SHARE in Seattle – Session 16645

Top 10 Things You Should Be Doing On Your HMC But ~~You're NOT~~ You Probably Are

March 4, 2015

Brian Valentine
HMC Development
bdvalent@us.ibm.com
File Updated: 2-28-15

Agenda

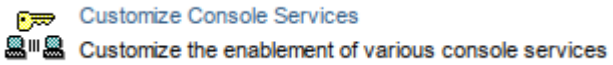
Setting up the HMC for Remote Use

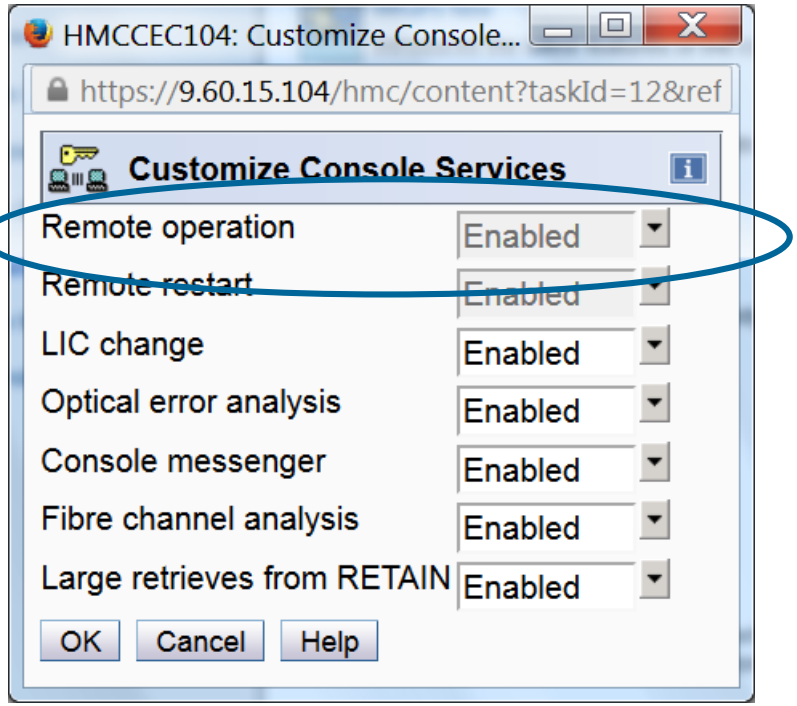
Setting up HMC for Remote Use

- Enables access from anywhere on the Local Area Network
  - Work with your Network Administrator to allow port 443 (HTTPS) and port 9960 (Applets)
  - Could also allow remote access using an existing business VPN
- Allows the HMC to be physically secured
  - Lock it in a restricted area and ask people to login remotely
- Multiple users can access the HMC at the same time
  - HMC is design to handle concurrent users
- Read more information on “IBM z Systems HMC Security”
  - http://www.share.org/p/do/sd/topic=64&sid=9171
  - https://www.ibm.com/servers/resourcelink/lib03011.nsf/pages/zHmcSecurity/$file/zHMCSecurity.pdf

Setting up HMC for Remote Use (cont.)

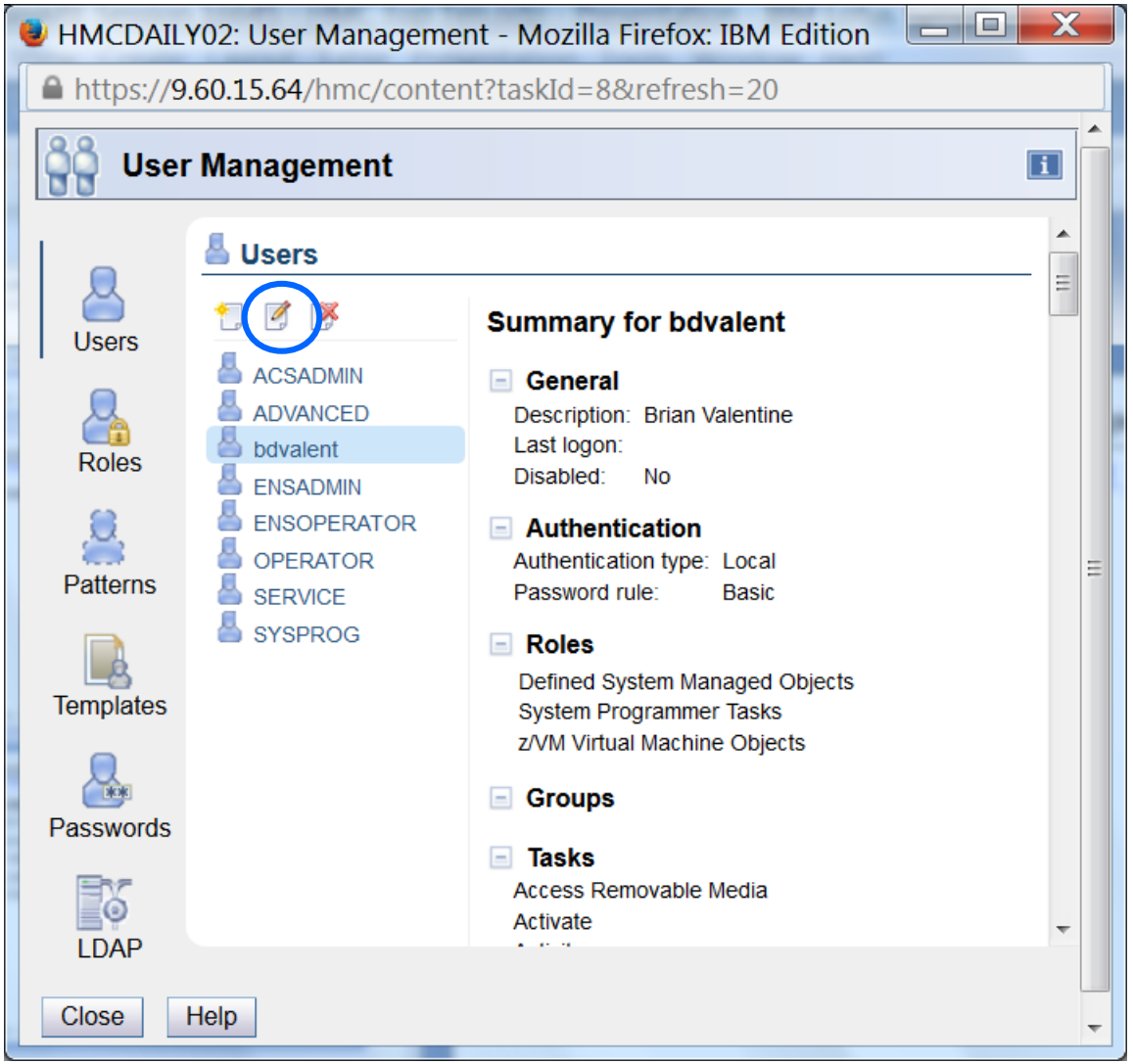
- Enable locally through the **Customize Console Services** task



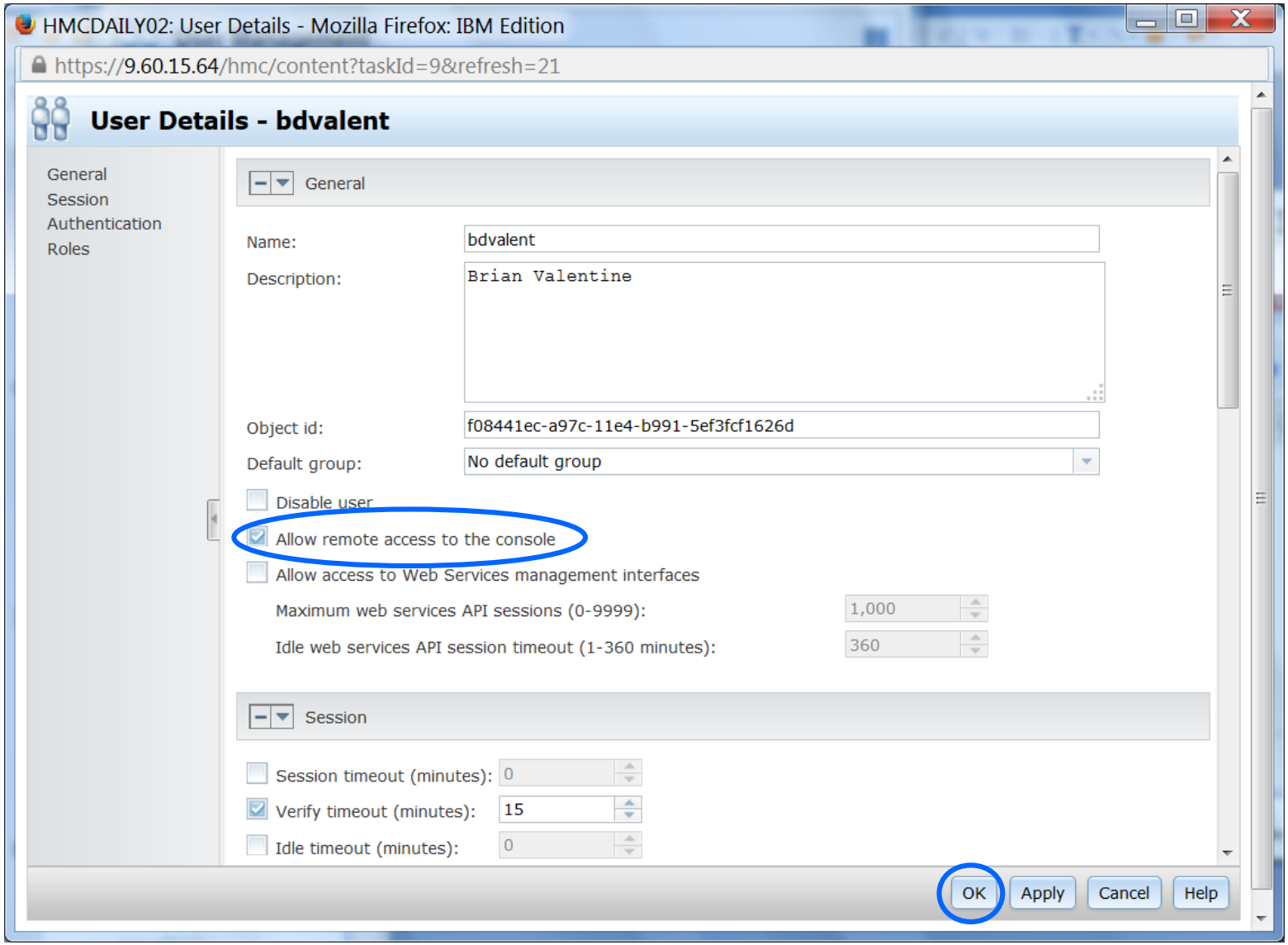


Setting up HMC for Remote Use (cont.)

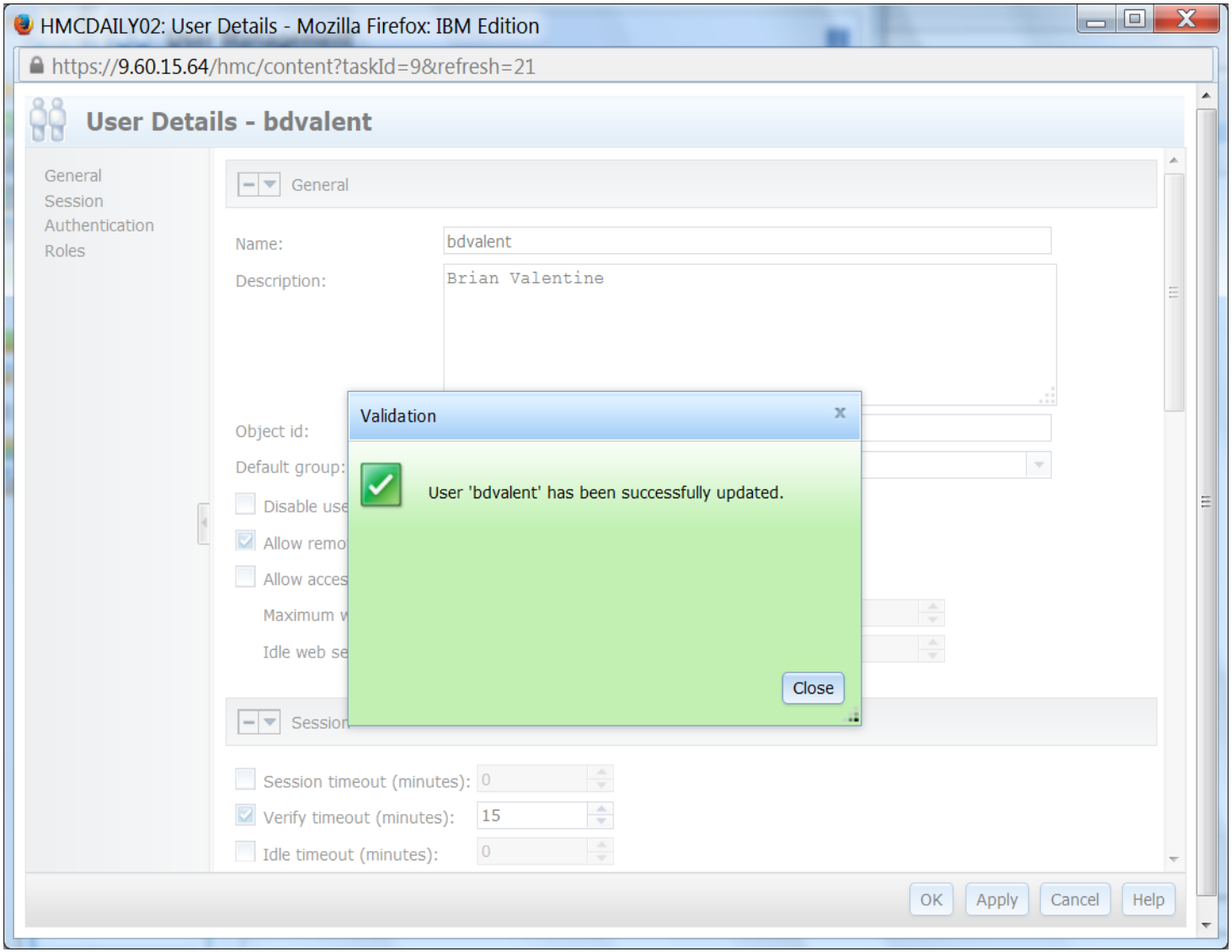
- Enable specific users
  - ACSADMIN log on
  - User management task
  - Select Users
  - Select User to enable
  - Select Details to edit



Setting up HMC for Remote Use (cont.)



Setting up HMC for Remote Use (cont.)



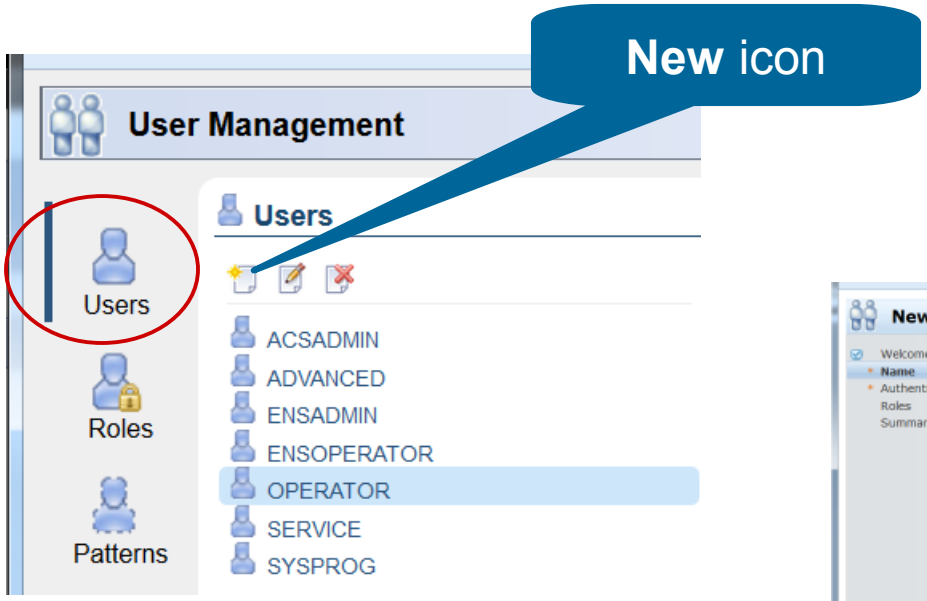
Securing User IDs

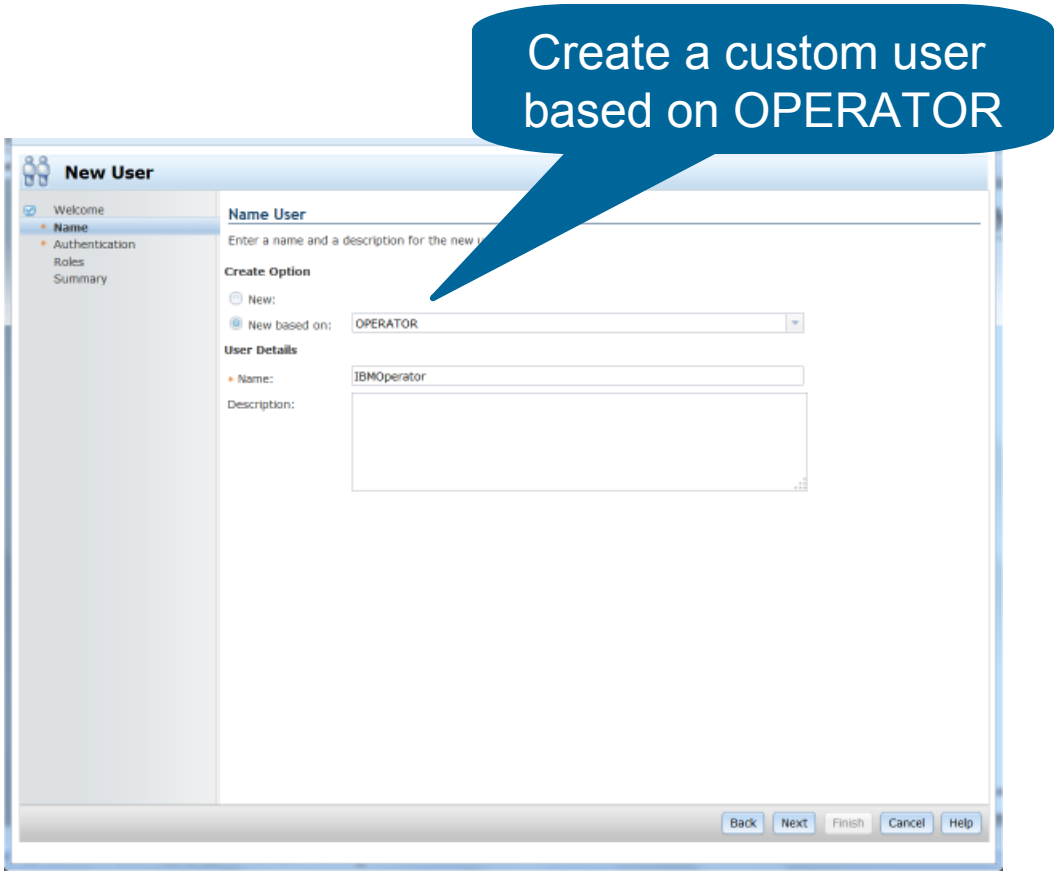
Securing User IDs

- Best Practices
  - Do not share HMC user IDs among multiple people
  - Make sure each user is permitted only access to the tasks and managed resources needed to perform job responsibilities (see slides)
  - Define password rules that adhere to the guidelines for the customer enterprise and make sure each user is configured to use these password rules (see slides)
  - Use data replication to ensure that User Profile information (users, roles, password rules, etc) are automatically synchronized among all HMCs installed in the enterprise (see slides)
  - Disable the default user IDs
    - Even better DELETE them
    - At a minimum change the default passwords for these users

Securing User Ids (cont.)

