Use the following command to re-enable shares:

   ```
   sd_sscmd addshare SDLIBRARY
   sd_sscmd addshare MSILIB
   ```

6. Apply Read access to the share using the operating system security setting.

7. Delete the files and folders under the *Install Drive and location*\SD\AUTOREG folder.

8. Create the local OS users who were added to the Remote Control Global Address Book (GAB) before the DSM manager rebuild. Typically, only the Windows domain manager accounts are added to the GAB. You are not required to recreate domain users though.

9. Recreate the role-based security for local users and groups, if you had set up the same before the rebuild.

10. Restart the domain manager.

11. Synchronize the domain and enterprise MDBs if you have a CA ITCM enterprise manager. To synchronize the MDBs, do the following:

    a. Unlink the domain manager from the enterprise manager.

    b. Link the domain manager to the enterprise manager.

Reconfigure the Enterprise Manager after Restoration

1. Reapply the test fixes, if any, that you had applied on the DSM manager before the rebuild.

2. Verify any special instructions included with the fix to validate whether certain steps are necessary, for example, a fix that modifies properties of the MDB may not need to be reapplied. When in doubt, contact CA Support for advice.

3. Restore data files related to Web Admin Console (WAC), if you are using WAC. The following WAC data files are used for configuring WAC and Patch Manager:

   ```
   Restore \Web Console\conf\server.xml
   Restore \Web Console\jakarta\workers.properties
   ```

4. Restore CA Patch Manager and CA Asset Intelligence, if they resided on the DSM manager computer. For more information, see chapters Restoring CA Patch Manager, Restoring CA Asset Intelligence.

5. Recreate the role-based security for local users and groups, if you had set up the same before the rebuild.
6. Restart the domain manager.
7. Synchronize the domain and enterprise MDBs. To synchronize the MDBs, do the following:
    a. Unlink all the domain managers from the enterprise manager
    b. Link all the domain manager to the enterprise manager

Consideration for Restoring a Remote MDB

The procedure for restoring a remote MDB differs depending on whether the restore is a planned or an unplanned operation.

The following considerations apply for a planned restore or move of a remote MDB:

- You must have a full synchronized backup of MDB. For more information, see the section Back Up the MDB.
- If the case of an MDB move, refer the Green Paper entitled "*How to Move the MDB for r11*".
- In the case of a rebuild of the DBMS server hosting the MDB, follow the instructions in the MDB Restore for Remote MDB DM with CCS Installation section in this document.
- You must stop the CAF services and any remote engines of the DSM manager during the MDB recover process.

The following considerations apply for a planned restore or move of a remote MDB:

- Consider the timings of the file and database backups and any activity that may have occurred between these time periods.
- In the case of a rebuild of the DBMS server hosting the MDB, follow the instructions in the MDB Restore for Remote MDB DM with CCS Installation section in this document.
- If after these considerations, if you do not feel the necessity to restore of the data, continue with the Post Installation Steps.

Restore the Data Files

To synchronize data in the file backup and MDB database backup, you must restore the data files of the same time period as the MDB backup. You must restore the data files to exactly the same paths from which the files were backed up, replacing all existing files and deleting new files added since the last backup.

Post-Installation Tasks

This section covers the additional post-installation tasks you must perform for remote MDBs.

Reconfigure the Domain Manager after Restoration

1. Reapply the test fixes, if any, that you had applied on the DSM manager before the rebuild.
2. Verify any special instructions included with the fix to validate whether certain steps are necessary, for example, a fix that modifies properties of the MDB may not need to be reapplied. When in doubt, contact CA Support for advice.
3. Restore data files related to Web Admin Console (WAC), if you are using WAC. The following WAC data files are used for configuring WAC and Patch Manager:

   ```
   Restore \Web Console\conf\server.xml
   ```

   ```
   Restore \Web Console\jakarta\workers.properties
   ```
4. Restore CA Patch Manager and CA Asset Intelligence, if they resided on the DSM manager computer. For more information, see chapters Restoring CA Patch Manager, Restoring CA Asset Intelligence.
5. Restart the domain manager.
6. Synchronize the domain and enterprise MDBs if you have a CA ITCM enterprise manager. To synchronize the MDBs, do the following:
   a. Unlink the domain manager from the enterprise manager
   b. Link the domain manager to the enterprise manager

Reconfigure the Enterprise Manager after Restoration

1. Reapply the test fixes, if any, that you had applied on the DSM manager before the rebuild.
2. Verify any special instructions included with the fix to validate whether certain steps are necessary, for example, a fix that modifies properties of the MDB may not need to be reapplied. When in doubt, contact CA Support for advice.
3. Restore data files related to Web Admin Console (WAC), if you are using WAC. The following WAC data files are used for configuring WAC and Patch Manager:

   ```
   Restore \Web Console\conf\server.xml
   ```

   ```
   Restore \Web Console\jakarta\workers.properties
   ```

4. Restore CA Patch Manager and CA Asset Intelligence, if they resided on the DSM manager computer. For more information, see chapters Restoring CA Patch Manager, Restoring CA Asset Intelligence.
5. Restart the domain manager.
6. Synchronize the domain and enterprise MDBs. To synchronize the MDBs, do the following:
   a. Unlink all the domain managers from the enterprise manager
   b. Link all the domain manager to the enterprise manager

Chapter 6: Restoring CA Patch Manager

Restoring CA Patch Manager involves two steps:

- Reinstalling CA Patch Manager
- Restoring data files

This section contains the following topics:

Reinstall CA Patch Manager

If you had installed CA Patch Manager on the DSM manager that you are rebuilding, you must reinstall CA Patch Manager after reinstalling CA ITCM Release 12.5.

