IBM XIV Storage System
Management Tools
Version 4.3

Operations and Administration Guide

GC27-5986-00

Note
Before using this information and the product it supports, read the information in "Notices" on page 55.

Management Tools Notices

This edition applies to Management Tools version 4, release 3, modification 0 of IBM XIV Storage System 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 4.3.

This set of documents include:

1. IBM® Hyper-Scale Manager User guides
   - User Guide for Virtual Appliance
   - User Guide for installation as application
2. Management Tools 4.3 Operations Guide

Who should use this guide

This document is for storage administrators that manage XIV Systems.

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.

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)

Ordering 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 book or any other IBM XIV® Storage System documentation:

- Go to the feedback form (publib.boulder.ibm.com/infocenter/ibmxiv/r2/topic/com.ibm.xiv.doc/icfeedback.htm) in the IBM XIV Storage System information center. You can use this form to enter and submit comments.
- 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. Introduction

IBM XIV Management Tools introduce the IBM Hyper-Scale Manager that reduces operational complexity and enhances capacity planning through integrated management for large and multi-site 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.

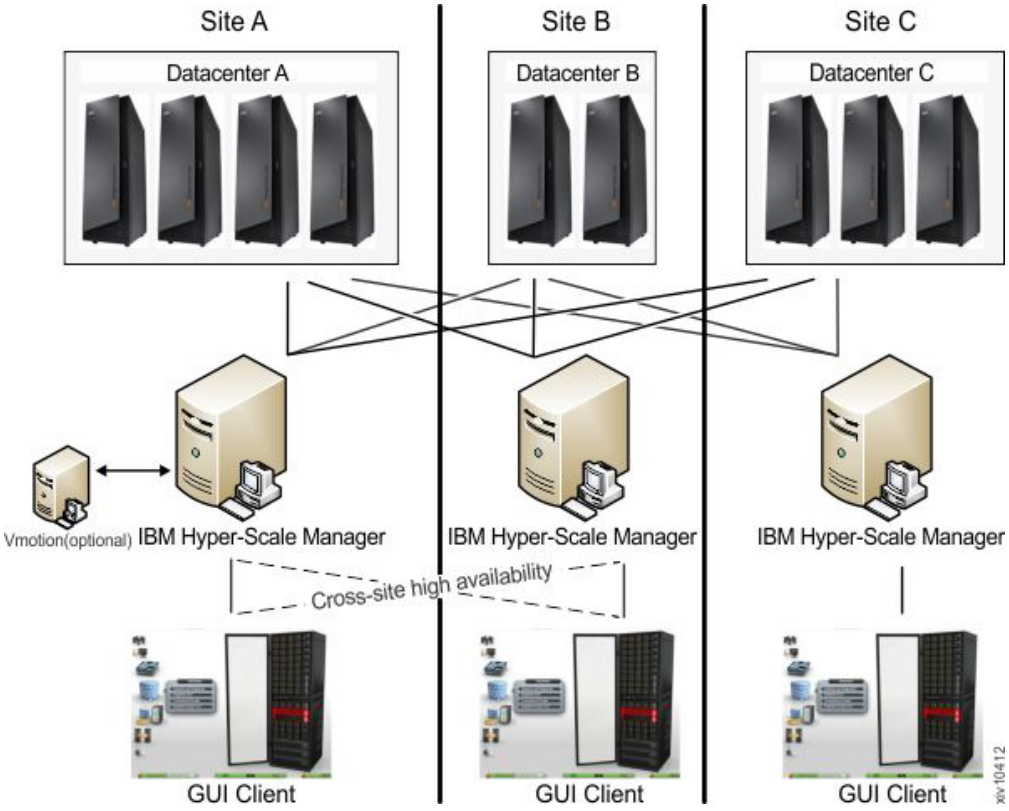


Figure 1. IBM Hyper-Scale Manager

Management Tools documentation set

As of release 4.3, the IBM XIV Management Tools documentation set includes the following publications:

- User guide and quick start guide
  - Installation as virtual appliance
  - Installation as application
- 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 XIV 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
An XIV user that monitors all XIV systems in the IBM Hyper-Scale Manager inventory. This user authenticates into all XIV systems in order to poll configuration data only.

- This user does not change the configuration
- This user's name is hardcoded: *xiv_msms*
- 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.

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 15.

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.

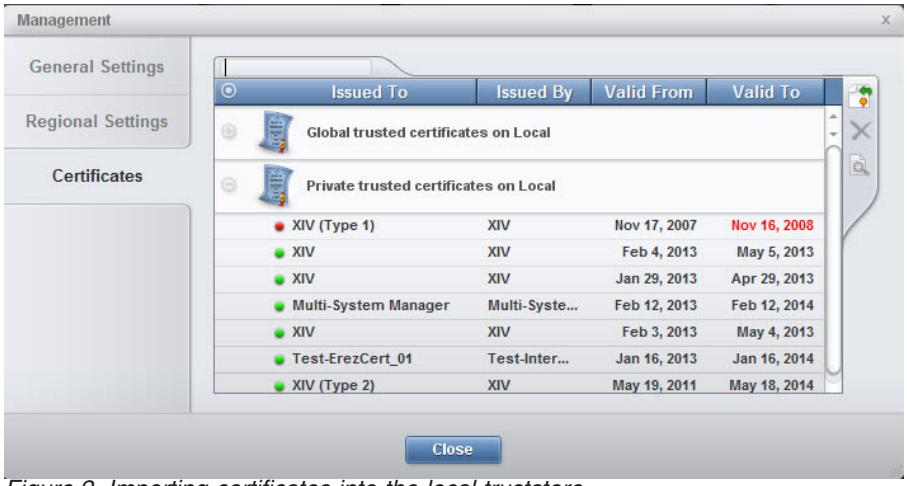


Figure 2. Importing certificates into the local truststore

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** screen 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** screen, 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 pop-up 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.

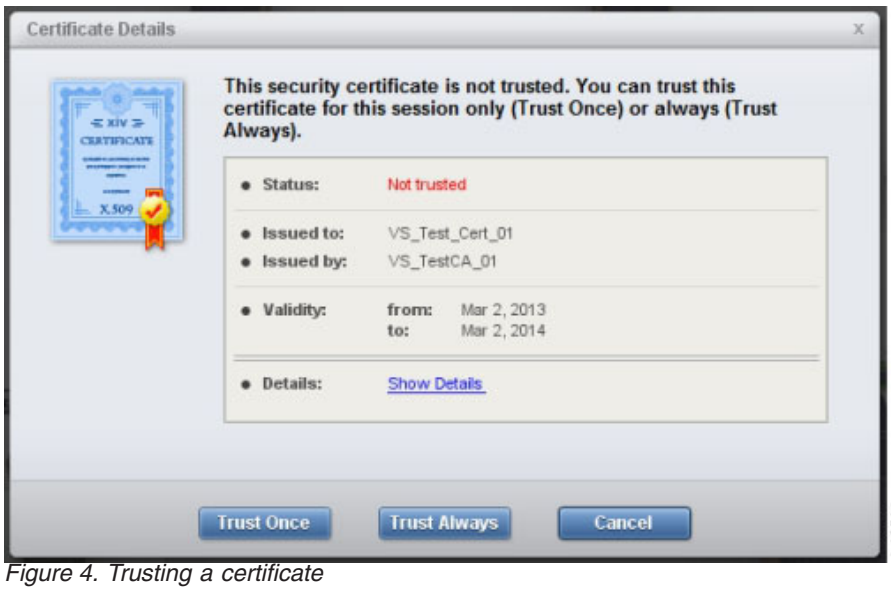


Figure 4. Trusting a certificate

Results

Following the confirmation, all XIV systems that have a Certificate Error status and are using the certificate that is now confirmed will be 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. Open **Systems > Manager Configuration > XIV Certificates (Tab)**.