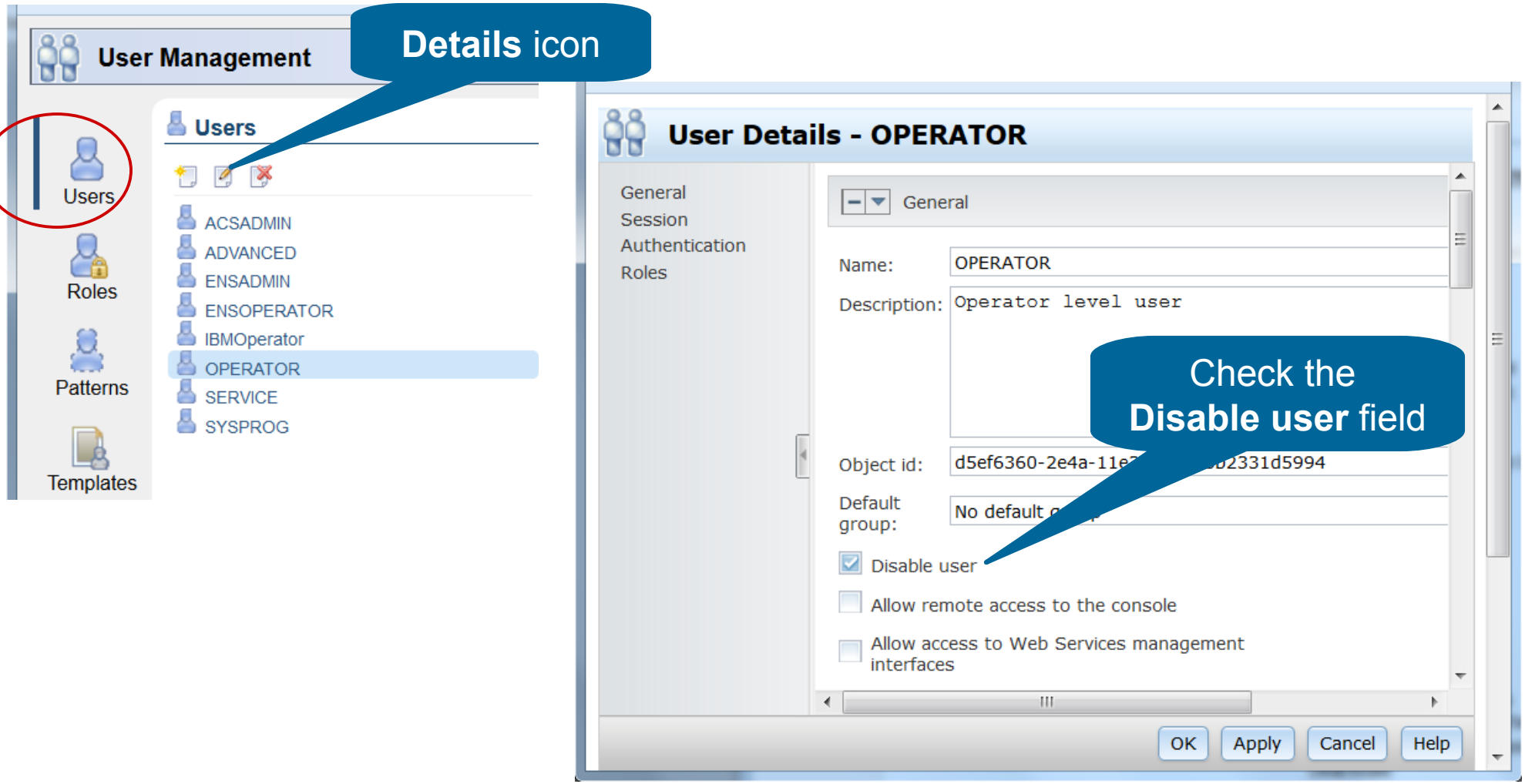
- Use the **User Management** task to create custom users





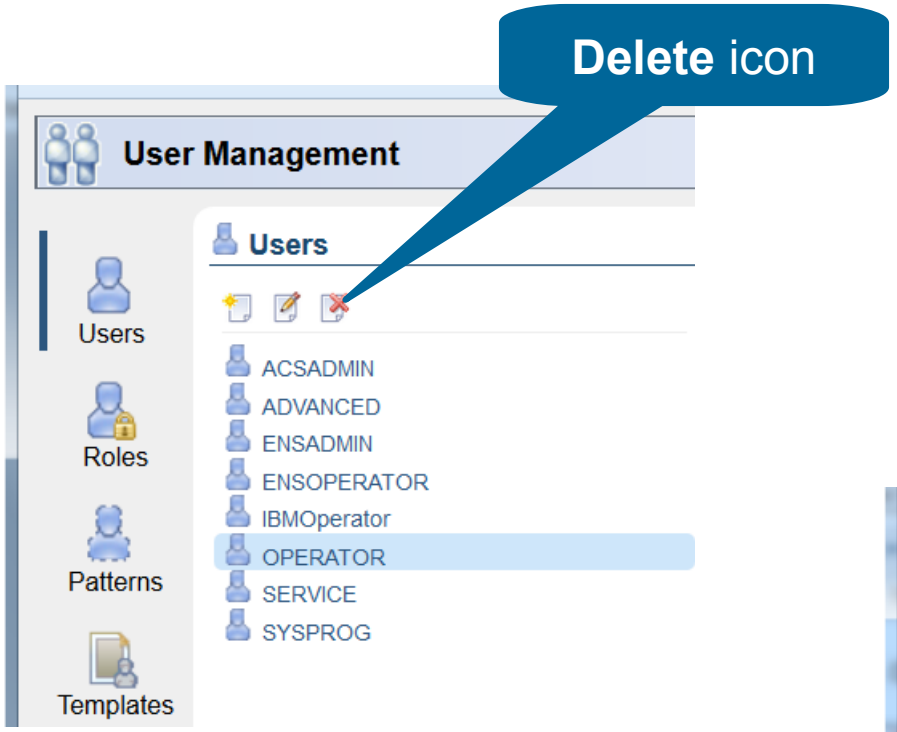
Securing User Ids (cont.)

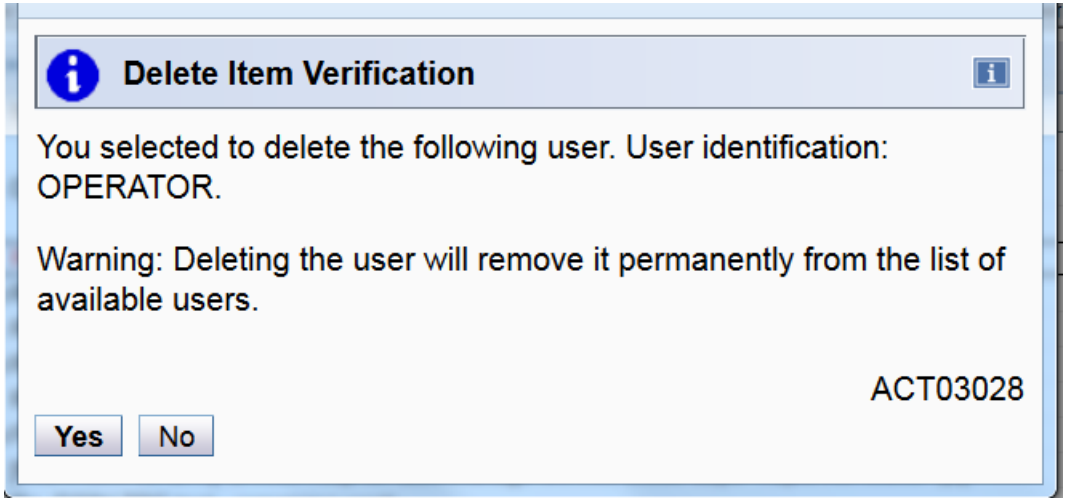
- Use the **User Management** task to modify existing default users



Securing User Ids (cont.)

- Or use the **User Management** task to delete existing users





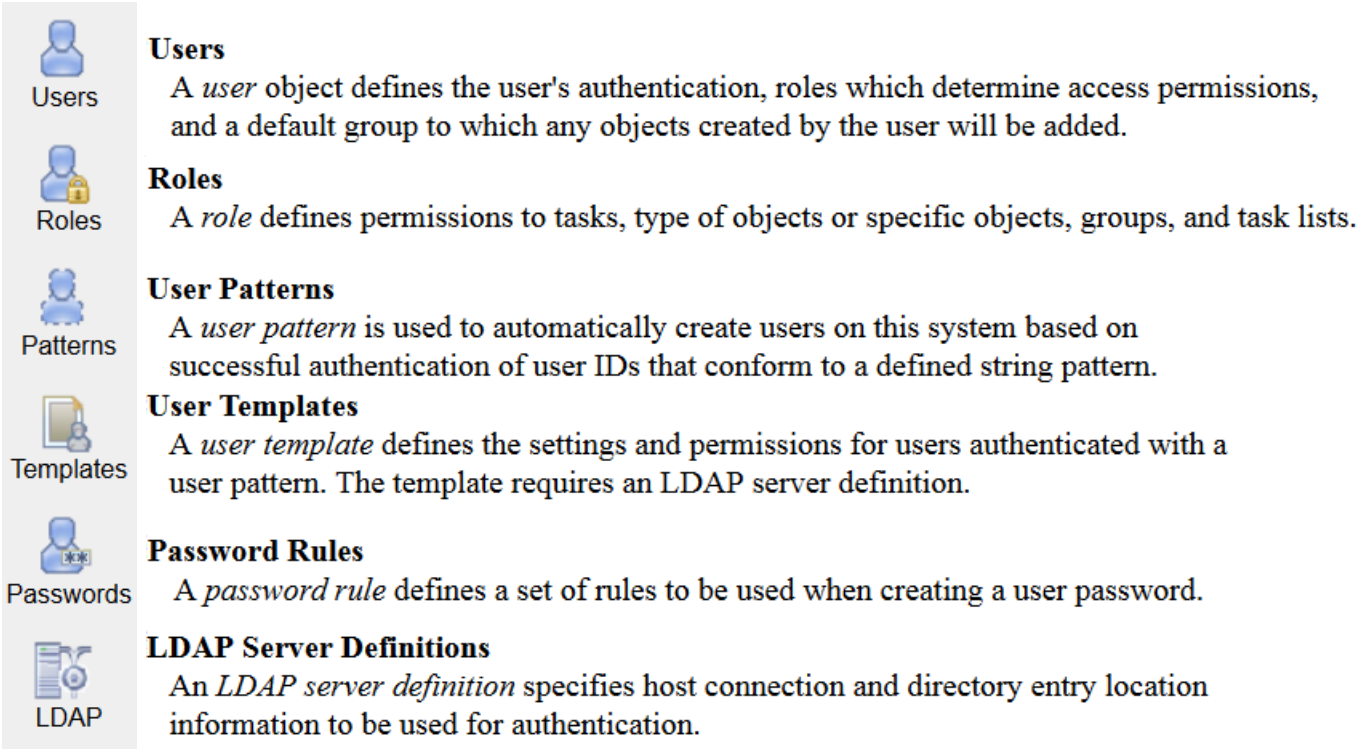
Create Custom Users and Roles

Create Custom Users and Roles

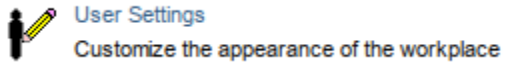
- Creating a custom user definition for each person that uses the HMC allows for the following benefits:
  - Specific access to the required objects for each user
  - Specific access to the required tasks for each user
  - More granularity in the audit logs, know exactly which person performed specific actions
  - No more sharing of user credentials and passwords
  - Each user will have unique saved sessions on disconnects

Create Custom Users and Roles (cont.)

- **User Management** task – convenient dashboard to manage all aspects of system users that log on to the HMC

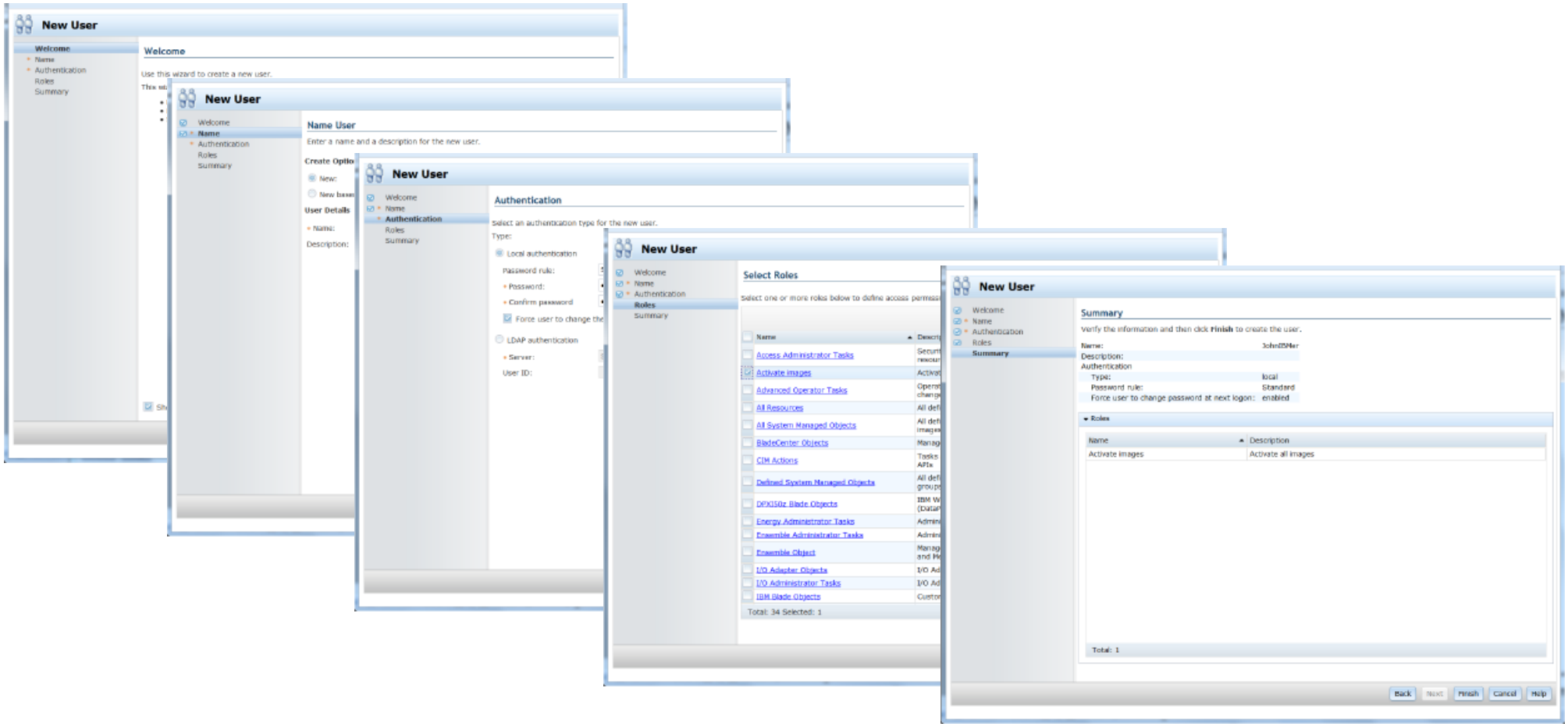


- **User Settings**



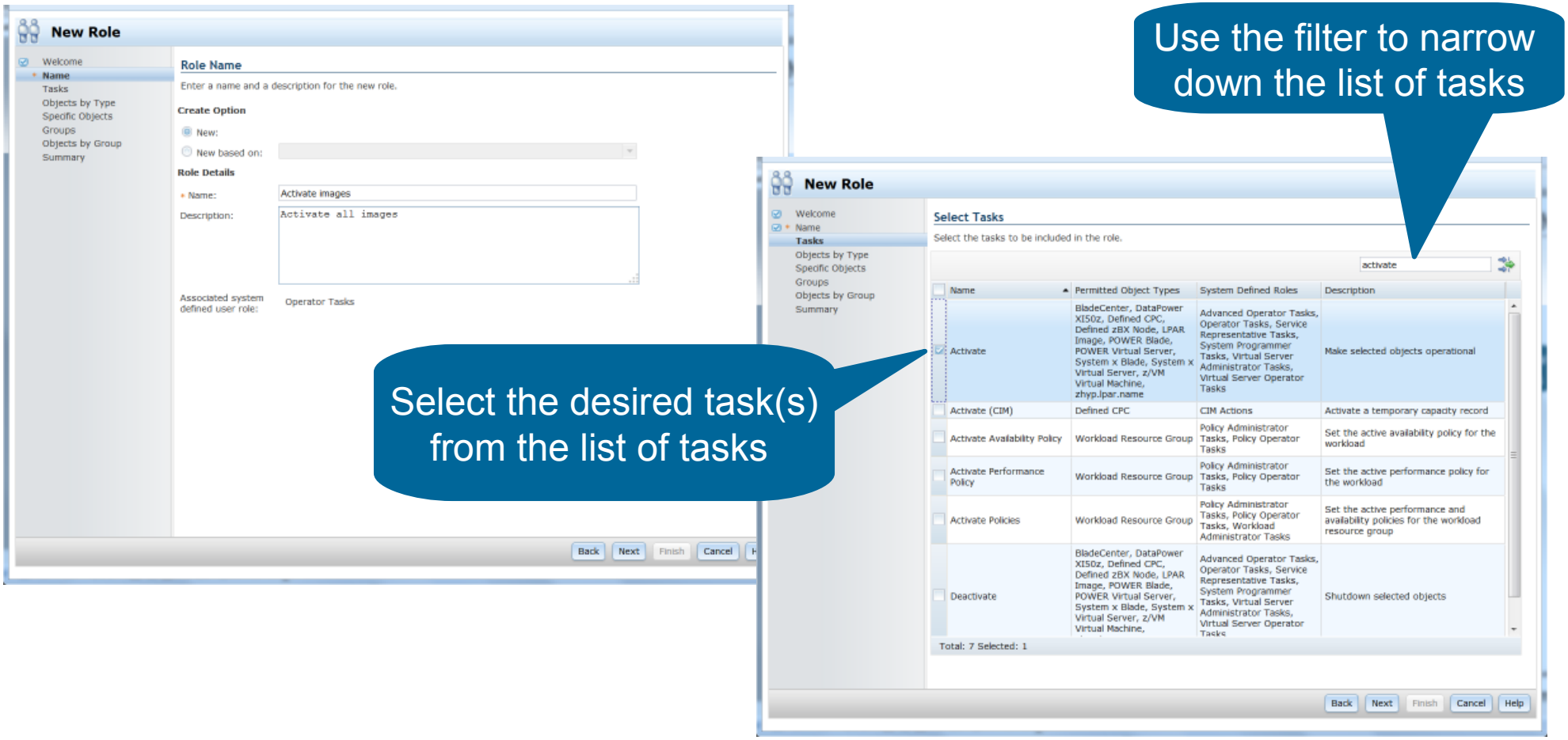
Create Custom Users and Roles (cont.)

- **User Management** wizards provide a guided step-by-step process for each new definition



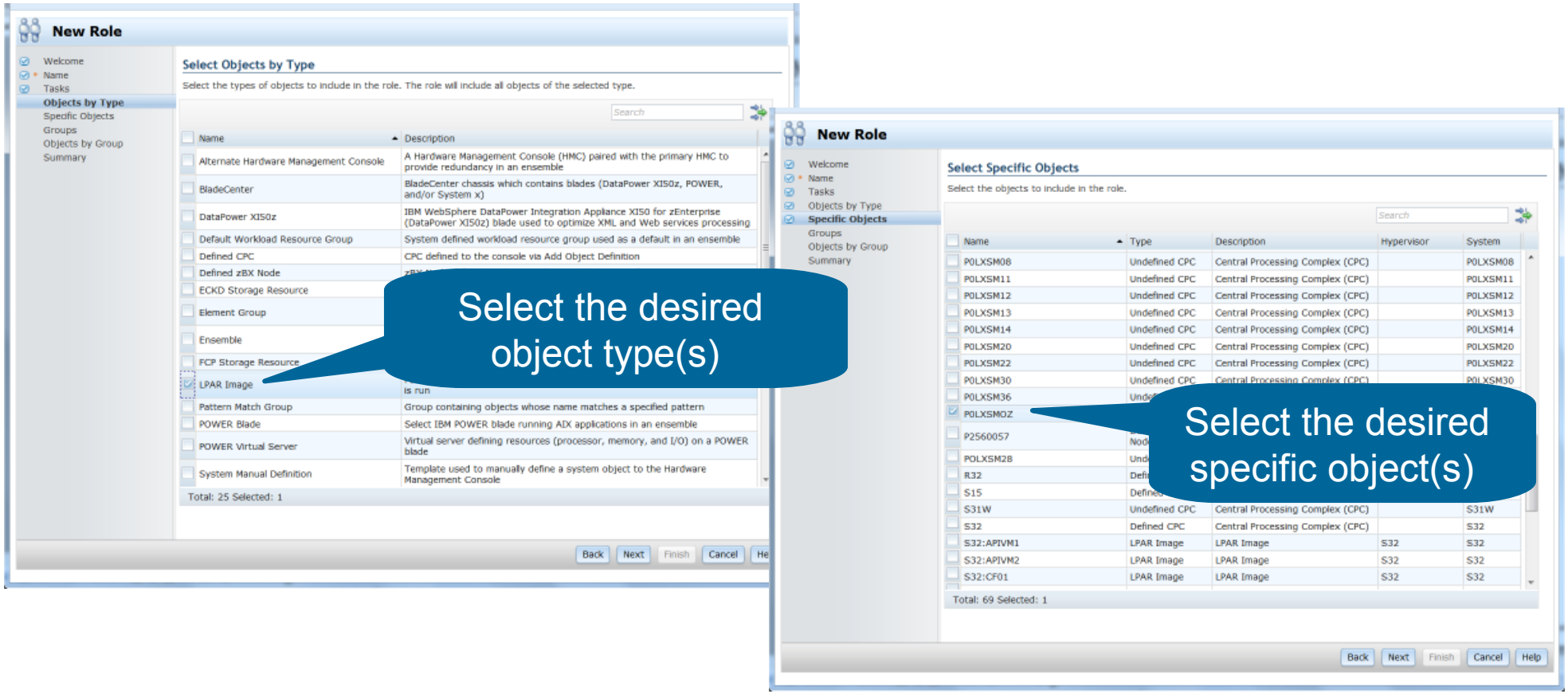
Create Custom Users and Roles (cont.)

- Limit access to specific tasks and objects
  - Create a role with specific task(s) a user should have access to



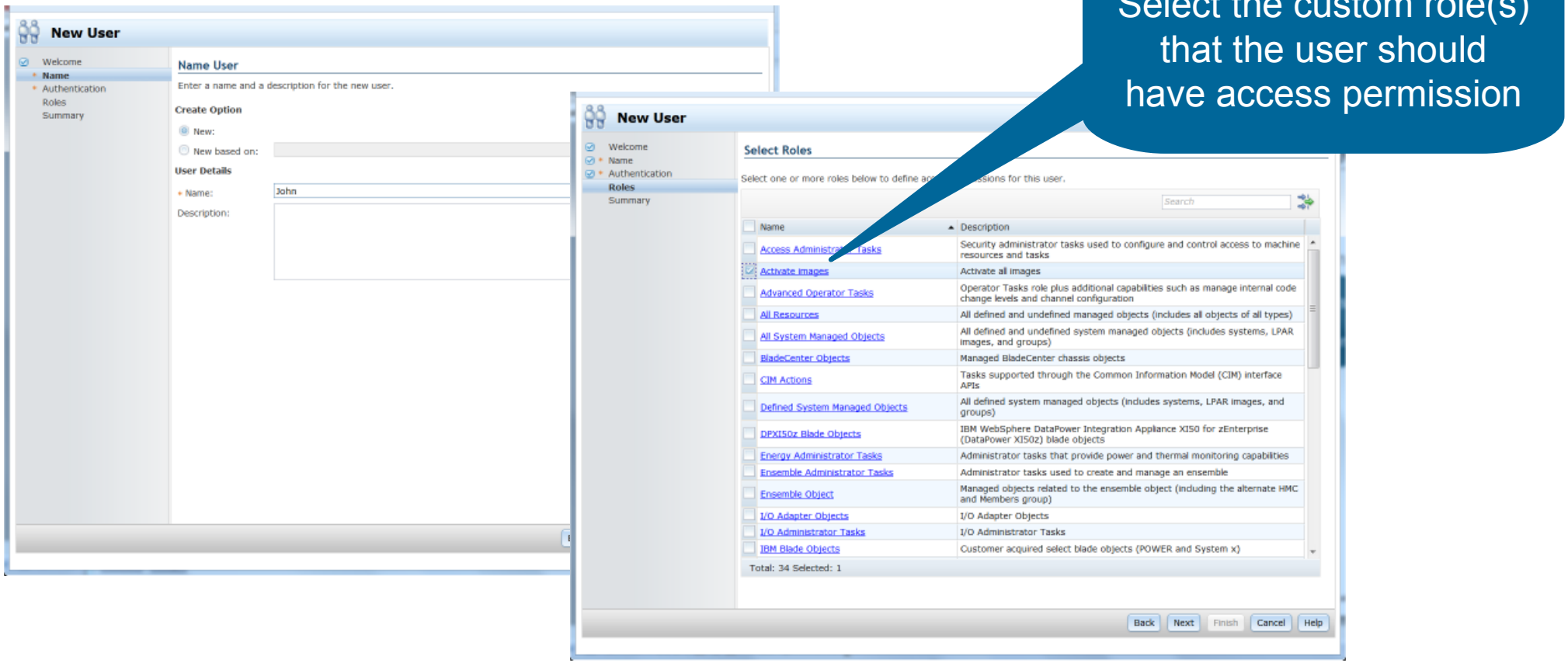
Create Custom Users and Roles (cont.)

