IBM XIV Storage System Management Tools
Version 4.5

Operations Guide

SC27-5986-03

Note
Before using this information and the product it supports, read the information in "Notices" on page 73.

Edition Notice

Publication number: SC27-5986-03. This edition applies to IBM XIV Management Tools version 4.5 and to all subsequent releases and modifications, until otherwise indicated in new editions.

Contents

Figures

About this guide

This Management Tools set of documents describe how to install and use the IBM XIV Management Tools 4.5.

This set of documents include:

1. IBM® Hyper-Scale Manager User guides:
   - User Guide for Virtual Appliance
   - User Guide for Installation as an Application
2. IBM XIV Management Tools 4.5 Operations Guide

Who should use this guide

This document is for Storage Administrators who manage XIV® Systems. If you are using IBM XIV Management Tools version 4.5 with IBM Spectrum Accelerate, refer to the *IBM Spectrum Accelerate Planning, Deployment, and Operation Guide (SC27-6695).*

Conventions used in this guide

These notices are used to highlight key information.

Note: These notices provide important tips, guidance, or advice.

Important: These notices provide information or advice that might help you avoid inconvenient or difficult situations.

Attention: These notices indicate possible damage to programs, devices, or data. An attention notice appears before the instruction or situation in which damage can occur.

Related information and publications

You can find additional information and publications related to IBM XIV Storage System and Management Tools on the following information source:

- IBM XIV Storage System on the IBM Knowledge Center (ibm.com/support/knowledgecenter/STJTAG) – on which you can find the following related publications:
  - IBM XIV Management Tools – Release Notes
  - IBM XIV Storage System – Product Overview
  - IBM XIV Storage System – XCLI Reference Guide
  - IBM Hyper-Scale Manager Installation and Quick-start Guides

Getting information, help, and service

If you need help, service, technical assistance, or want more information about IBM products, you can find various sources to assist you. You can view the following websites to get information about IBM products and services and to find the latest technical information and support.

- IBM website (ibm.com®)

- IBM Support Portal website (www.ibm.com/storage/support)
- IBM Directory of Worldwide Contacts website (www.ibm.com/planetwide)

How to order publications

The IBM Publications Center is a worldwide central repository for IBM product publications and marketing material.

The IBM Publications Center website (www.ibm.com/shop/publications/order/) offers customized search functions to help you find the publications that you need. Some publications are available for you to view or download at no charge. You can also order publications. The publications center displays prices in your local currency.

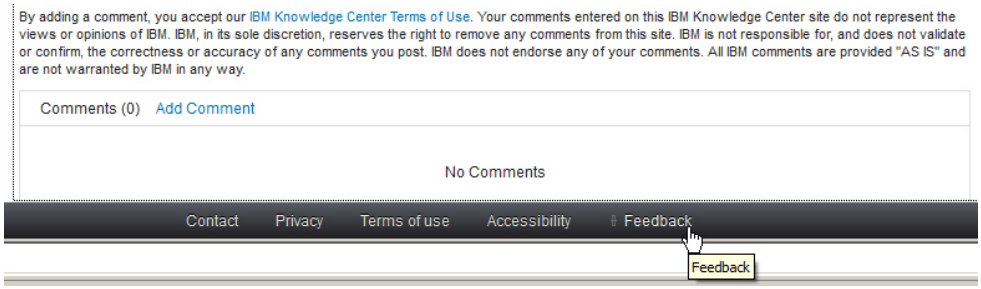
Sending your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

Procedure

To submit any comments about this guide or any other IBM XIV Storage System documentation:

- Go to http://www-01.ibm.com/support/knowledgecenter/STJTAG/com.ibm.help.xivgen3.doc/xiv_kcwelcomepage.html (http://www-01.ibm.com/support/knowledgecenter/STJTAG/com.ibm.help.xivgen3.doc/xiv_kcwelcomepage.html), drill down to the relevant page, and click the **Feedback** link that is located at the bottom of the page.



  You can use this form to enter and submit comments privately.
- Post a public comment on the Knowledge Center page that you are viewing by clicking **Add Comment**. For this option, you must first log in to IBM Knowledge Center with your IBM ID.
- Send your comments by email to starpubs@us.ibm.com. Be sure to include the following information:
  - Exact publication title and version
  - Publication form number (for example, GA32-0770-00)
  - Page, table, or illustration numbers that you are commenting on
  - A detailed description of any information that needs to be changed

Chapter 1. Introducing IBM Hyper-Scale Manager

IBM XIV Management Tools introduces the IBM Hyper-Scale Manager that reduces operational complexity and enhances capacity planning through integrated management for large and multisite XIV deployments. The Management Tools:

- Shift the paradigm to an integrated management of XIV Systems across the enterprise
- Provide powerful health monitoring by integrating events and alerts across the managed XIV Systems

Diagram

The following diagram depicts the way the IBM Hyper-Scale Manager interacts with the XIV GUI and XIV Systems.

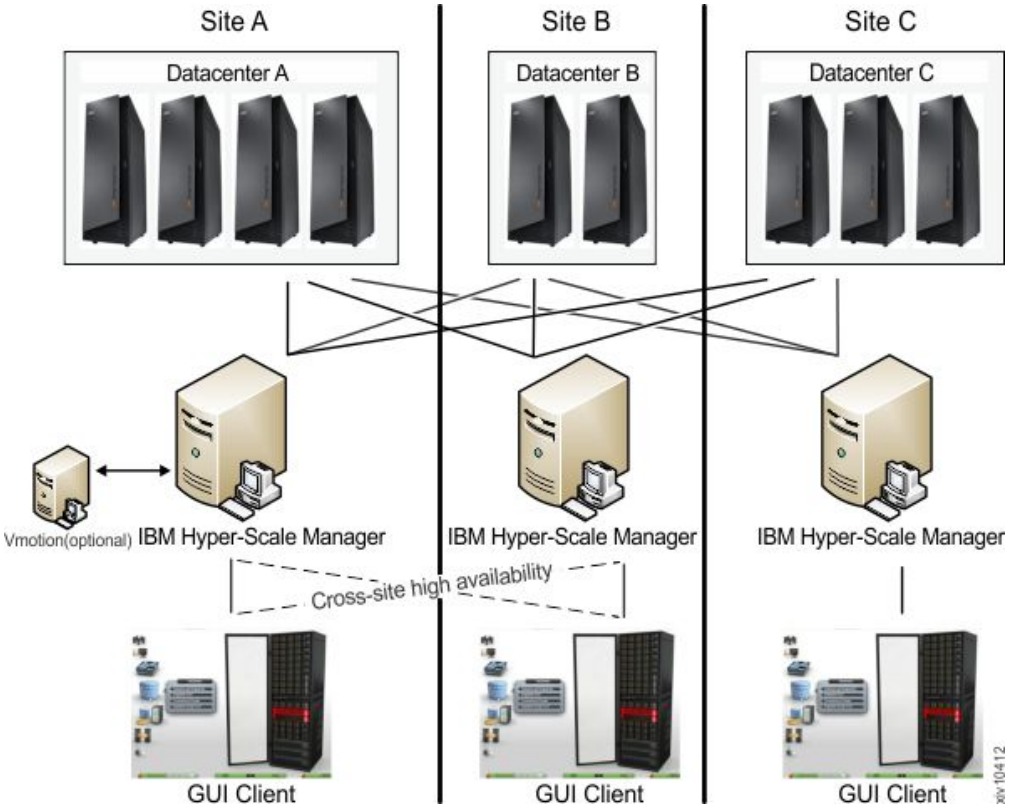


Figure 1. IBM Hyper-Scale Manager

Management Tools documentation set

The IBM XIV Management Tools documentation set includes the following publications:

- IBM Hyper-Scale Manager Installation guides and Quick-start guides:
  - Installation as Virtual Appliance
  - Installation as Application
- IBM XIV Management Tools Operations and Administration guide

Definitions

The following definitions are in wide use throughout this document:

Manager Mode versus Direct Mode from the login dialog of the GUI
With the introduction of the IBM Hyper-Scale Manager, there are two ways to use the IBM XIV Management Tools:

Manager mode
Moving the GUI to work with the IBM Hyper-Scale Manager.

Direct mode
Using the GUI without IBM Hyper-Scale Manager. In this mode, the GUI manages the XIV Systems directly.

'Maintenance' account
Applicable to the Virtual Appliance installation only.

A IBM Hyper-Scale Manager SFTP user that transfers files to and from the IBM Hyper-Scale Manager. The default password is *xivmsMaintenance*. You can change this password through the root menu. See **Changing the maintenance password** on the **Installation Guide for VM**.

System machine account
The account which is used by the IBM Hyper-Scale Manager to connect to XIV systems.

- This user does not change the configuration
- This user's name default is: *xiv_msms* and can be edited
- This user can be defined in LDAP (make sure it is added to all XIV storage admin groups in the LDAP)
- This user must have a storage administrator role (similarly to the *admin* user)
- This user must be defined with the same password on all XIV systems in the IBM Hyper-Scale Manager inventory
- This user must be defined in the IBM Hyper-Scale Manager (through the GUI or CLI)

Diagnose/Fix authentication problem
A process in which the GUI tries to fix the System Machine Account authentication issues among all XIV systems in the inventory.

- You need to supply admin credentials when starting this operation
- These credentials are used to add the System Machine Account automatically to all your XIVs (if needed)
- If some of the XIV systems use LDAP authentication, it informs you to manually add the System Machine Account to your LDAP directory

Discover new systems
A process in which the IBM Hyper-Scale Manager tries to authenticate a specific user in front of all of the systems that the IBM Hyper-Scale Manager knows that the user is not authenticated to.

- This button is on the **Systems > Preferences** dialog.
- Use this button only when it is known that the user was added to the system's access list and you need to display this system on the GUI screen. This is not done automatically, because of potential LDAP locking issues, due to authentication errors.

- Upon a successful completion of the process, if the user was granted with an access to a system that was not previously seen in the GUI, it will now be seen.

Manager Access Code

Any administrative action on the IBM Hyper-Scale Manager, that is performed from the GUI requires the Manager Access Code. This code can be changed from GUI and from the management menu. The default manager access code is *adminadmin*. See Changing the Manager Access Code on the User Guides.

GUI keyboard shortcuts

Table 1 provides a list of keyboard shortcuts that can be used while working with the XIV GUI.

Table 1. GUI keyboard shortcuts

Shortcut	Task
Ctrl+F	Search
Alt+S	Open the System Selector and switch systems
Alt+X	Open the View Selector
Alt+O	Show all menu items (Dynamic Menus)
Alt+E	Edit menu pinned items (Dynamic Menus)
Alt+Left Arrow	Go back on the History
Alt+Right Arrow	Go forward on the History

Chapter 2. Managing the XIV and IBM Hyper-Scale Manager certificates

The Management Tools provides the ability to manage the XIV and IBM Hyper-Scale Manager certificates.

When the XIV GUI connects to a IBM Hyper-Scale Manager, or directly to an XIV system, or when the IBM Hyper-Scale Manager connects to an XIV system, they are attempting to identify the certificates of the XIV system or the IBM Hyper-Scale Manager.

This chapter describes the methods of handling certificates on the GUI. For handling certificates from the IBM Hyper-Scale Manager menu, see "Replacing the IBM Hyper-Scale Manager certificate" on page 16.

GUI certificate management in direct mode

Importing certificates into the local truststore

The GUI manages a truststore for XIV systems certificates.

Before you begin

In order to import a certificate, you need:

- The certificate file

Procedure

1. Open **Tools > Management > Certificates (Tab)** on the XIV GUI menu. The **Certificates Management** screen opens.

Figure 2. Importing certificates into the local truststore

2. Click the **Import certificate** icon.

Results

Following the certificates import into the local truststore and exiting the **Management** screen, all XIV systems with certificate errors are reloaded.

Removing certificates from the local truststore

This option removes a certificate from the local trust store.

Procedure

1. Open **Tools > Management > Certificates (Tab)** on the XIV GUI menu. The **Certificates Management** window opens.
2. Select a certificate and click the **Remove Certificate** icon. Click **Yes** to approve.

Results

Following the certificates removal from the local truststore and exiting the **Management** window, all XIV systems are reloaded.

Handling errors of XIV systems certificates

This option reviews a certificate that is already assigned to an XIV system.

Procedure

1. Right-click an XIV system with a Certificate Error status and select **Manage Certificate** from the popup menu.

Figure 3. Handling errors of XIV systems certificates

2. Review the certificate that is displayed on screen, ensure that it can be trusted and select from the following options:
   - Trust Once - confirm that the certificate of this XIV system can be trusted throughout the current GUI session only.
   - Trust Always - confirm that the certificate can be trusted. The certificate will be added to the local truststore.

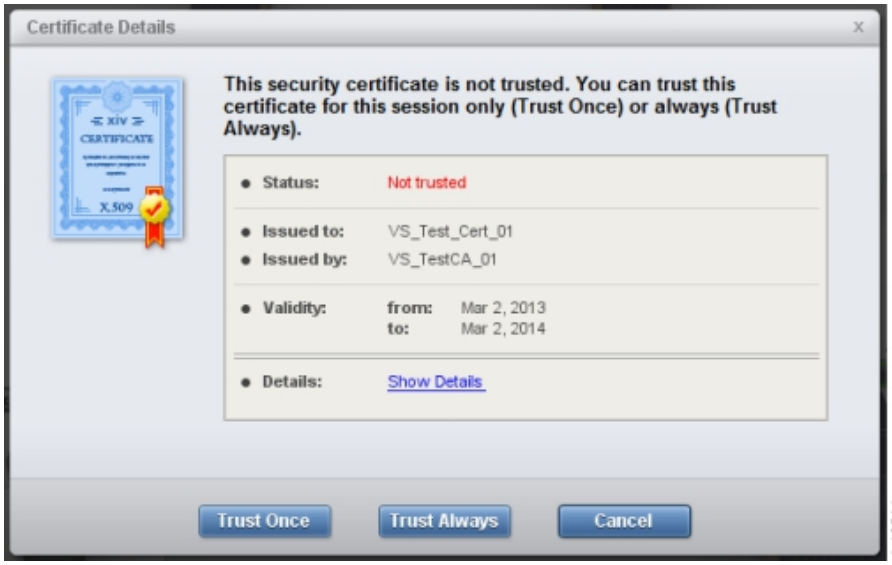


Figure 4. Trusting a certificate

Results

Following the confirmation, all XIV systems that have a Certificate Error status, and are using the certificate that is now confirmed, are automatically reloaded and validated.

GUI certificate management in manager mode

In manager mode the IBM Hyper-Scale Manager maintains a truststore that manages XIV systems certificates.

Working in manager mode, the GUI does not directly connect to the XIV system. The IBM Hyper-Scale Manager maintains a truststore that validates the certificates of the XIV systems, and the GUI provides the ability to do so.

Note: IBM Hyper-Scale Manager certificate management can also be done via server scripts.

Importing a certificate into the IBM Hyper-Scale Manager trust store

This option imports certificates into the truststore that is maintained by the IBM Hyper-Scale Manager.