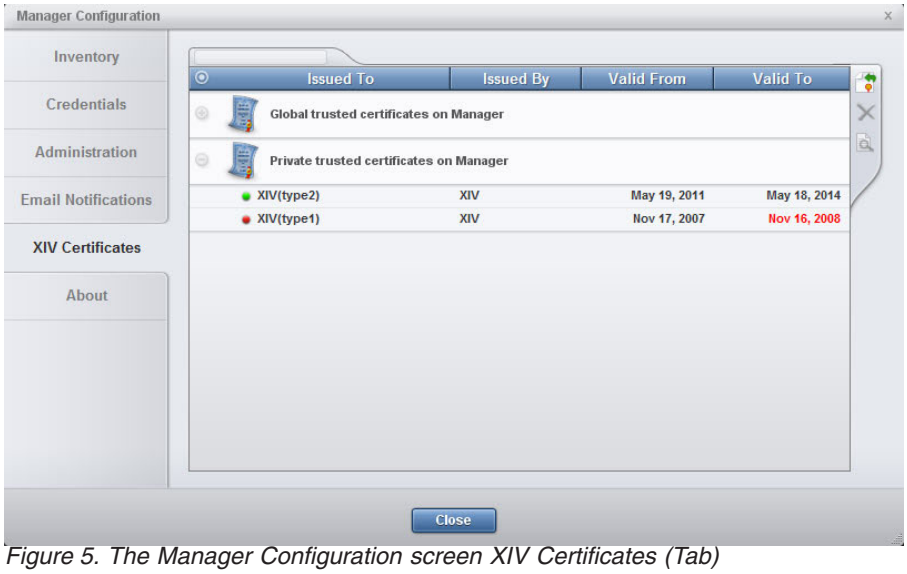


Figure 5. The Manager Configuration screen XIV Certificates (Tab)

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. Open **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 you to view and re-trust certificates on the truststore that is maintained by the IBM Hyper-Scale Manager.

Procedure

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

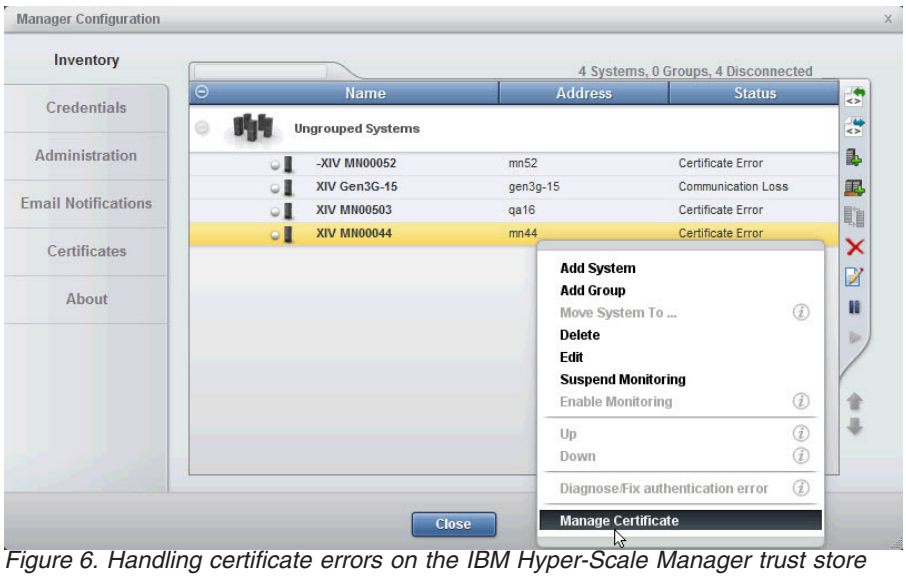


Figure 6. Handling certificate errors on the IBM Hyper-Scale Manager trust store

The certificate opens on screen.

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

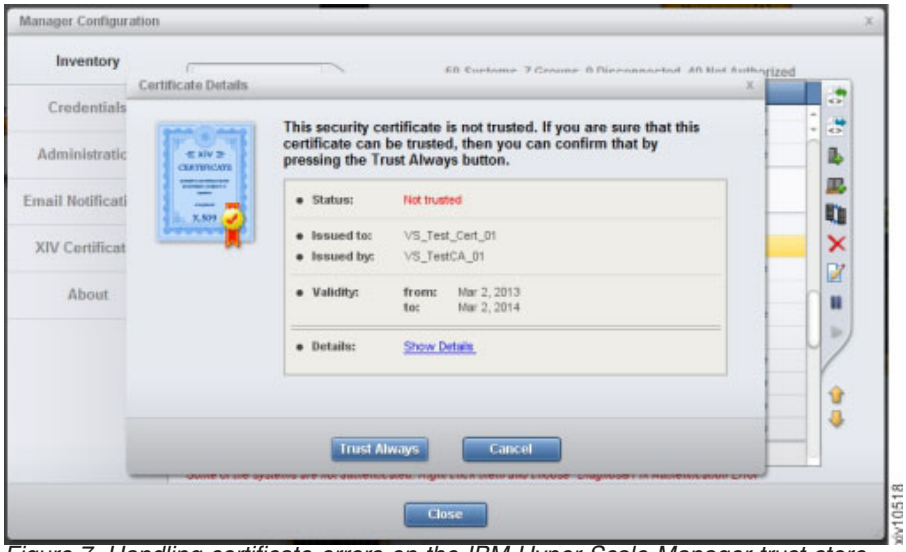


Figure 7. Handling certificate errors on the IBM Hyper-Scale Manager trust store

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.

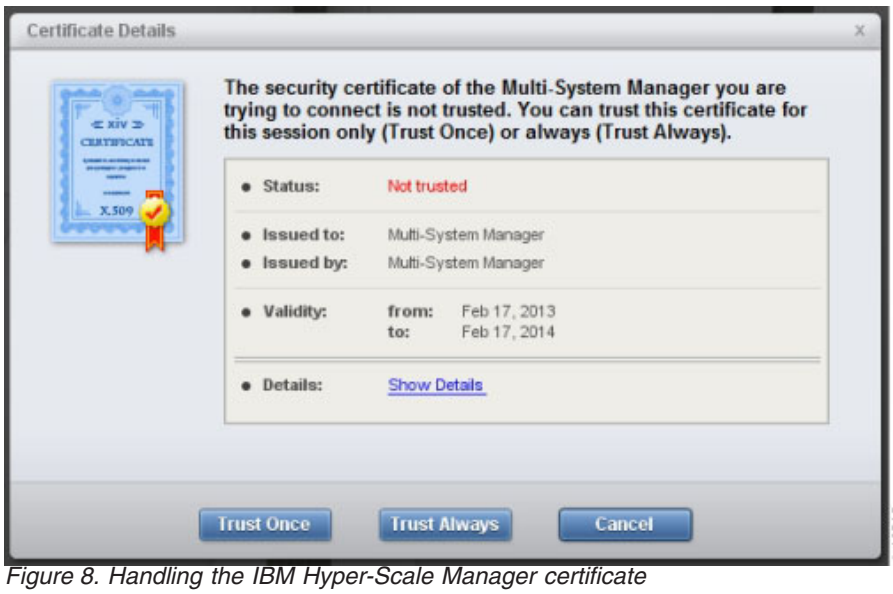


Figure 8. Handling the IBM Hyper-Scale Manager certificate

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

In order 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. Open **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** screen opens.