- Limit access to types of objects and/or specific objects
  - Add to the custom role the object type(s) and specific object(s) a user should have access to



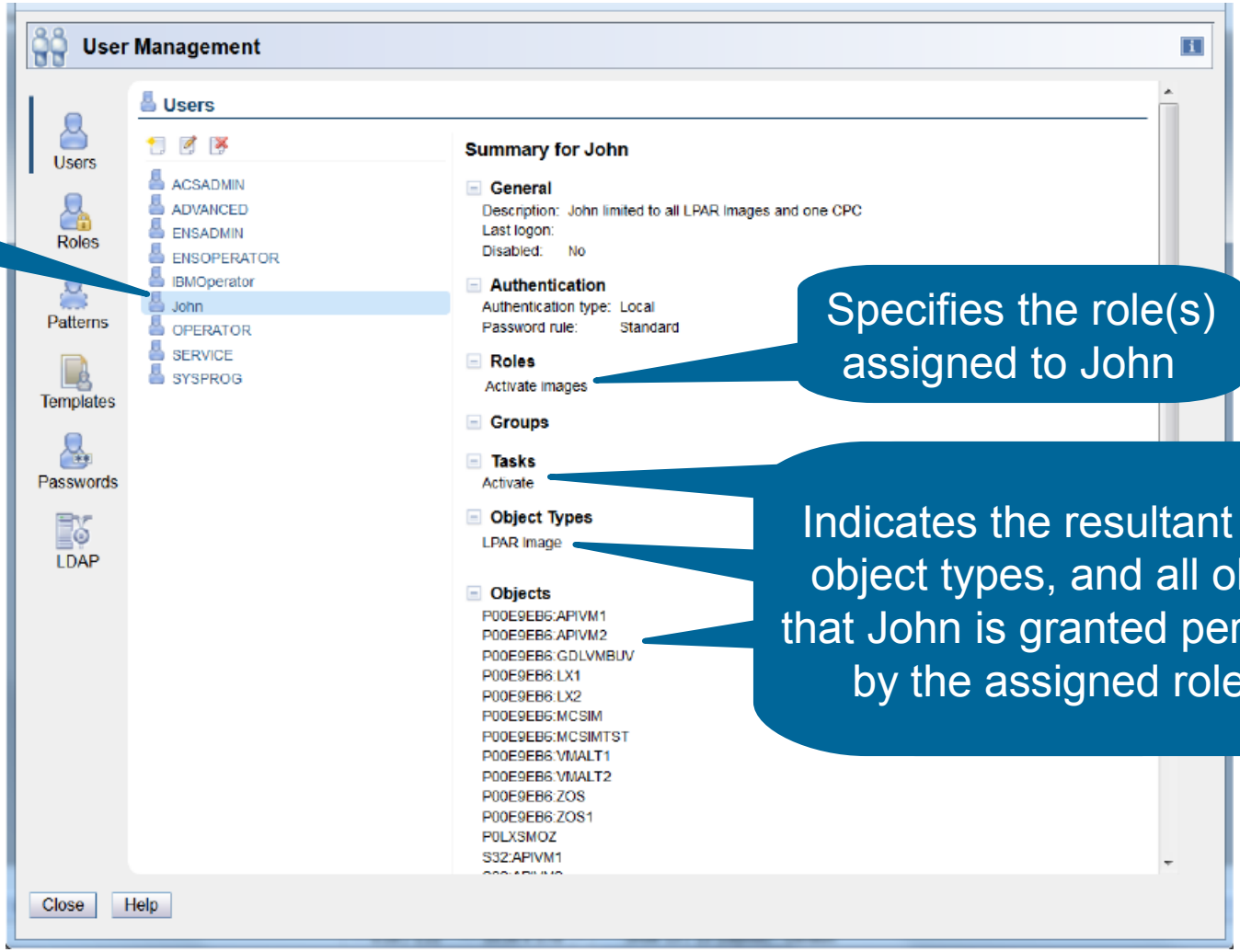
Create Custom Users and Roles (cont.)

- Assign custom roles to users
  - The user permissions are limited to the specific objects and tasks specified in the roles assigned to that user



Create Custom Users and Roles (cont.)

- **User Management** dashboard shows the newly created user summary



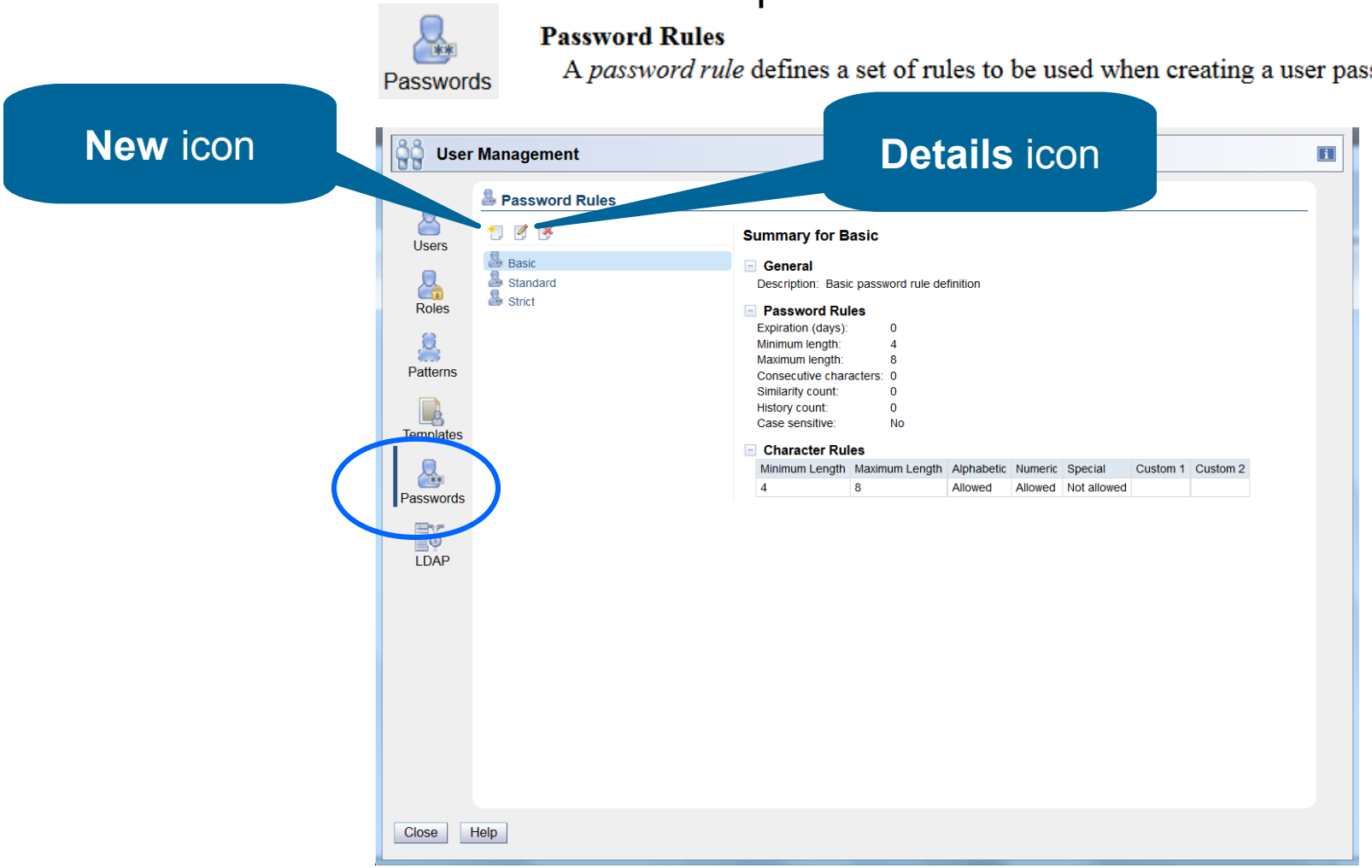
Custom Authentication Settings

Custom Authentication Settings

- Users can be configured for either local authentication or LDAP
- Local Authentication
  - Governed by Password Rules
  - Allows HMC users to meet corporate password rules
- Lightweight Directory Access Protocol (LDAP)
  - Provided by many enterprise directory servers
    - IBM Security Directory Server
    - Microsoft Active Directory
    - Apple Workgroup Manager
  - Allows HMC users to hook into existing corporate authentication
  - Single password across all HMCs and corporate network

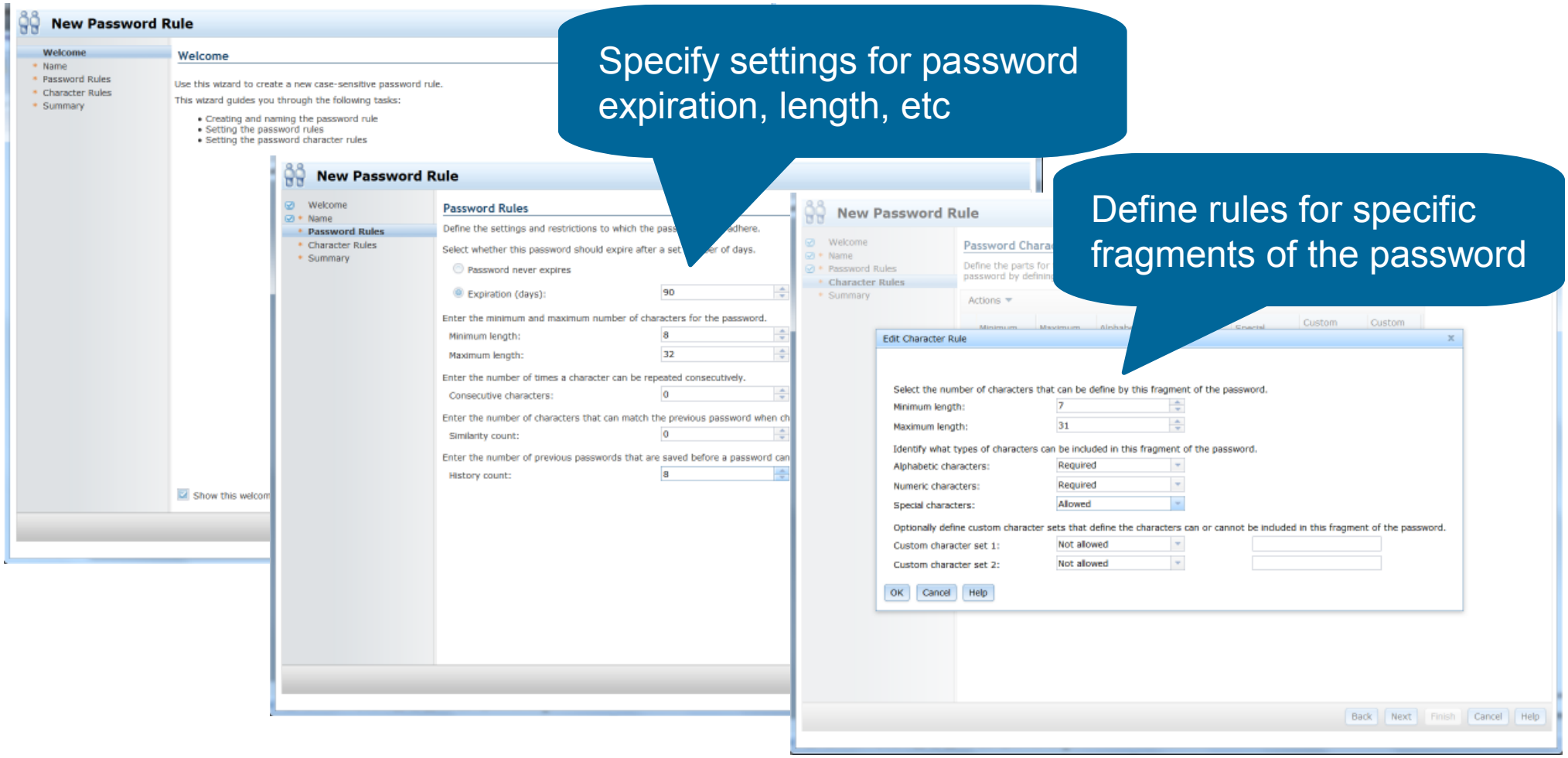
Custom Authentication Settings – Password Rules

- Use the **Password Rules** navigation icon in the **User Management** task, then select the **New** icon to create a new password rule



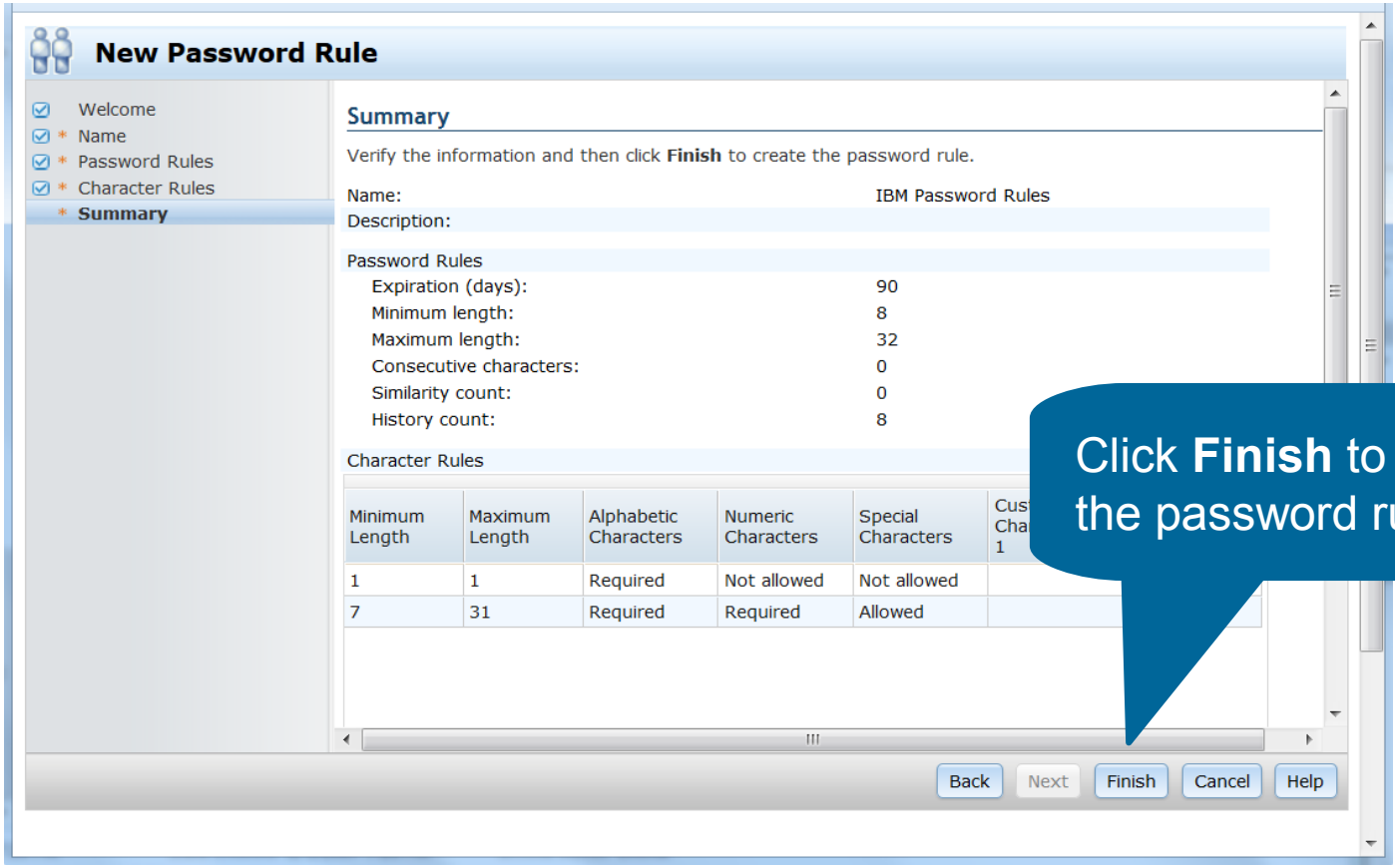
Custom Authentication Settings – Password Rules (cont.)

- Custom password rules are defined and managed through the **New Password Rule** wizard and **Password Rule Details**



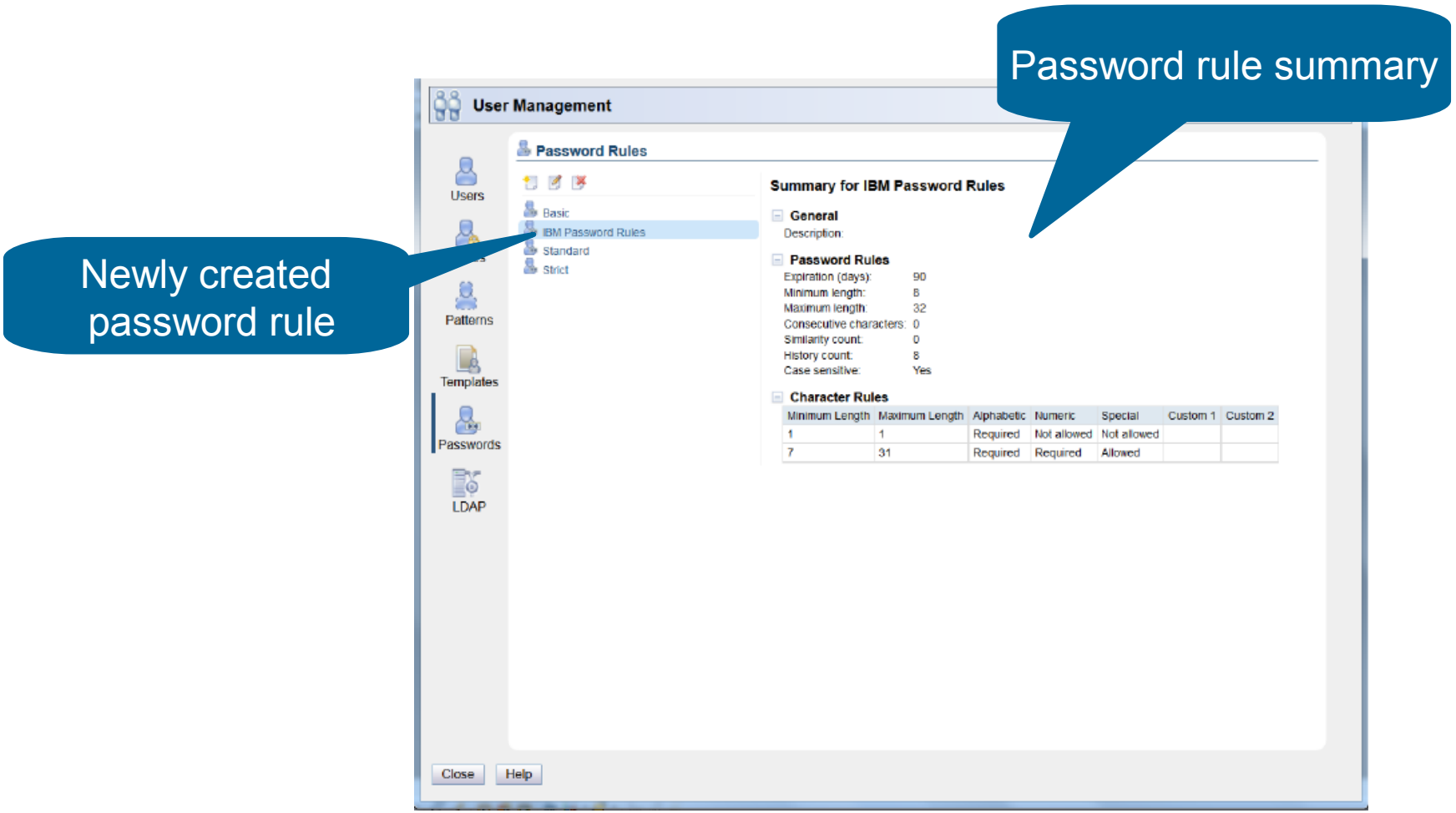
Custom Authentication Settings – Password Rules (cont.)

- **New Password Rule** wizard summary



Custom Authentication Settings – Password Rules (cont.)