Procedure

1. Select **Systems > Manager Configuration > XIV Certificates (Tab)**.

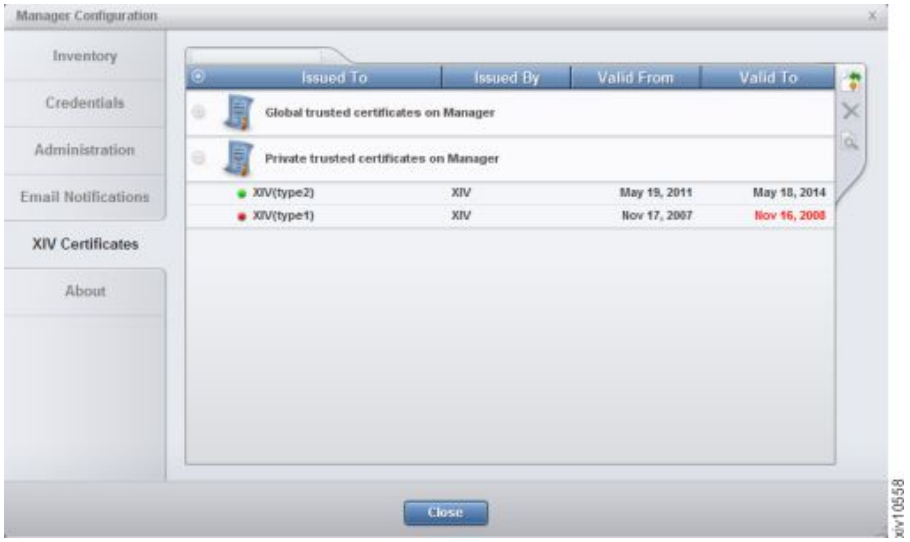


Figure 5. The Manager Configuration screen XIV Certificates (Tab)

2. Click the **Import Certificate** icon.

Results

Following the import of new certificates into the IBM Hyper-Scale Manager trust store, and moving to another tab - or exiting the window - all XIV systems with a certificate error are reloaded.

Removing a certificate from the IBM Hyper-Scale Manager trust store

This option removes certificates from the truststore that is maintained by the IBM Hyper-Scale Manager.

Procedure

1. Select **Systems > Manager Configuration > XIV Certificates (Tab)**.
2. Select a certificate and click the **Remove Certificate** icon.

Results

Following the certificates removal from the IBM Hyper-Scale Manager trust store and exiting the **Management** screen - or switching to another tab - all XIV systems are reloaded.

Handling certificate errors on the IBM Hyper-Scale Manager trust store

This option allows to view and re-trust certificates on the truststore that is maintained by the IBM Hyper-Scale Manager.

Procedure

1. Open **Systems > Manager Configuration > Inventory (Tab)**.
2. Right-click an XIV system with a certificate error and select Manage Certificate from the pop-up menu.

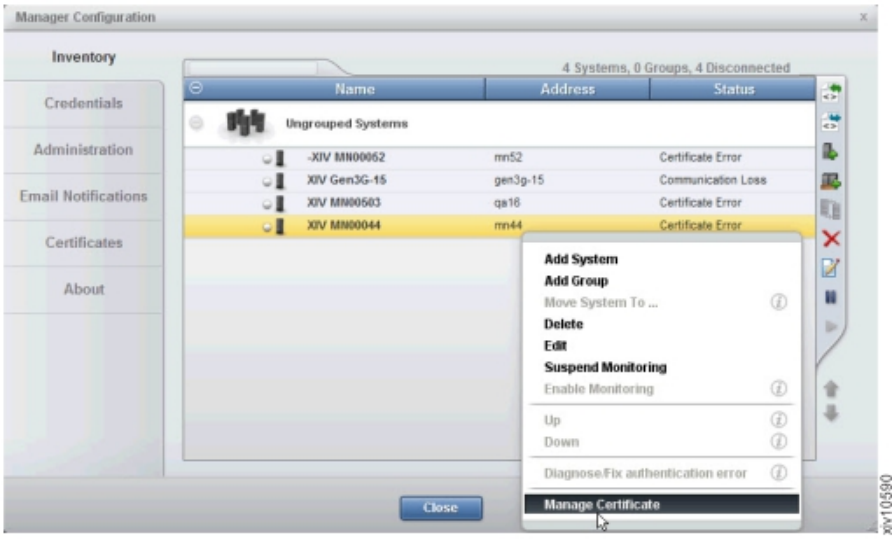


Figure 6. Handling certificate errors on the IBM Hyper-Scale Manager trust store

The certificate opens on screen.

3. Review the certificate. Click **Trust Always** to import it to the IBM Hyper-Scale Manager trust store.

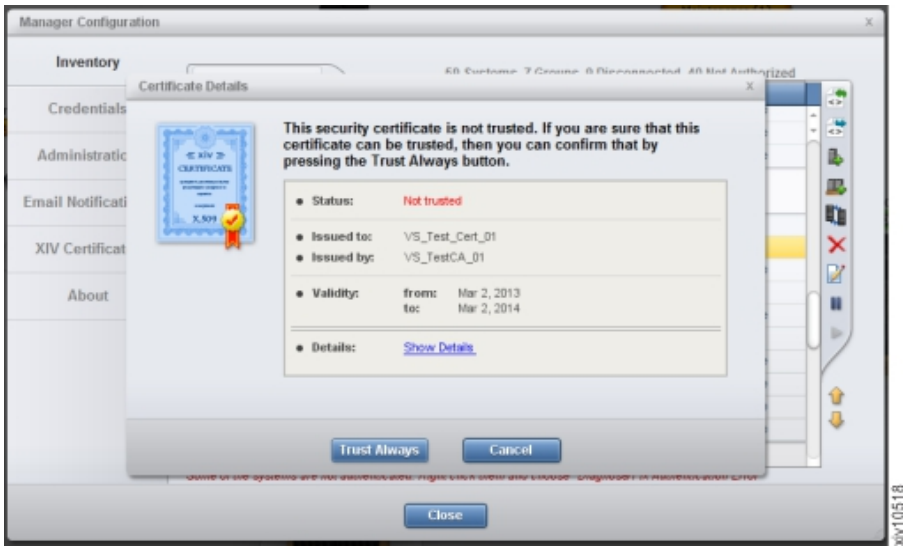


Figure 7. Handling certificate errors on the IBM Hyper-Scale Manager trust store

Results

Following the certificates removal from the IBM Hyper-Scale Manager trust store and exiting the **Management** screen - or switching to another tab - all XIV systems that are using this certificate are reloaded.

Handling the IBM Hyper-Scale Manager certificate

This option handles the certificate of the IBM Hyper-Scale Manager itself.

About this task

The GUI uses a local truststore that validates the IBM Hyper-Scale Manager.

Procedure

When the XIV GUI connects to the IBM Hyper-Scale Manager, or switching from one server to another, the IBM Hyper-Scale Manager certificate will be validated. If the certificate cannot be validated, the **Certificate Details** window will be displayed.
To start working with the IBM Hyper-Scale Manager, the certificate has to be trusted in one of the following ways:

1. Trust Once - the certificate will be treated as trusted throughout the current GUI session.
2. Trust Always - the certificate is trusted and imported to the local truststore.

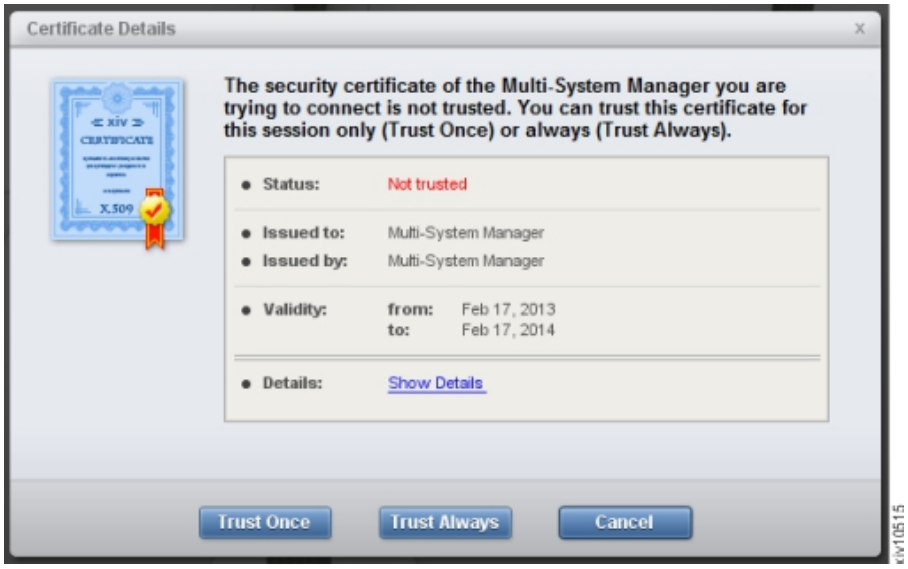


Figure 8. Handling the IBM Hyper-Scale Manager certificate

Managing XIV systems certificates

Importing a PKCS#12 certificate of an XIV system

The PKCS#12 certificate of an XIV system includes both public and private keys.

Before you begin

To import a PKCS#12 certificate, you need:

- The certificate file
- The password of the private key

About this task

This task guides you through importing the PKCS#12 certificate of an XIV system.

Procedure

1. Select **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** window opens.

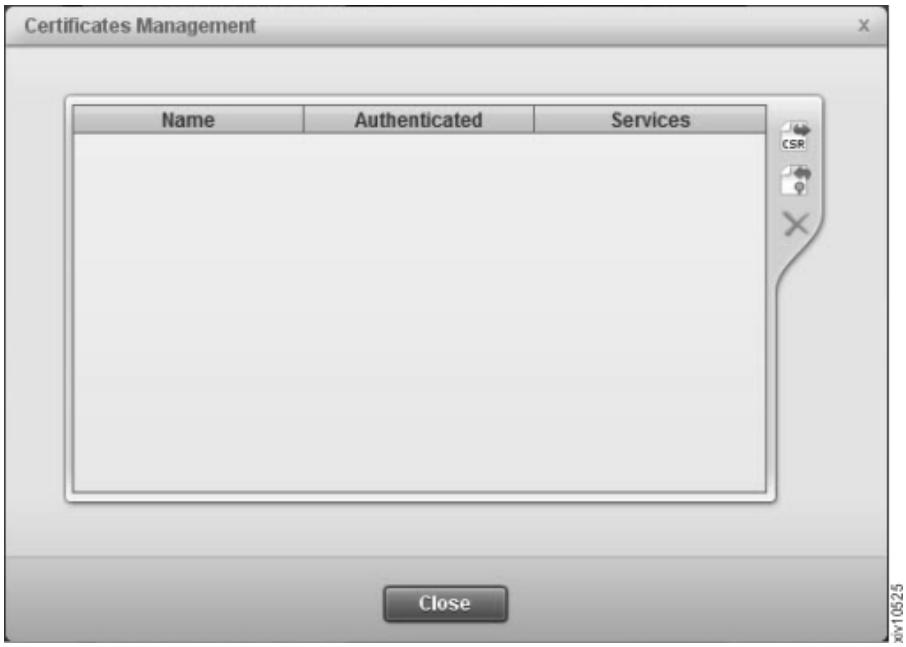


Figure 9. The Certificate Management screen

2. Click the **Import** button. The **Import Certificate (*.pem, *.p12)** window opens.

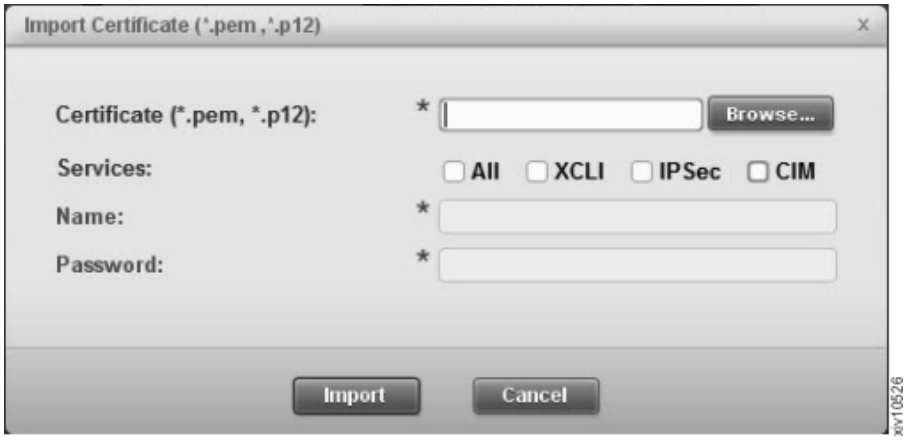


Figure 10. The Import Certificate window

   a. Browse for the certificate file.
   b. Check the services that will use this certificate.
   c. Choose an alias for the imported certificate. This name can be any distinguished name that will help you easily identify it among the rest of your certificates.
   d. Enter the password of the private key.
3. Click **Import**. The certificate file is imported.

Importing certificate

Generating a Certificate Signing Request (CSR)

This task describes how to generate a Certificate Signing Request that will be sent to the Certificate Authority.

Procedure

1. Click the Import Certificate toolbar icon. The **Generate CSR** window opens.

Figure 11. The Generate CSR window

2. Enter a certificate name. This should be a distinguishable name for further reference.
3. Enter the certificate subject in standard DN format. For example: */CN=TestCert/O=Organization/OU=OrganizationUnit*.
4. Select a bit length from the list.

   Note: A bit length of 4096 requires unrestricted policies.
5. Click **Generate**. Select a local path where to save the CSR file.
6. Open the Certificate Management window and verify that the newly generated certificate is awaiting authentication. The value of the **Authenticated** field is **No**.

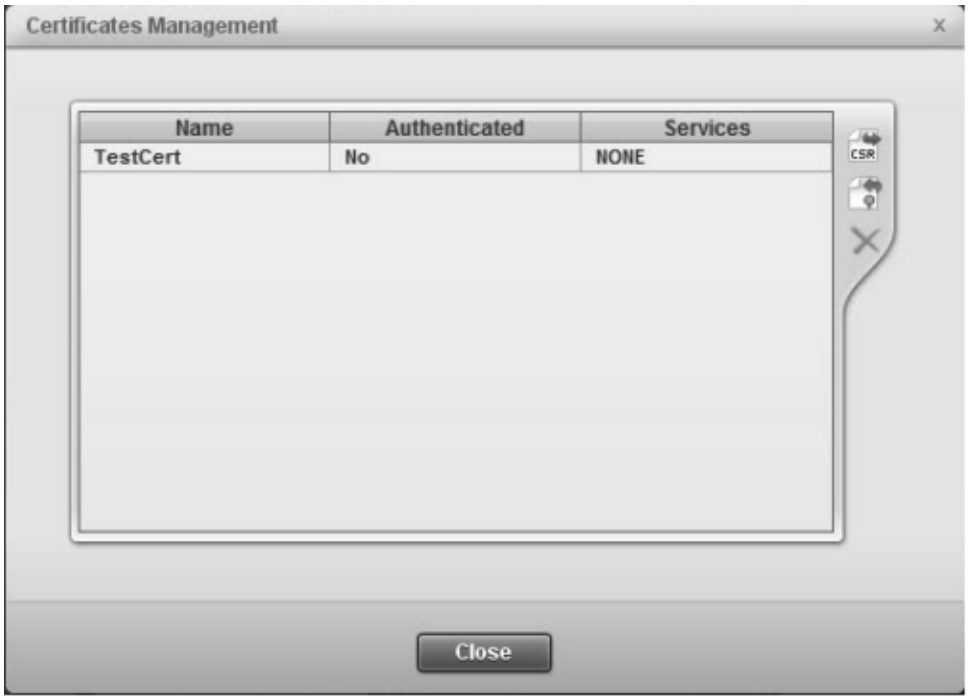


Figure 12. The newly generated certificate awaiting authentication

What to do next

Proceed to "Importing a signed certificate request."

Importing a signed certificate request

Importing signed certificate request into the XIV in order to authenticate it.