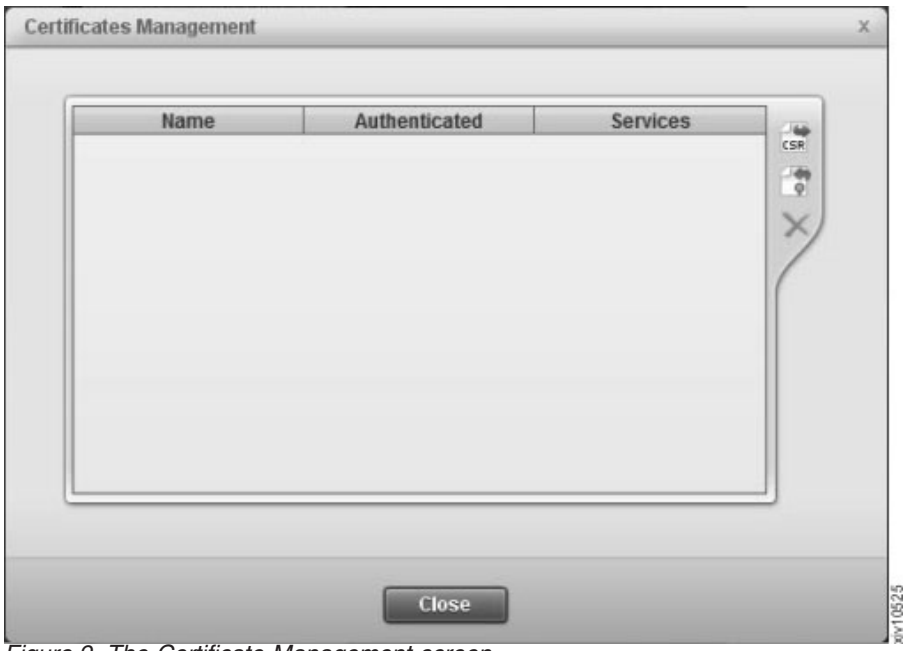


Figure 9. The Certificate Management screen

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

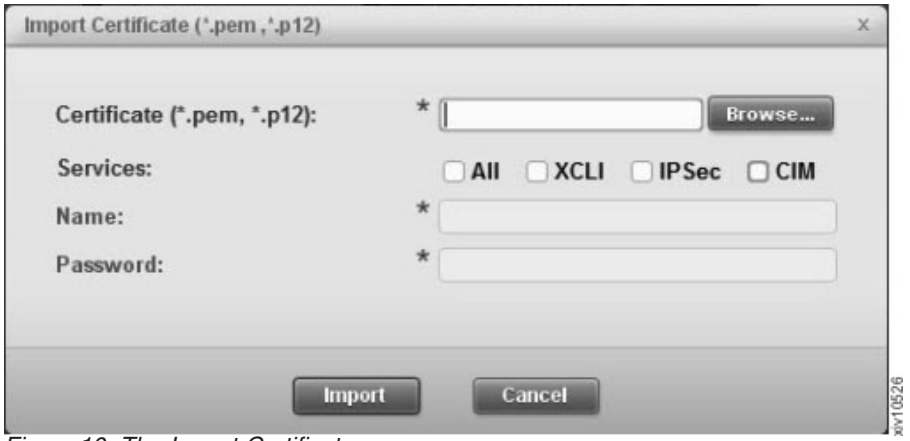


Figure 10. The Import Certificate screen

   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** screen opens.

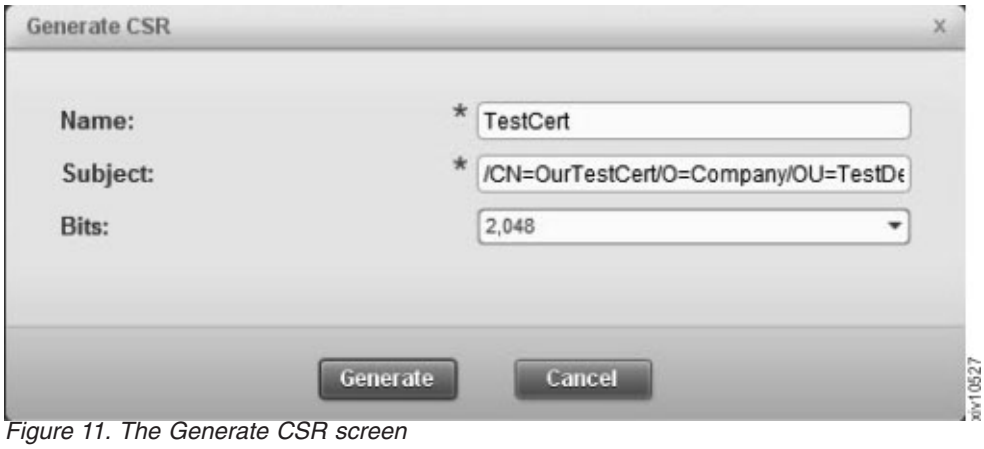


Figure 11. The Generate CSR screen

2. Enter a certificate name. This has to a be 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 the CSR file will be saved to.
6. Open the Certificate Management screen and verify that the newly generated certificate is awaiting authentication. The value of the **Authenticated** field is **No**.

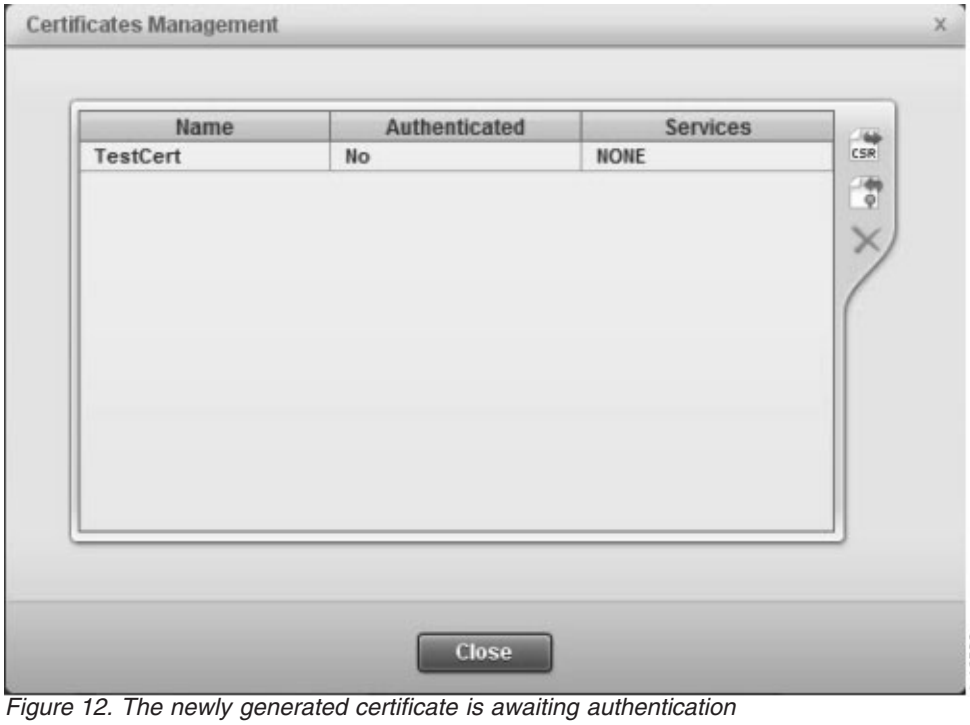


Figure 12. The newly generated certificate is awaiting authentication

What to do next

Proceed to "Importing a signed certificate request."