- The new password rule is added to the list of password rules and the summary is shown in the **User Management** dashboard

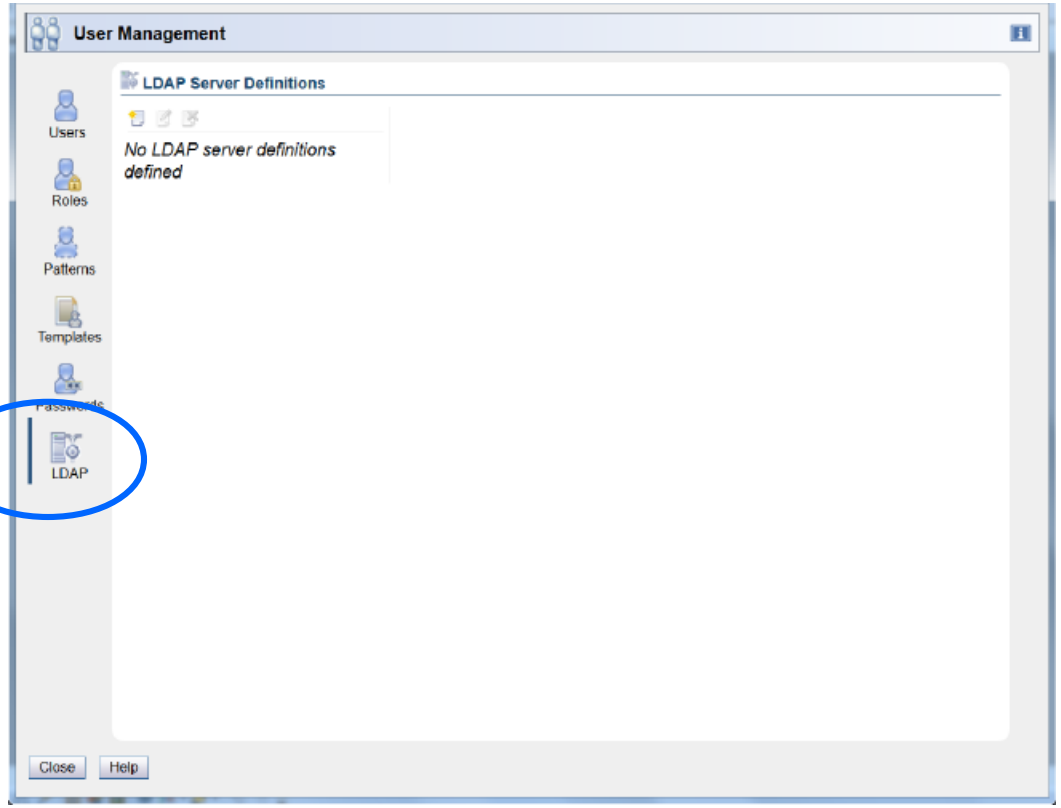


Custom Authentication Settings – LDAP Server Definitions

- LDAP servers are configured through the **LDAP Server Definitions** navigation icon in the **User Management** task

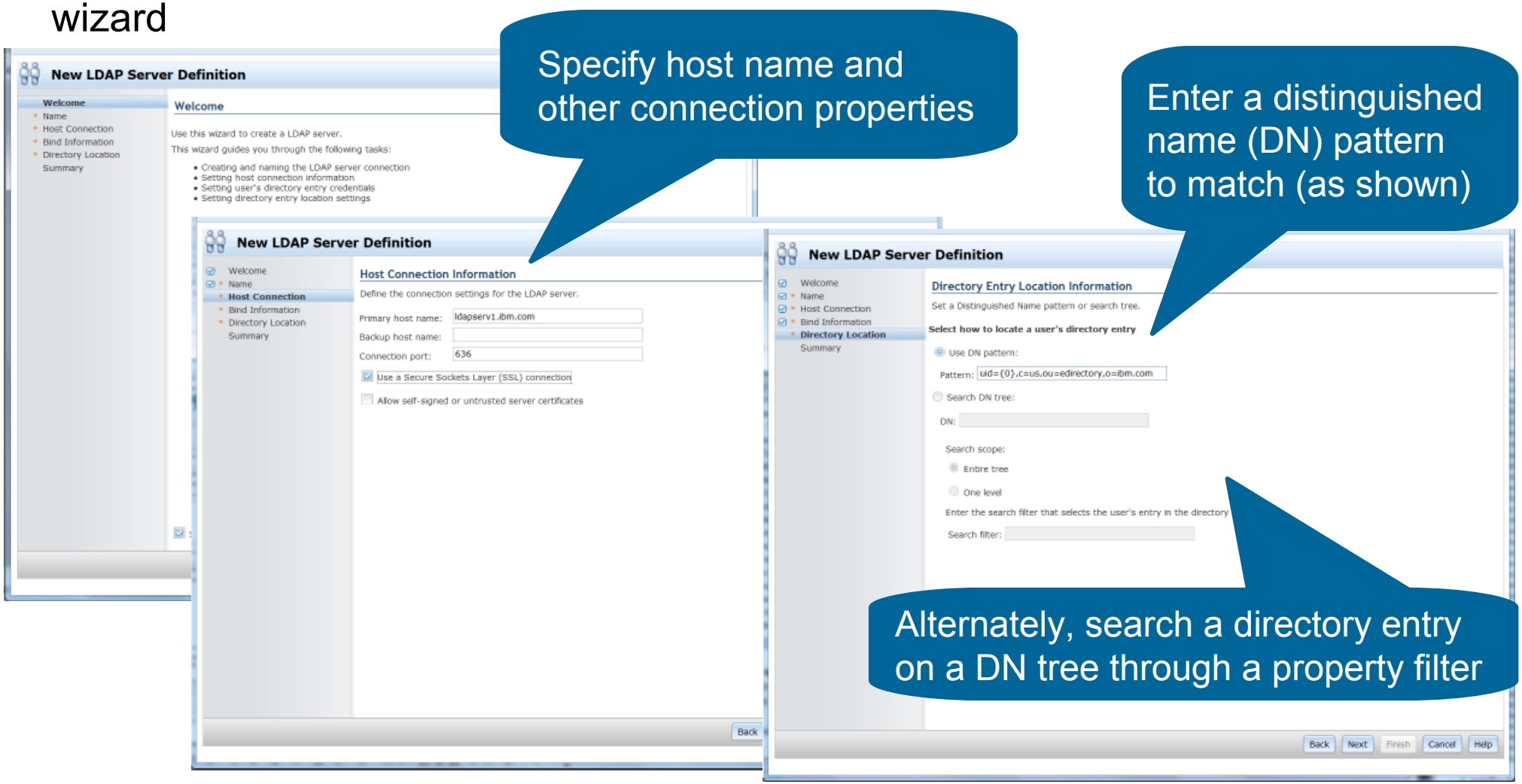
LDAP Server Definitions

An *LDAP server definition* specifies host connection and directory entry location information to be used for authentication.



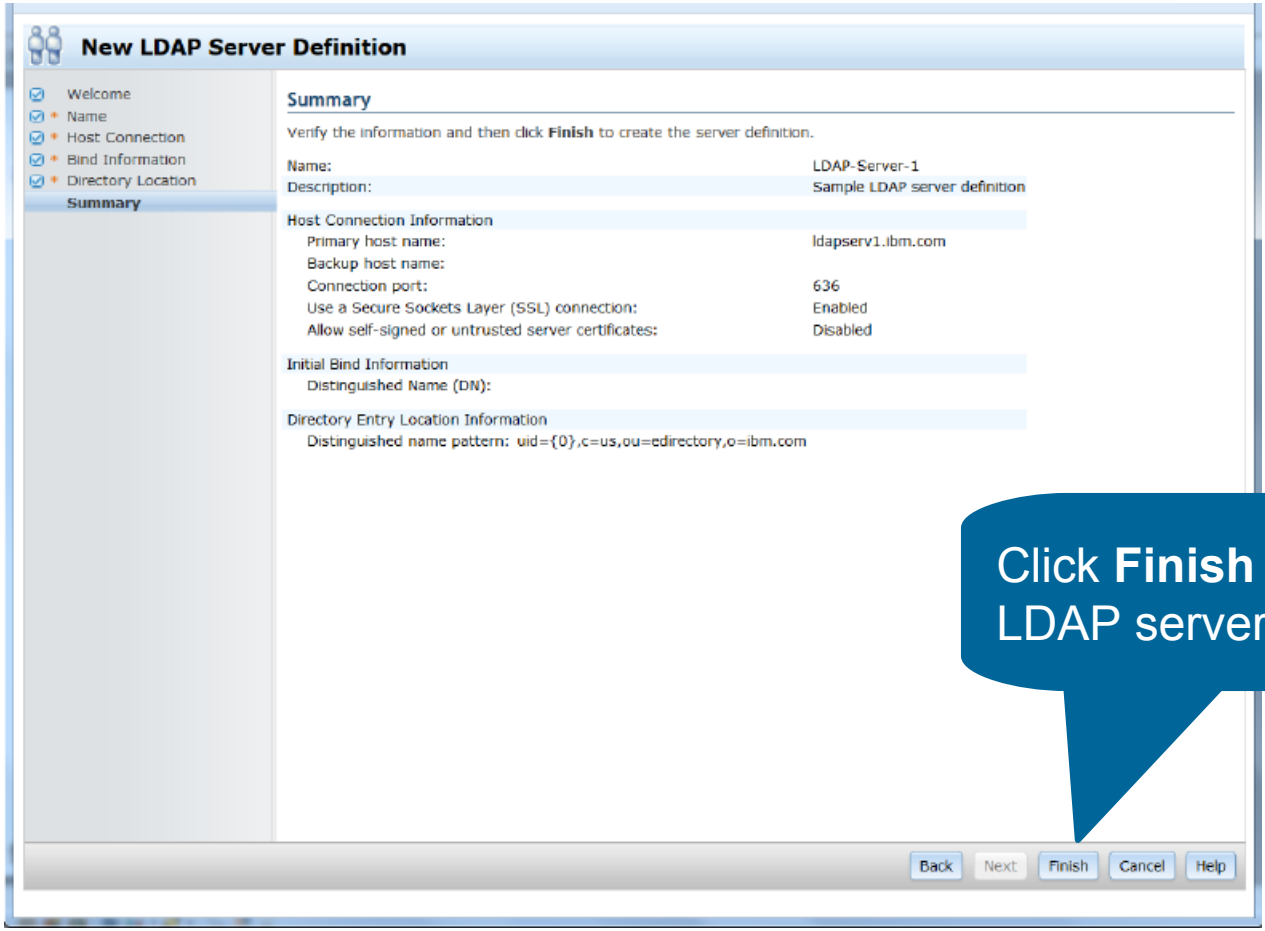
Custom Authentication Settings - LDAP Server Definitions (cont.)

- LDAP server definitions are created through the **New LDAP Server Definition** wizard



Custom Authentication Settings - LDAP Server Definitions (cont.)

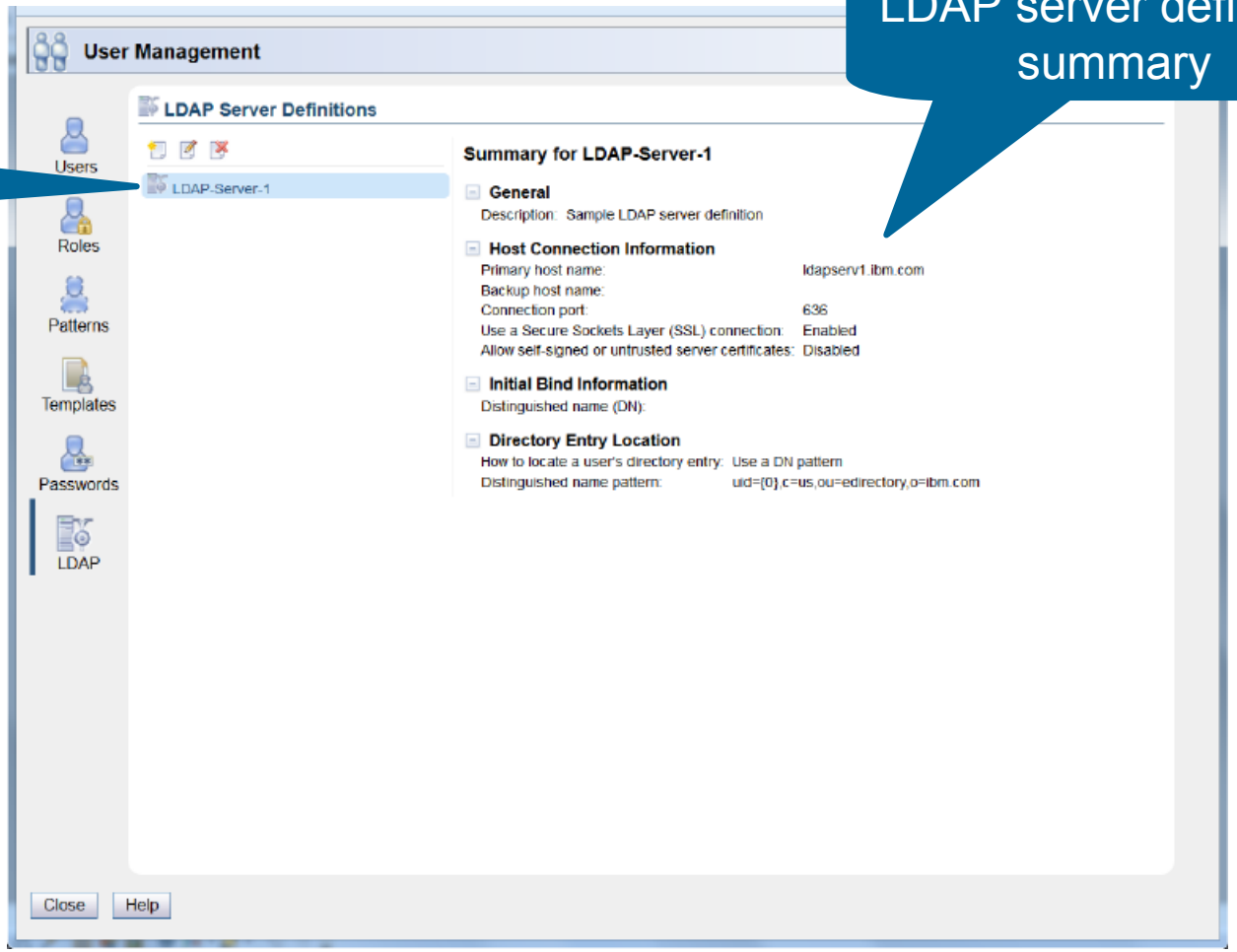
- **New LDAP Server Definition** wizard summary



Click **Finish** to create the LDAP server definition.

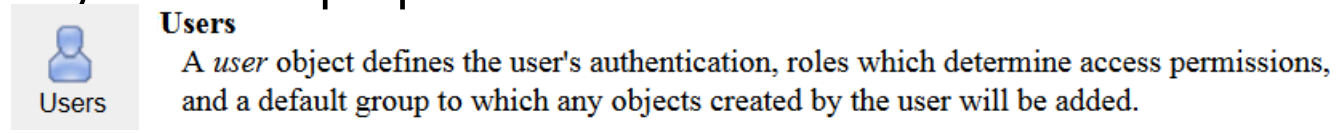
Custom Authentication Settings - LDAP Server Definitions (cont.)

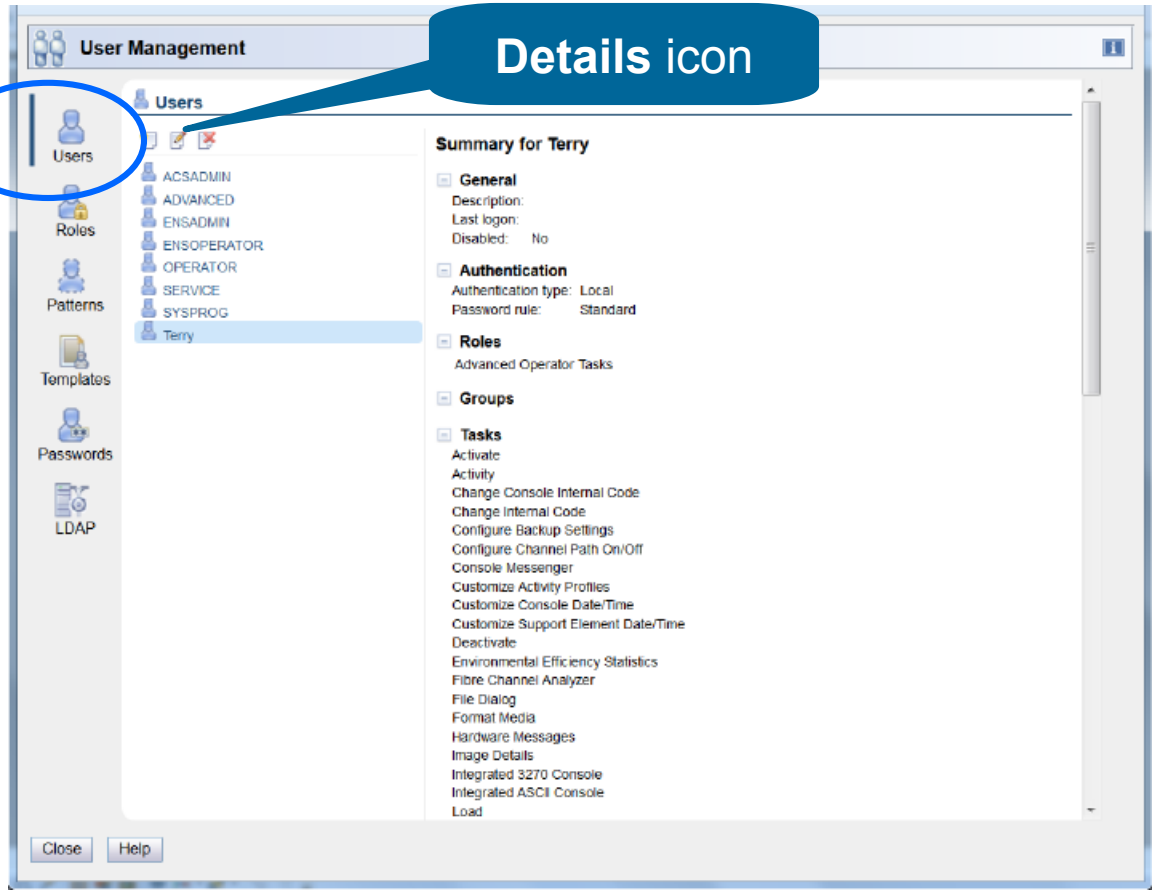
- The new LDAP server definition is added to the list and the summary is shown in the **User Management** dashboard



Custom Authentication Settings - Users

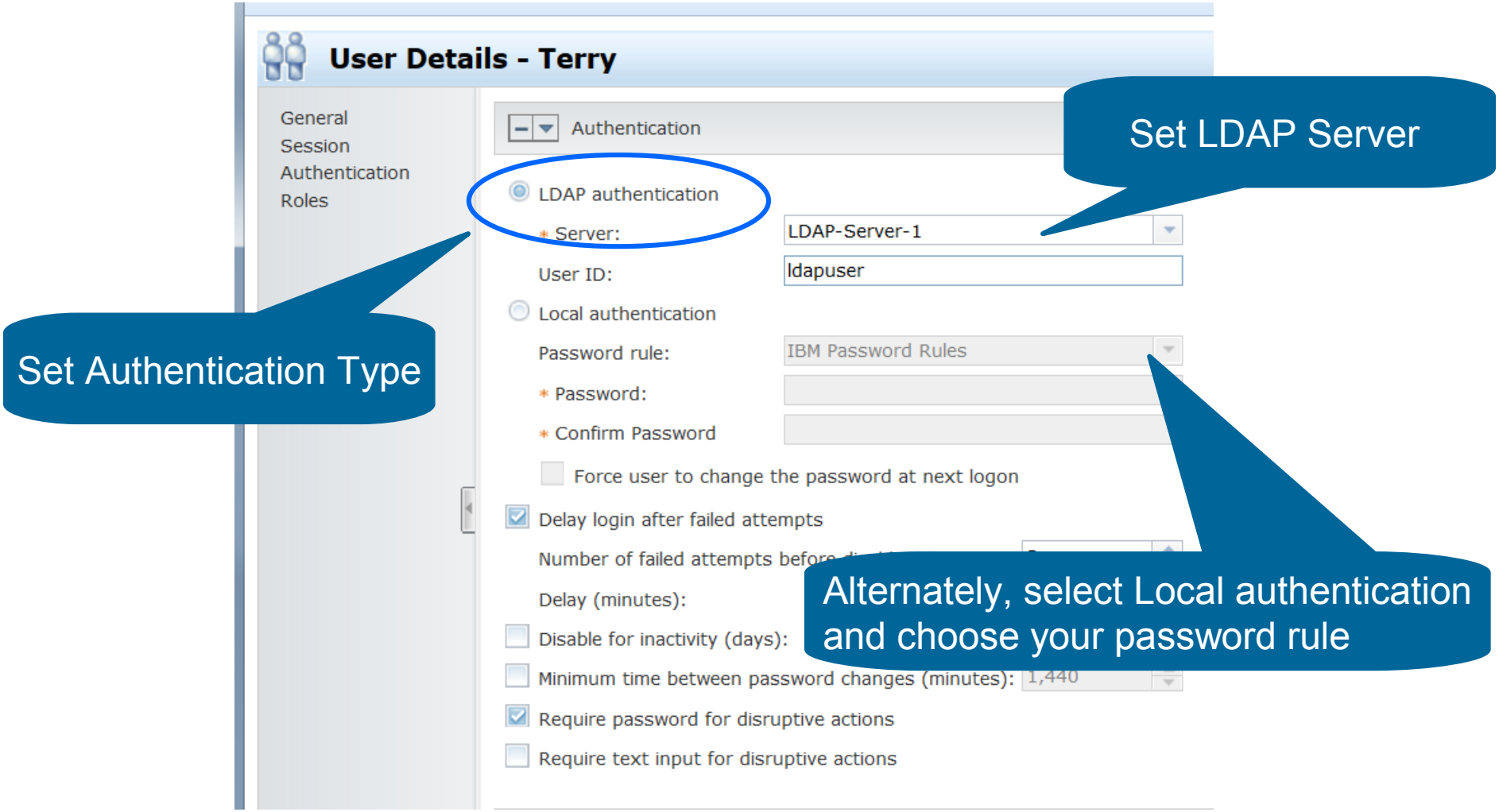
- Use the **Users** navigation icon in the **User Management** task, then select the **Details** icon to modify the user properties





Custom Authentication Settings – Users (cont.)