Before you begin

In order to replace a signed certificate, you need:

- The certificate file
- The password of the private key

About this task

Once you have authorization from the certificate authority, you can import the signed certificate.

Procedure

1. Click the **Import Certificate** toolbar icon.

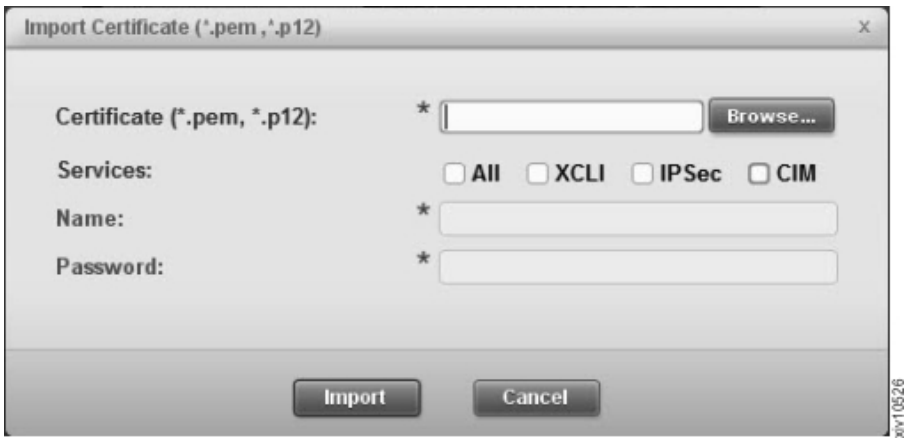


Figure 13. The Import Certificate window

2. Select a certificate file (in *PEM* format).
3. Select among the services that will use the certificate.
4. Click **Import**. The certificate file is imported.

Removing a certificate

This section describes how to remove a certificate.

About this task

This task removes the certificate from the system.

Procedure

1. Open **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** screen opens.
2. Select a certificate and click **Delete**. The certificate is removed.

Renaming an XIV system certificate

This task describes how to rename an XIV system certificate.

Procedure

1. Select **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** window opens.
2. Right-click on a certificate and click **Rename**.
3. Enter a new name and click **OK**.

Regenerating a CSR for an XIV system certificate

This task describes how to regenerate a CSR (Certified Signing Request) for an XIV system certificate.

Procedure

1. Select **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** window opens.
2. Right-click on a certificate and click **Regenerate CSR**.
3. Enter a new subject and click **Generate**.
4. Select the local file path to save the generate CSR file into.

Updating a certificate of an XIV system

Both the certificate and the certified services can be updated.

Procedure

1. Select **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** window opens.
2. Right-click on a certificate and click **Update certificate**. The **Update Certificate** window opens.

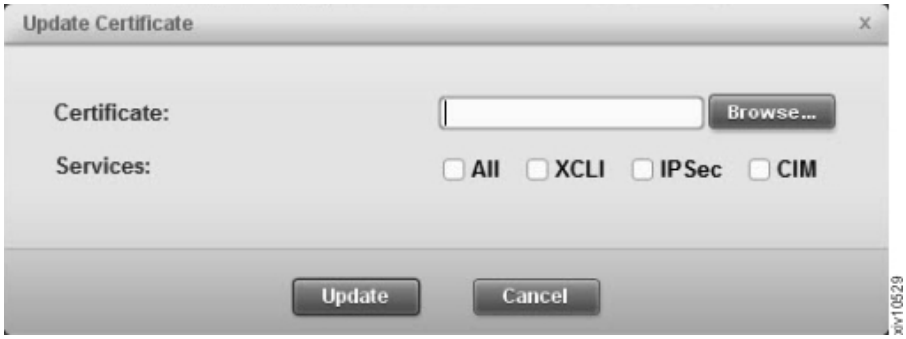


Figure 14. The Update Certificate window

3. Optionally: browse to a new certificate file and import it.
4. Optionally: check and un-check services according to your needs.
5. Click **Update**.

Managing the Manager certificate

Replacing the IBM Hyper-Scale Manager certificate

This task describes how to replace the IBM Hyper-Scale Manager certificate.

About this task

When the XIV GUI connects to a IBM Hyper-Scale Manager, it is attempting to identify the certificate of the IBM Hyper-Scale Manager. If needed, you can replace the certificate from either the GUI or from the IBM Hyper-Scale Manager menu.

Procedure

1. From the GUI:
   a. Open **Systems > Manager Configuration > Administration** on the XIV GUI menu.

Figure 15. Replacing the Manager Certificate

Click **Show Certificate** to view the certificate.

b. Clicking **Replace Certificate**.

Figure 16. Replacing the Manager Certificate

c. Click **Browse** to import a certificate file in *PKCS#12* format. Type the password and click **Import**.

2. For steps from the IBM Hyper-Scale Manager menu, see the IBM Hyper-Scale Manager User Guide.

Chapter 3. Managing Encryption

The IBM Hyper-Scale Manager supports Data-at-Rest encryption of self-encrypting disks.

This chapter includes tasks for key server management, working with a recovery key, and enabling encryption on XIV systems.

Encryption workflows

Managing data-at-rest of self-encrypting disks involves the following workflows.

Perform the following tasks in the order the appear here.

"Setting up the Tivoli Key Lifecycle Manager key server" on page 20
This task sets up the Tivoli Key Lifecycle Manager to work with the XIV system.

"Defining a Security Administrator" on page 21
XIV introduces a new user type. This user carries out encryption-related tasks and is not necessarily a storage administrator. The storage administrator, on the other hand, does not have permissions to carry out security-related tasks.

Now that the Tivoli Key Lifecycle Manager is configured to work with XIV systems and there are security administrators available, proceed to:

"Configuring the XIV system for encryption" on page 23
This task instructs you how to enable encryption in a single procedure.

Other Encryption tasks
Refer to the following sections in order to carry out administrative tasks

- "Editing a key server" on page 29 - You may rename the key server, its address, and the certificate file through which the key server authenticates the XIV systems.
- "Deleting a key server" on page 30 - You can remove the key server so it will not be able to provide encryption services to the XIV systems.
- "Setting a key server as master" on page 30
- "Generating recovery keys" on page 31 - The security administrators specify the minimum number of recovery keys that is required for enabling the XIV system to unlock its encrypted disks, and the security administrators that can participate in the recovery.
- "Acquiring the recovery key" on page 33 - Each of the security administrators that was specified as a recovery key recipient logs in to the XIV system and receives their part of the key.
- "Activating the encryption" on page 33 - now that have a recovery key that was dispensed among the security administrators, the encryption can be enabled.
- "Deactivating the encryption" on page 34 - to stop data-at-rest encryption, the XIV system must fulfill the following conditions: there are no volumes on the system and all of the recovery keys are invalidated.

Setting up the Tivoli Key Lifecycle Manager key server

Set up the Tivoli Key Lifecycle Manager key server to work with XIV systems.

Before you begin

You need permissions to log in to the Tivoli Key Lifecycle Manager web UI as `TKLMAdmin`.

About this task

IBM XIV supports the following key servers:

- Tivoli Key Lifecycle Manager 2.0.1

This procedure carries out the following tasks:

Generating a certificate.
Use the Tivoli Key Lifecycle Manager to generate a certificate file that allows the XIV system to trust the Tivoli Key Lifecycle Manager.

Importing the Tivoli Key Lifecycle Manager certificate on the XIV system.
Use the XIV GUI to add the Tivoli Key Lifecycle Manager as a key server that is recognized by the XIV system.

Exporting the XIV systems' certificate to the Tivoli Key Lifecycle Manager interface.
The XIV system certificate is provided with the XIV system itself. Export it to the Tivoli Key Lifecycle Manager so that the Tivoli Key Lifecycle Manager can trust the XIV system.

Procedure

1. Generating a certificate.
   a. Log in to the Tivoli Key Lifecycle Manager web UI as `TKLMAdmin`.
   b. Go to **Tivoli Key Lifecycle Manager -> Advanced Configuration->Server Certificates**. Select **Add** and then **SSL/KMIP Certificate**. Select **Create self-signed certificate** and enter the certificate label and certificate description.

      Note: Use the same name for both label and description.
   c. Export the certificate

      Windows
      Type at the DOS prompt:

      ```
      cd<TKLMPATH> (e.g. in windows: C:\ibm\tivoli\tiptklmV2\bin)
      wsadmin -username tklmadmin -password <tklmadmin password>
      -lang jython
      ```

      Linux Type:

      ```
      cd<TKLMPATH> (e.g. in RHEL: cd /opt/IBM/tivoli/tiptklmV2/bin)
      rm -f /tmp/cert.der
      ./wsadmin.sh -username TKLMAdmin -password <tklmadmin password>
      -lang jython
      ```

   d. To view all of the certificates use:

      ```
      print AdminTask.tklmCertList()
      ```

   e. To print the specific certificate, type:

      ```
      wsadmin>print AdminTask.tklmCertList
      ('[<the label that was provided above.]')
      ```

The output:

```
CTGKM0001I Command succeeded.

uuid = CERTIFICATE-a44aba79-6bcc-47dd-94c0-23ddb5db102c
alias = nachos
key store name = defaultKeyStore
key state = ACTIVE
issuer name = CN=nachos
subject name = CN=nachos
creation date = 10/26/12 11:06:32 AM MST
expiration date = 10/26/15 11:06:27 AM MST
serial number = 1410337117550384
```

f. Take the UUID information and use that for export:

```
wsadmin>print AdminTask.tklmCertExport
('[-uuid  CERTIFICATE-a44aba79-6bcc-47dd-94c0-23ddb5db102c
-format base64 -fileName /tmp/cert.der ]')
CTGKM0001I Command succeeded.
```

This `.pem` file is the certificate that passes as a parameter to the IBM Hyper-Scale Manager in the next step.

2. Install the Tivoli Key Lifecycle Manager Certificate on the XIV system. See instructions here: "Adding a key server" on page 27.
3. Import the XIV system's certificate to the Tivoli Key Lifecycle Manager interface. On the Tivoli Key Lifecycle Manager main menu, go to **Advanced Configuration -> Client Certificates** and click **Import**. The **Import** pane opens. Browse to the certificate file and click **Import**. The certificate is imported.

Results

- The Tivoli Key Lifecycle Manager server is now certified to work with the XIV system.
- Repeat this procedure for every SED-enabled XIV system.
  - Shorten the procedure by right-clicking on an XIV system that is configured with key server, select **Copy System Configuration** and paste onto other SED-enabled XIV system. This action passes the already configured key server details to many XIV systems instantly. See instructions here: "Mass configuration copy-pasting" on page 59.
  - Repeat only step 3 above.

Defining a Security Administrator

All SED management tasks are performed by a Security Administrator.

Before you begin

Prepare the Security Administrator's user and password.

About this task

This task gives the Security Administrator access rights to the XIV GUI and to XIV systems that support SED. The rights are given by the Storage Administrator.

Procedure

1. Log into the XIV GUI with Storage Administrator credentials.
2. Select an XIV system that supports SED.

Note: You may select several systems at once.

3. Select **Add User** from the **Actions** menu.
4. Add a user. Select **Security Administrator** from the **Category** dropdown list, and click **Add**. The new user is displayed in the **Users** table.

Figure 17. Creating a Security Administrator user

5. Click the user name button on the toolbar in order to re-login with the Security Administrator credentials. Enter the user and password of the Security Administrator and click **Login**. The GUI now displays only the XIV systems that the new user applies to.

Figure 18. Logging into the XIV GUI as a Security Administrator

Results

- You have a new Security Administrator user.
- You are logged into the XIV GUI with this user.

Configuring the XIV system for encryption

This workflow explains everything you need in order to set the XIV system for encryption.

Before you begin

Prepare the following information:

1. Key server
   - Name, address and port
   - A certificate file
   - Decide whether this is going to be the master key server
2. TKLM server version 2.0.1 and up
3. Identify the security administrators that will be responsible for generating and retaining the recovery keys

About this task

This workflow explains how to set the following:

1. Import a PKCS#12 certificate of an XIV system
2. Add a key server
3. Generate a recovery key
4. Acquire the recovery key
5. Enable the encryption

Procedure

1. Importing a PKCS#12 certificate. This certificate permits communication between the XIV system and the key server.
   a. In order to import a PKCS#12 certificate, you need:
      - The certificate file
      - The password of the private key
   b. Select **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** window opens.

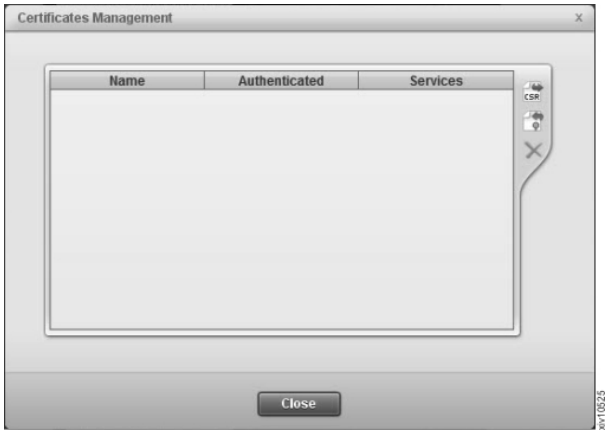


Figure 19. The Certificate Management window

c. Click the **Import** button. The **Import Certificate (*.pem, *.p12)** window opens.

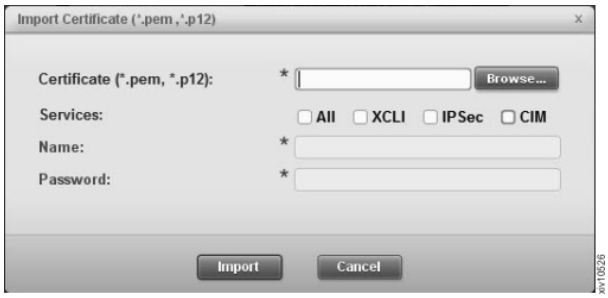


Figure 20. The Import Certificate window

1) Browse for the certificate file.
2) Check the services that will use this certificate.
3) Choose an alias for the imported certificate. This name can be any distinguished name that will help you easily identify it among the rest of your certificates.
4) Enter the password of the private key.

d. Click **Import**. The certificate file is imported.

2. Log into the XIV GUI as a security administrator. Click the user name button on the toolbar in order to re-login with the security administrator credentials. Enter the user and password of one of the security administrators and click **Login**. The GUI now displays only the XIV systems that the security administrator can access.

Figure 21. Logging into the XIV GUI as a security admin

3. Add a key server that will generate a recovery key and provide it to the security administrators.
   a. Prepare the following key server information:
      - Name
      - Server Address and port
      - Certificate file

      Note: One key server must be defined as *master*.
   b. Select a single XIV system. Right-click the system or select **System Setting > Manage Key Servers** from the **Systems** menu.
   c. Enter the Key Server details. Determine whether this is the Master key server and click **Create**.

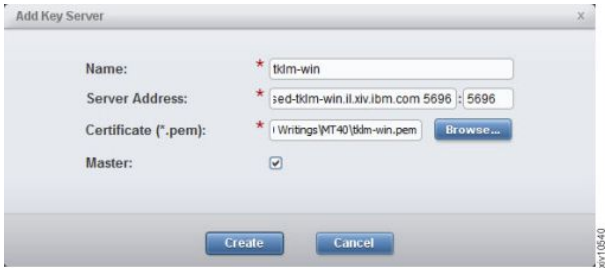


Figure 22. Adding a key server

The key server is added to the table.