Importing a signed certificate request

Importing a 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.

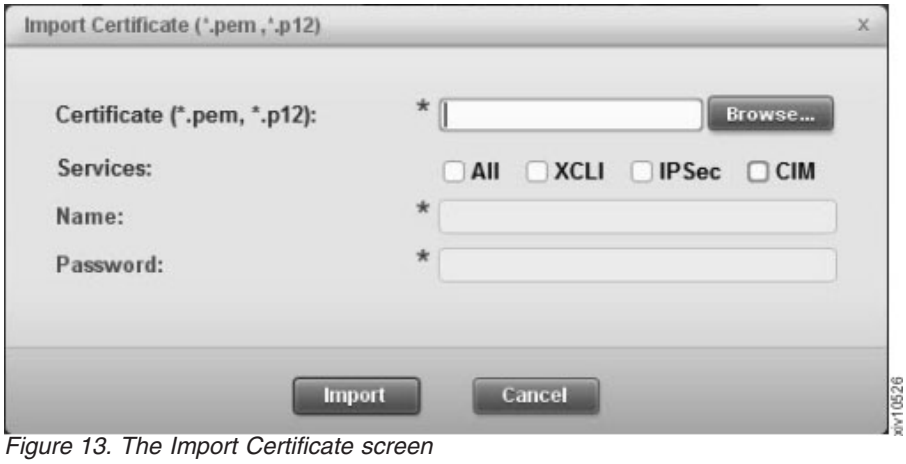


Figure 13. The Import Certificate screen

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. Open **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** screen 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. Open **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** screen 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 generated CSR file into.

Updating a certificate of an XIV system

Both the certificate and the certified services can be updated.

Procedure

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

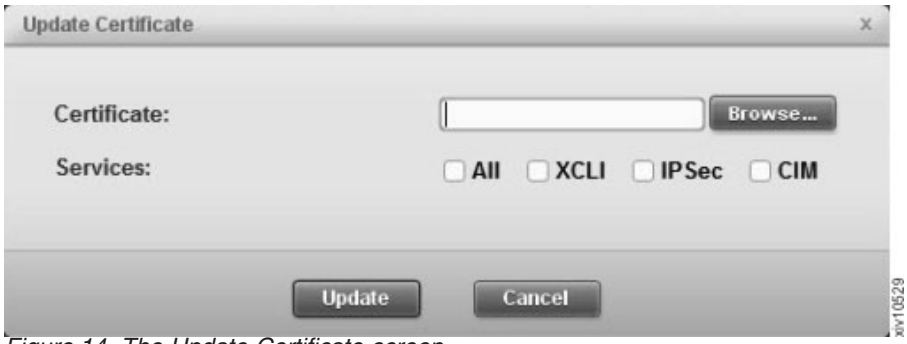


Figure 14. The Update Certificate screen

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. Click **Replace Certificate**.

Figure 16. Replacing the Manager Certificate

   c. Click **Browse** to navigate to a certificate file in *PKCS#12* format. Type the password and click **Import**.
2. 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 18
This task sets up the Tivoli Key Lifecycle Manager to work with the XIV system.

"Defining a security administrator" on page 19
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 21
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 26 - 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 27 - 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 27
- "Generating recovery keys" on page 28 - 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 30 - 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 30 - now that have a recovery key that was dispensed among the security administrators, the encryption can be enabled.
- "Deactivating the encryption" on page 31 - 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 on the next step.

2. Install the Tivoli Key Lifecycle Manager Certificate on the XIV system. See instructions here: "Adding a key server" on page 25.
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 43.
  - 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 admin's user and password.

About this task

This task grants the security admin with access rights to the XIV GUI and to XIV systems that support SED. The rights are granted 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** drop-down list-box, and click **Add**. The new user is displayed on the **Users** table.

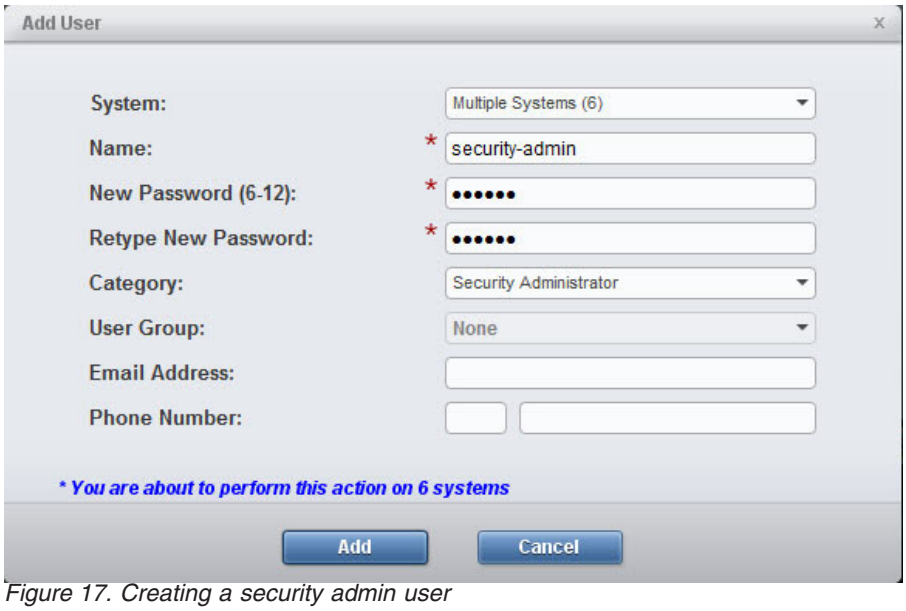


Figure 17. Creating a security admin user

5. Click the user name button on the toolbar in order to re-login with the security admin credentials. Enter the user and password of the security admin 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 admin

Results

- You have a new security admin 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. Open **Systems > System Settings> Manage Certificates** on the XIV GUI menu. The **Certificates Management** screen opens.

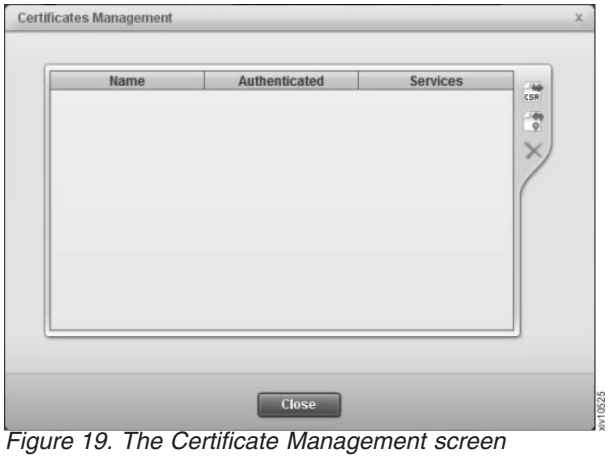


Figure 19. The Certificate Management screen

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

Figure 20. The Import Certificate screen

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**.