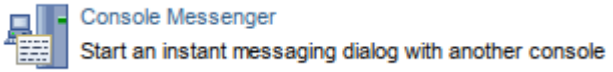
- Configure the authentication type for the user



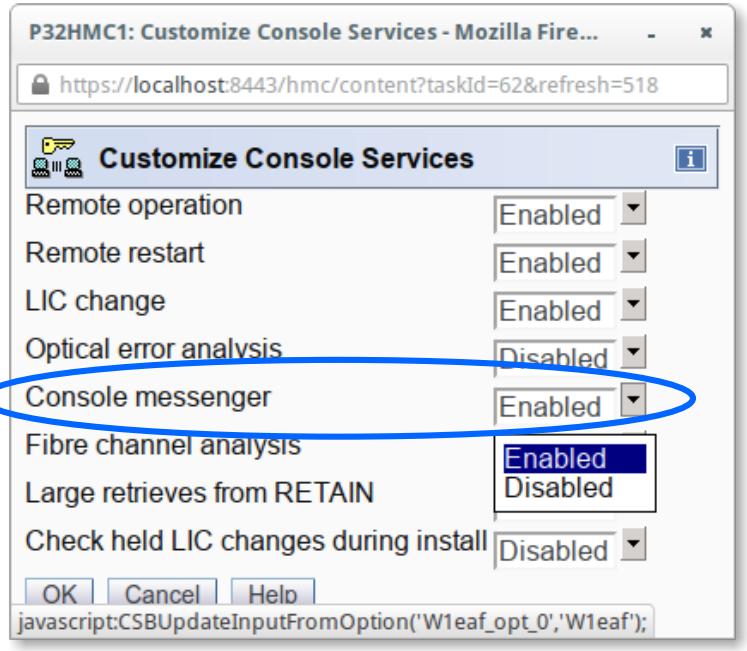
Communicating with Other Users

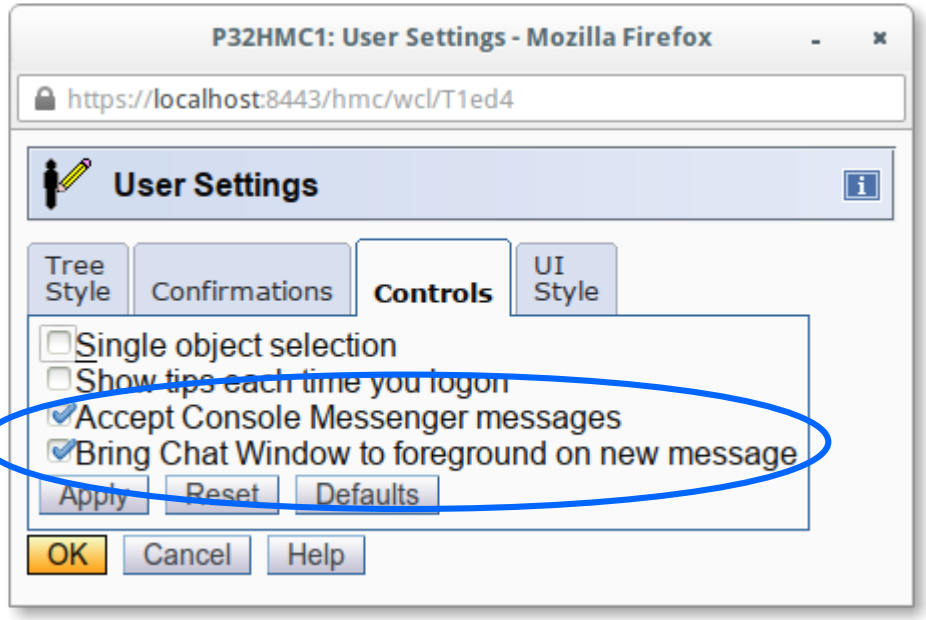
Communicating With Other Users

- **Console Messenger** task allows sending broadcast messages or start one-on-one chat sessions with other users



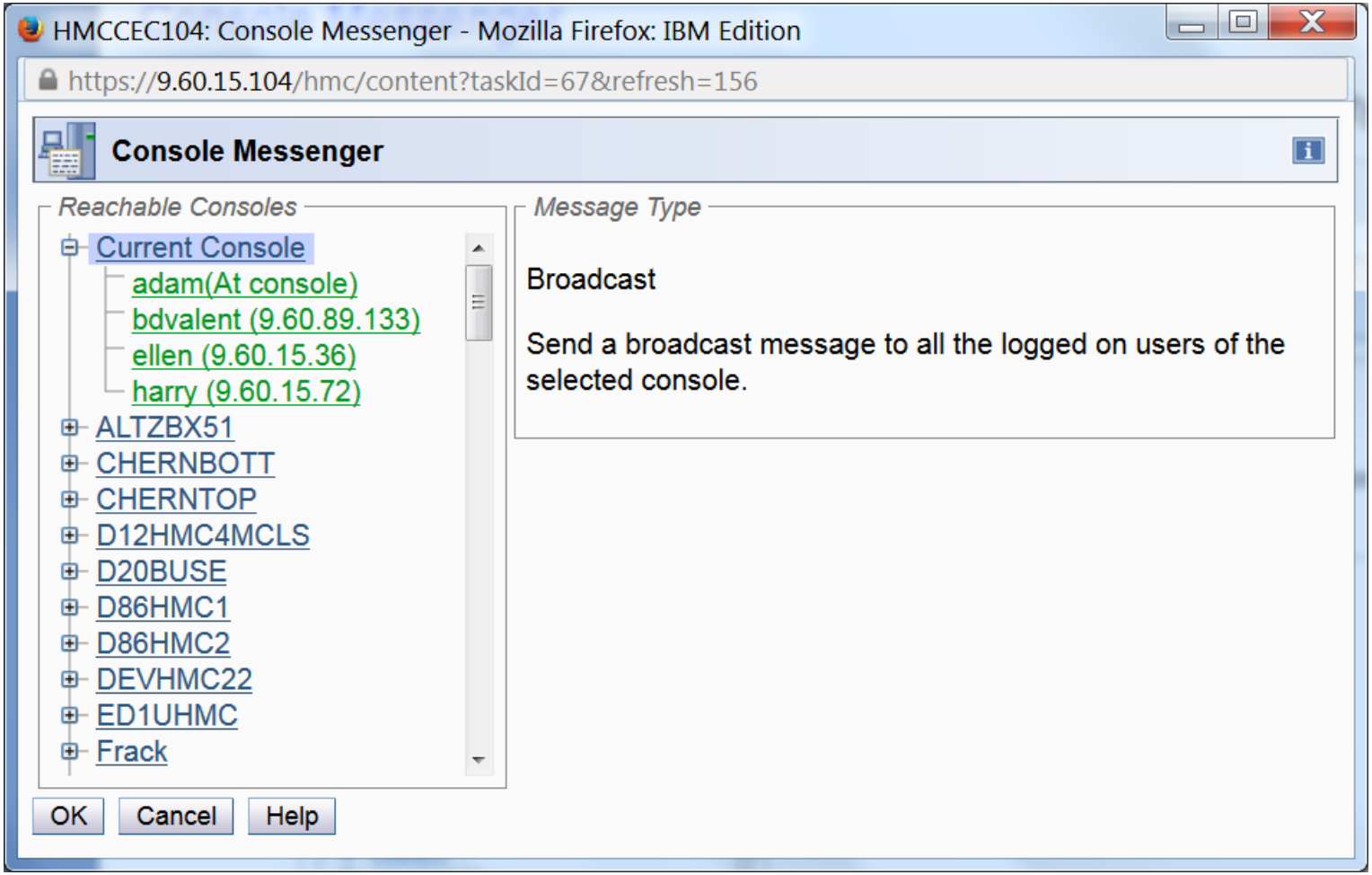
- Must be enabled on the console and for the user



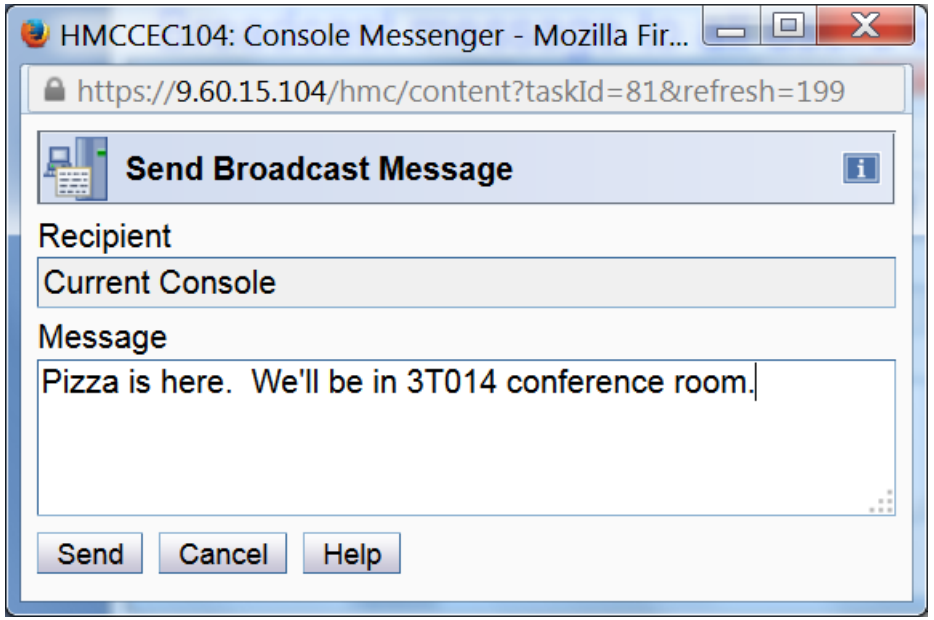


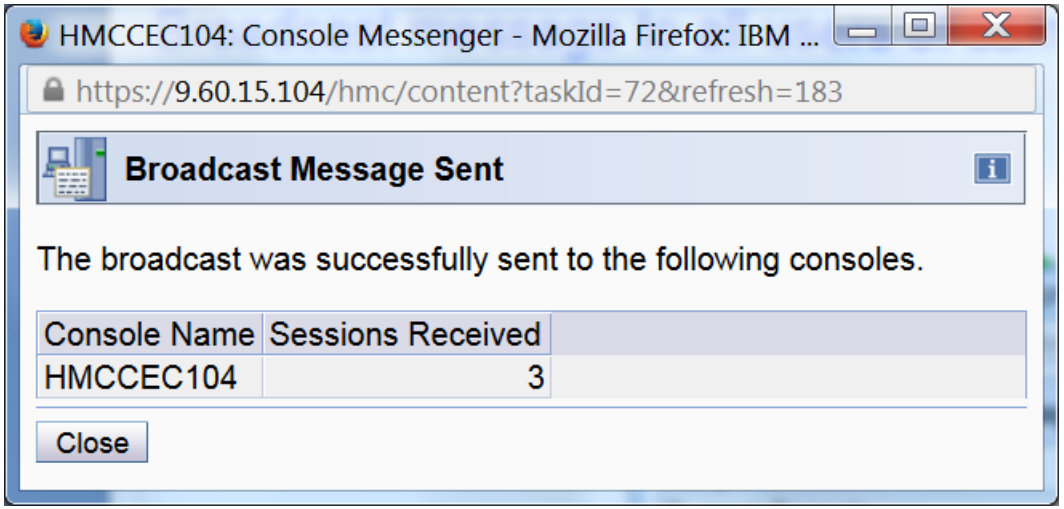
Console Messenger

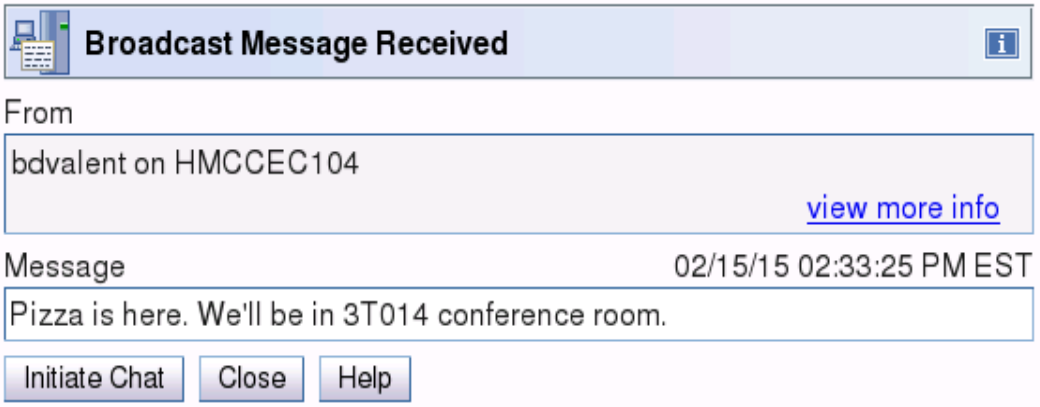
All HMCs with console messenger enabled and with the same security domain are listed.



Broadcast message to all users of same console

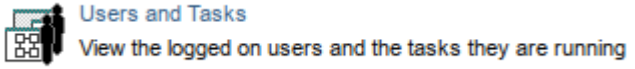






Users and Tasks

- Can also be initiated from the **User and Tasks** task



HMCCEC104: Users and Tasks - Mozilla Firefox: IBM Edition

https://9.60.15.104/hmc/content?taskId=69&refresh=158

Users and Tasks

The following is the list of users currently logged on. The table below lists all tasks running in the system.

Users Logged On

Select	Session Id	User Name	Logon Time	Running Tasks	Access Location	Notes
☐	19	adam	2/15/15 1:51 PM	0	At console	
☑	20	harry	2/15/15 1:54 PM	0	9.60.15.72	
☐	21	ellen	2/15/15 1:56 PM	0	9.60.15.36	
☐	23	bdvalent	2/15/15 2:03 PM	1	9.60.89.133	This is your session

Chat With

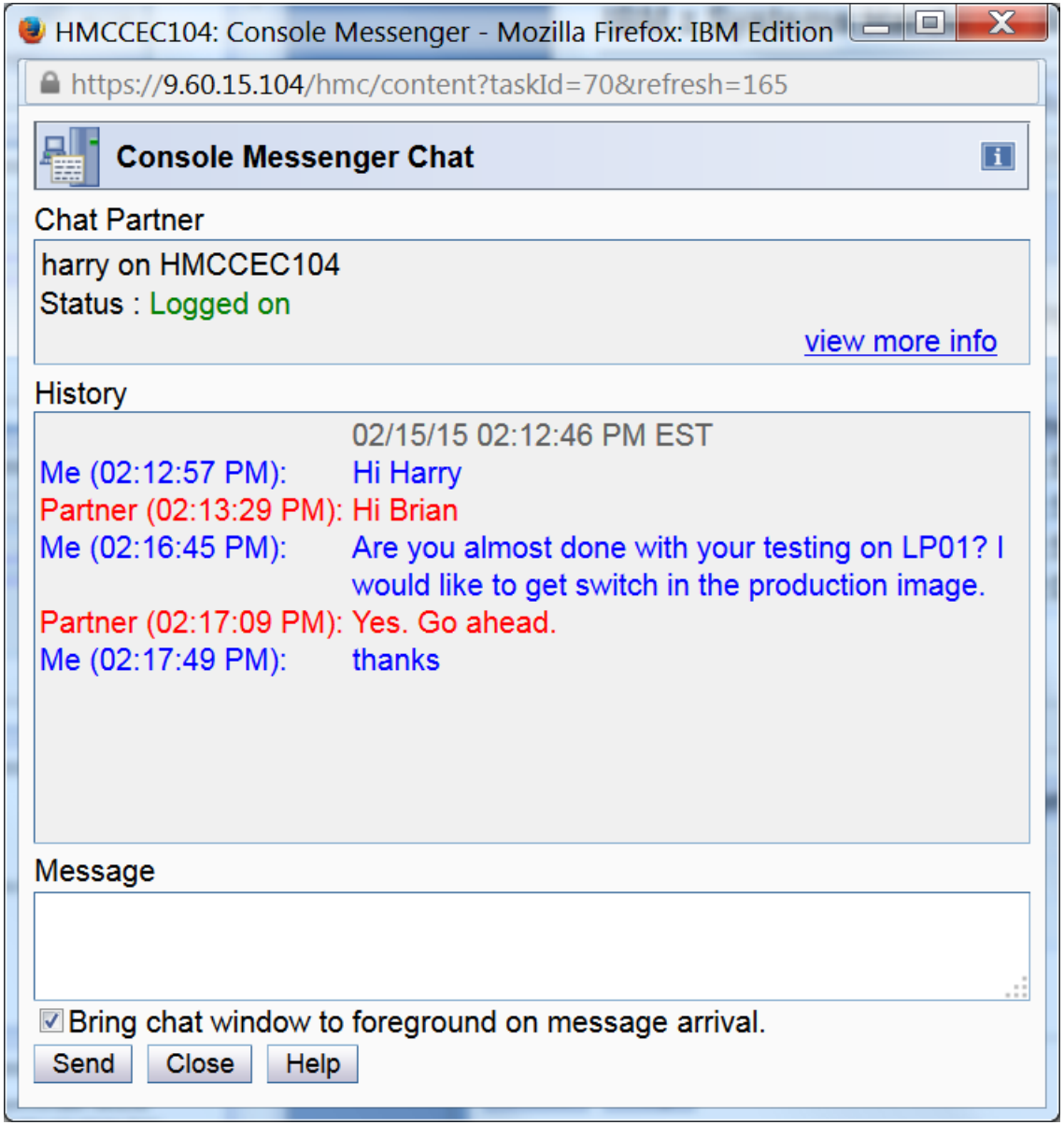
Running Tasks

Select	Task Id	Task Name	Targets	Session Id	Start Time
◉	69	Users and Tasks		23	2/15/15 2:07 PM

Switch To | Terminate

Close | Help

Two-Way Communication



HMC Data Replication

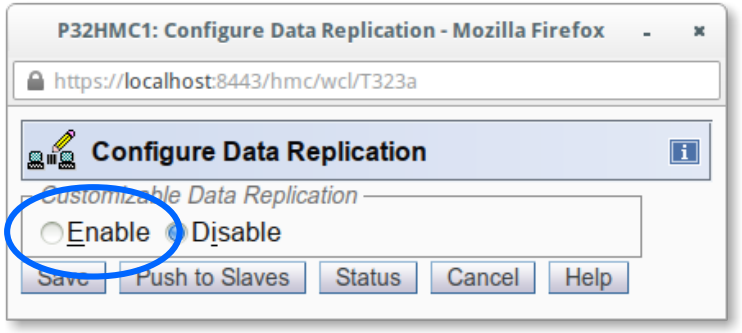
HMC Data Replication

- An HMC task and underlying communication framework
- Allows the exchange of configuration data between linked machines:
  - Acceptable Status Settings
  - Associated Activation Profiles
  - Customer Information Data
  - Group Data
  - Monitor System Events Data
  - Object Locking Data
  - Outbound Connectivity Data
  - User Profile Data
- A convenient way to keep multiple HMC synchronized
- Can be disabled to prevent this exchange
- Exchanges of data (inbound and outbound) are logged

HMC Data Replication (cont.)