Figure 23. The key servers table

The key server properties can be edited. See the following sections later on this chapter:

- "Editing a key server" on page 29
- "Deleting a key server" on page 30
- "Setting a key server as master" on page 30

4. Generate a recovery key. The recovery key allows access to an encryption-enabled XIV system whenever the key server is unreachable upon system startup.
   a. Right-click the XIV system and select **Generate Recovery Key** from the menu.

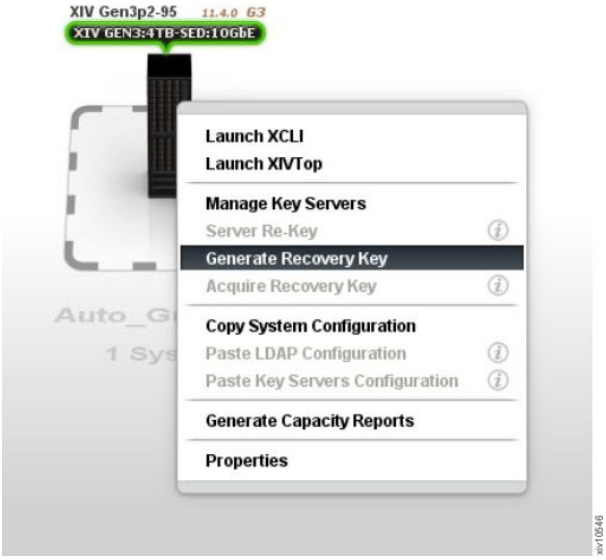


Figure 24. Right-click the XIV system and select **Generate Recovery Key** *from the menu.*

The Generate recovery key window opens.

   b. Set the minimum number of users in the recovery group. This is the number of security administrators that is required in order to approve access to the encrypted disk. Move security administrators to the Recovery Group pane. Click **Start**.

Figure 25. The **Generate Recovery Key** *window*

The recovery key is generated and is available for the security administrators.

5. Acquire the recovery keys.

   In this step, the security administrators acquire their recovery keys that were generated by the key server.

   Each of the security administrators must perform this step, so all of the recovery keys are acquired by the respective security administrators.

   a. Select **Actions > Acquire recovery key** from the XIV GUI menu. The **Acquire Recovery Key** window opens.
   b. The window displays two fields. Copy the key from the **Recovery Key** field and paste it to the **Verify Key** field for verification. Paste it aside (to somewhere outside the XIV GUI) and save it.
   c. Click **Activate Recovery Key** and approve the message on the window.

   The key was acquired by the security administrator and saved in a secure place outside the XIV GUI. It is available in case the recovery key is required.

6. Enable the encryption.
   a. Select an XIV system.
   b. Select **Systems > System Settings > Activate Encryption**. Enable Encryption window opens.
   c. Review the information in the window, verify that the key servers are listed correctly, and that the recovery key is verified by the relevant security administrators.
   d. Click **Enable**.

Results

The XIV system is encryption enabled.

Other Encryption tasks

Adding a key server

Add a key server that will generate a recovery key and provide it to the encrypted XIV systems.

Before you begin

1. Log into the XIV system as a security administrator. See instructions here: "Defining a Security Administrator" on page 21.
2. Prepare the following key server information:
   - Name
   - Server Address and port
   - Certificate file

About this task

One key server must be defined as *master*.

Procedure

1. Select a single XIV system. Right-click the system or select **System Setting > Manage Key Servers** from the **Systems** menu.
2. Enter the Key Server details. Determine whether this is the Master key server and click **Create**.

Figure 26. Adding a key server

The key server is added to the table.

Figure 27. The key servers table

Results

The key servers' properties can be edited. See the following sections:

- "Editing a key server"
- "Deleting a key server" on page 30
- "Setting a key server as master" on page 30

What to do next

Transfer the key server certificate to the XIV system.

Editing a key server

You may rename the key server, its address and the certificate file through which the key server authenticates XIV systems.

Before you begin

1. Log into the XIV system as a Security Administrator. See instructions here: "Defining a Security Administrator" on page 21.
2. Prepare the key server information that you would like to edit:
   - Name
   - Server Address
   - Certificate file

Procedure

1. Select a single XIV system to which you have already added a key server. Select **System Setting > Manage Key Servers** from the **Systems** menu.
2. Select a key server and click **Edit**. Alternately, right-click the server and select **Edit** from the pop-up menu. Edit the server's details and click **Update**. The key server details are updated.

Deleting a key server

You can remove the key server so it will not be able to provide encryption services to the XIV systems.

Before you begin

Log into the XIV system as a security administrator. See instructions here: "Defining a Security Administrator" on page 21.

If you have XIV systems with encryption enabled, you have to have at least one key server for each of them. Make sure that the key server you are about to delete is not the sole key server for an XIV system.

Note: You can't delete the last key server as long as it is assigned to an encrypted XIV system.

Procedure

1. Select a single XIV system. Select **System Setting > Manage Key Servers** from the **Systems** menu.
2. Select a key server and click **Delete**. Click **OK** on the confirmation screen.

Results

The key server is no longer associated with the XIV system.

Setting a key server as master

Set one of the key servers as master.

Before you begin

Log into the XIV system as a Security Administrator. Refer to "Defining a Security Administrator" on page 21 for further instructions.

Procedure

Right-click a server that is not marked as master and select **Set as Master** from the popup menu. Click **OK** to approve. The key server is set as master.

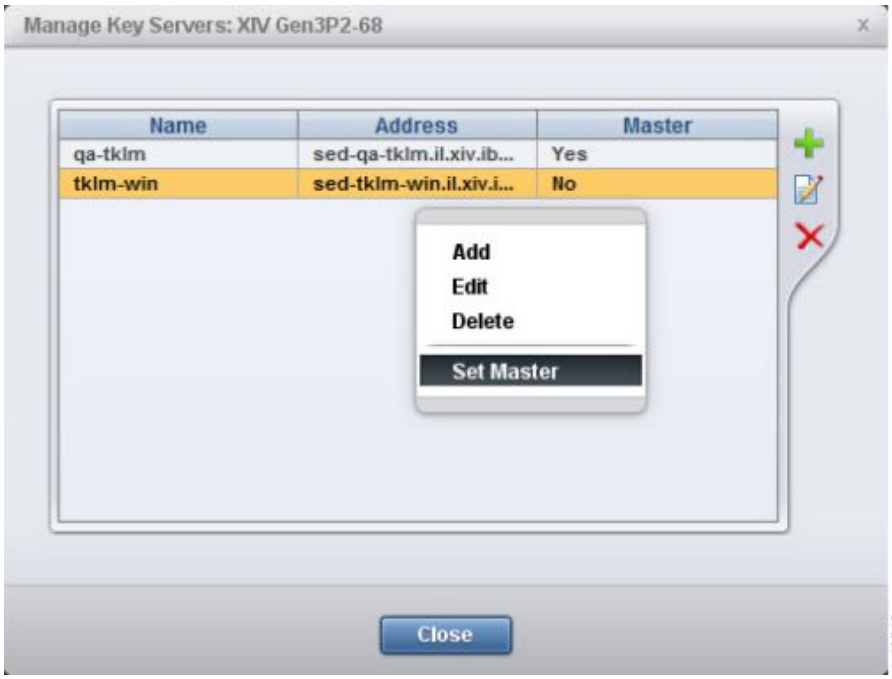


Figure 28. Re-keying a server

Results

The key server is set as master. The previous key server is no longer a master.

Generating recovery keys

The recovery keys allow an XIV system to access encrypted disks when the key server is unreachable upon system startup.

Before you begin

Define a key server. See instructions for "Adding a key server" on page 27.

About this task

Once the XIV system has security administrators (at least 2) and a key server, a recovery key must be generated for each security administrator.

Procedure

Repeat the following steps for each security administrator.

1. Right-click the XIV system and select **Generate Recovery Key** from the menu.

Figure 29. Right-click the XIV system and select **Generate Recovery Key** *from the menu.*

The Generate recovery key screen opens.

2. Set the minimum number of users in the recovery group. This is the number of security administrators that is required to approve access to the encrypted disk. Move security administrators to the Recovery Group pane. Click **Start**.

Figure 30. The **Generate Recovery Key** *screen*

Results

The recovery key is generated and is available for the security administrators.

Acquiring the recovery key

The security administrators acquire their recovery keys that were generated by the key server.

Before you begin

Log into the XIV GUI as a security administrator.

Procedure

1. Right-click an XIV system from the **Systems** or the **List** views, and select **Acquire recovery key**. The **Acquire Recovery Key** window opens.
2. The window displays two fields. Copy the key from the **Recovery Key** field to the **Verify Key** field for verification, copy it aside (to somewhere outside the XIV GUI) and click **Activate Recovery Key**.
3. Approve the message.

Results

The key is acquired by the security administrator and is available in case the recovery key is required.

Activating the encryption

Once you have a recovery key, you can activate the encryption.

Before you begin

In order to activate the encryption, the XIV system has to fulfill the following:

- At least one master key server configured successfully
- Recovery key were verified and passed along to the security administrators

Activating the encryption is done by the security administrator.

Procedure

1. Select an XIV system.
2. Select **Systems > System Settings > Activate Encryption**. Activate Encryption screen opens.
3. Review the information on screen: verify that the key servers are listed correctly, and that the recovery key is verified by the relevant security administrators.
4. Click **Enable**.

Results

The XIV system is encryption activated.

Deactivating the encryption

Deactivate encryption of an XIV system so its data will no longer be protected.

Before you begin

In order to deactivate the encryption, the XIV system has to fulfill the following:

- The XIV system has no volumes

Deactivating the encryption is done by the security administrator.

Procedure

1. Select an encrypted XIV system.
2. Select **Systems > System Settings > Deactivate Encryption**. A Disable Encryption message opens.
3. Confirm the message.

Results

The XIV system is no longer encrypted. A cryptographic erase erases all of the encryption-related data on all of the protected bands.

Chapter 4. Setting the activity level for Support access

An activity level can be set for Support access allowable by the customer.

About this task

Select the activity level for Support access. Any activity level above the selected level is subject to customer permission.

Procedure

1. From the XIV GUI, select **Systems** > **System Settings** > **Support**. The following window is displayed:

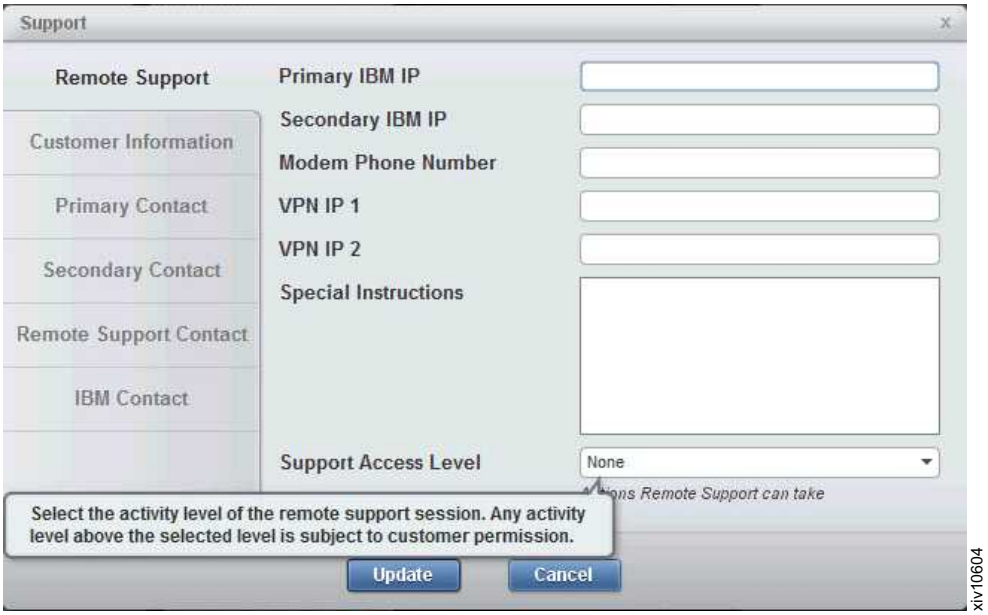


Figure 31. Support settings window

2. In the **Support Access Level** field, select one of the following options:
   - **Undefined** - No **Support Access Level** has been defined.
   - **No Access** - No access is allowed without customer permission. Connecting to the system requires previous approval from the customer. If approval is received, all actions can be performed. Once approved, connecting to the system, guided repairs, reports and the rest are not blocked.
   - **Diagnostic** - Access is granted for diagnostic purposes only (for example, X-Ray). Allows X-Ray collection and view/list/status actions. Other actions require permission.
   - **No impact** - Access is granted for diagnostic and non-impacting changes. Any change that could possibly result in impaired/reduced/impacted host IO requires customer permission.
   - **Full Access** - No prior permission is required to perform any repair action. Access is granted for all activities.
3. Click **Update** to save your settings.

Chapter 5. Capacity planning

The IBM Hyper-Scale Manager collects usage statistics and calculates a forecast of the future use of XIV systems, domains, and pools. This statistics are also available for external analytics tools.

The IBM Hyper-Scale Manager provides capacity data for any selection of XIV systems. The raw capacity data can be moved among various instances of the IBM Hyper-Scale Manager to maintain continuity of the collected data. This data can also be exported to a CSV file or PDF to be used by common analytical tools.

The capacity report is generated from the XIV GUI. Instructions on how to generate the report, how to read the CSV files and PDF, and how to create a graph within a few clicks, are provided in "Generating a capacity analytics report" on page 38.

Moving the capacity data from one IBM Hyper-Scale Manager to another is done using the following tasks:

- "Exporting the raw capacity data" on page 45 - The raw data is exported to make it available for import to another IBM Hyper-Scale Manager. The file is exported in the same manner as other files (i.e. backups, logs and more) are exported.
- "Importing the raw capacity data" on page 46 - A raw capacity data file that was created on one IBM Hyper-Scale Manager can be exported to be used by another IBM Hyper-Scale Manager in order to maintain the continuity of XIV systems history.
- "Resetting the raw capacity data" on page 47 - To clear the XIV system history from irregularities (for example, machine re-purposing), and to allow for collecting raw data from scratch, you can clear the machine history from the previously collected raw data. Data can be reset for either a specific system, or for all of the monitored systems.

Collecting usage data for an XIV system included in the inventory

The capacity data for the systems included in the inventory is collected daily (once a day) by the Hyper-Scale Manager server and stored in a database on the server. Since capacity data is available in the database, there is no interaction with the XIV systems when the administrator asks for a report to be generated.

The capacity data must meet several criteria for the forecast to be calculated:

- User must have sufficient access rights (role must be *storage administrator* or *read-only*) for all of the XIV systems included in the inventory.
- To present the trends, a sampling of 30 days is needed.
- A sufficient number of samples must be available. The forecast trend is not calculated if the number of samples is less than 30. If the system was not sampled for 14 days, then the system gathers 30 new samples, before the trend can again be presented.

  If the sample fails, the Hyper-Scale Manager samples the system every 15 minutes for a period of 12 hours. If the sample still fails, the operation is repeated the following day.

- System or storage pool utilization must be above 10%. If the system, or storage pool utilization, is less than 10%, no forecast is calculated.
- Trends cannot be calculated on pools that have no available space for volumes allocation.
- If capacity is fluctuating or flat, or space utilization is decreasing, there is no trend.