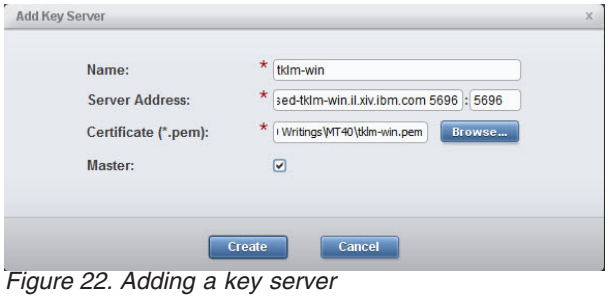


Figure 22. Adding a key server

The key server is added to the table.

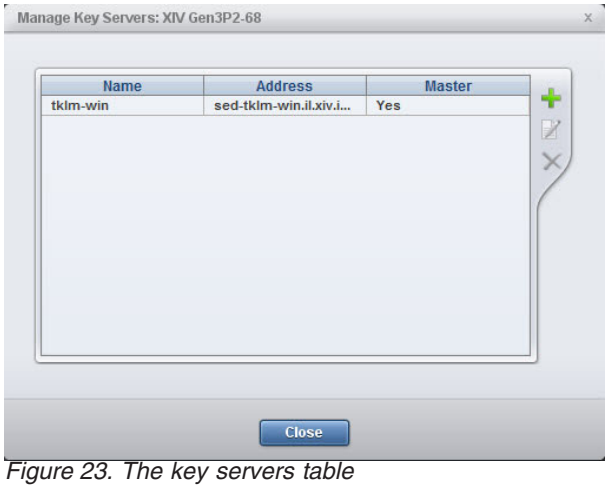


Figure 23. The key servers table

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

- "Editing a key server" on page 26
- "Deleting a key server" on page 27
- "Setting a key server as master" on page 27

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.

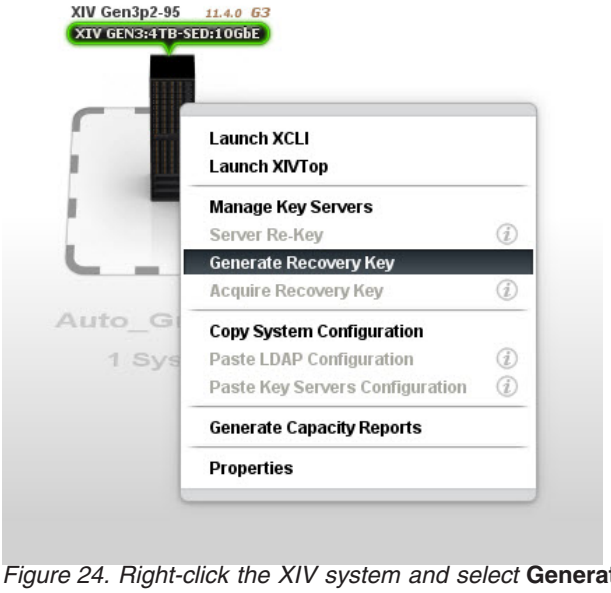


Figure 24. Right-click the XIV system and select **Generate Recovery Key** *from the menu.*

The Generate recovery key screen 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** *screen*

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** screen opens.

   b. The screen 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 screen.

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 screen opens.
   c. 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.
   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 19.
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**.

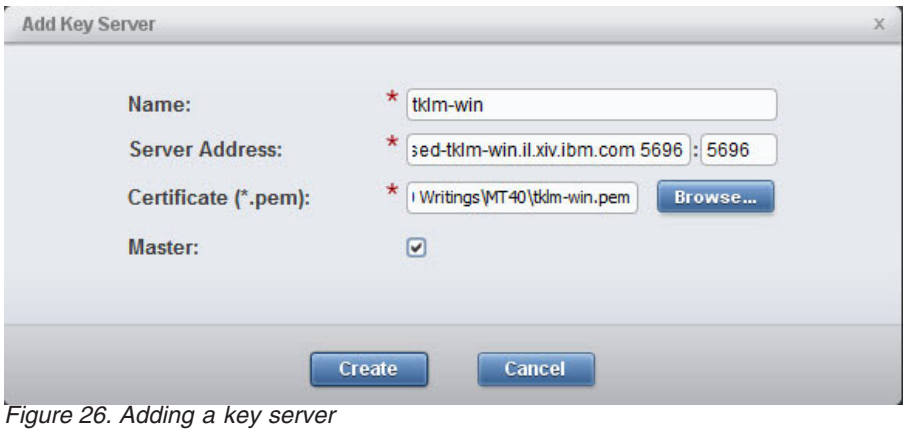


Figure 26. Adding a key server

The key server is added to the table.

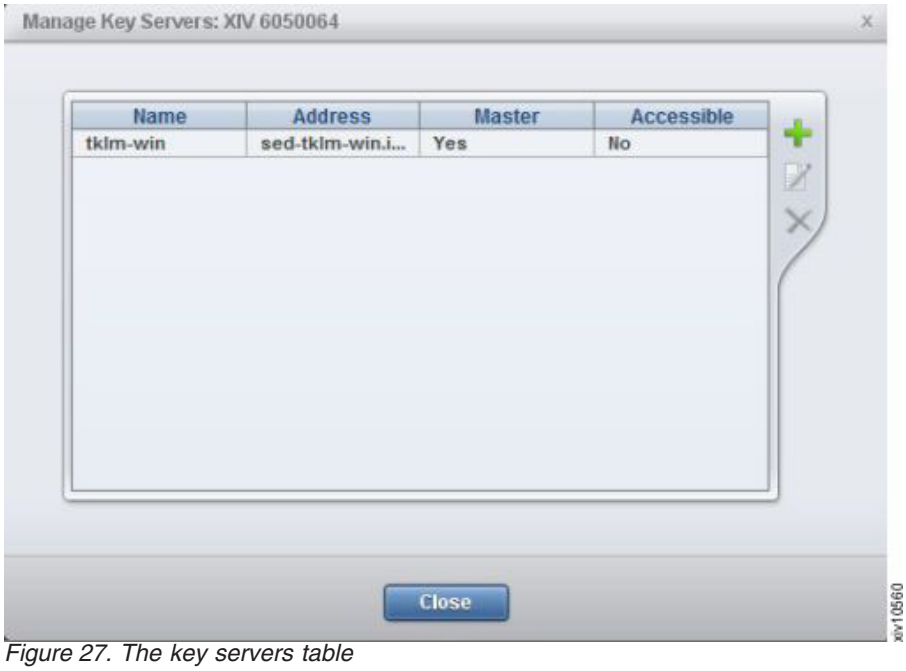


Figure 27. The key servers table

Results

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

- "Editing a key server"
- "Deleting a key server" on page 27
- "Setting a key server as master" on page 27

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 the XIV systems.

Before you begin

1. Log into the XIV system as a security administrator. See instructions here: "Defining a security administrator" on page 19.
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 19.

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. See instructions here: "Defining a security administrator" on page 19.