- Enabled via **Configure Data Replication** task

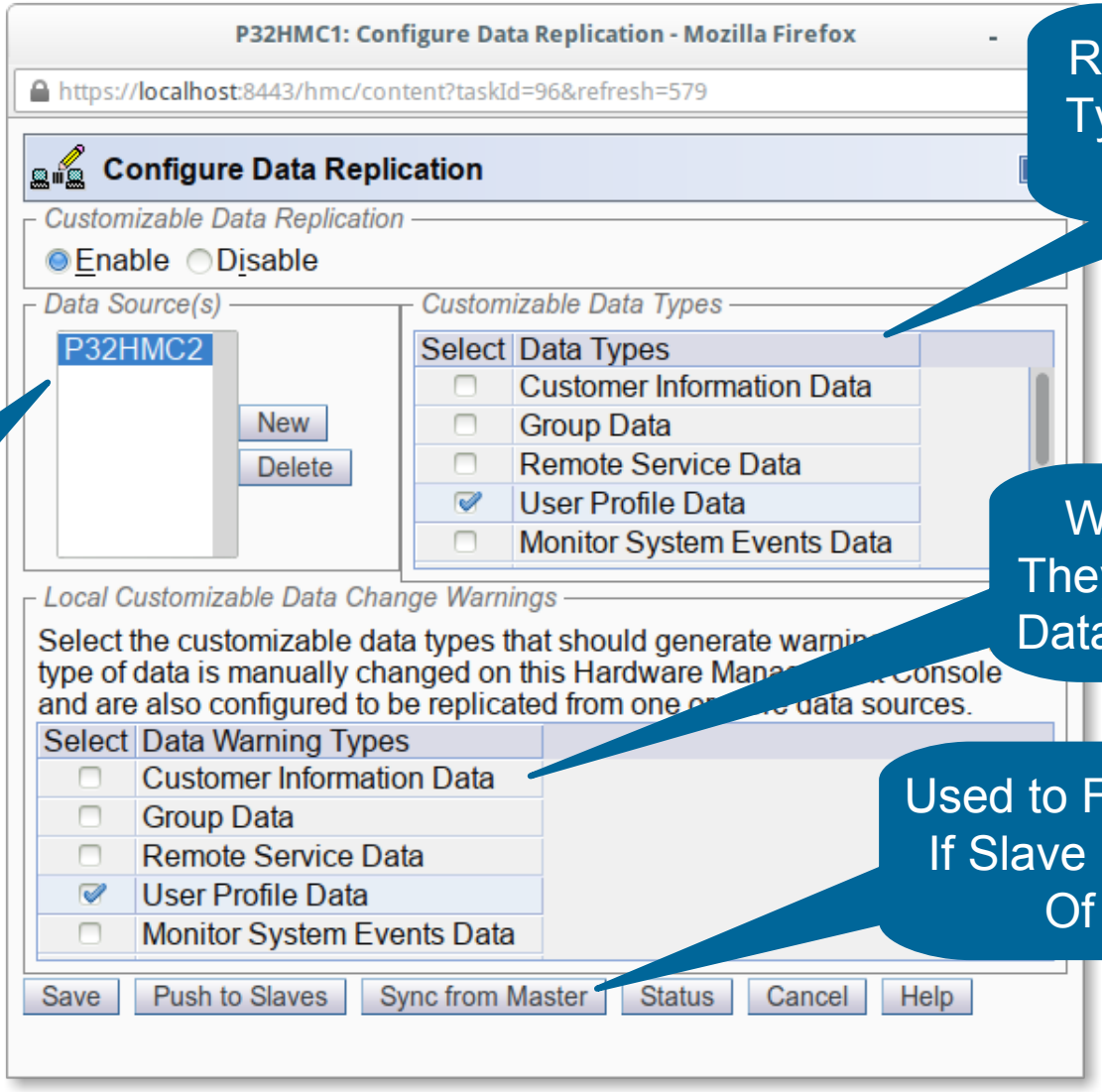
- Occurs from the slave machine
- Master must be runnable/reachable
- Master need not be enabled for slave configuration, but it does need to be enabled for actual data exchange



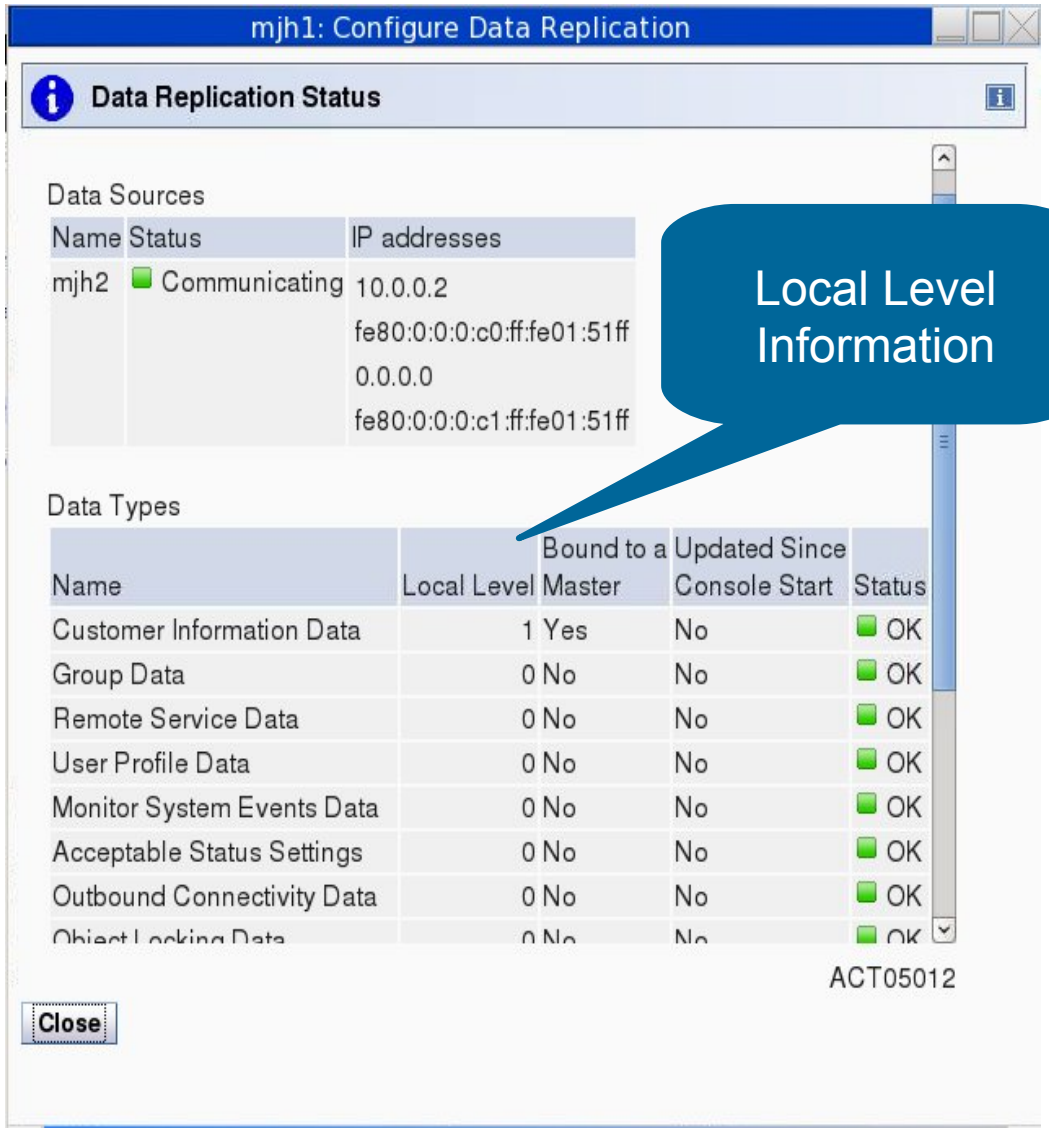
HMC Data Replication (cont.)

- Configuration task allows you to
  - Search for/select masters
  - Select which data types to replicate
  - Establish 'local' modification warnings
    - Warns task user, on the slave, that their changes may interfere with data that is being replicated
    - It may cause a data item to become 'ahead' of the master

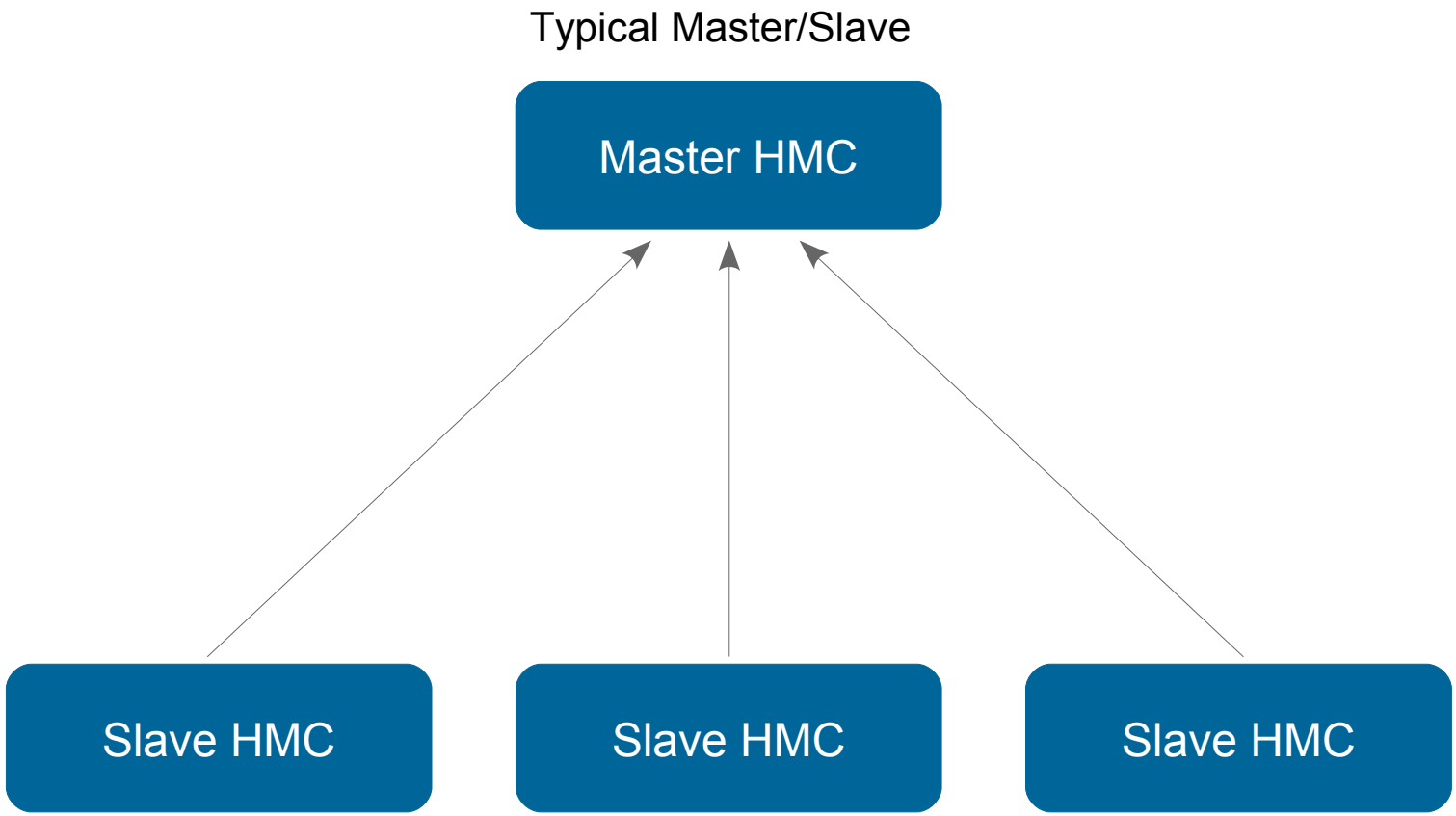
HMC Data Replication (cont.)



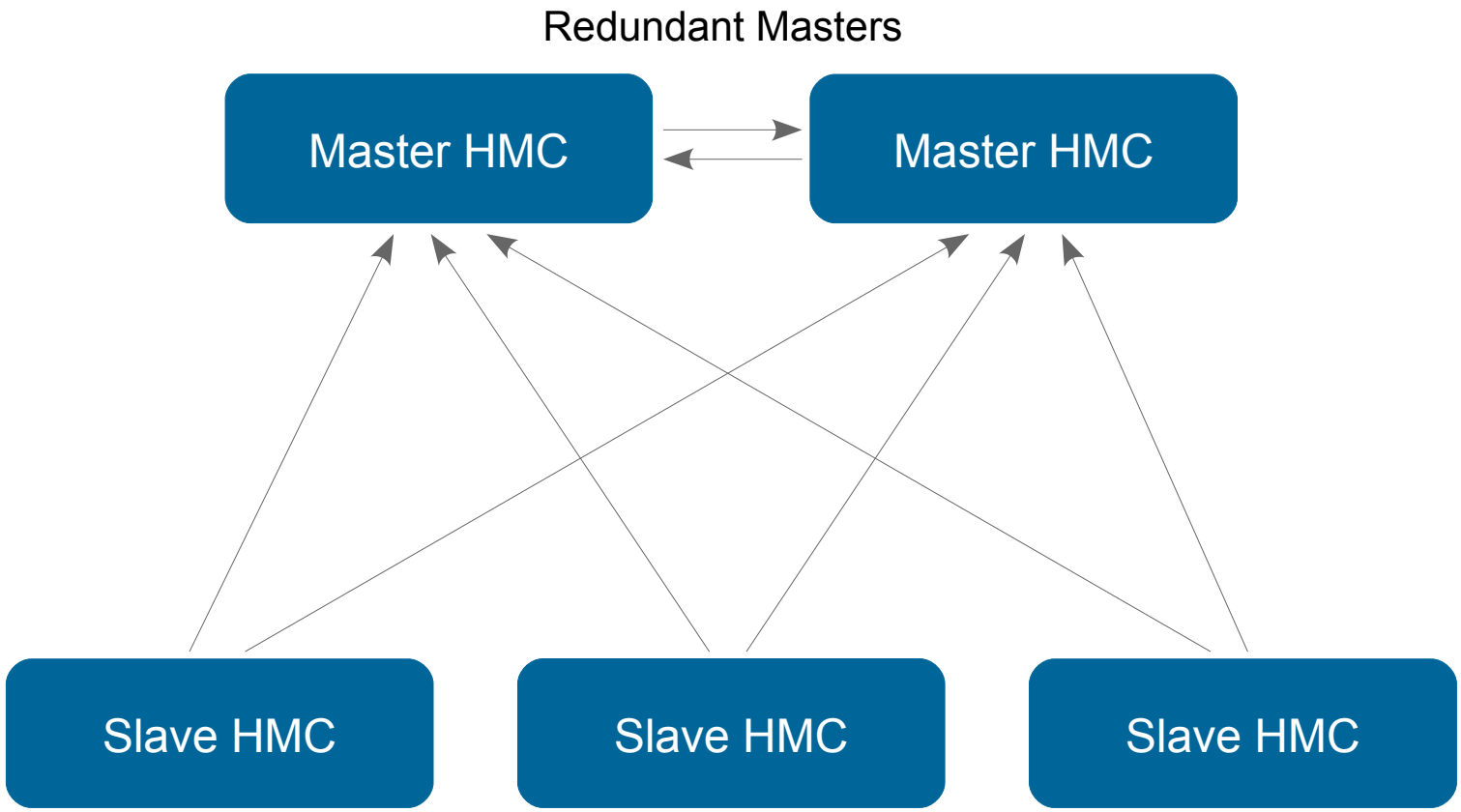
HMC Data Replication (cont.)



HMC Data Replication (cont.)



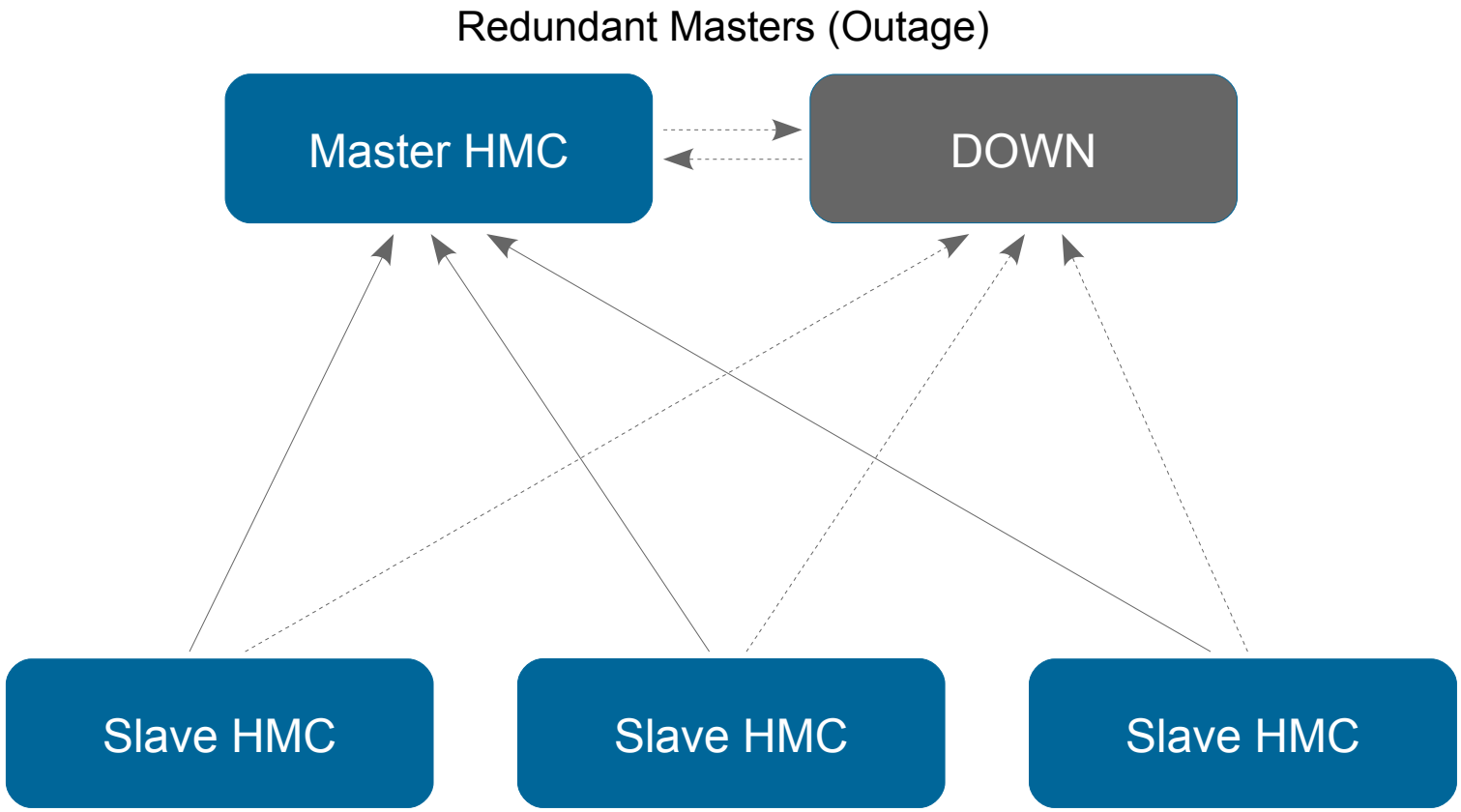
HMC Data Replication (cont.)



Changes made on either master:

- Propagate to all slaves
- And the peer master

HMC Data Replication (cont.)



HMC Certificate Management

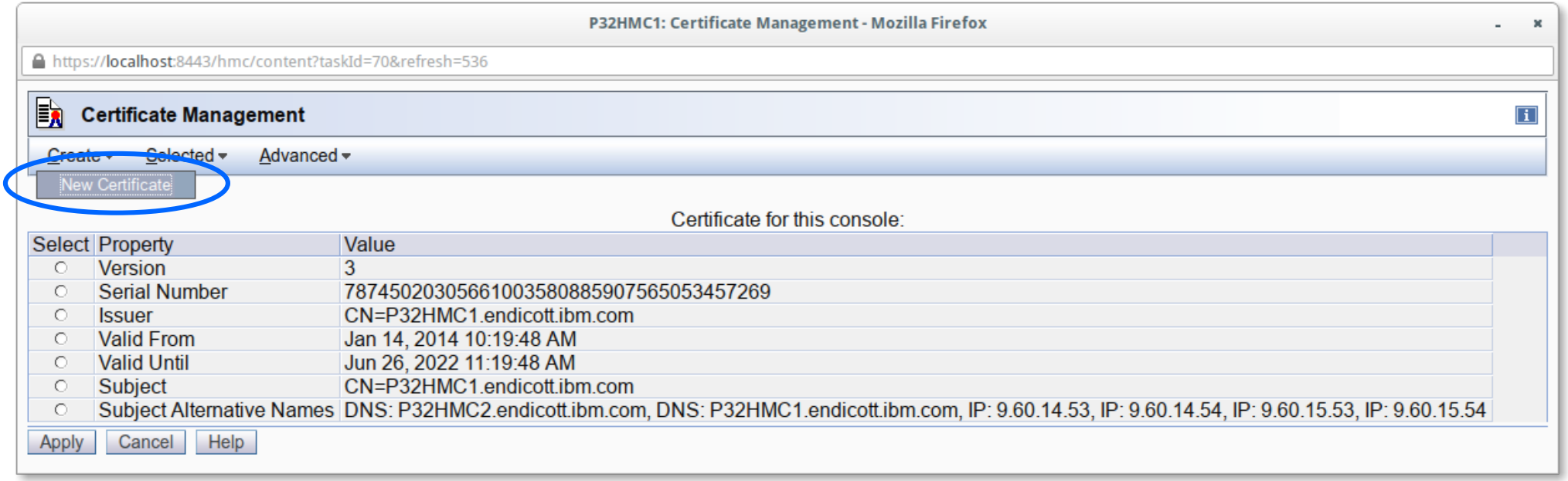
HMC Certificate Management

- Self-signed certificate created at the time of HMC installation
  - Not used until remote communications enabled
- Recommend replacing the self-signed certificate with one signed by a Certificate Authority (CA)
  - If the remote users using a network which potentially isn't secure
- If the self-signed certificate is not replaced and a user adds the certificate as an exception, there is a risk of the HMC being “spoofed” and capturing HMC credentials
- If your company does not have its own CA, you can purchase a certificate from a commercial CA that is already in your browser
  - Check your browser for a list of CA certificates already installed and trusted

HMC Certificate Management (cont.)

- Use the *New Certificate* action in the **Certificate Management** task to change the current certificate

Certificate Management
Create, modify, delete, and import certificates used on the HMC, and view certificate signing information

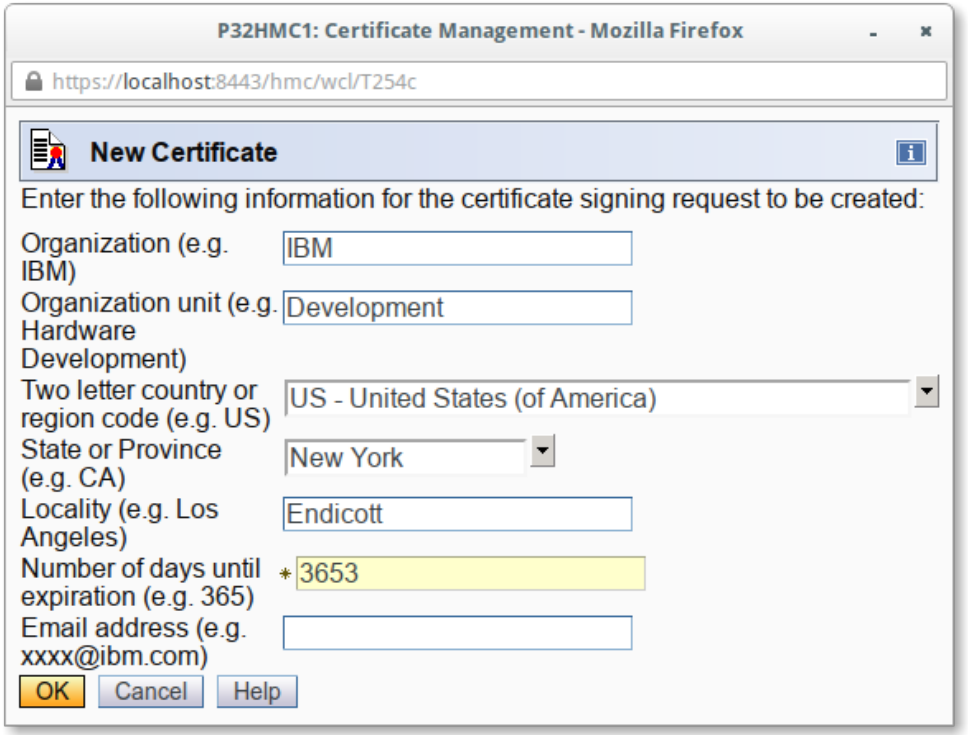


HMC Certificate Management (cont.)