Collecting usage data for an XIV system that is removed from the inventory

The IBM Hyper-Scale Manager collects capacity data for XIV systems that are listed on the inventory. Removing a system from the inventory implies stopping the data collection. However, to overcome situations in which the system was mistakenly removed from the inventory, or removed from the inventory for a short period of time, the IBM Hyper-Scale Manager applies the following rules on collecting capacity data for systems that are removed from the inventory:

- As long as the system is listed on the inventory, the IBM Hyper-Scale Manager collects and keeps its capacity data.
- Whenever the system is removed from the inventory, its capacity data is not immediately deleted. It is kept until the next timeslot on which the data is collected from the machine.
- If the system is returned to the inventory prior to arriving to the next collection timeslot, the capacity data and its continuity are kept.
- If the system is removed from the inventory, it is impossible to reset its capacity data. To reset the capacity data, the system has to be listed in the inventory.
  - If the user chooses to reset capacity data for all systems, even non-monitored systems capacity data will be reset.

Generating a capacity analytics report

You can generate a capacity analytics report from the XIV GUI.

About this task

The report is generated for the systems selection on the XIV GUI, as displayed on the Systems Selector (i.e. all systems, a system group, a single system).

The structure of the file's name is: `XIV_capacity_report_yyyy-mm-dd_hhmm.zip`.

The zip contains the Capacity Planning PDF file and multiple CSV files named `XIV_capacity_report_yyyy-mm-dd_hhmm.<N>.csv`, cut into long 65000-line files. The filenames (ZIP, PDF, and CSV) can be determined by the user.

Procedure

1. Select the systems the report will be generated for and right-click **Generate Capacity Report**. Alternatively, open **Tools > Generate Capacity Report** from the menu.

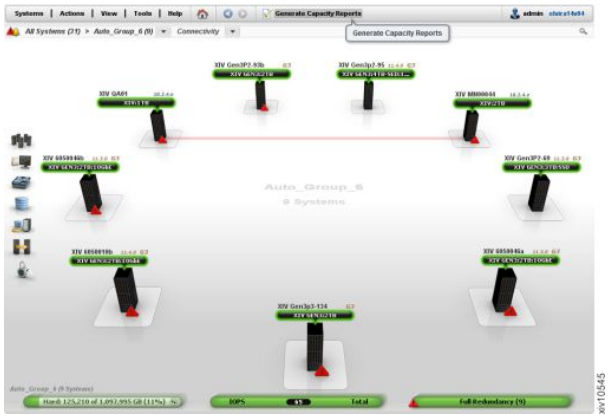


Figure 32. Right-click **Generate Capacity Report**

2. Select where to save the CSV file. A **Command executed successfully** notification is displayed on screen.
3. Keep the **Open containing folder** checkbox checked and click **OK**.
4. Open the CSV file using MS-Excel.

The structure of the capacity analytics report

The Capacity Analytics report provides information on the capacity of systems, domains, and pools.

This section explains the structure of the CSV file and PDF reports:

- "Capacity analytics CSV report structure"
- "Capacity Analytics PDF report structure" on page 42

Capacity analytics CSV report structure

The CSV file contains the raw data, collected over time by the Hyper-Scale Manager for each XIV Storage system inventoried. This raw data can be used for further analysis, or to create your own, customized reports.

The report legend

The legend provides information on the format and units of the information that is displayed in the CSV file.

```
IBM XIV Capacity Planning Report
Report Legend
All capacity metrics represents the hard capacities only.
Forecast is presented by the date when 80%/90%/100% threshold is reached.
System threshold is calculated based on the system total size.
Pool threshold is calculated of the total pools size available for allocation.
Dates are presented in this report in format: M/d/yy.
Detailed report tables are showing up to 250 values.
Samples are not necessarily consecutive, but are always evenly distributed.
Capacity numbers are shown in GB.
```

System Report Summary

This section provides a summary for each of the XIV systems whose capacity information was gathered (regardless of whether they have a trend).

The timestamp of the report and the number of systems are displayed.

```
The report was generated on 7/21/13 03:24 for 50 systems.
```

For each of the systems, the following information and the collected data are displayed:

- Name
- Model
- Status
- Total No. of Volumes (Snapshots)
- Usable hard capacity (GB)
- Allocated hard capacity (GB)
- Used hard capacity (GB)
- Unused hard capacity (GB)
- Unallocated hard capacity (GB) - The total of the system's free hard capacity and the sum of the domains' free hard capacity.
- % Used
- % Allocated
- Current growth rate (GB/week) - The growth rate is calculated from the date on which the trend was identified onward
- 80% Threshold - available values are: reached (if already above the threshold); projected day of reaching the threshold
- 90% Threshold - available values are: reached (if already above the threshold); projected day of reaching the threshold
- 100% Threshold - available values are: reached (if already above the threshold); projected day of reaching the threshold

For systems for which no trend was calculated, the reason is displayed. For more information on calculating the capacity forecast trend, see "Collecting usage data for an XIV system included in the inventory" on page 37.

Domain Report Summary

This section provides a summary for each of the domains, according to the user domain association. A global administrator sees all of the system domains, regardless of the access policy. If the policy is *closed*, the global administrator sees only the pools in the associated domain. The domain administrator sees only the specific domain.

The timestamp of the report and the number of systems are displayed.

```
The report was generated on 7/1/14 04:35 for 38 domains.
```

The report displays actual and projected capacity for domains:

All capacity metrics represent the allocated and hard capacities. *Domain threshold* is calculated from the total domains size available for allocation. The *usage threshold* value is calculated relatively to the total allocated size.

- Domain name
- System name
- Total number of pools
- Usable hard capacity (GB)
- Allocated hard capacity (GB)
- Used hard capacity (GB)
- Unused hard capacity (GB)
- Unallocated hard capacity (GB) - The total of the system's free hard capacity and the sum of the domains' free hard capacity.

- % Used
- % Allocated
- Current allocated growth rate (GB/week) - The growth rate is calculated from the date on which the trend was identified onward
- Current used growth rate (GB/week)
- 80% Used threshold - available values are: reached; projected day of reaching the threshold
- 90% Used threshold - available values are: reached; projected day of reaching the threshold
- 100% Used threshold - available values are: reached; projected day of reaching the threshold
- Used forecast failure reason
- 80% Allocated threshold - available values are: reached; projected day of reaching the threshold
- 90% Allocated threshold - available values are: reached; projected day of reaching the threshold
- 100% Allocated threshold - available values are: reached; projected day of reaching the threshold
- Allocated forecast failure reason

If the number of domains is less than 51, then all of the domains are displayed. Otherwise, a message is displayed with the number of domains for which the capacity trend was not calculated. Only the domains with forecasted data will be displayed.

Pool Report Summary

This section provides a summary for each of the storage pools whose capacity information was gathered (regardless of whether they have a trend).

The timestamp of the report and the number of systems are displayed.

```
The report was generated on 7/30/13 10:12 for 18 pools.
```

The report displays actual and projected capacity for storage pools:

All capacity metrics represents the hard capacities only.

- Pool name
- System name
- Number of volumes
- Usable capacity (GB)
- Used capacity (GB)
- % Used
- Growth Rate (GB/week) - The growth rate is calculated from the date on which the trend was identified onward
- 80% Threshold - available values are: reached; projected day of reaching the threshold
- 90% Threshold - available values are: reached; projected day of reaching the threshold
- 100% Threshold - available values are: reached; projected day of reaching the threshold

The number of pools for which the capacity trend was not calculated is also displayed.

System Detailed Report

This section provides a detailed report for each of the XIV systems whose capacity information was gathered (regardless of whether they have a trend).

This section of the CSV displays a detailed report for each of the XIV systems. The report includes day-by-day information on the current capacity (the intervals are not necessarily daily), the calculated 80%, 90% and 100% thresholds and a forecast summary.

The forecast summary details the date on which the trend was detected and the projected dates by which the capacity is expected to reach each of the thresholds.

The system threshold values use 15 months as the long-term forecast.

Domains Detailed Report

Information similar to the System Detailed Report is available for each of the Domains. In addition, the Domains Detailed Report shows two detailed report blocks (different graphs). One graph displays *used capacity*, and one displays the *allocated hard capacity*. The used and allocated hard capacity histories are real domain capacity samples, while the forecast capacities are calculated based on the aggregated pools capacity history.

The domain threshold values use 15 months as the long-term forecast.

Pools Detailed Report

Information similar to the System Detailed Report is available for each of the Pools.

The pool threshold values use 15 months as the long-term forecast.

Capacity Analytics PDF report structure

The PDF file contains a formatted report with summarized informational graphics and graphs for each monitored XIV system, domain, and pool.

The PDF report is divided into three parts:

- Part 1 - System Allocation
- Part 2 - Domain Usage and Allocation
- Part 3 - Pool Usage

For all three parts (systems, domains and pools), graphical representation illustrates the capacity allocation or usage over periods of time, growth rate per week, and detailed graphs per object, respectively.

For example, Figure 33 on page 43 shows an overall view for all of the XIV systems in the inventory and a capacity forecast over the next 12 months

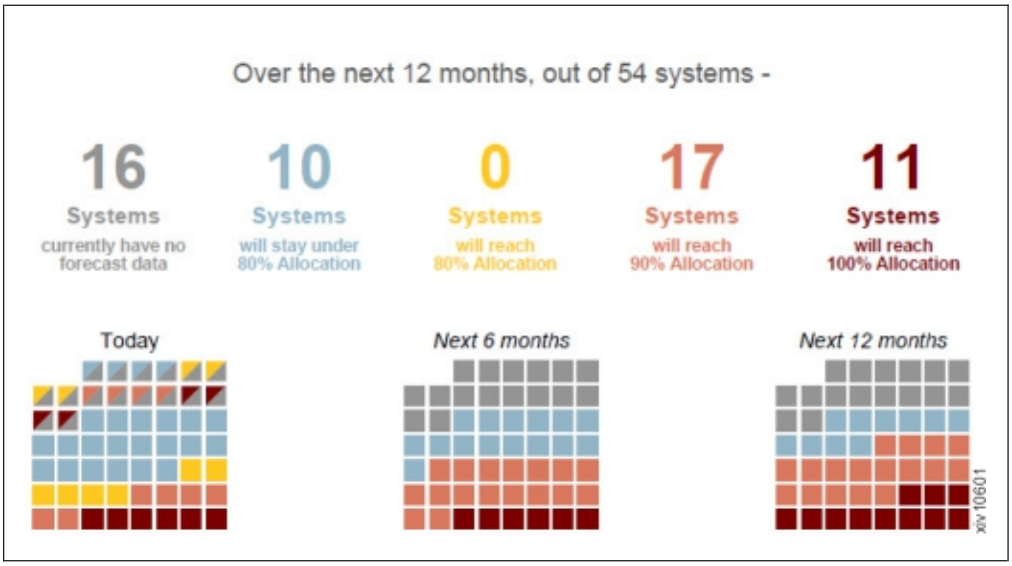


Figure 33. System capacity allocation over time

The graph, Figure 34, ranks the system per capacity growth rate.

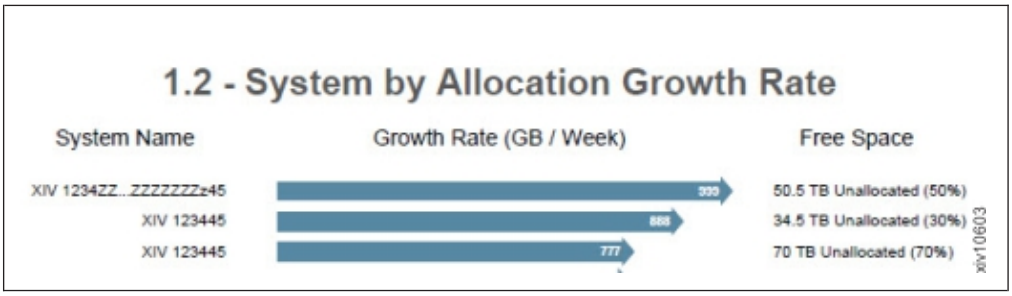


Figure 34. System by allocation growth rate

And for each XIV Storage system, individual graphs show the progression of the system capacity allocation growth. See Figure 35.

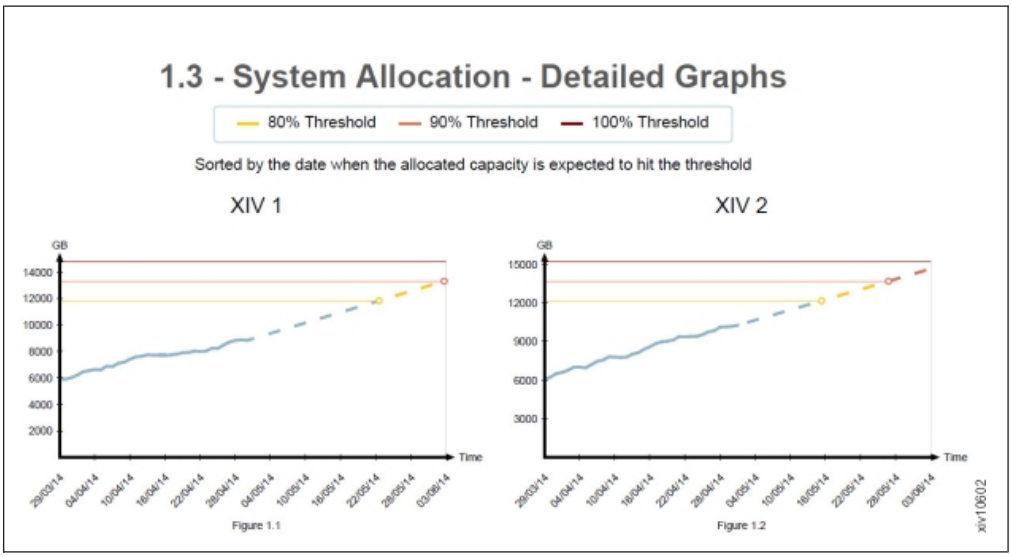


Figure 35. System allocation - detailed graphs

Creating the capacity graph within 3 clicks

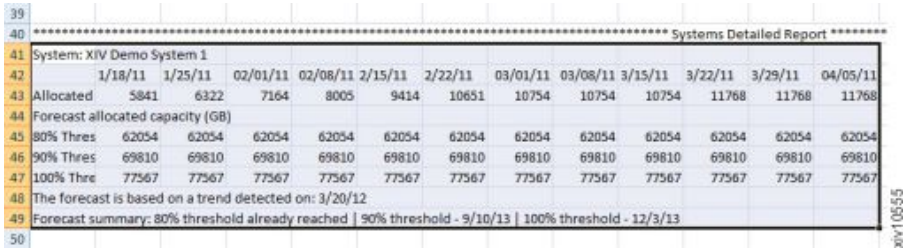
You can easily create the capacity graph within a few clicks.

About this task

Use the exported CSV file to create a capacity graph.

Procedure

1. On MS-Excel 2007:
   a. Select the information to be displayed on the graph from the System Detailed Report or Pools Detailed Report sections.



39													
40	********** Systems Detailed Report *********												
41	System: XIV Demo System 1												
42		1/18/11	1/25/11	02/01/11	02/08/11	2/15/11	2/22/11	03/01/11	03/08/11	3/15/11	3/22/11	3/29/11	04/05/11
43	Allocated	5841	6322	7164	8005	9414	10651	10754	10754	10754	11768	11768	11768
44	Forecast allocated capacity (GB)												
45	80% Thres	62054	62054	62054	62054	62054	62054	62054	62054	62054	62054	62054	62054
46	90% Thres	69810	69810	69810	69810	69810	69810	69810	69810	69810	69810	69810	69810
47	100% Thre	77567	77567	77567	77567	77567	77567	77567	77567	77567	77567	77567	77567
48	The forecast is based on a trend detected on: 3/20/12												
49	Forecast summary: 80% threshold already reached | 90% threshold - 9/10/13 | 100% threshold - 12/3/13												
50													

xiv10555

Figure 36. Selecting the information to be displayed

   Note: It is recommended to include the headers in the selection, in order to receive a nicely scaled graph.
   b. Click **Insert**.
   c. Click **Line** and select a line graph. The graph is displayed on screen.
2. On MS-Excel 2003:
   a. Select the information to be displayed on the graph from the System Detailed Report or Pools Detailed Report sections.
   b. Do either:
      - Click the **Chart Wizard** icon on the toolbar.
      - Select **Insert > Chart** from the menu.