To reinstall CA Patch Manager

1. Delete the existing upmuser and upmadmin users from the MDB.
2. Verify the CAF status using the following command:

   ```
   caf status
   ```

   The command returns a list of CAF component names. If the list does not contain all the component names, restart CAF using the following commands:

   ```
   caf stop
   caf start
   ```

3. Start the CA Patch Manager installation. Specify the same installation path as your original Patch Manager installation, and wait until the installer has extracted its components and created a folder in the TEMP folder, usually with a name similar to this example: {E7135B45-D2D0-42BA-A8B8-EBBD7CA64B7B}.

4. Open the new folder, {E7135B45-D2D0-42BA-A8B8-EBBD7CA64B7B} for example, in the TEMP folder and do the following:

    a. Delete all the contents of the InstallMDBPatch.bat file and add an entry ‘exit 0’ to it.

    b. Delete all the contents of the PatchMDB.bat file.

5. Continue with the PM installation.

    Important! Do *not* restart the machine if you are prompted to do so when the installation completes.

6. Stop CA Patch Manager by running the following command:

    ```
    caf stop tomcat
    ```

Restore Data Files

Restore the Patch Manager data files from the backup. The exact restore location of the files depends on the drive and path you entered during the CA Patch Manager installation. The example below uses the default install directories:

C:\Program Files\CA\Unicenter Patch Management\conf\Config.properties

C:\Program Files\CA\Unicenter Patch Management\conf\UPMReports.properties

C:\Program Files\CA\Unicenter Patch Management\conf\UserReports.properties

C:\Program Files\CA\Unicenter Patch Management\reports*.*

Once the file restore is complete, restart the computer. If you have previously used CA Workflow functionality, you can re-enable it.

Chapter 7: Restoring CA Asset Intelligence

Restoring CA Asset Intelligence involves the following steps:

- Restore the MDB
- Install CA Asset Intelligence
- Restore configuration files

This section contains the following topics:

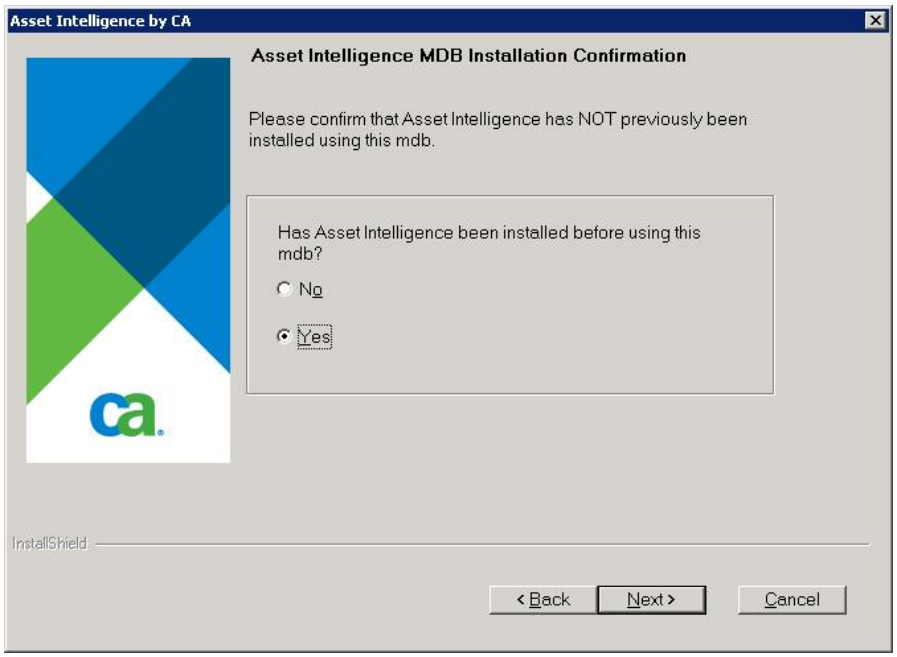
Restore the MDB

The procedure for restoring the MDB is the same as restoring the CA ITCM MDB. If you have already restored the CA ITCM MDB, ignore this step.

Reinstall CA Asset Intelligence

To reinstall CA Asset Intelligence

1. Start the CA Asset Intelligence installation. Specify the same installation path as your original CA Asset Intelligence installation.
2. On the Asset Intelligence MDB installation Confirmation page, select Yes as shown in the following screenshot:



3. Follow the instructions in the wizard to complete the installation.

Restore the configuration files

To restore the configuration files

1. Restore the CA Asset Intelligence configuration files from the backup to the appropriate location.
2. Recreate the data sources that you created before the Asset Intelligence rebuild.
3. Run dbextract.