- Select *Signed by a Certificate Authority*

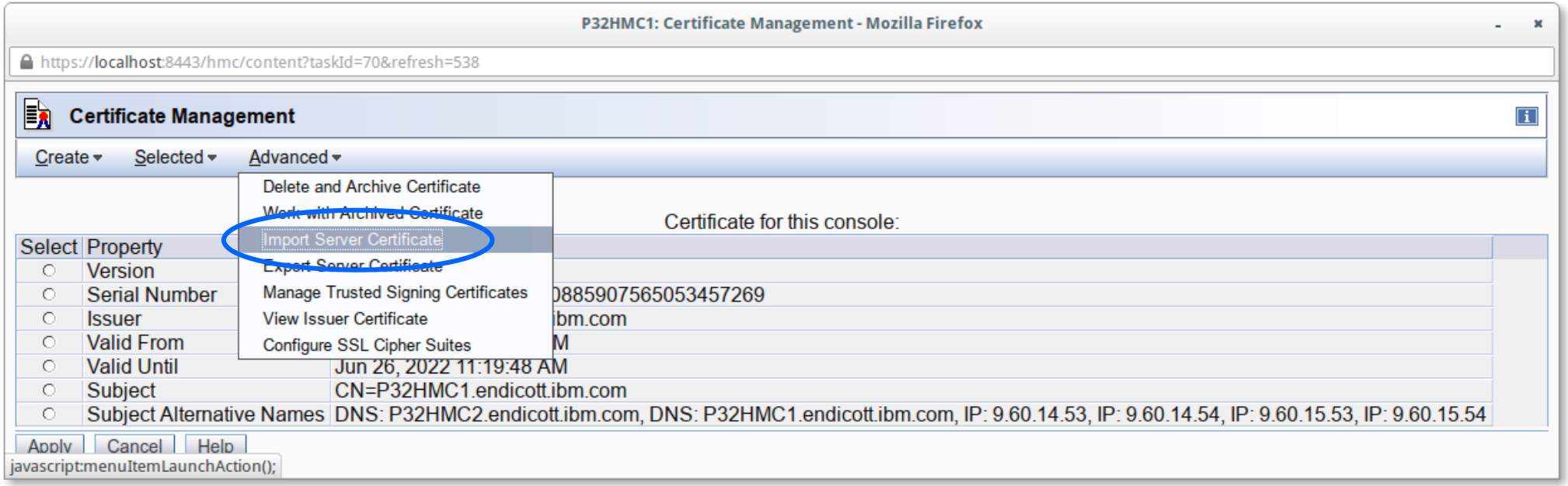
HMC Certificate Management (cont.)

- Fill in the specifics for the HMC (e.g. your organization and company)
- The IP address (v4 and/or v6) and the TCP/IP host name of the HMC is included automatically in the certificate
- You will be guided to write the Certificate Signing Request (CSR) to the USB Flash Drive (UFD)



HMC Certificate Management (cont.)

- After generating a new certificate using the CSR, use *Import Server Certificate* to load the new certificate



- Load the new certificate using removable media
- The new certificate will now be used for new HMC connections

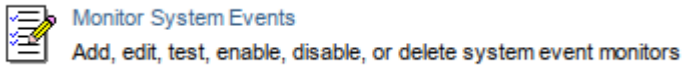
Monitor System Events

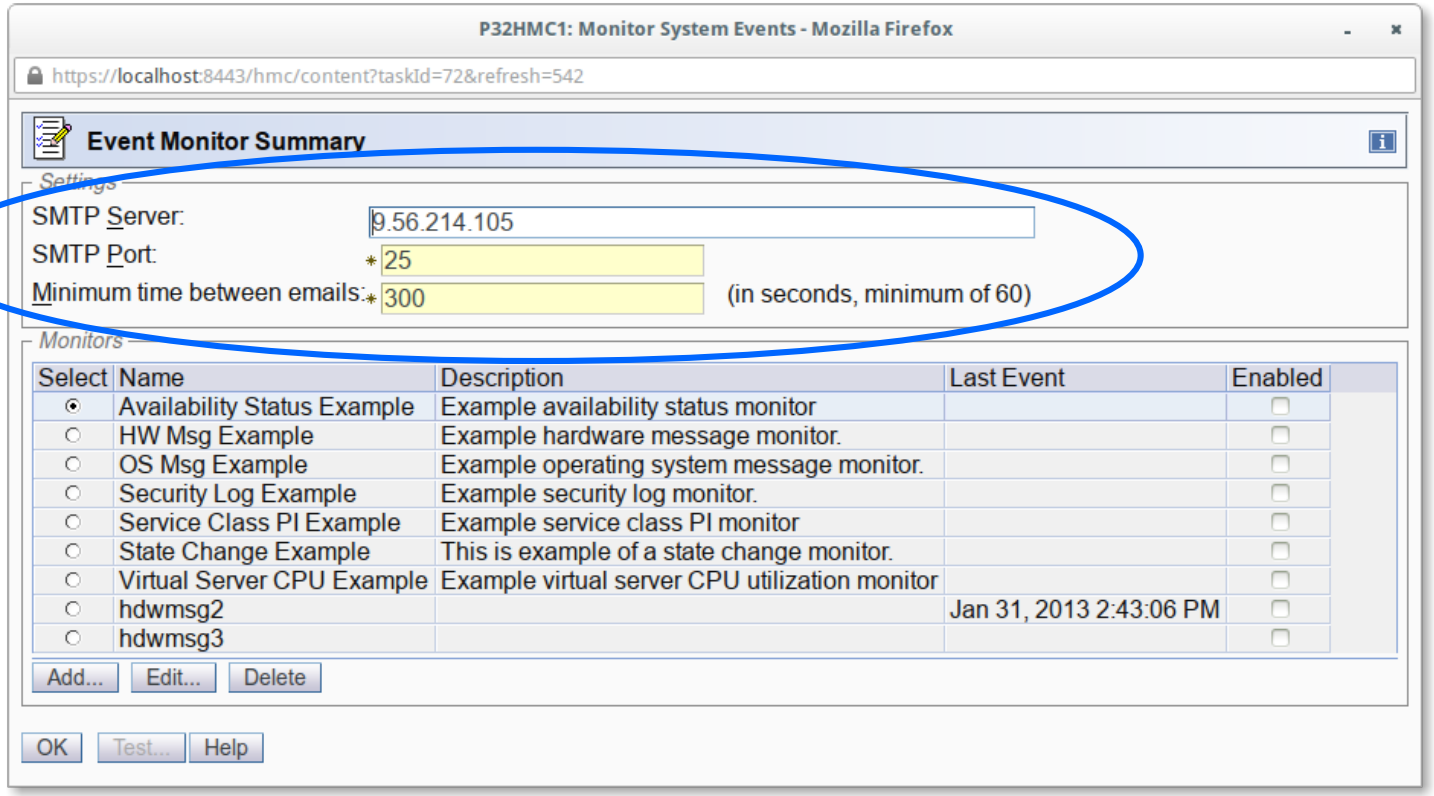
Monitor System Events

- Allows you to receive an email when a particular event happens for objects that you're interested in
- Supported event types
  - State Changes
  - Hardware Message
  - Operating System Messages
  - Security Log
  - Performance Index
  - Availability Status
- Uses an SMTP server to send out email
  - It's recommended that you use a private SMTP server designated just for the HMCs use

Monitor System Events (cont.)

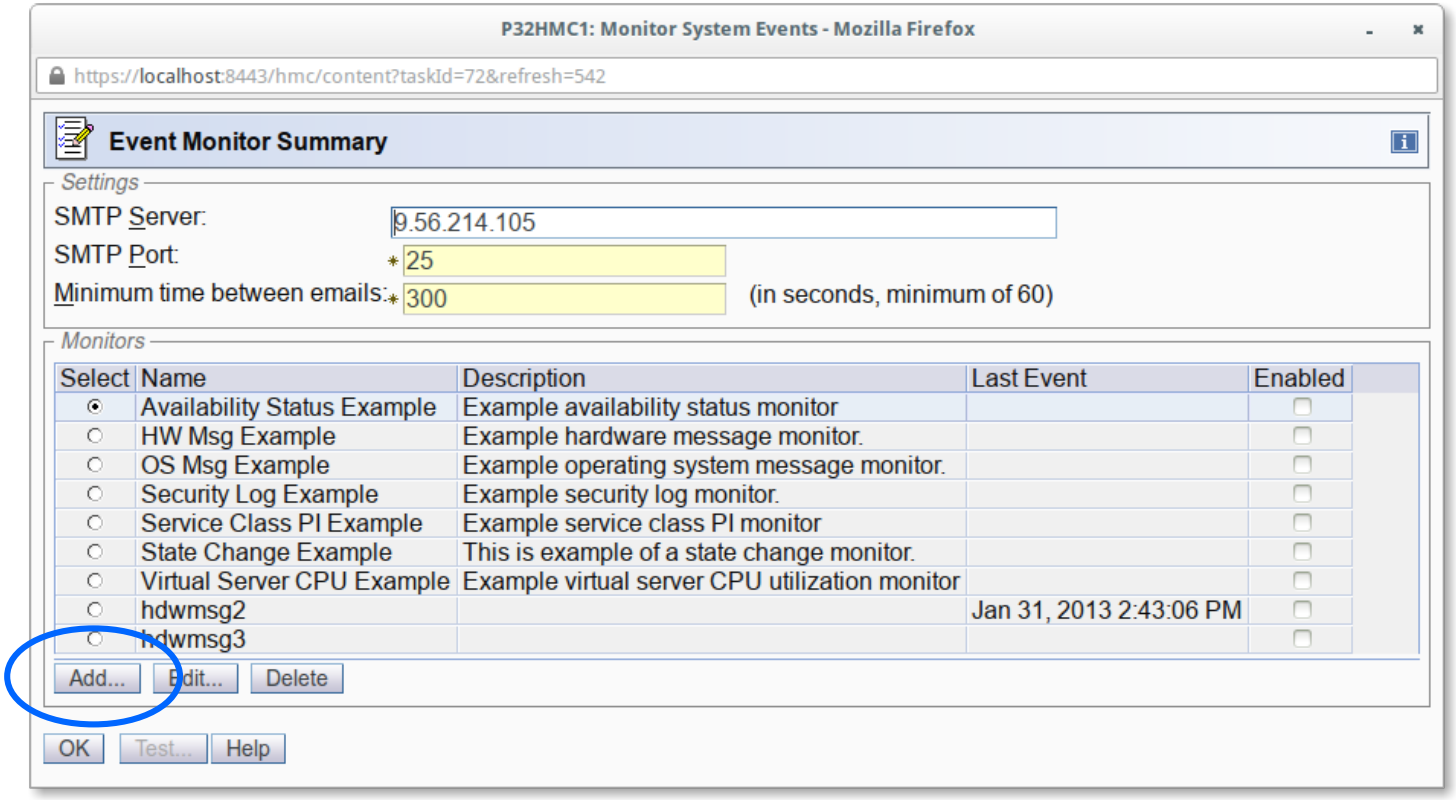
- Launch **Monitor System Events** task
- Configure SMTP settings





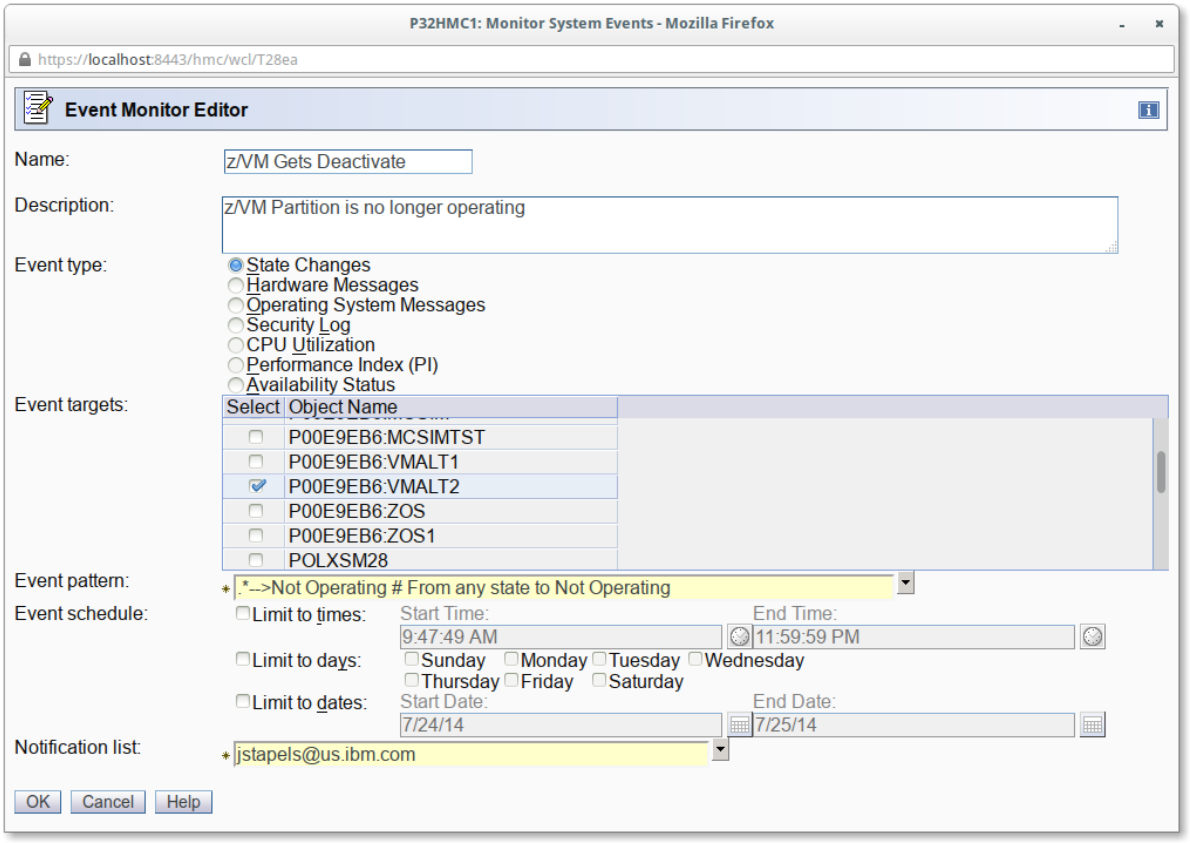
Monitor System Events (cont.)

- Manage existing monitors or click the *Add* button to create a new monitor



Monitor System Events (cont.)

- Enter in a name for the monitor
- Choose the event type
- Select event targets and details
- Select/Enter Event Pattern for matching events
- Limit to a particular schedule
- Enter in one or more email addresses to be notified when the monitor is triggered



Monitor System Events (cont.)

- Email contains events summary since last email

Who	Subject	Date	Size
P32HMC1_EventM	Monitor System Events, Message Count: 1	07/24/2014 10:46 AM	6K

Monitor System Events, Message Count: 1
P32HMC1_EventMonitor to: Jason Stapels

Message Number: 1 **********
Event: 'State Change'
Source: 'P00E9EB6 VMALT2'
Text: 'Operating-->Not Operating'
Time: 'Jul 24, 2014 10:46:24 AM EDT'
Monitor:
Name: 'z/VM Gets Deactivate'
Description: 'z/VM Partition is no longer operating'
Enabled: 'true'
Regular Expression: '.*-->Not Operating # From any state to Not Operating'
Start Time: 'unspecified'
End Time: 'unspecified'
Start Date: 'unspecified'
End Date: 'unspecified'
Active Days: '[Sun, Mon, Tue, Wed, Thu, Fri, Sat]'
Email Addresses: 'jstapels@us.ibm.com'
Locale: 'en_US'

Absolute Capping

Absolute Capping

- Existing ways to cap the utilization of a partition
  - Dedicated processors
  - Active manipulation of LPAR weights (i.e. WLM)
  - capping via LPAR weights
  - Limit number of shared logical processors to physical capping requirement (may actually cause LPAR to have under-defined logical processors as compared to the partition's weight)

Absolute Capping (cont.)

- Potential drawbacks with methods mentioned
  - Dedicated processors
    - Not very granular, may want to cap less than one processor's worth of capacity
    - May not be possible if there aren't enough engines
    - Loses processor utilization efficiency of shared processors
  - Existing shared processor capping is based off of the weight of all **active** partitions
    - Customers may fail to compute the capacity correctly
    - Configuration change (processors add) may lead to more capacity being allocated than desired
  - If partitions are deactivated, other active partitions capping increases
    - If only one shared active partition left, result => no capping (100 % of shared pool)

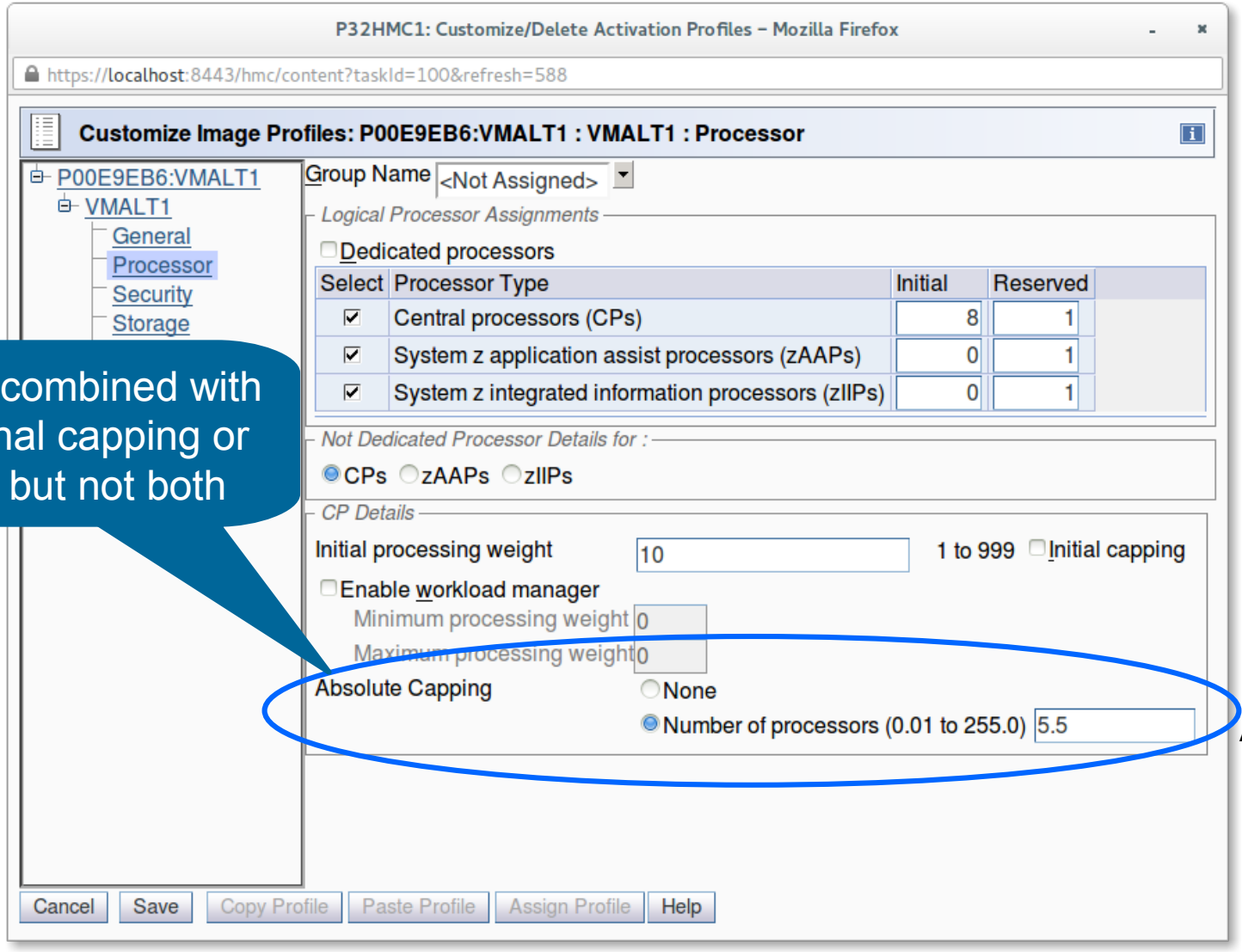
Absolute Capping (cont.)

