IBM System z Hardware Management Console (HMC) Security

August 7, 2012

SHARE in Anaheim

Brian Valentine
HMC Development
bdvalent@us.ibm.com

Kurt Schroeder
HMC Development
schroedk@us.ibm.com

Patrick Callaghan
HMC Development
patrickc@us.ibm.com

File Updated: 07-31-12

Topics

Topics (cont.)

Topics (cont.)

HMC System support

- **The HMC Version 2.11.1 supports the systems/SE (Support Element) versions shown in the table.**
- **Both Classic and Tree UI Styles supported**

Machine Family	Machine Type	Firmware Driver	SE Version
z114	2818	93	2.11.1
z196	2817	93	2.11.1
z10 BC	2098	79	2.10.2
z10 EC	2097	79	2.10.2
z9 BC	2096	67	2.9.2
z9 EC	2094	67	2.9.2
z890	2086	55	1.8.2
z990	2084	55	1.8.2
z800	2066	3G	1.7.3
z900	2064	3G	1.7.3
9672 G6	9672/9674	26	1.6.2
9672 G5	9672/9674	26	1.6.2

Objectives

- Show the many security related controls available on the HMC and SE consoles
- Explain the benefits and risks associated with the controls
- Describe a best practices approach
- Ultimately, provide knowledge to make business decisions for adhering to your company security policies

Initial State of the Consoles

- Network is locked down initially
  - For the utmost security, limit and/or audit physical access to the SE and HMC consoles
    - e.g. prevents HMC/SE boot from other media
  - Network traffic blocked
- Pre-defined users exist for out-of-the-box configuration
  - After installation, the passwords of the default users must be changed
  - Create your own roles (objects/resources and tasks) and users
    - Consider removing the default users other than ACSADMIN (see the Appendix)
    - The roles of the default users cannot be modified
- You decide how much to open the console and to whom

What do you need to know about the basics of Networking and the HMC?

Do you know all HMC communication is SSL encrypted?

Do you know there are two Network Adapters in HMC?
-- One for Dedicated LAN connection to SEs (System z Servers)
-- One for Remote Browser Users & Broadband connection to RSF IBM Servers

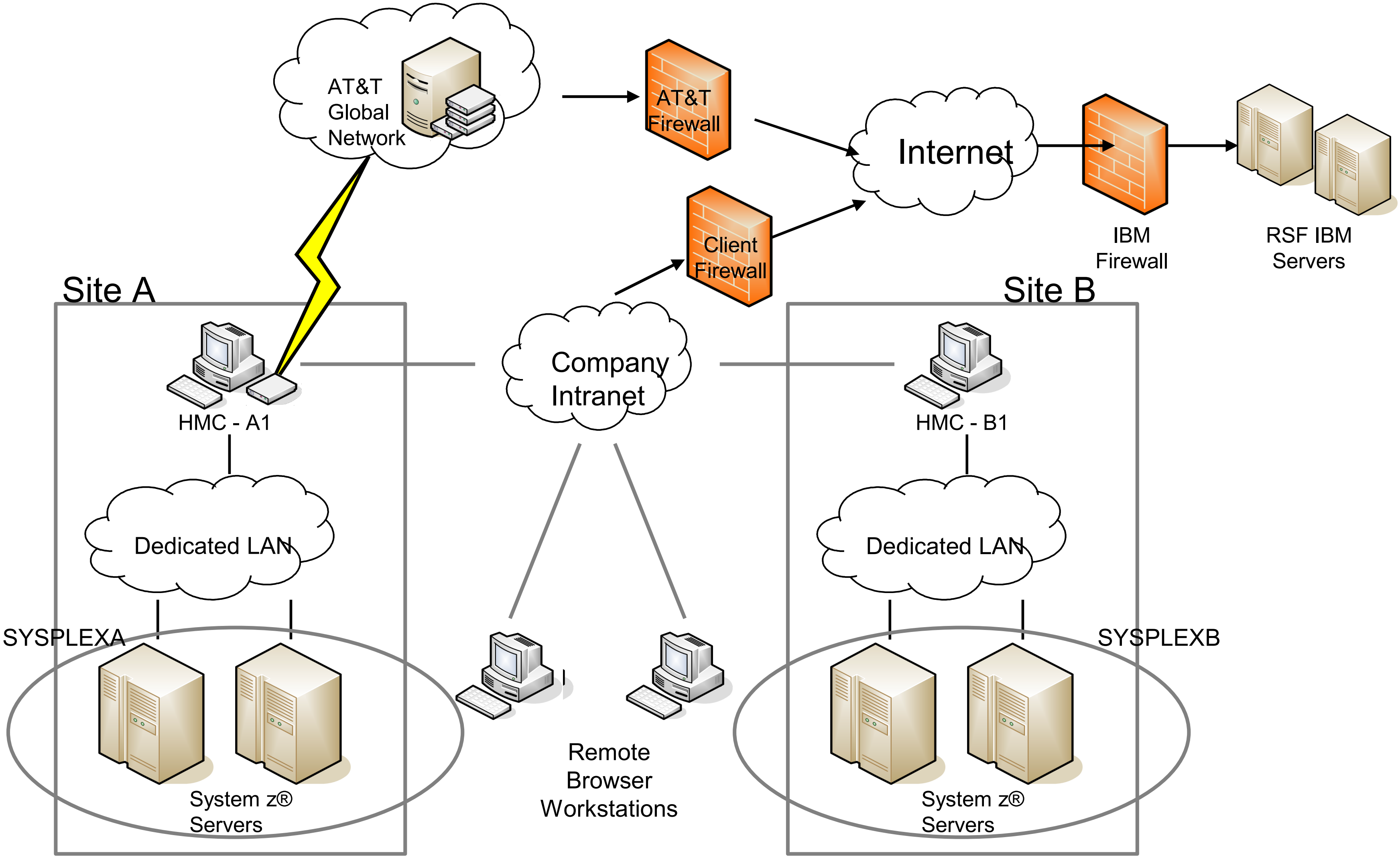
Do you know the HMC has an internal Firewall, & the HMC never acts as a network router?