Chapter 8: Restoring the MDB

Restore the MDB on Microsoft SQL Server

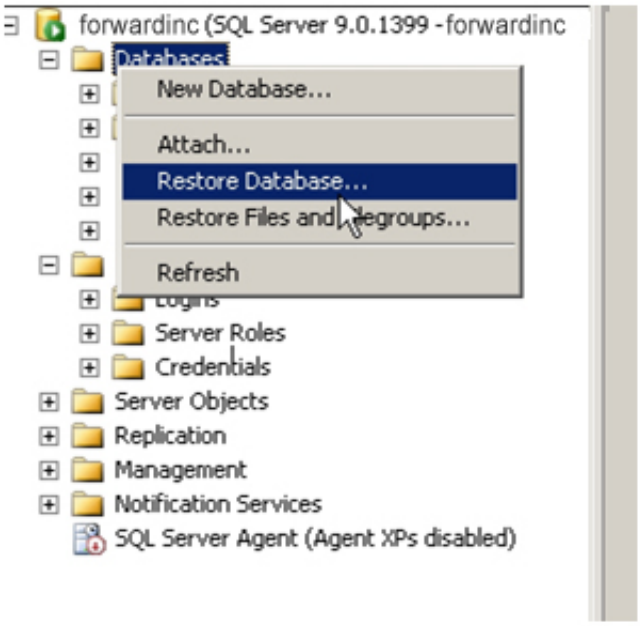
To restore the MDB on Microsoft SQL Server

1. Restore the full backup, the last differential backup, and the transaction log backups after the last differential backup. To restore backups, follow these steps:

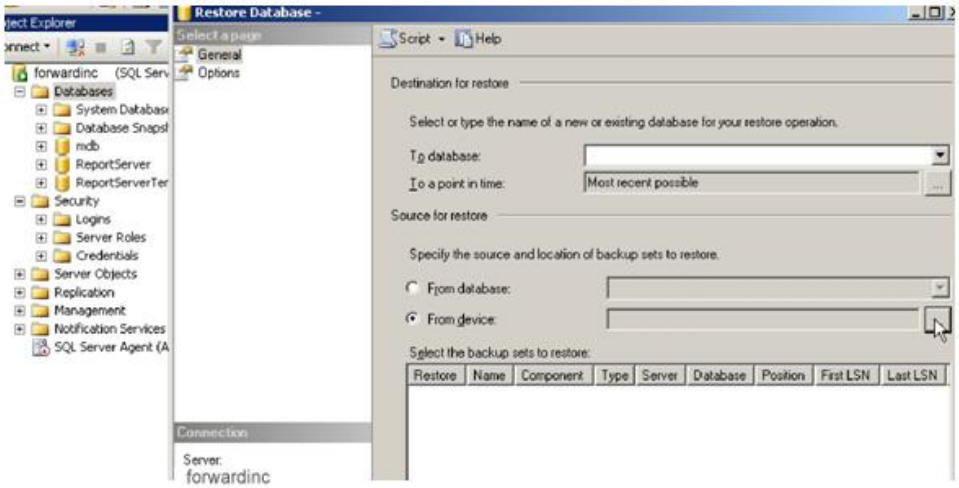
    a. Open Microsoft SQL Server Management Studio.

    b. Right-click the Databases node and select Restore Database.

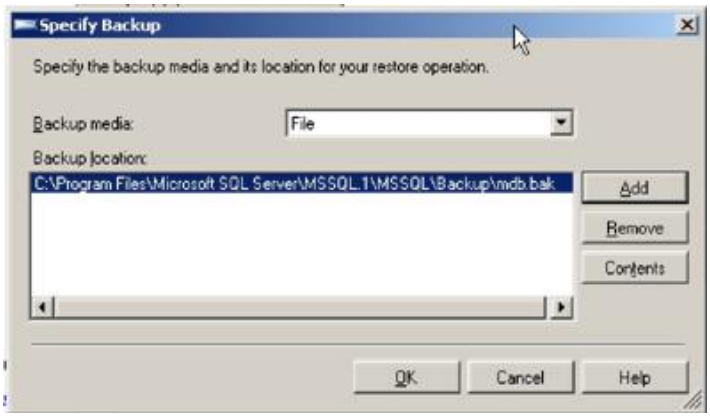
    The Restore Database window opens.



c. On the General page, select the From device option and click the button next to it.