      The **Chart Wizard** opens on screen.
   c. Select **Line** on the **Standard Types** tab. Select the **Chart sub-type**. Click **Finish**. The graph is displayed on screen.

Example

The capacity report graph displays the following information:

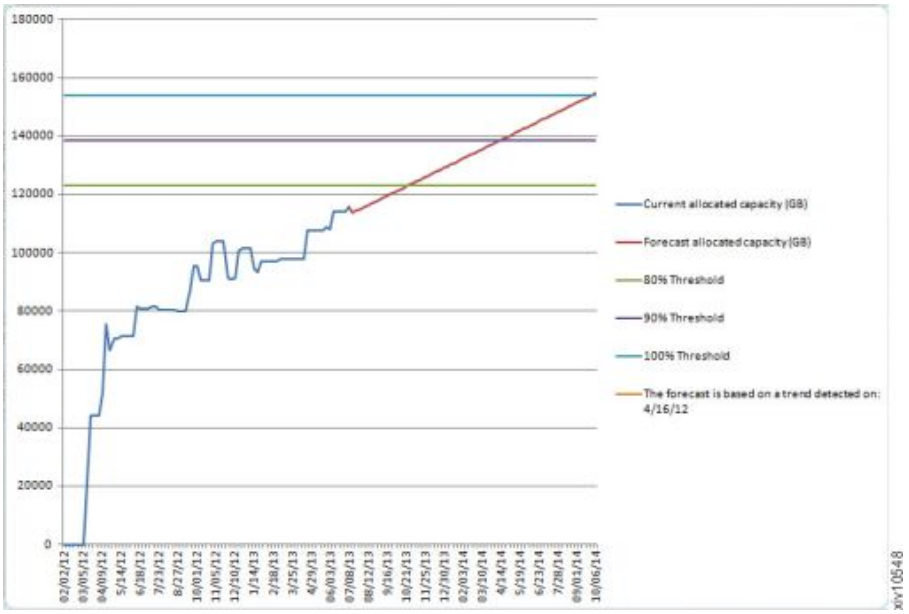


Figure 37. Creating a capacity graph

Actual values - the blue line
The actual capacity as measured at a given date.

Forecasted - the red line
The calculated forecast trend of the capacity.

80% threshold - the green line
The calculated 80% of the total capacity.

90% threshold - the purple line
The calculated 90% of the total capacity.

100% threshold - the light blue line
The calculated 100% of the total capacity.

Note: The colors on the graph may vary.

Moving the capacity data among Manager instances

Exporting the raw capacity data

The raw capacity planning data can be transferred from one IBM Hyper-Scale Manager to another.

About this task

The raw data that was collected on one IBM Hyper-Scale Manager can be used by another IBM Hyper-Scale Manager in order to maintain the continuity of XIV systems history.

Procedure

1. Open the **Manage Inventory Options** menu.
2. Click 2 on the **Manage Capacity Planning Data** menu.

```
------------------------------------------------------------------
------------ IBM Hyper-Scale Manager v1.x.x.x ---------------
------------------------------------------------------------------


Manage Capacity Planning Data
-----------------------------
1) Import Capacity Data
2) Export Capacity Data
3) Reset Capacity Data
4) Exit
Your Selection>2
The capacity data file (*.csv) was exported to the (/home/msms/hyperscale/files/export)
folder
Press any key to continue
```

3. Press any key. The file is exported.

What to do next

The capacity data file that you are creating in this task will need to be exported out of the IBM Hyper-Scale Manager in either of the following ways:

Virtual appliance
SFTP from the target IBM Hyper-Scale Manager using the maintenance account. Take the CSV file from the `export` folder.

Standalone application
Copy the file from the `export` folder.

Importing the raw capacity data

The capacity planning raw data can be transferred from one IBM Hyper-Scale Manager to another.

Before you begin

Prepare a capacity data file that was created by another IBM Hyper-Scale Manager.

Virtual appliance
SFTP to the target IBM Hyper-Scale Manager using the maintenance account. Put the CSV file in the `upload` folder.

Standalone application
Copy the file to the `upload` folder.

About this task

A report that was created on one IBM Hyper-Scale Manager can be used by another IBM Hyper-Scale Manager to maintain the continuity of XIV systems history.

Procedure

1. Click 1 on the **Manage Capacity Planning Data** menu.

```
------------------------------------------------------------------
------------ IBM Hyper-Scale Manager v1.x.x.x ---------------
------------------------------------------------------------------


Manage Capacity Planning Data
-----------------------------
1) Import Capacity Data
2) Export Capacity Data
3) Reset Capacity Data
4) Exit
Your Selection>1
Put the capacity data file (*.csv) in the (/home/msms/hyperscale/files/upload) folder
Press any key to continue
```

   Note: This screen refers to the way the Standalone menu looks. The Virtual Appliance menu looks slightly different.

2. Select from the available files in the `upload` folder. Press any key. The file is imported.

What to do next

Whenever you generate a new report, the IBM Hyper-Scale Manager unifies the imported data according to the following continuity rules:

- Data of XIV systems that are not managed by both IBM Hyper-Scale Manager instances is no longer tracked.
- Data for XIV systems that were already tracked by both IBM Hyper-Scale Manager instances will be overridden, in order to avoid duplicates.
- Data for systems that are currently tracked and whose data was not imported remains unchanged.

Resetting the raw capacity data

The raw capacity planning data can be reset to allow for collecting it anew.

About this task

In order to clear the XIV system history from irregularities (i.e. machine re-purposing), you can clear the machine history that is collected by the IBM Hyper-Scale Manager and start gathering data from scratch. You can reset the capacity data for a single XIV system, or for all of the systems that are managed by the IBM Hyper-Scale Manager.

Note: The system has to be tracked in order for its data to be reset.

Procedure

1. Click 3 on the **Manage Capacity Planning Data** menu. In the following example, the capacity data for an XIV system called *mn52* is reset.

```
------------------------------------------------------------------
------------ IBM Hyper-Scale Manager v1.x.x.x ---------------
------------------------------------------------------------------

-------------------------07/09/2013 05:48--------------------------



Manage Capacity Planning Data
-----------------------------
1) Import Capacity Data
2) Export Capacity Data
3) Reset Capacity Data
4) Exit
Your Selection>3
Please choose which system(s) capacity data to delete:
 system - system address to delete its capacity data
 --all - delete all systems capacity data
> mn52
Are you sure you want to delete all capacity data for system: mn52? [Y/N] >y
Capacity data was reseted for:   mn52
Press any key to continue
```

2. Press any step to return to the **Manage Capacity Planning Data** menu.

Chapter 6. Multi-tenancy

This section explains how to set up a multi-tenancy environment on your system.

Multi-tenancy allows an XIV system owner to allocate storage resources to several independent administrators with the assurance that one administrator cannot access resources associated with another administrator. This resource allocation is best described as a partitioning of the system's resources to separate administrative domains.

A *domain* is a subset, or partition, of the system's resources. It is a named object to which users, pools, hosts/clusters, targets, etc. may be associated. The domain restricts the resources a user can manage to those associated with the domain.

A domain maintains the user relationships that exist on the XIV system-level (when multi-tenancy is inactive). A *domain administrator* is associated with a domain, and is restricted to performing operations on objects associated with a specific domain:

- A user is created and assigned a role (for example, storage administrator, application administrator, or read-only).
- When assigned to a domain, the user retains his given role, limited to the scope of the domain.
- Access to objects in a domain is restricted up to the point where the defined user role intersects the specified domain access.
- By default, domain administrators cannot access objects that are not associated with their domains.

Creating a domain

This section explains how to create a domain, allocate its system resources, and manage the objects associated with it.

About this task

Follow the steps in this task to create a new domain and update the domain attributes. From the **Create Domain** window, you can associate users and resources to the domain.

Procedure

1. Select **Actions** > **Create Domain**. The **Create Domain** window is displayed:

Figure 38. Create Domain window

2. Click the tabs on the left of the window to define the properties of the domain, manage users, and user group associations, as well as the hosts, clusters, targets, and pools.

   Note: Suggested values appear throughout the domain creation options.
3. Click **Create** to complete the domain configuration.

Setting the domain access policy

This section explains how to set the Domain access policy to allow Global domain administrators to manage the domain's resources.

About this task

Note: Only a Security Administrator can set the domain access policy.

The default for accessing a domain's resources is *open*. To restrict a Global domain administrator from accessing the domain resources, the domain access policy must be set to *closed*.

Follow the steps below to set the domain access policy:

Procedure

1. Select **Systems** > **System Settings** > **System**. The **Settings** window is displayed.
2. Click on the **Parameters** tab:

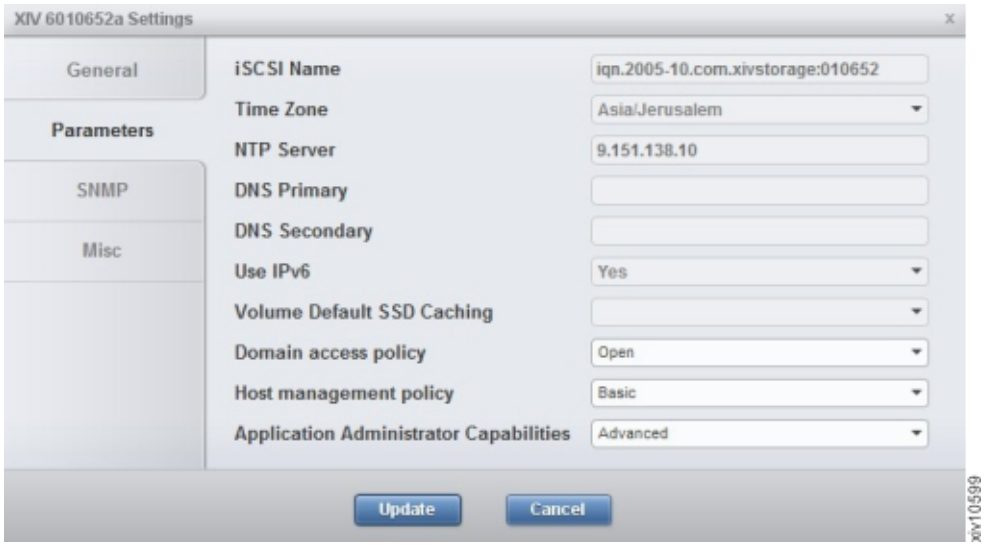


Figure 39. Setting the Domain access policy

3. In the **Domain access policy** field, select **Open** or **Closed** from the dropdown list.
4. Click **Update** to save the changes and close the window.

Chapter 7. Multi-site mirroring

The IBM XIV Storage Management GUI supports extending of an existing 2-way mirroring relation (synchronous or asynchronous) to a 3-way mirroring relation.

Creating a multi-site mirroring relation involves creating mirroring relations between each pair of volumes.

Defining a multi-site mirror

To establish a multi-site mirroring relation, two pairs of mirroring relations must first be created, and then defined as a multi-site mirroring relation.

About this task

This tasks explains how to create a 3-way mirroring relation from a 2-way mirroring relation.

Procedure

1. Right-click on a mirrored volume and select **Convert to 3-way**. If the mirroring relation has the source and target connectivity (or at least its definitions) in place between all of the systems, then the following window is displayed:

Figure 40. Converting to 3-way Mirror (when the mirror relation connectivity is in place)

   If the mirroring relation connectivity is not defined, then the following window is displayed:

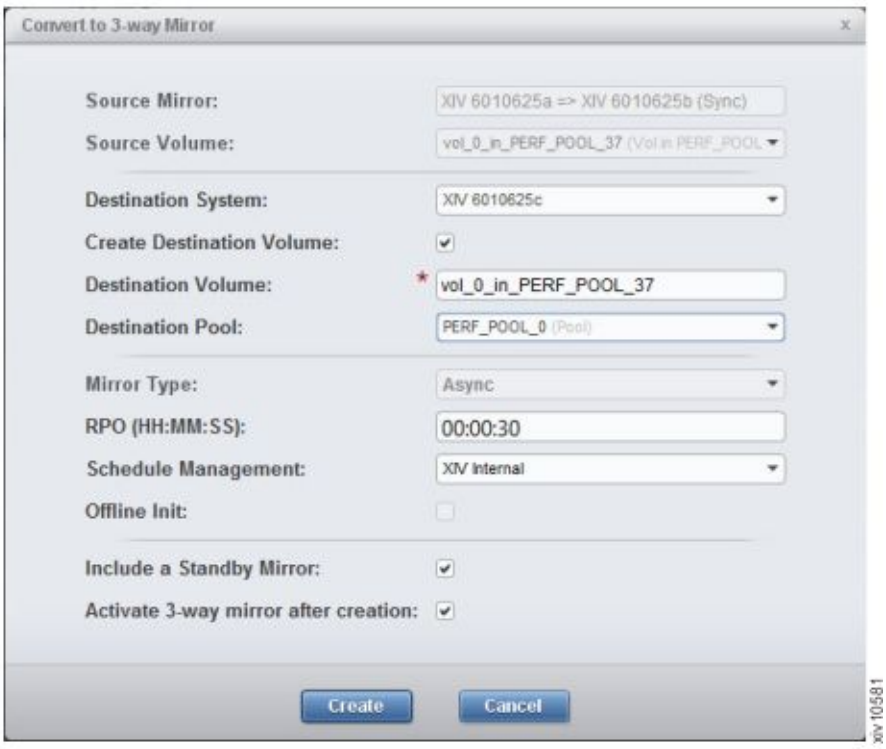


Figure 41. Convert to 3-way Mirror definition window

2. Complete the mirroring details. Select **Display Standby Mirror** to add the third asynchronous mirror of the multi-site mirroring definition. The Standby mirror becomes operational only by request, in case of disaster recovery.
3. Click **OK** or **Create**.

What to do next

If you haven't previously defined a Standby Mirror, you can do so now.

Defining a standby mirror

The standby mirror is the third mirror of the multi-site mirroring definition.

About this task

Defining the standby mirroring relation, in advance, requires that the target connectivity between B and C (or at least its definitions) needs to be in place between all systems when the multi-site mirroring relation is configured.

The mirroring relation that comprises the B-C mirroring relation can be either of the following types:

- Standby mirror - the third mirror of the multi-site mirroring definition, which is defined in advance
- Live mirror - an operational mirroring relation, which becomes operational only by request in case of disaster recovery

If there is no standby mirror defined in advance, you can add a standby mirror at a later time:

Procedure

1. Right-click on a 3-way mirrored volume.
2. From the menu, select **Add Standby Mirror**. An additional row displaying the standby mirror as inactive is added to the mirroring view.

Reverting from a 3-way to 2-way mirror relation

This tasks explains how to revert from a 3-way mirroring relation to a 2-way mirroring relation.

Procedure

1. Right-click on a 3-way mirroring relation.
2. Select **Revert to 2-way** from the menu. The **Revert to 2-way Mirror** window displays the following information:

Figure 42. Revert to 2-way Mirror window

3. Select the mirroring relation to keep from the dropdown list and click **OK**. The selected mirroring relation is kept and the others are deleted.