Procedure

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

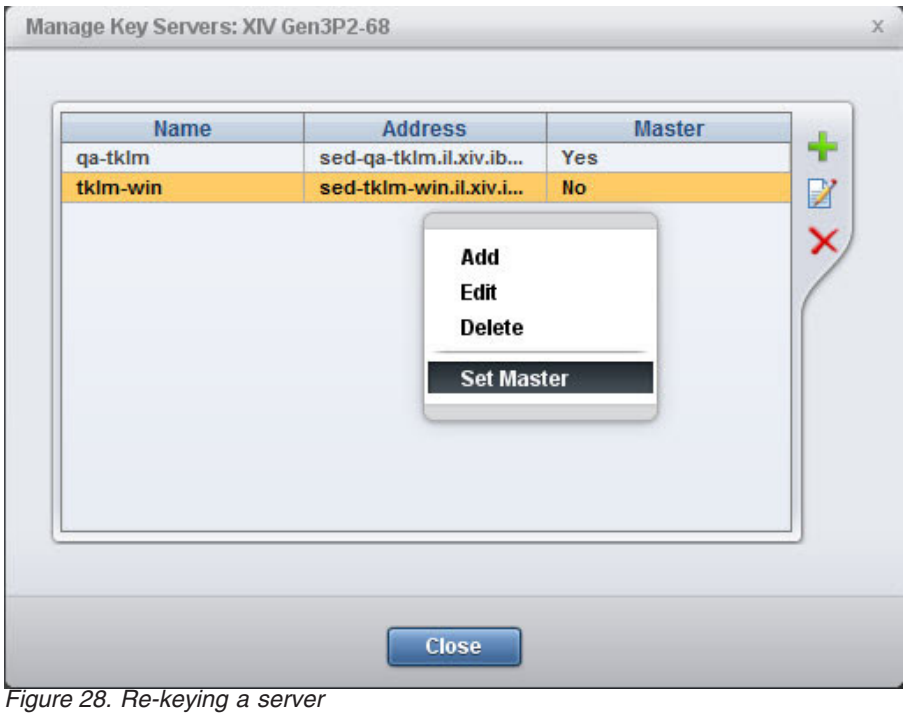


Figure 28. Re-keying a server

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 here: "Adding a key server" on page 25.

About this task

Once the XIV system has security administrators (at least 2) and a key server, you need to generate a recovery key for each security administrator.

Procedure

Repeat the following steps fro 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 in order 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

You must 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** screen opens.
2. The screen 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 on screen.

Results

The key was acquired by the security admin 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. Capacity planning

The IBM Hyper-Scale Manager collects usage statistics and calculates a forecast of the future use of XIV systems and pools. This statistics is 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 in order to maintain continuity of the collected data. This data can also be exported to a CSV file in order 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 file and how to create a graph within a few clicks are provided in this section onward: "Generating a capacity analytics report" on page 34.

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

- "Exporting the raw capacity data" on page 39 - The raw data is exported in order to make it available for import to another IBM Hyper-Scale Manager. The file is exported in the same method other files (i.e. backups, logs and more) are exported.
- "Importing the raw capacity data" on page 39 - A raw capacity data file that was created on one IBM Hyper-Scale Manager and was exported so it can 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 40 - In order to clear the XIV system history from irregularities (i.e. machine re-purposing), and to allow for collecting raw data from scratch, you can clear the machine history from the previously collected raw data.

Collecting usage data for 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 on 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 will be 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 multiple CSV file named `XIV_capacity_report_yyyy-mm-dd_hhmm.<N>.csv`, cut into 65000 lines long files. The files names (both ZIP 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.

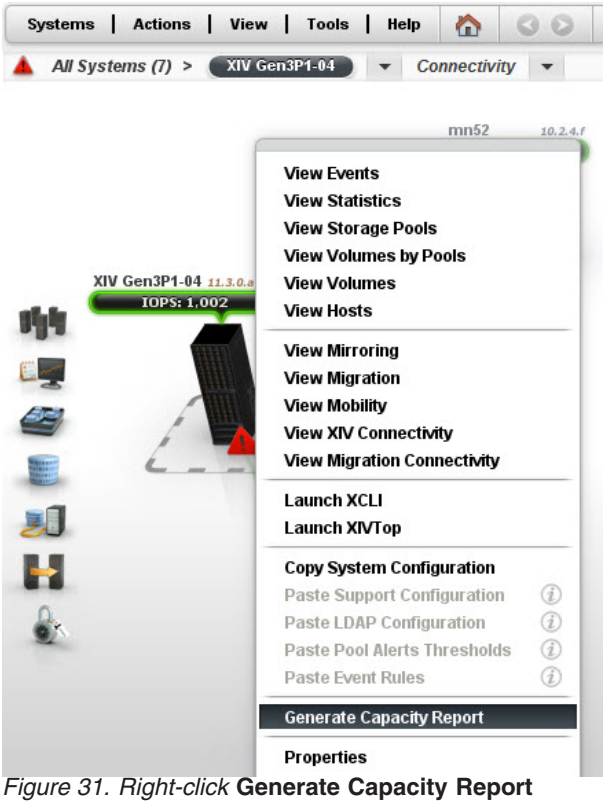


Figure 31. Right-click **Generate Capacity Report**

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 and pools

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
Pools statistics 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.
```

Systems 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
- No. of Volumes
- Usable capacity (GB)
- Allocated capacity (GB)
- Used capacity (GB)
- Unused capacity (GB)
- Unallocated capacity (GB)
- % Used
- % Allocated
- 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 a full list of reasons for not calculating the capacity trend, see here: “Cases in which the forecast is not calculated” on page 36.

Pools 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:

- 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 whom 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.

Pools Detailed Report

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

Cases in which the forecast is not calculated

The capacity data must meet several criteria so the forecast to be calculated.

Capacity forecast is not calculated for the following reasons:

Insufficient access rights

Users with a role other than storage administrator and read-only are not allowed to calculate the capacity forecast. The user must have access rights to all of the XIV systems that are included in the report.

Insufficient number of samples
The first condition that the capacity data is required to meet is enough samples. If this number is below 30, no forecast is calculated.

Utilization is too low
Next, the system, or storage pool, is checked for utilization. In case the utilization is smaller than 10%, no forecast is calculated.

Trend cannot be calculated on pools
Trend cannot be calculated on pools that have no available space for volumes allocation.

No trend
The forecast is calculated for systems, or storage pools, that pass the criteria above. However, the forecast is not displayed if no trend was identified:

Capacity is fluctuating
In case the capacity data is fluctuating, the forecast is not displayed.

Capacity is on a negative slope
In case the capacity utilization is descending, the forecast is not calculated.

Capacity is flat
In case the capacity does not change much, the forecast is not calculated.

Capacity changed too rapidly
If there is a 5% descending capacity between two consecutive measurements, no forecast is calculated.

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													

Figure 32. 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:

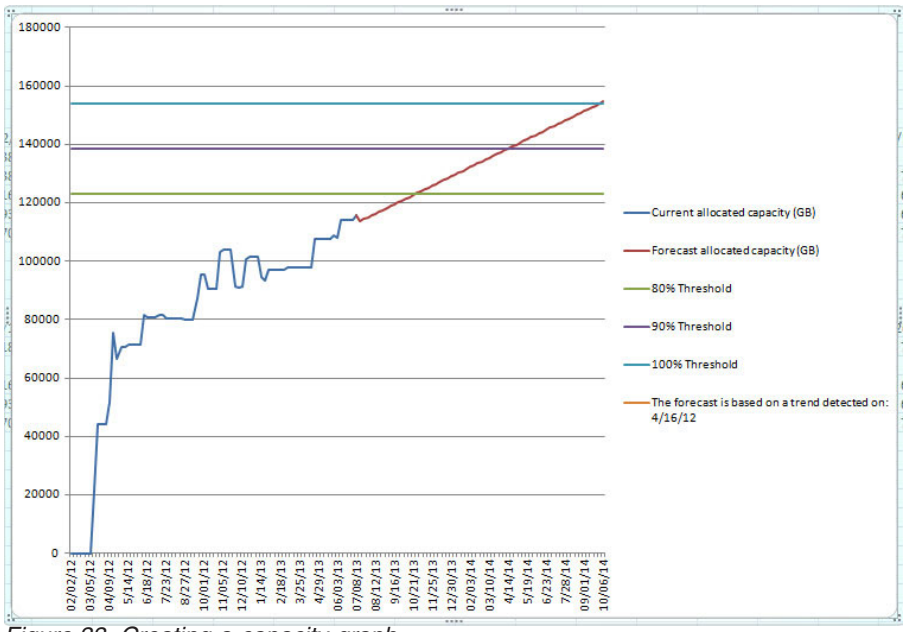


Figure 33. Creating a capacity graph

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 v1.4.0.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 in order to maintain the continuity of XIV systems history.

Procedure

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

```
------------------------------------------------------------------
------------ IBM Hyper-Scale Manager v1.4.0.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 screenshot 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 v1.4.0.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.