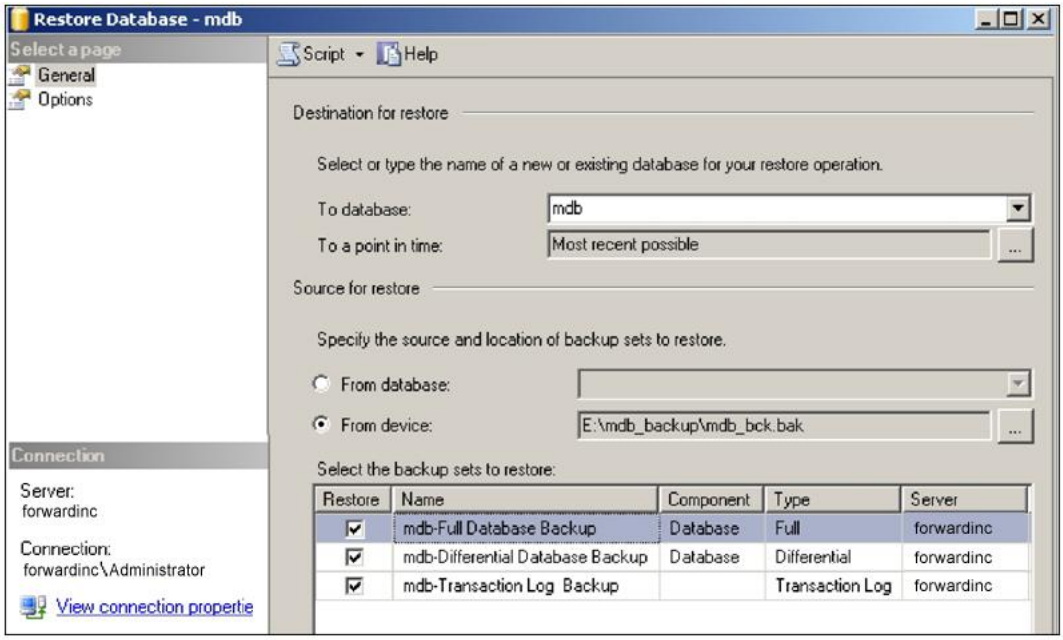


The Specify Backup dialog opens.



d. Specify the location where you have the MDB backup and click OK.

The General page displays the data that you can restore from the backup as shown in the following screenshot:



e. Select the latest full, differential, and transaction log backups.

f. Click OK.

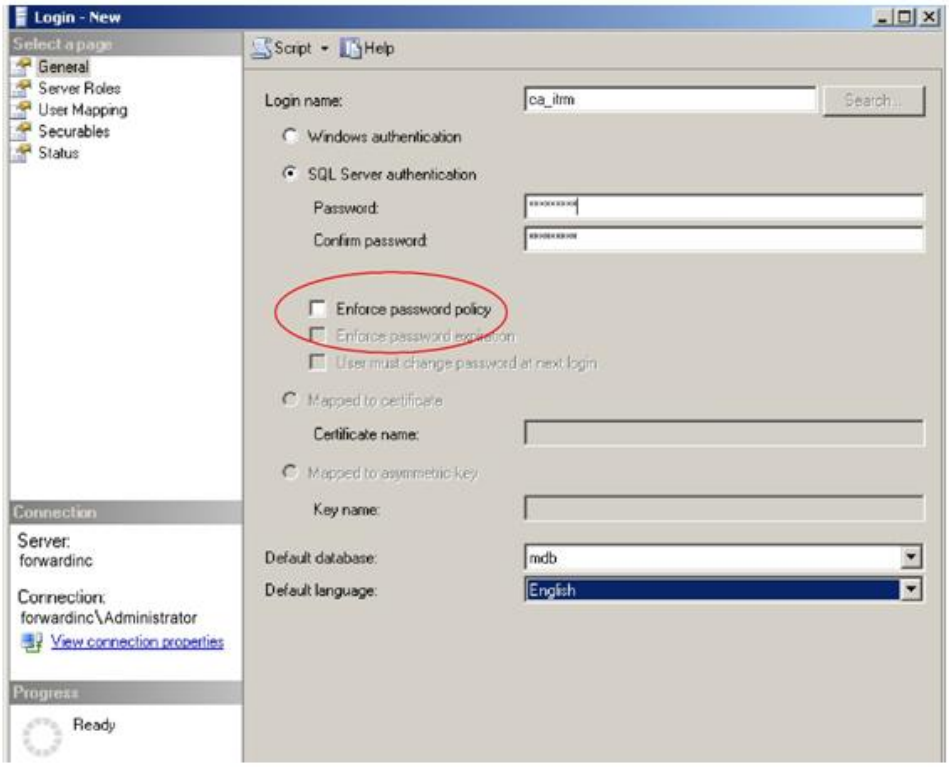
The restore operation starts.

2. Create the users, ca_itrm and ca_itrm_ams, with the same password as specified during the original installation, or if you have used the default password, the password is *NOT_changedR11*. To create users, follow these steps:

a. Right-click the Security, Logins node and select New Login.

The SQL Server Login Properties – New Login dialog opens.