Chapter 8. XIV Mobile Notification Service configuration

The XIV Mobile Notification Service allows Storage Administrators to receive push notifications about major or critical events in XIV systems straight to a mobile device.

Initial registration for push notifications occurs automatically when a mobile user installs the XIV Mobile Dashboard application and logs in from the mobile device. When new events occur that are relevant to a mobile user, the notification is pushed to the registered mobile client. By default, major and critical issues are sent in *preview only* mode.

From the XIV GUI, a user who is a Storage Administrator can change user preferences.

Figure 43. Access to Mobile Notifications configuration

The Storage Administrator can configure Notification Previews to entail informative event descriptions, as well as set the minimum severity level (critical or major) of the XIV system even that the user receives. The subscription to the push service is on a user-system basis. That is, each XIV system is subscribed to separately.

From the mobile device, the user controls whether or not to receive notifications from all of the XIV systems in the mobile system list. On an iOS platform, after installing and logging in to the mobile application for the first time, a confirmation to accept push notifications appears. Once the user confirms, push notifications for relevant events will be sent to the mobile application. On an Android platform, users are automatically enabled for notifications. These device system settings can be modified at any time.

The XIV Mobile Dashboard runs without any interference to the other device system resources, such as battery and data plan.

User permissions and status are managed from the XIV GUI:

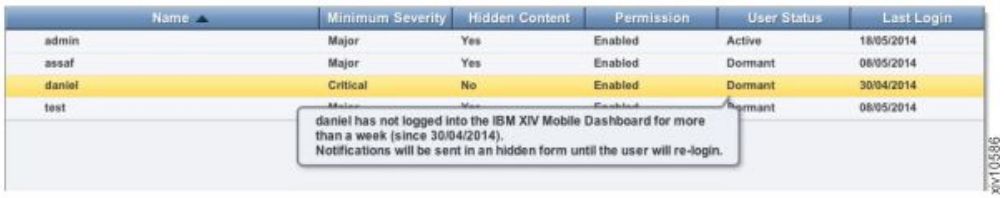


Figure 44. Mobile notifications window

The following permissions are assigned by the Storage Administrator:

Enable
User receives push notifications.

Disable
User does not receive user notifications.

The following user status is according to the last time the user logged in to the system:

Active user
An *active* user receives notifications based on the defined preferences.

Dormant user
If a user has not used the service for over a week, the service is considered to be *dormant*. In this case, the user receives push notifications, but with no content, regardless of the defined preferences.

Non-active user
If a user has not logged in for more than 30 days, the user subscription is considered *inactive* and the user will not receive push notifications.

Logging out from the XIV Mobile application disables push notifications. Notifications can also be disabled from the Settings window of the mobile device. If you want to removed a mobile user from the push notifications list, the user needs to be removed from the XIV system first . Once removed, the user can be unsubscribed.

Troubleshooting Push Notifications

If you are having trouble receiving push notifications, the following steps might help you identify and resolve the problem.

1. From the XIV GUI Mobile Notifications screen, ensure the user permission is set to **Enabled**.
2. From the XIV Mobile Dashboard Settings panel, make sure *Auto-login* and *Notifications* are both set to *on*.
3. Ensure the system time and timezone are set correctly.
4. Ensure that the XIV system is properly configured to send events to the XIV Service Center.
5. Turn off the WiFi on your mobile device. Some corporate networks block the ports used by Android and/or iOS to receive push notifications. If this is the case, refer to the Android/iOS documentation to configure the appropriate ports.
6. Ensure you have Administrator permissions on the system. For multi-tenant systems, you must be a Global Administrator and the system **Domain access policy** must be set to *Open*. See “Setting the domain access policy” on page 50.

Chapter 9. Multi-system configuration

Multi-system configuration allows to change the configuration on mass of XIV systems within a single click.

Before you begin

Multi-system configuration is available for:

- LDAP configuration
- Support parameters
- Pool alert thresholds
- Event rules configuration
- Key server configuration (for SED enabled XIV systems)
- Adding and editing users and user groups
- Adding and editing hosts, clusters and host ports

About this task

- Multi-system configuration can be run on GUI in Manager mode as well as in Direct mode.
- Multi-system configuration requires access rights to all involved GUI systems.

Procedure

Launch mass configuration in either of the following ways:

- Change the configuration on selected systems. This applies for all operations (add, edit, change password).
- Copy the configuration and paste it from one system to the specifically selected systems.

What to do next

Proceed with either of the following tasks:

- "Multi system configuration of user-related information" on page 66
  - "Adding a user on multiple systems" on page 66
  - "Editing, deleting or changing the password of a user" on page 67
- "Mass configuration copy-pasting"

Mass configuration copy-pasting

The system configuration of one system can be copied and pasted to multiple XIV systems.

About this task

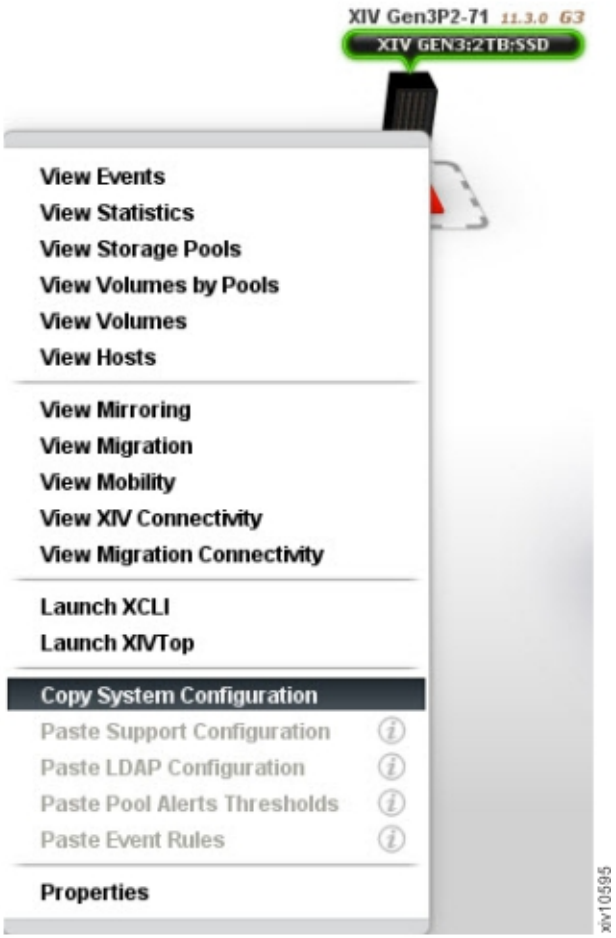
The following configurations can be copied from one system to another:

- Support configuration
- LDAP configuration
- Pool alerts threshold

- Event rules configuration
- Key server configuration

Procedure

1. From the XIV GUI, right-click a system and select **Copy System Configuration** from the popup menu.



   This system configuration is now copied to the memory and the popup menu closes.
2. Select systems to which to copy the configuration. Right-click a system, or several systems, and select the respective **Paste** option. In this example, **Paste Support Configuration** should be selected.

The **Multi-System Configuration of Support information** window opens.

Note: A grayed-out menu option means that the option is not available. Hover over the option to display a tooltip explaining the reason. In this example, the **Paste LDAP Configuration** is grayed-out and the tooltip shows that the target system's version is not compatible with the source system.

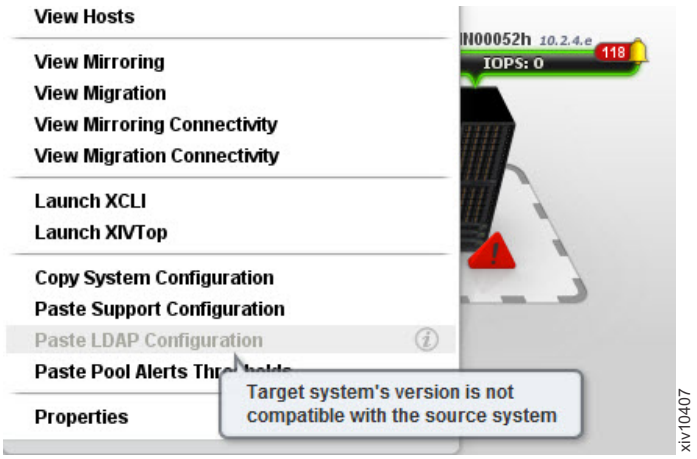


Figure 45. Grayed-out paste option

3. Click **Start**.

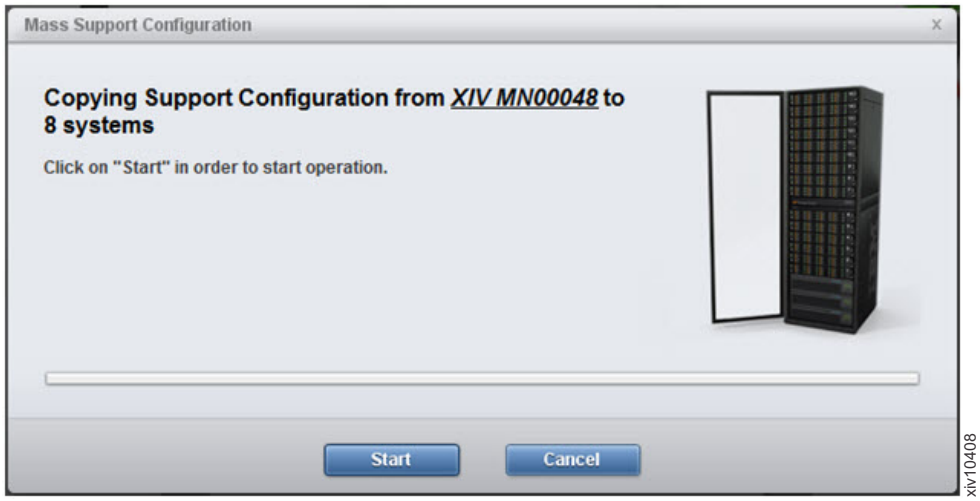


Figure 46. Mass Support configuration window

A progress bar is displayed on screen. Clicking **Cancel** right after clicking Start and during the preparation phase stops the multi-system configuration. When the copy operation is done, a summary of the results is displayedn. Click **Show Results** to display a detailed report.

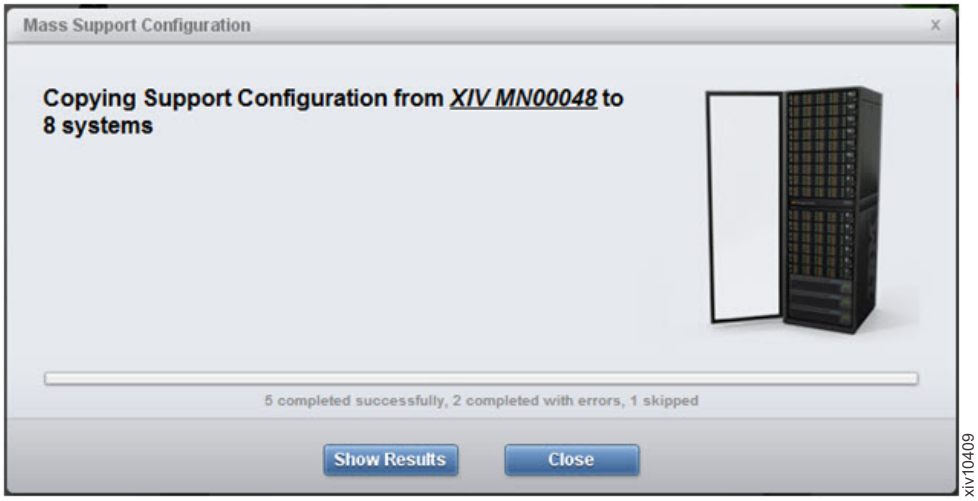


Figure 47. Displayed results of mass configuration

Results

Following this task, the configuration of one system was deployed on other systems.

Multi-System Configuration does not stop on error
Mass Configuration does not stop on error, means it tries to configure all systems although some may fail.

Closing the GUI amidst the paste operation
Closing the GUI amidst the operation disconnects the GUI view from the operation, that keeps proceeding on the server (in manager mode). In direct mode, the operation terminates.

In such a case, it is advised to go over the systems and see what has already been properly configured and what still needs to be configured.

Managing hosts and clusters

Adding a cluster

You may add a cluster to multiple XIV systems at once.

Procedure

1. Select the systems you would like to add a cluster to by clicking them in the System Selector, or by clicking a group of systems.

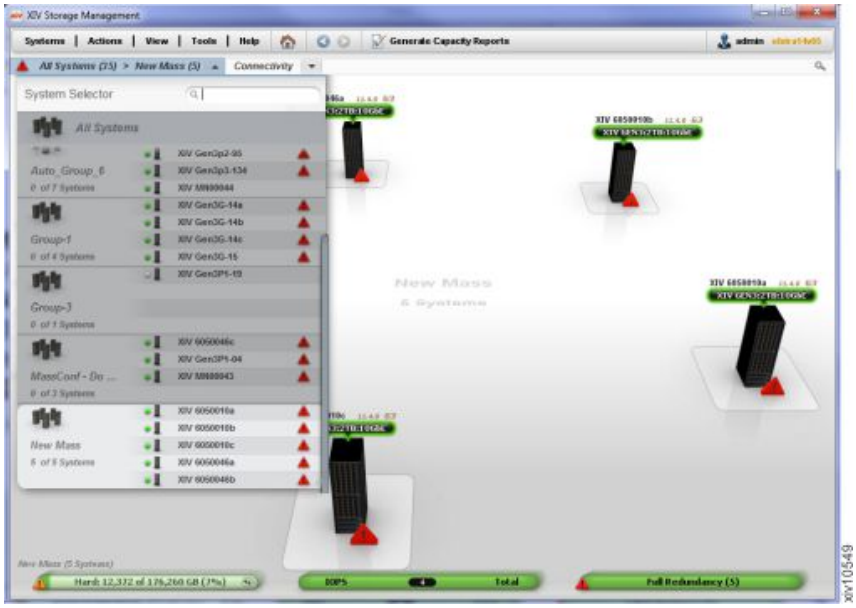


Figure 48. The System Selector

2. Select **Actions > Add Cluster** from the menu. The **Add Cluster** window opens. The systems that were selected on the System Selector are already displayed on the **System** field.