- Absolute Capping
  - Additional method introduced to ensure software licensing Terms and Conditions related to capacity are always met (ie. Software Pricing)
- A method to define an absolute cap for a given partition
  - If specified, always works independently of any other capping
  - Defines an absolute number of processors to cap the partition's activity to
  - Specified to hundredths of a processor (eg. 4.56 processors) worth of capacity
  - Value not tied to the LICCC processors maximum
    - A value from 0.01 to 255 valid
    - Activation profiles more portable as you migrate to higher machine capacity or newer systems
    - If you specify a value above current machine maximum or number of processors defined for an LPAR (Image), absolute capping will be ignored but other capping means will still be honored

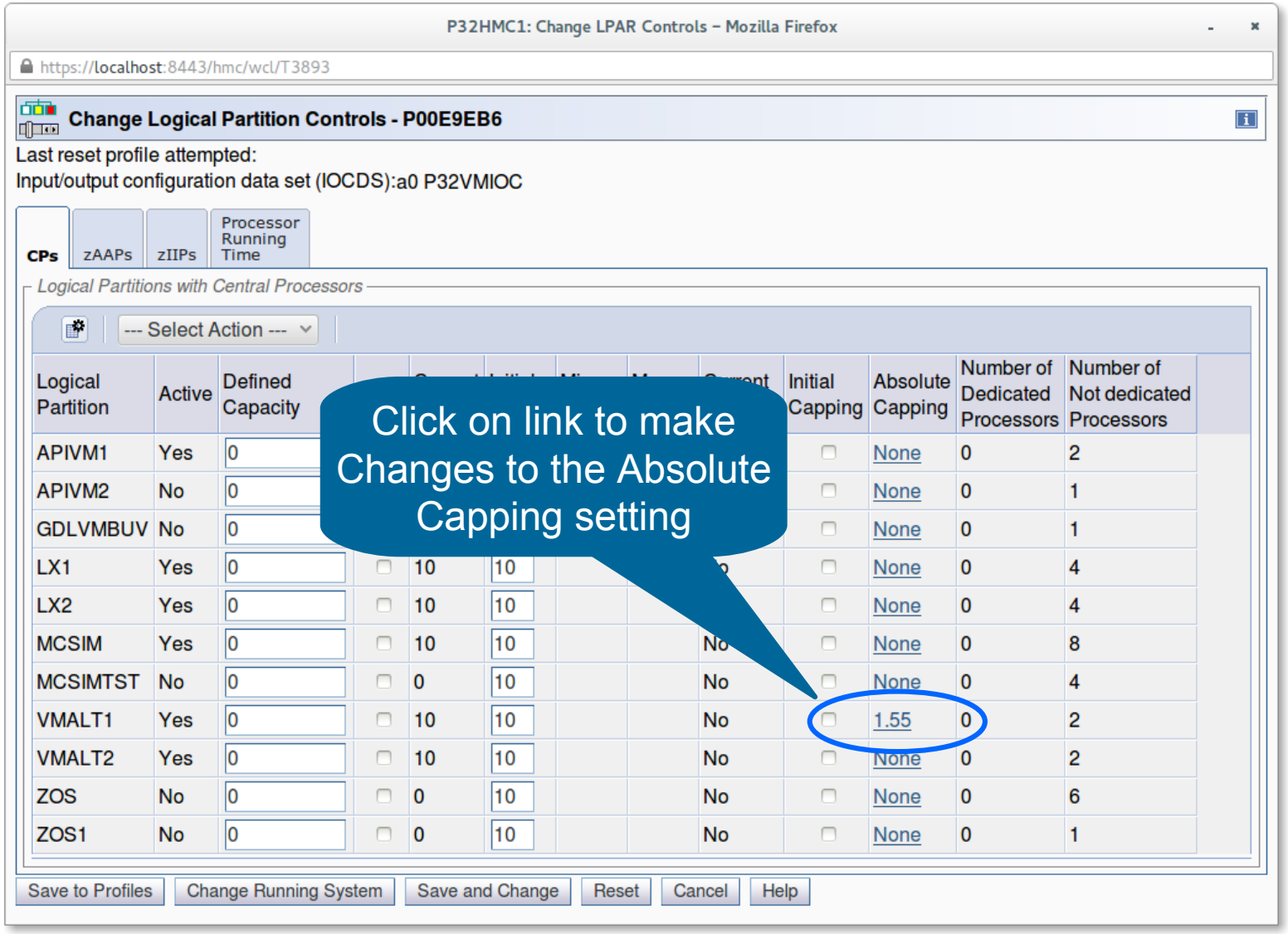
Absolute Capping (cont.)

- Absolute Capping Controls:
  - Activation Profiles
    - Customize Activation Profiles
      - Classic editor
      - Profile wizard
    - Change LPAR Controls Task
    - Change LPAR Weights Scheduled Operation
  - APIs
    - SNMP APIs
    - CIMMOM APIs
    - WebServices APIs

Absolute Capping (cont.)



Absolute Capping (cont.)



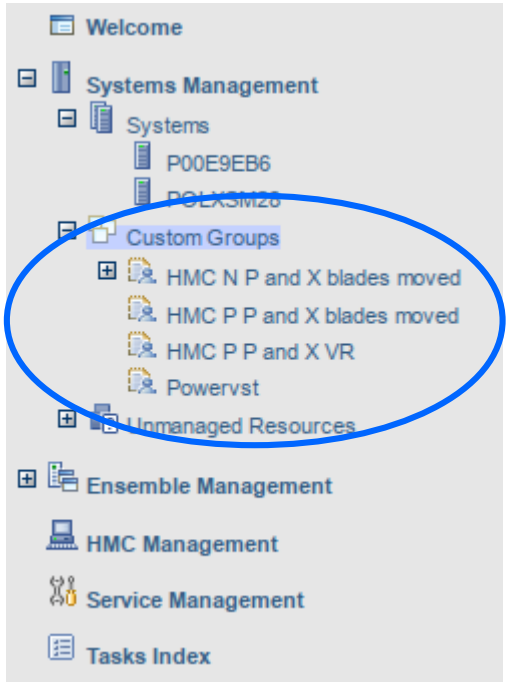
Custom Groups

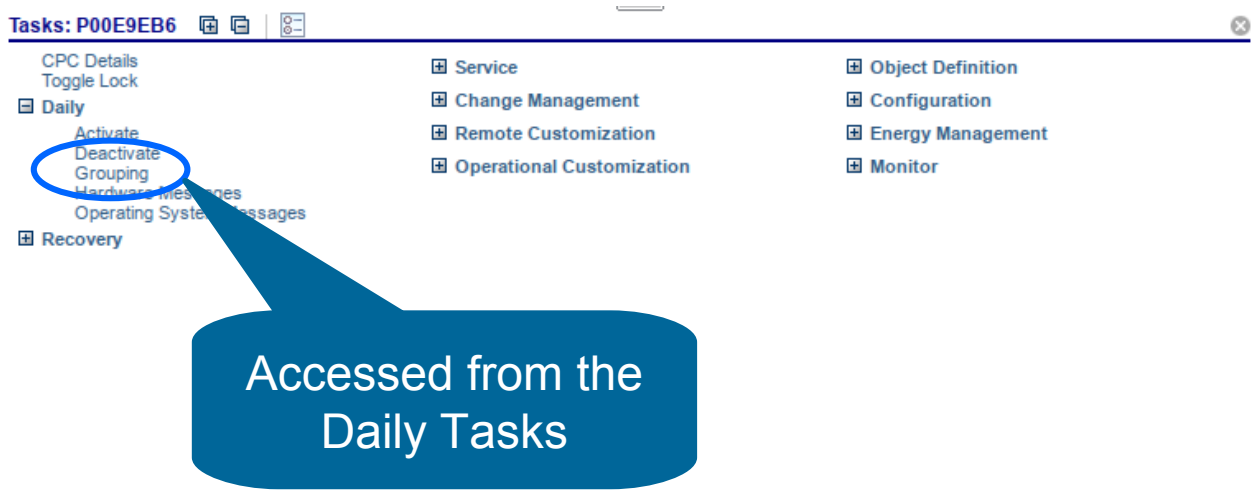
Custom Groups

- A custom group is a set of objects that have been grouped based on a specific set of criteria:
  - Group based on a name pattern
  - Group based on an object type
  - Group based on a specific selection of objects
- A convenient way to work with only the objects that you care about
- Set your group up based on a location or a environment type
- Easily run tasks against the custom group

Custom Groups

- Quickly access from the Tree Navigation pane

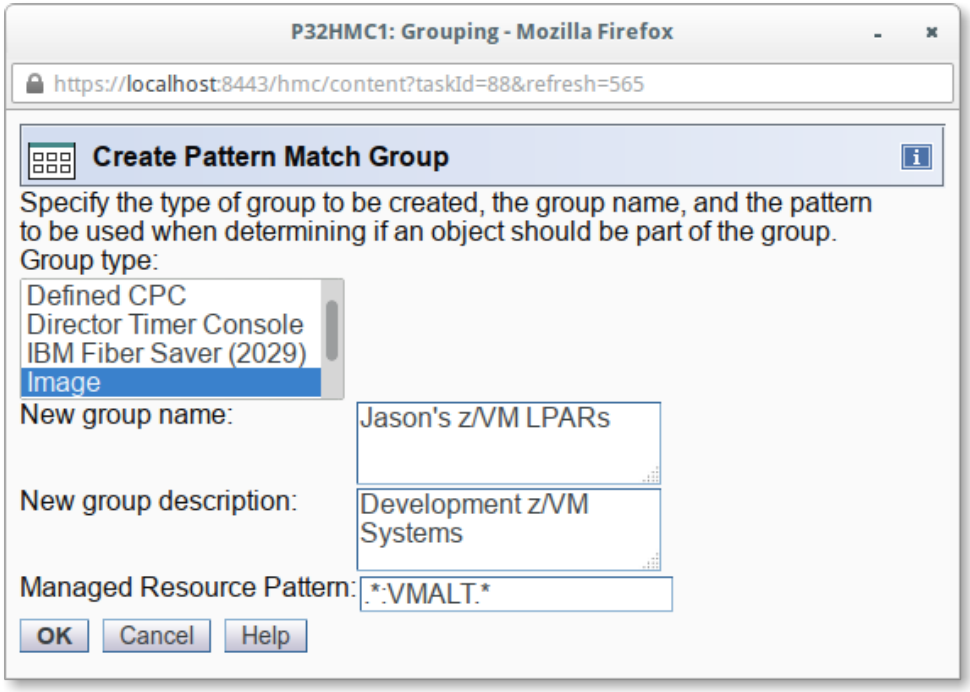


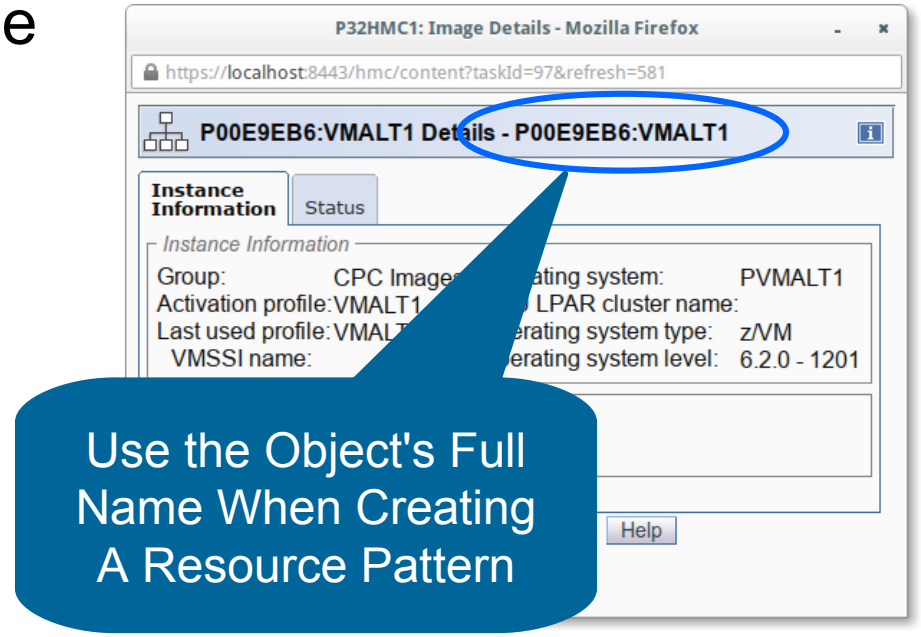


- Use the **Grouping** task to configure

Custom Groups (cont.)

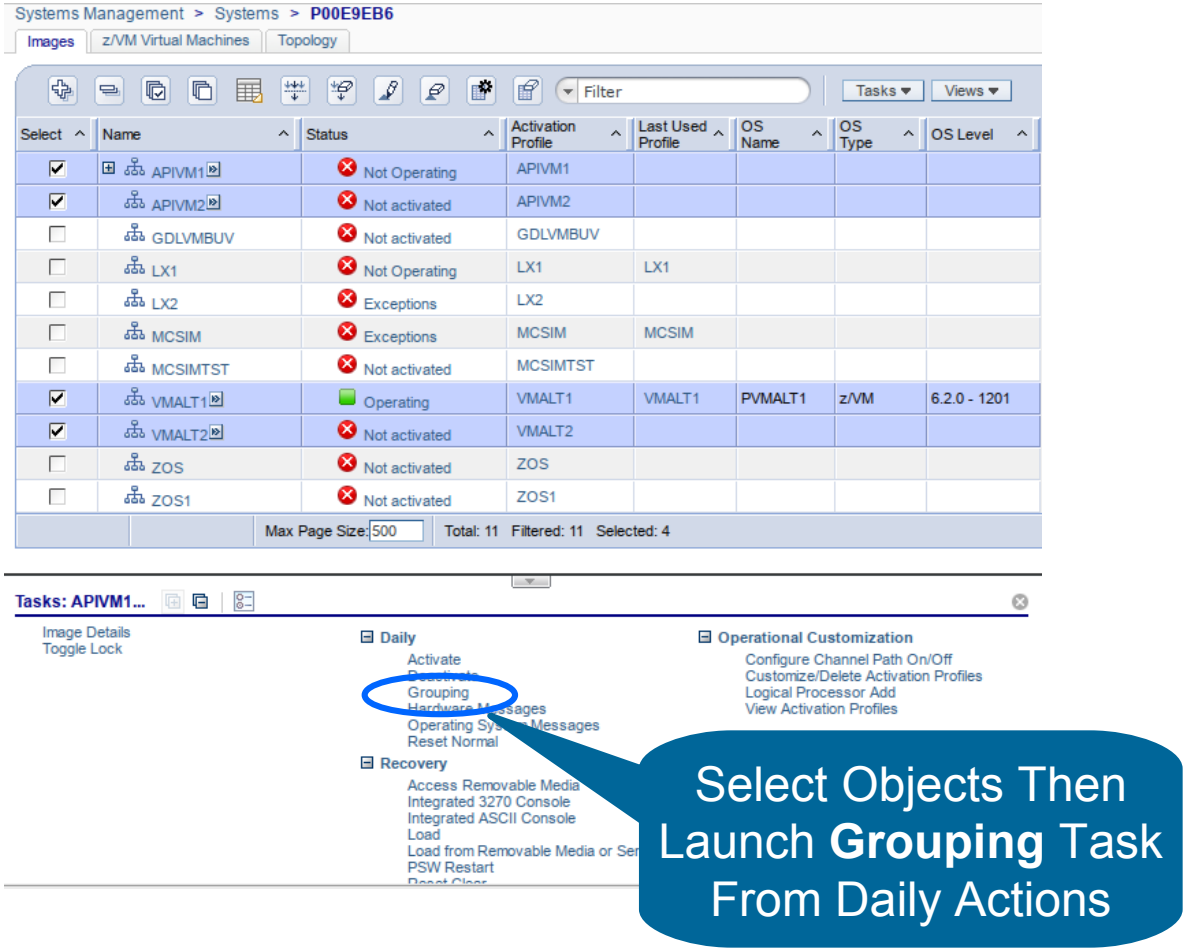
- Creating a new custom group based on name filters
- Be sure to use the FULL object name

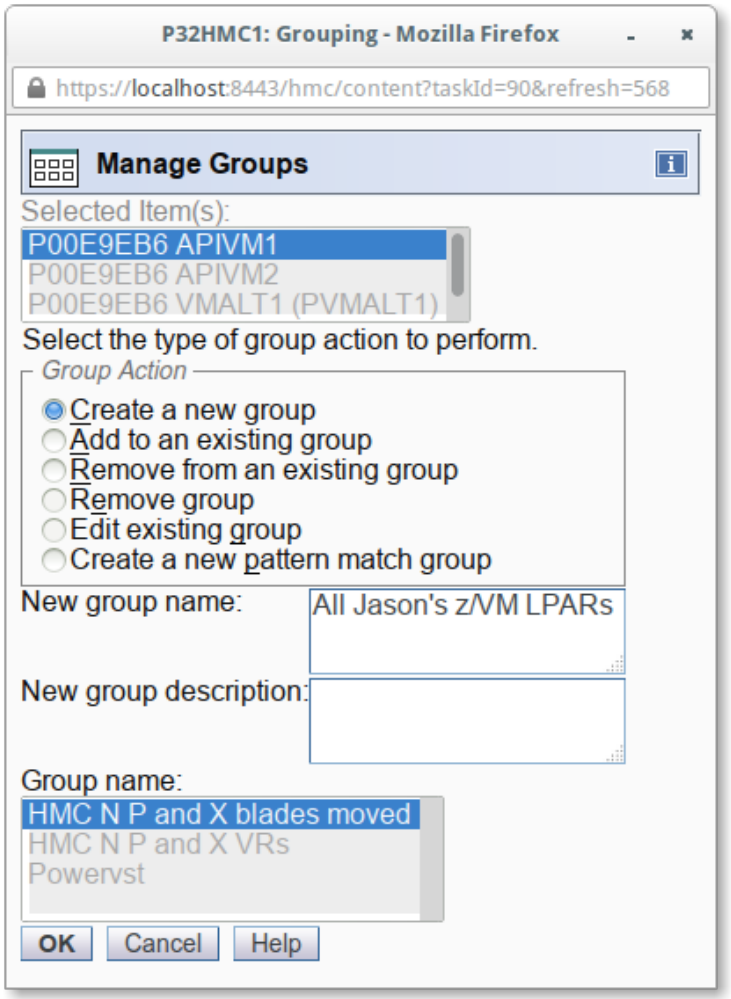




Custom Groups (cont.)

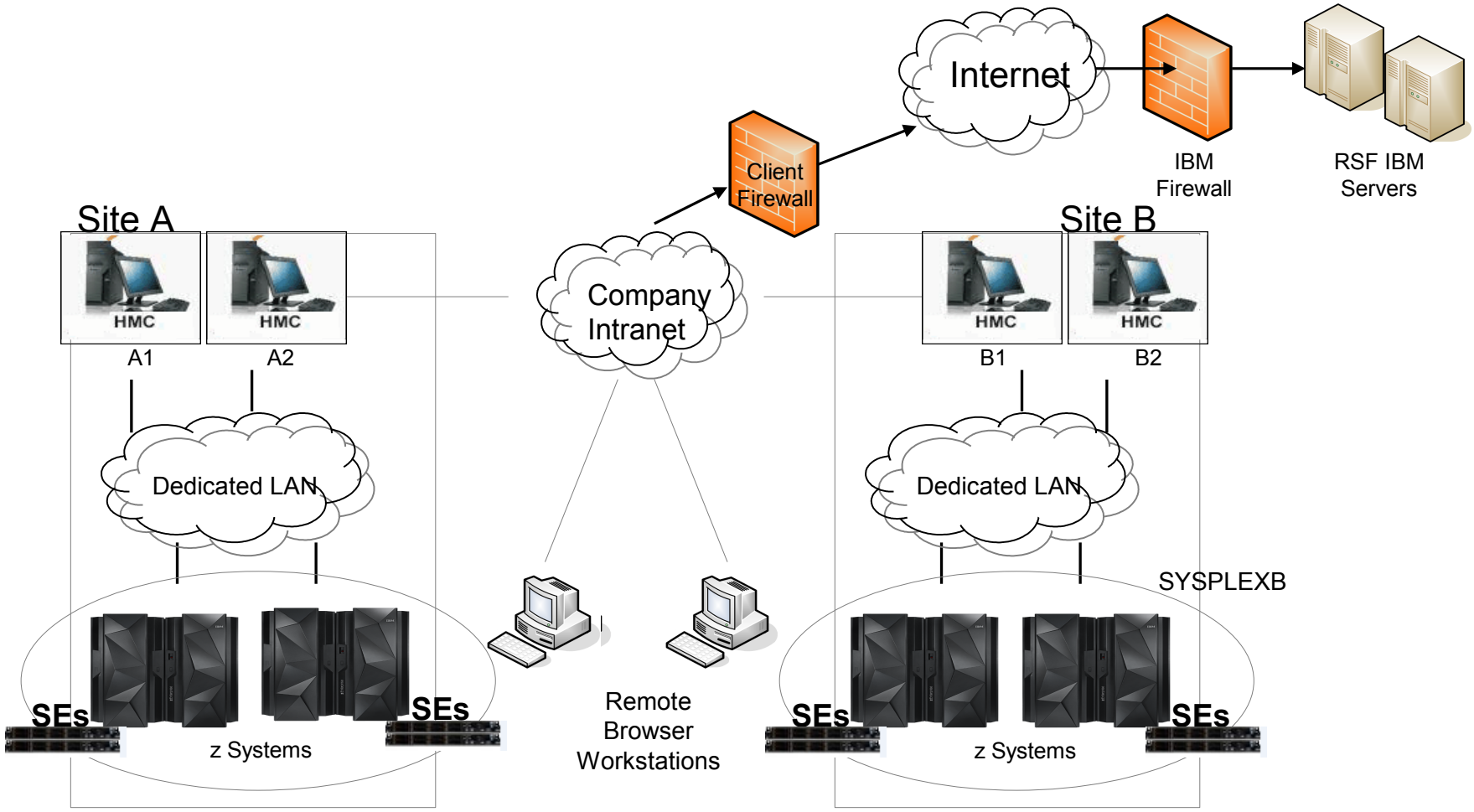
- Or create a group from a selection of objects





Setting up HMCs for Redundancy

Multiple Sysplex Network Topology



Setting up HMCs for Redundancy

- Enable 2 HMCs as Problem Call Home Servers
  - Execute Customize Outbound Connectivity task on each HMC to enable
- Ensure that 2nd HMC Outward Intranet LAN to RSF Servers has outward firewall ports opened for port of multiple RSF servers
  - See HMC 2.13.0 SHARE presentation for list of RSF ips/ports to open
  - Could be two different outward subnets
    - HMC A1 2nd ethernet => subnet intr1, HMC A2 2nd ethernet => subnet intr2
- Have HMCs on different subnet connections to CPCs/SEs
  - Each SE has two network connections
  - Ensure each network connection goes to a different HMC
    - Primary SE em3 => HMC A1 subnet ded1,
    - Primary SE em4 => HMC A2 subnet ded2
    - Alternate SE configured same

Thank you for your time and consideration….

Brian Valentine

HMC/SE Team

Contact for any Questions:

Brian Valentine, (607) 429-4382, bdvalent@us.ibm.com

Other SHARE Sessions of Related Interest

- March 3rd, 10:00 – 11:00 AM
  - **16704:** *The New IBM z13 Part 1: Processor Design, Server Structure, z/Architecture Enhancements, and Operating System Support*
- March 3rd, 11:15 AM – 12:15 PM
  - **16459:** *The New IBM z13 Part 2: Crypto, I/O Design, Features, and Functions, Parallel Sysplex and Implementation Planning*
- March 3rd, 9:30 – 10:30 AM
  - **16705:** *IBM z Systems Hardware Management Console (HMC) 2.13.0*
- March 4th, 1:45 – 2:45 PM
  - **16930:** *IBM z Systems z13 Simultaneous Multi-Threading (R)Evolution*
- March 4th, 3:15 – 4:15 PM
  - **16626:** *How to Make the Most out of BCPii*
- March 5th, 8:30 – 9:30 AM
  - **16821:** *Capping, Capping, and Capping. Comparison of Hard and Soft-Capping Capacity Controls*

Trademarks

Please see
http://www.ibm.com/legal/copytrade.shtml
for copyright and trademark information.