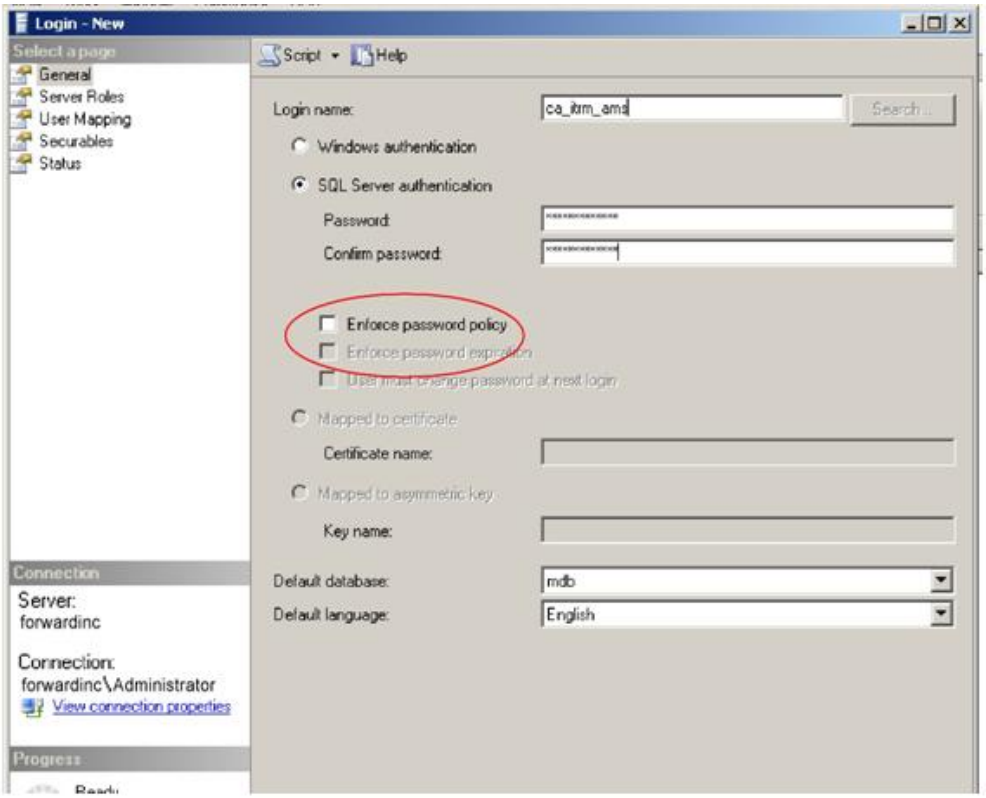
b. Select the General page and provide the Login name as ca_itrm and specify the password



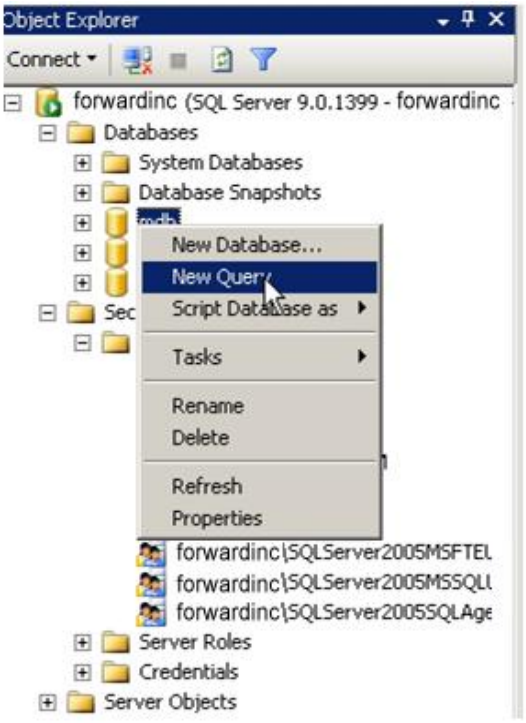
c. Select MDB as the default database and English as the default language.

d. Clear the Enforce password policy option.

e. Repeat the above steps for the ca_itrm_ams user.



3. Right-click the MDB database from the Object Explorer and select New Query.



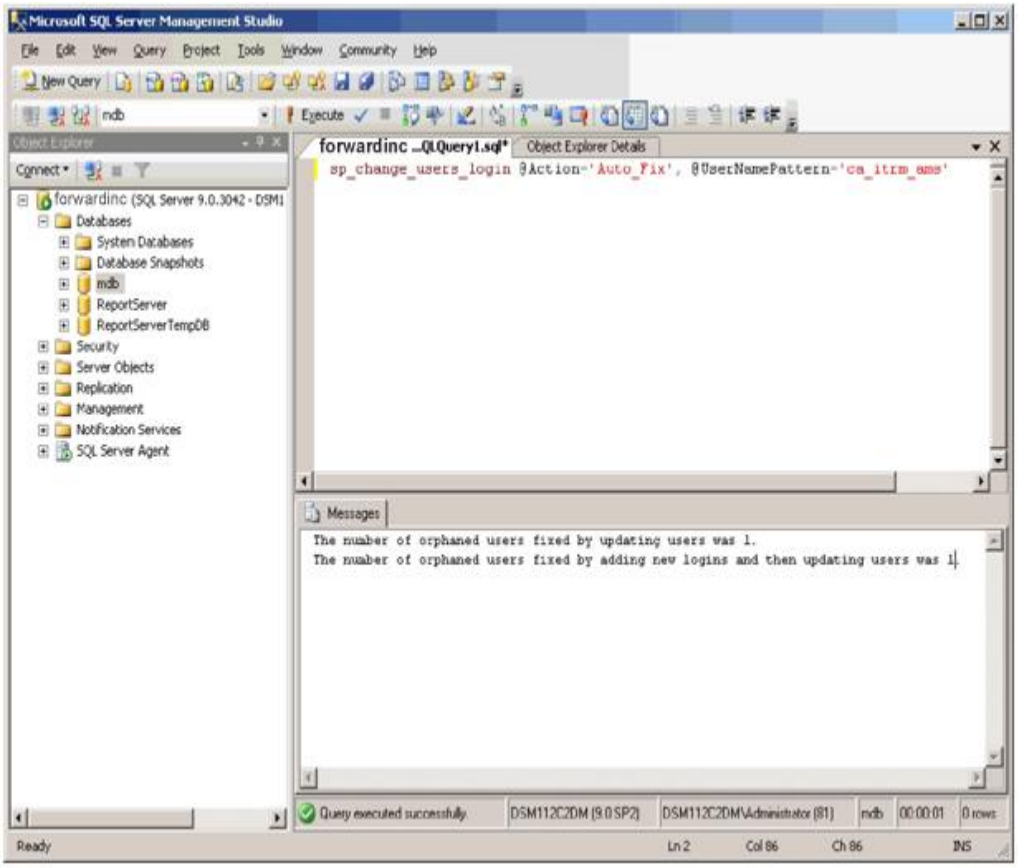
A blank query window opens.