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

To ensure continuity, in some case data of removed systems keeps being collected.

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, 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 before 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 must be listed on the inventory.
  - If the user chooses to reset capacity data for all systems, even non-monitored systems capacity data is reset.

Chapter 5. 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 50
  - "Adding a user on multiple systems" on page 50
  - "Editing, deleting or changing the password of a user" on page 51
- "Mass configuration copy-pasting"

Mass configuration copy-pasting

You may copy system configuration from one system and paste it onto multiple XIV systems.

About this task

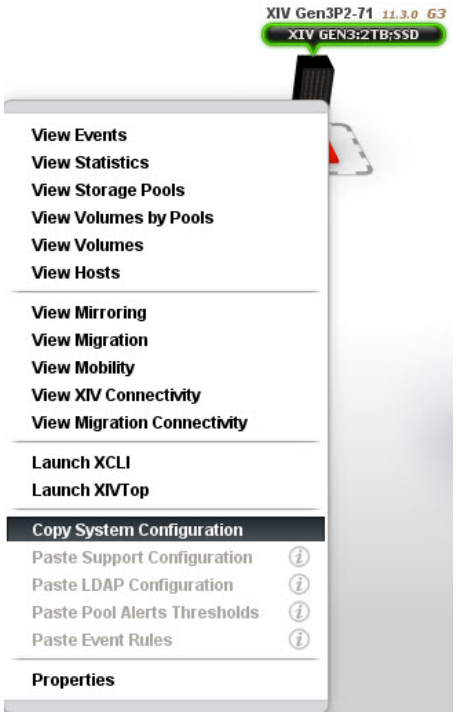
The configuration that can be copied from one system to another:

- Support configuration
- LDAP configuration
- Pool alerts threshold

- Event rules configuration
- Key server configuration

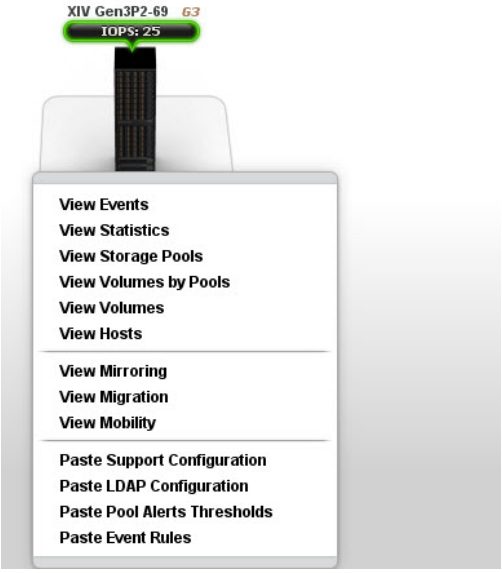
Procedure

1. On the XIV GUI, right-click a system and select **Copy System Configuration** from the pop-up menu.



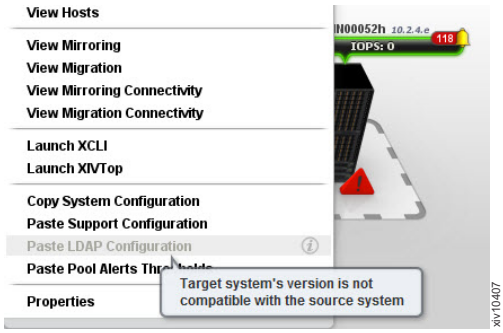
   This system configuration is now copied to the memory and the pop-up menu closes.

2. Select systems to copy the configuration to. Right-click a system, or several systems, and select **Paste ... Configuration** from the pop-up menu. In this example, **Paste Support Configuration** is selected.

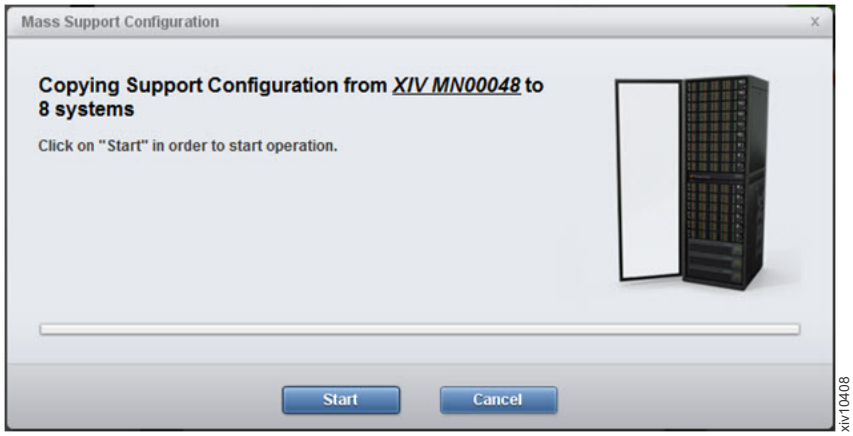


The **Multi-System Configuration of Support information** screen opens.

Note: Whenever a paste option is grayed-out, meaning that it is not available, mouse-over the option to display a tooltip that explains the reason. In this example, the Paste LDAP Configuration is grayed-out and the tooltip says that the target system's version is not compatible with the source system.

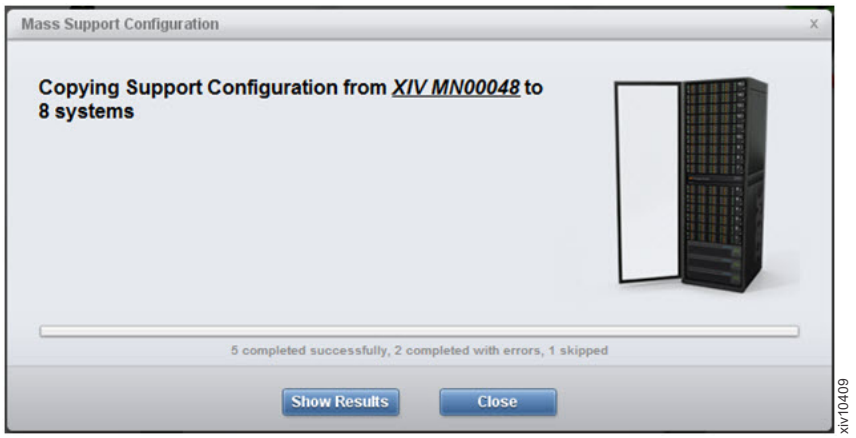


3. Click **Start**.



A progress bar is displayed on screen. Clicking **Cancel** right after clicking Start and during the preparation phase, cancels the multi-system configuration.