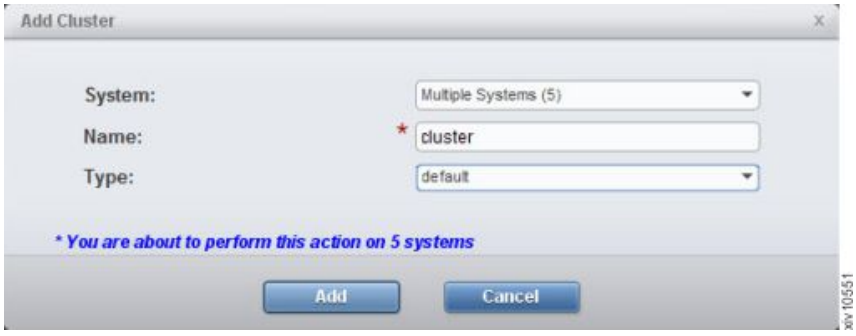


Figure 49. The Add Cluster window

3. Enter the cluster's name and type. Click **Add**.
4. A progress bar is displayed in the window. Clicking **Cancel** at this stage will cancel the mass configuration. When the **Add** operation is complete, a

summary of the results is displayed. Clicking the **Show Results** button displays a detailed report:

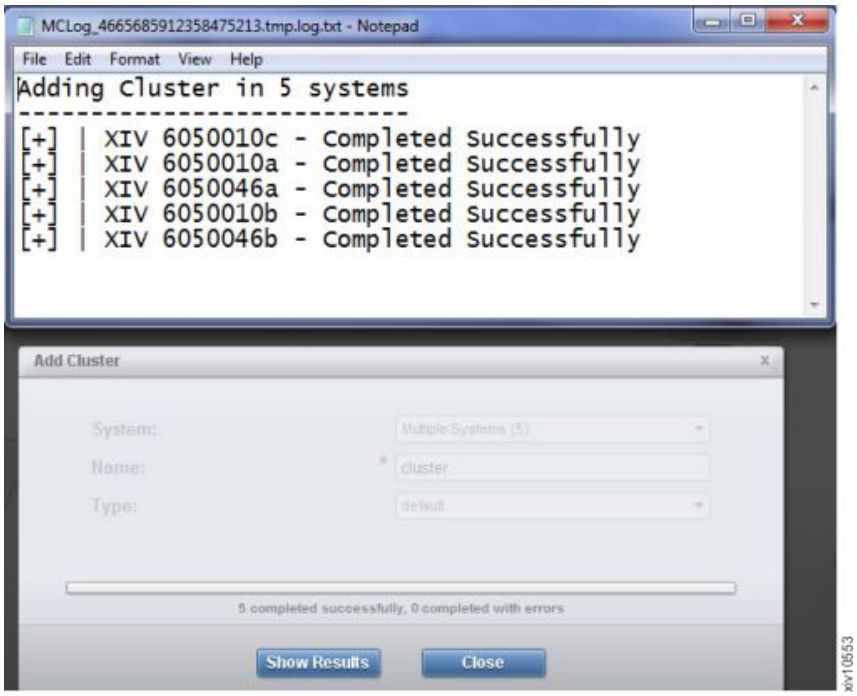


Figure 50. Results summary

Results

Following this task, the cluster was added to the selected systems.

Mass Configuration does not stop on error
The Mass Configuration operation is performed in its entirety on all of the selected systems, even though it might fail on some systems.

Closing the GUI amidst the paste operation
Closing the GUI amidst the operation disconnects the GUI view from the operation, but proceeds on the server (in manager mode). In direct mode, the operation terminates.

In such a case, it is recommended to review the systems to see what has been properly configured and what still needs to be configured.

Editing properties of a cluster

You may edit the properties of a cluster that belongs to multiple XIV systems.

Procedure

1. In the GUI, select **View > Hosts and Clusters > Clusters** from the menu.
2. Right-click a Cluster and select **Edit** from the popup menu. The **Edit Cluster** window is displayed.

Figure 51. The Edit Cluster window

3. From this window, you can rename the cluster and change its type. Click **Update**.

Results

The cluster properties have been edited on the selected systems.

Mass Configuration does not stop on error
The Mass Configuration operation is performed in its entirety on all of the selected systems, even though it might fail on some systems.

Closing the GUI amidst the paste operation
Closing the GUI amidst the operation disconnects the GUI view from the operation, but proceeds on the server (in manager mode). In direct mode, the operation terminates.

In such a case, it is recommended to review the systems to see what has been properly configured and what still needs to be configured.

Adding a host

You may add a host to multiple XIV systems at once. The host can belong to a cluster but does not have to.

Procedure

1. Select the systems you would like to add a host to by clicking them in the System Selector, or by clicking a group of systems.
2. Select **Actions > Add Host** from the menu. The **Add Host** screen opens. The systems that were selected on the System Selector are already displayed on the **System** field.
3. Select whether the host belongs to a Cluster, enter the host's name. You may also select CHAP name and secret. Click **Add**.
4. A progress bar is displayed on screen. Clicking **Cancel** at this stage will cancel the mass configuration. When the **Add** operation is complete, a summary of the results is displayed on screen. Clicking the **Show Results** button opens a detailed report on screen.

Results

Following this task, the host was added to the selected systems.

Mass Configuration does not stop on error
The Mass Configuration operation is performed in its entirety on all of the selected systems, even though it might fail on some systems.

Closing the GUI amidst the paste operation

Closing the GUI amidst the operation disconnects the GUI view from the operation, but proceeds on the server (in manager mode). In direct mode, the operation terminates.

In such a case, it is recommended to review the systems to see what has been properly configured and what still needs to be configured.

Editing a host

You may edit a host that belongs to multiple XIV systems.

Procedure

1. On the GUI, open **View > Hosts and Clusters > Hosts** from the menu.
2. Right-click a host and select Edit from the pop-up menu. The **Edit Host** screen opens.
3. On this screen, you may rename the host and change its type, CHAP name and CHAP secret. Click **Update**.

   Note: You can't add the host to a cluster from this screen.

Results

Following this task, the host was edited for the selected systems.

Mass Configuration does not stop on error

The Mass Configuration operation is performed in its entirety on all of the selected systems, even though it might fail on some systems.

Closing the GUI amidst the paste operation

Closing the GUI amidst the operation disconnects the GUI view from the operation, but proceeds on the server (in manager mode). In direct mode, the operation terminates.

In such a case, it is recommended to review the systems to see what has been properly configured and what still needs to be configured.

Multi system configuration of user-related information

You may configure user-related information on multiple XIV systems at once.

About this task

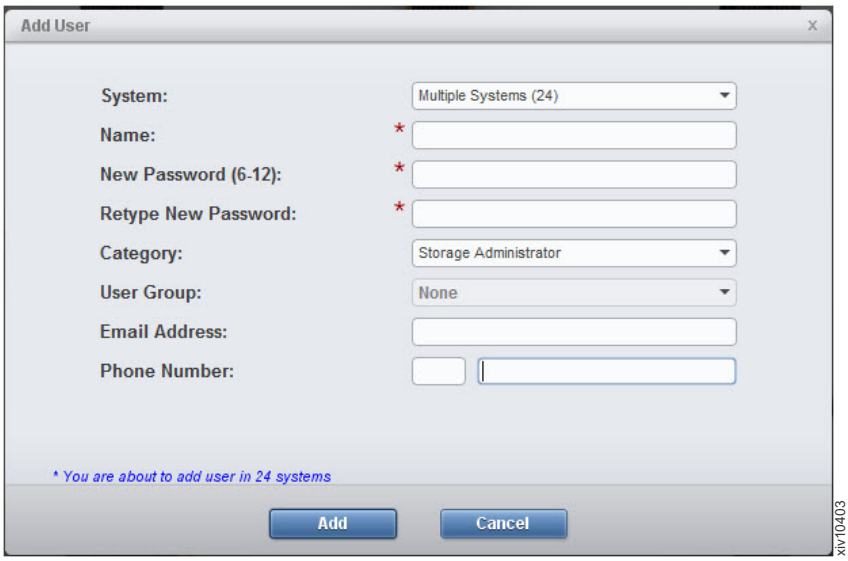
This task describes how to configure user-related information on multiple XIV systems at once.

Adding a user on multiple systems

You may add a user on multiple XIV systems at once.

Procedure

1. Select the systems you would like to configure and click **Add User**. The **Add User** screen opens.
2. Enter the user's name, password and other details as displayed on the screen. Click **Add**.



The new user is added to the selected systems.

3. A progress bar is displayed on screen. Clicking **Cancel** at this stage will cancel the mass configuration. When the **Add** operation is complete, a summary of the results is displayed on screen. Clicking the **Show Results** button opens a detailed report on screen.

Results

Following this task, the user was added to the selected systems.

Mass Configuration does not stop on error
The Mass Configuration operation is performed in its entirety on all of the selected systems, even though it might fail on some systems.

Closing the GUI amidst the paste operation
Closing the GUI amidst the operation disconnects the GUI view from the operation, but proceeds on the server (in manager mode). In direct mode, the operation terminates.

In such a case, it is recommended to review the systems to see what has been properly configured and what still needs to be configured.

Editing, deleting or changing the password of a user

You may edit or delete a user, as well as change the password on multiple XIV systems at once.

Procedure

1. On the GUI, mouse-over the **Access** icon and click on **Users**. The **Users** view opens on screen.
2. Select the systems that will be displayed on this view.
3. Use the CTRL key to multiple select the users to be edited.

   Note: Mass editing of users can be applied only to users with the same user name.
4. Right-click the users selection and select **Edit**, **Delete** or **Change password**.

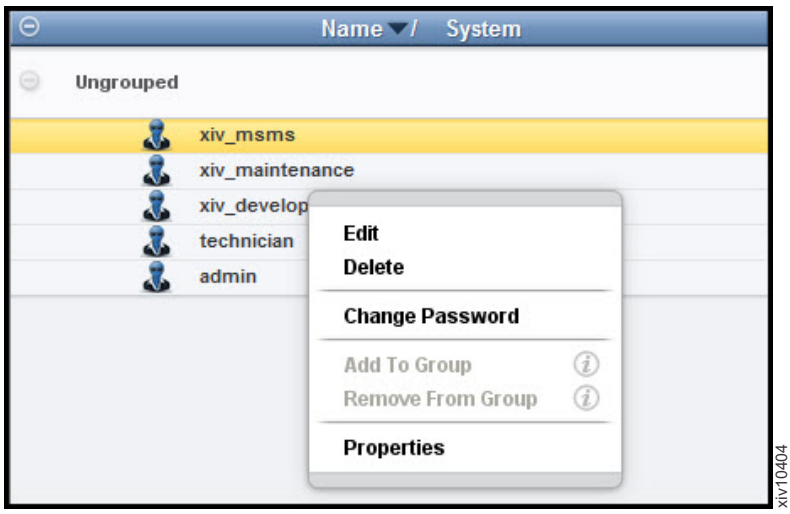


Figure 52. Right-clicking the user selection

- **Delete** – displays the progress of the deletion.
- **Edit** or **Change Password** – displays a dialog. Edit the details or password and click **Update**.
  - A progress bar is displayed on screen. Clicking **Cancel** at this stage cancels the mass configuration. When the operation is done, a summary of the results is displayed. Clicking the **Show Results** button opens a detailed report.

Note: The availability of the edit, delete and change password configuration options is subject to your access rights.

Results

Following this task, the user is edited to the selected systems.

Mass Configuration does not stop on error
The Mass Configuration operation is performed in its entirety on all of the selected systems, even though it might fail on some systems.

Closing the GUI amidst the paste operation
Closing the GUI amidst the operation disconnects the GUI view from the operation, but proceeds on the server (in manager mode). In direct mode, the operation terminates.

In such a case, it is recommended to review the systems to see what has been properly configured and what still needs to be configured.

Editing the user's access control rights

You may grant a user with access control to XIV systems and to hosts.

About this task

This action is not available for multiple users or multiple user groups.

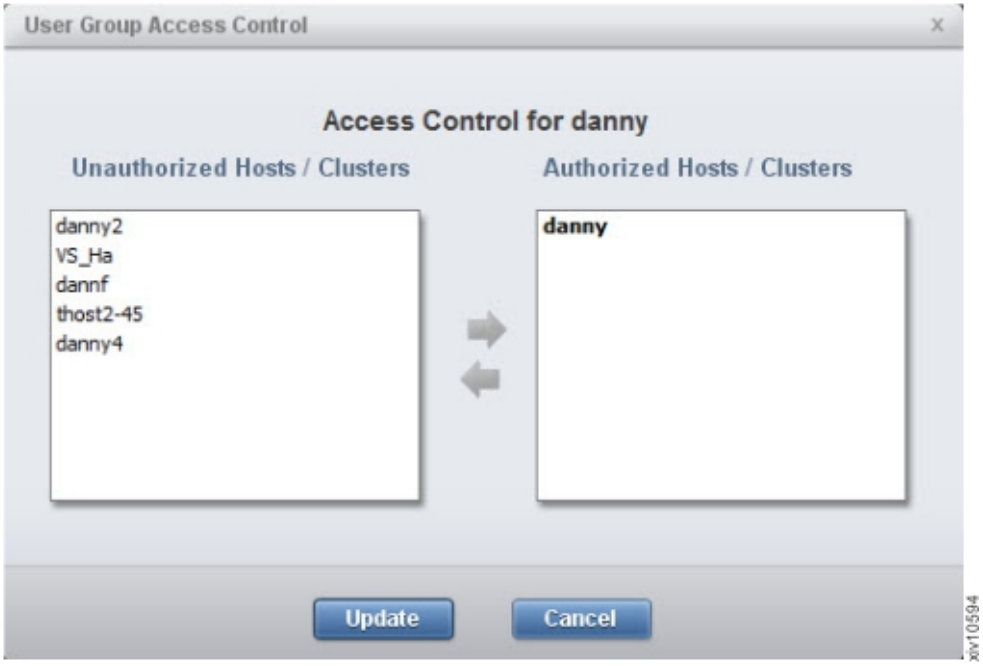
Procedure

1. On the GUI, mouse-over the **Access** icon and click on **Users**. The **Users** view opens on screen.

2. Select the systems to display in this view.
3. Use the <CTRL> key to select multiple users to be edited.

   Note: Mass editing of users can be applied only to users with the same user name.
4. Right-click the users selection and select **Update Access Control**.
   User Group Access Control screen opens.

   Note: The availability of the **Update Access Control** option depends on the users you select.
5. Move hosts and clusters from the **Unauthorized** pane to the **Authorized** pane and click **Update**.



Results

The access control rights for the selected users are changed.

Mass Configuration does not stop on error
The Mass Configuration operation is performed in its entirety on all of the selected systems, even though it might fail on some systems.

Closing the GUI amidst the paste operation

Closing the GUI amidst the operation disconnects the GUI view from the operation, but proceeds on the server (in manager mode). In direct mode, the operation terminates.

In such a case, it is recommended to review the systems to see what has been properly configured and what still needs to be configured.

Adding and editing a users group

You may add a users group on multiple XIV systems at once.

Procedure

1. Select the systems to configure and click **Add User Group**. The **Add User Group** screen opens.
2. Enter the user group name and other details as displayed on the screen. Click **Add**. The new user is added to the selected systems.
3. A progress bar is displayed in the window. Clicking **Cancel** at this stage will cancel the mass configuration. When the **Add** operation is complete, a summary of the results is displayed. Clicking the **Show Results** button displays a detailed report.

Results

Following this task, the user group was added to the selected systems.

Mass Configuration does not stop on error

The Mass Configuration operation is performed in its entirety on all of the selected systems, even though it might fail on some systems.

Closing the GUI amidst the paste operation

Closing the GUI amidst the operation disconnects the GUI view from the operation, but proceeds on the server (in manager mode). In direct mode, the operation terminates.

In such a case, it is recommended to review the systems to see what has been properly configured and what still needs to be configured.

Chapter 10. Deploying an IBM Spectrum Accelerate System from the XIV GUI

If you are using a Windows deployment host, you can deploy IBM Spectrum Accelerate systems from XIV Management Tools version 4.5 in both direct mode and manager mode (from the **Manager Configuration** window).

Important: IBM Spectrum Accelerate requires certain hardware, software, and configurations of VMware ESXi host machines and vSwitches, interconnect network, and deployment host. Refer to the *IBM Spectrum Accelerate Planning, Deployment, and Operation Guide (SC27-6695)* for further information on deploying IBM Spectrum Accelerate.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Almaden Research
650 Harry Road
Bldg 80, D3-304, Department 277
San Jose, CA 95120-6099
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information website (www.ibm.com/legal/copytrade.shtml).

Adobe, the Adobe logo, and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Other company, product, and service names may be trademarks or service marks of others.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Printed in USA

SC27-5986-03