4. Run the following SQL commands:

```
sp_change_users_login @Action='Auto_Fix', @UserNamePattern='ca_itrm'

sp_change_users_login @Action='Auto_Fix',
@UserNamePattern='ca_itrm_ams'

sp_change_users_login @Action='Auto_Fix', @UserNamePattern='cicuser'
```



5. Run the following SQL commands from the ca_itrm user login:

```
Delete from ca_manager where host_name = Host_Name
```

Where *Host_Name* is the name of the old DSM manager, for example:

```
Delete from ca_manager where host_name = 'test650513-32.abc.com
```

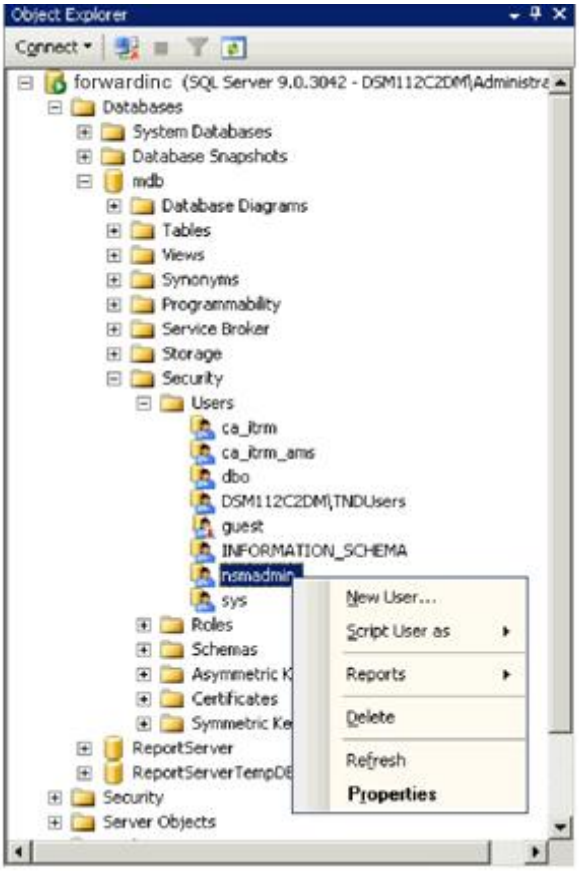
6. Perform additional steps if you have CCS installation. Depending on whether you have a local or remote MDB the additional steps vary.

   - MDB Restore for Local MDB Domain Manager with CCS Installation
   - MDB Restore for Remote MDB Domain Manager with CCS Installation

MDB Restore for Local MDB Domain Manager with CCS Installation

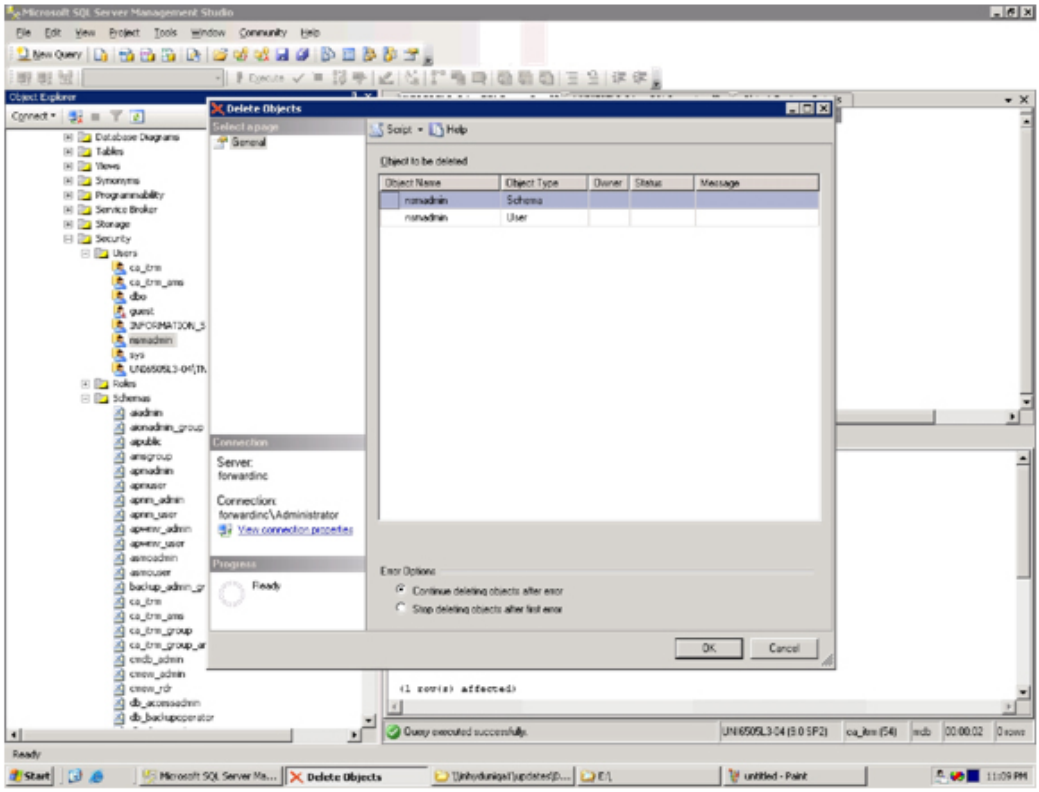
If you have installed CCS on a domain manager that has a local MDB, follow these additional steps to restore the CCS-related MDB data:

1. Delete the nsmadmin user that exists in MDB, Security, Users.



A confirmation dialog appears.

2. Click Yes to delete the user and the security schema associated with the user.

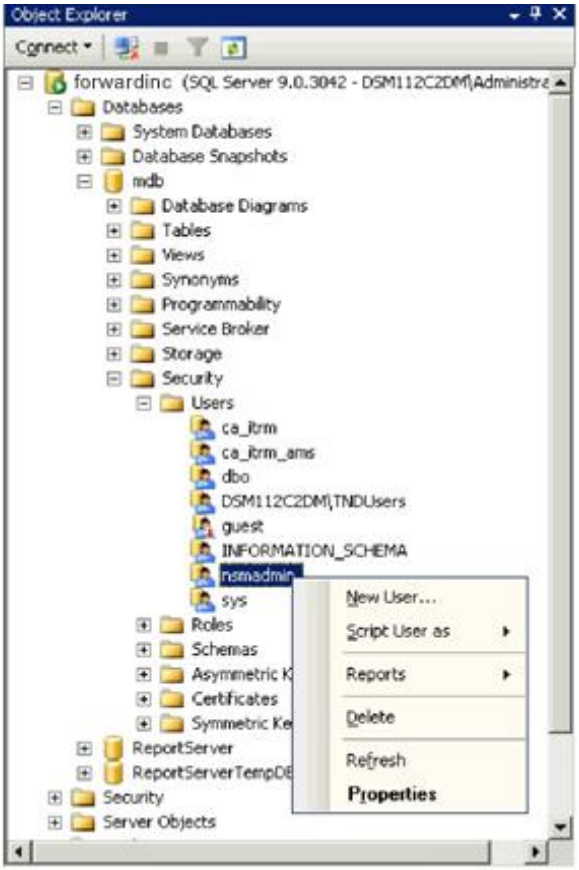


3. Click OK to continue with the deletion.

MDB Restore for Remote MDB Domain Manager with CCS Installation

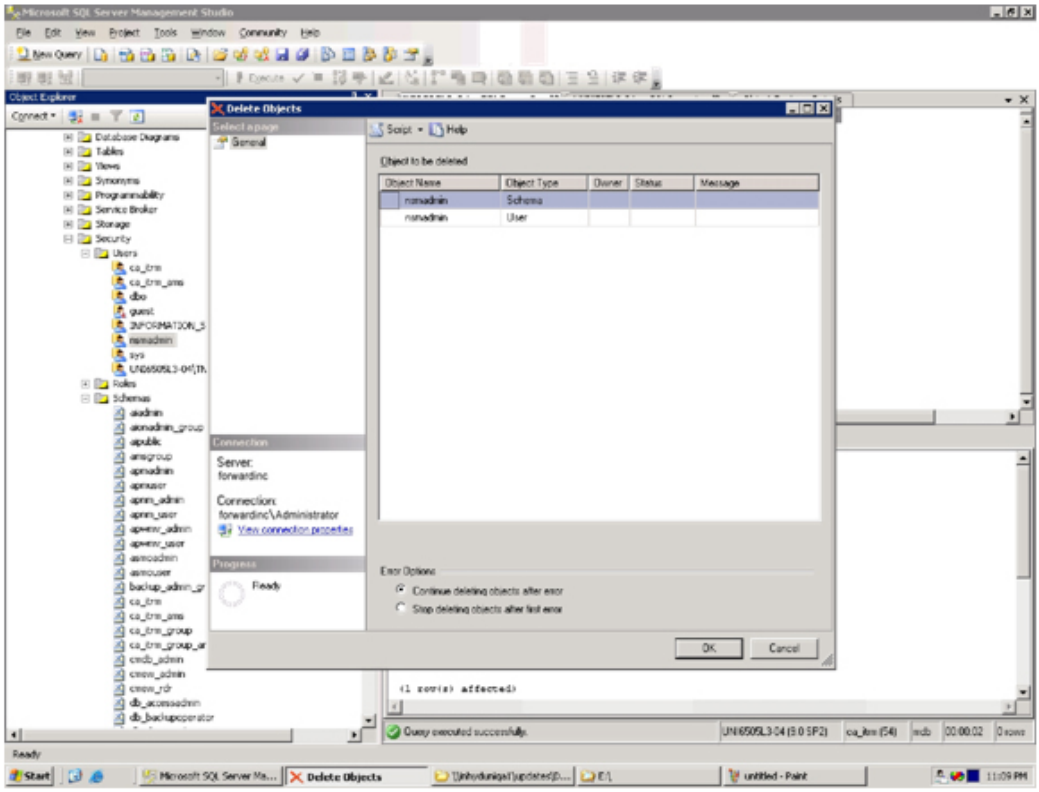
If you have installed CCS on a domain manager that has a remote MDB, follow these additional steps to restore the CCS-related MDB data:

1. Delete the nsmadmin user that exists in MDB, Security, Users.



A confirmation dialog appears.

2. Click Yes to delete the user and the security schema associated with the user.

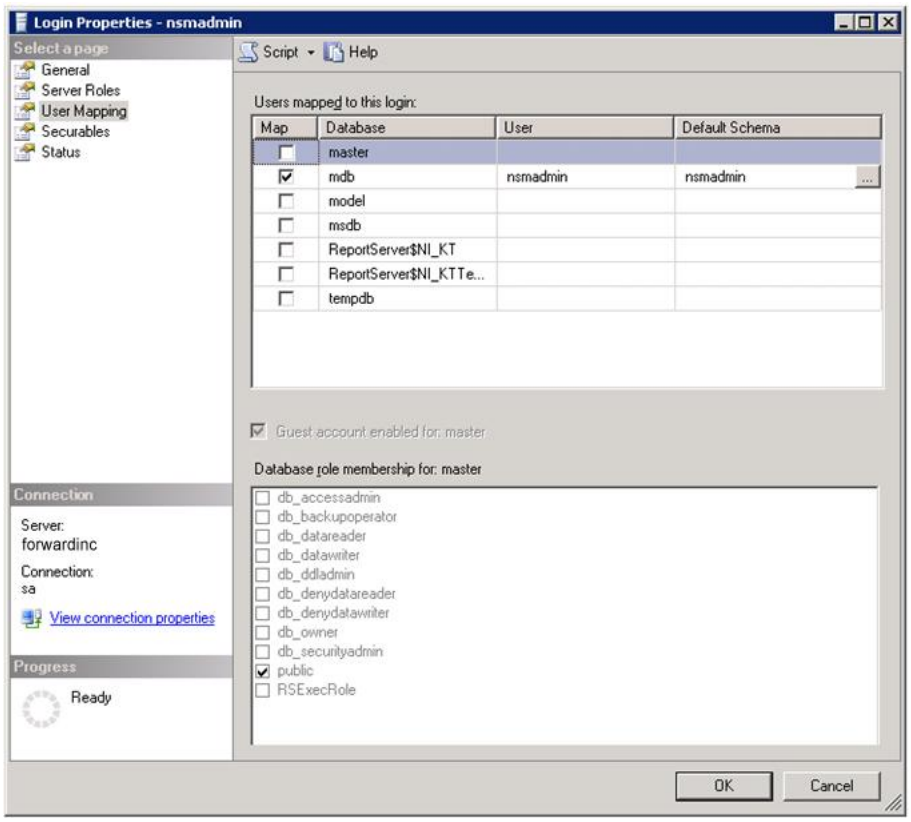


3. Click OK to continue with the deletion.

4. In the Object Explorer, navigate to SQL Server, Logins, nsmadmin. Right-click and select Properties.

   The Properties dialog opens.

5. Select the User Mapping tab. For the MDB database, add the database role memberships for db_owner, regadmin, and uniadmin as shown in the following screenshot:



Chapter 9: Known Issues

Internal error - Exception caught by Server: Failed to initialize server [SDM000038]

Reason:

After a successful restore, when you try to deploy a software package to a target computer, the job fails with an error message "Internal error - Exception caught by Server: Failed to initialize server [SDM000038]." This error occurs if there was an active software job for deploying a software package at the time of MDB backup. If you try to deploy the same package to a different target computer after the restore, the restore fails.

Action:

Delete the corresponding folder from %SDROOT%\\ASM\LIBRARY\activate directory and then renew the jobs.

Prompts for Valid Credentials after Restore

Reason:

CA ITCM supports a type of encryption called "System Wide Encryption." The encryption key is dependent on the volume serial number, MAC address, and system name. Two of these items must match to be able to decrypt data. So, changing a disk and a network card at the same time may result in certain data from the backup becoming unusable to CA ITCM. This data includes credentials stored by dmdeploy, DTS filter settings, and Remote Control settings. In most cases, you will only be prompted to enter valid credentials again, but in some cases, it can cause the DSM Explorer to fail to communicate with the manager.

Action:

Run the following commands:

```
ccnfcmda -cmd DeleteParameter -ps itrm/cfencrypt -pn LOCALID
caf stop
caf start
```

If the system crashes again after the data restore, it can be restored by following the same backup and restore procedure mentioned in this document. This is possible only for fresh installations (CA ITCM Release 12.5 installed directly) and not for CA ITCM upgrades.