When the copy operation is done, 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 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.

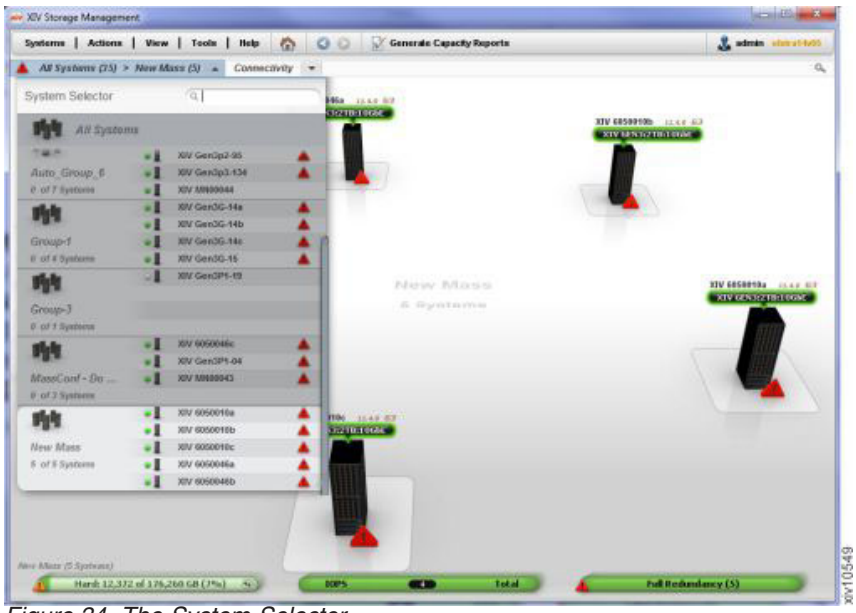


Figure 34. The System Selector

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

Figure 35. The Add Cluster screen

3. Enter the cluster's name and type. 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.

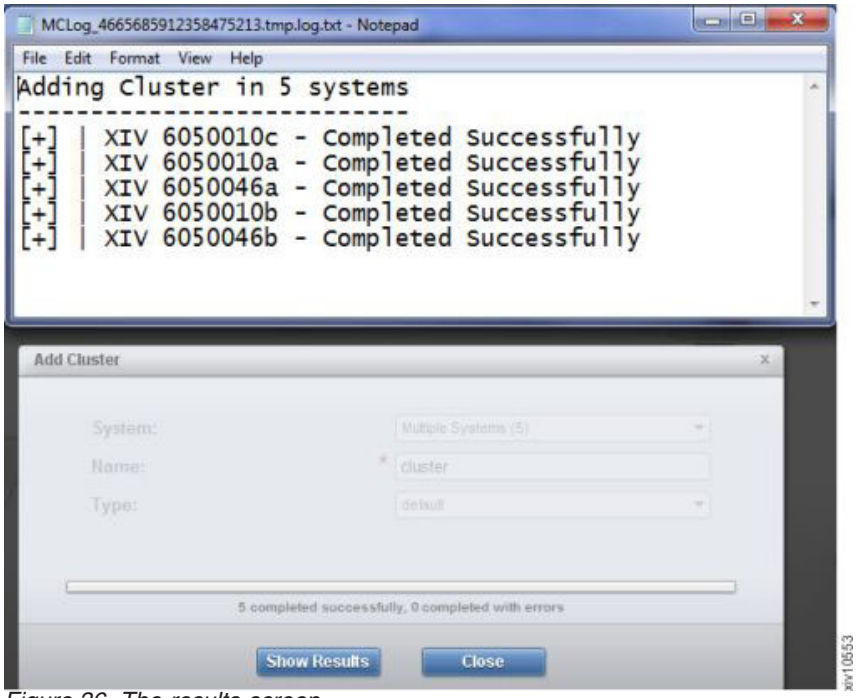


Figure 36. The results screen

Results

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

Mass 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.

Editing a cluster

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

Procedure

1. On the GUI, open **View > Hosts and Clusters > Clusters** from the menu.
2. Right-click a Cluster and select Edit from the pop-up menu. The **Edit Cluster** screen opens.

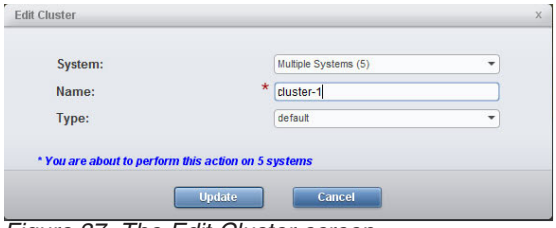


Figure 37. The Edit Cluster screen

3. On this screen, you may rename the cluster and change its type. Click **Update**.

Results

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

Mass 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.

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
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.

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
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.

Multi system configuration of user-related information

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

About this task

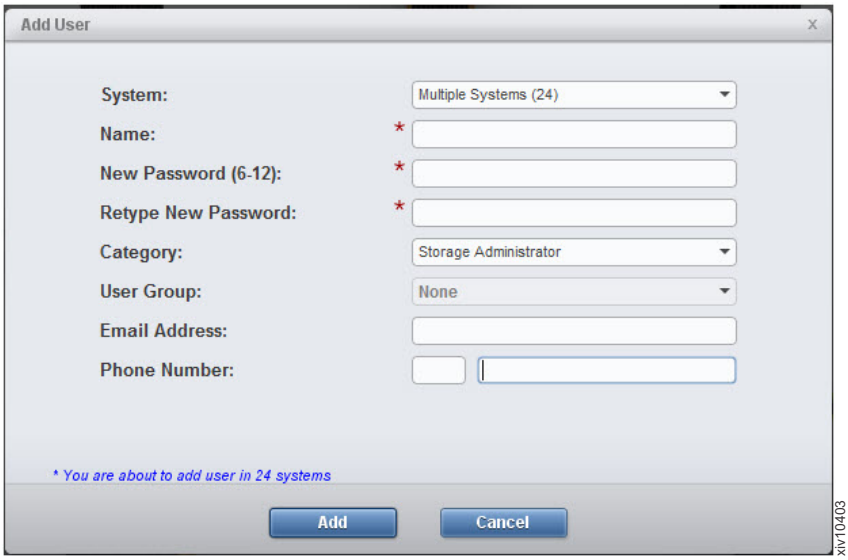
This task describes how to configure user-related information on multiple XIV systems at once.

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
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.

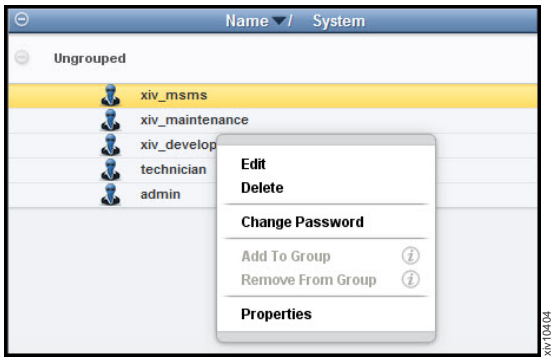
Editing, deleting or changing the password of a user

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**.



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

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

Results

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

Mass 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.

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 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 **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

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.

Adding and editing a users group

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

Procedure

1. Select the systems you would like 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 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 group was added to the selected systems.

Mass 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.

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

GC27-5986-00