Do you know that you can further isolate a subset of HMCs & SEs via HMC Domain Security?

Networking Overview

- Both IPv4 and IPv6 network addresses supported for HMC to SE communications and HMC to IBM communications
- SSL encrypted communications
  - HMC to SE
  - HMC to IBM
  - HMC to HMC
  - Remote browser to HMC
- HMC never acts a general purpose IP router
- HMC and SE have a built in firewall to control inbound network connectivity

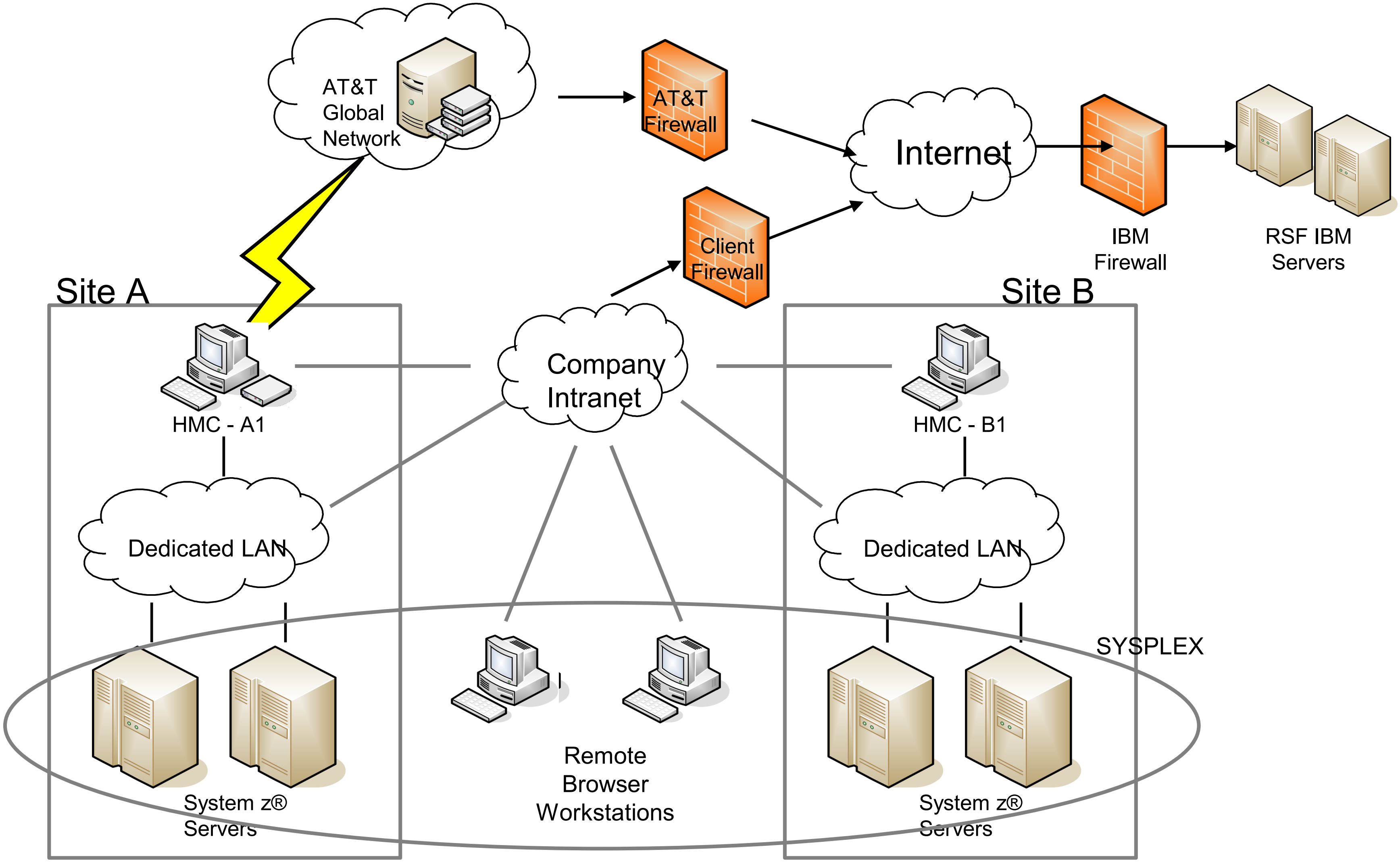
Example Multiple Sysplex Network Topology



Example Multiple Sysplex Topology (continued)

- System z servers at 2 locations; Site A and Site B
  - SYSPLEX does not span both sites
- Dedicated LAN at both sites
  - Could be physical subnet
  - Could be accomplished via VLANS
  - Only requirement is local (from a network point of view) HMC for service
- All HMCs only have connectivity to System z servers at their respective local site
  - HMC-A1 is a call home HMC using dial up connectivity
  - HMC-B1 is a call home server using internet connectivity

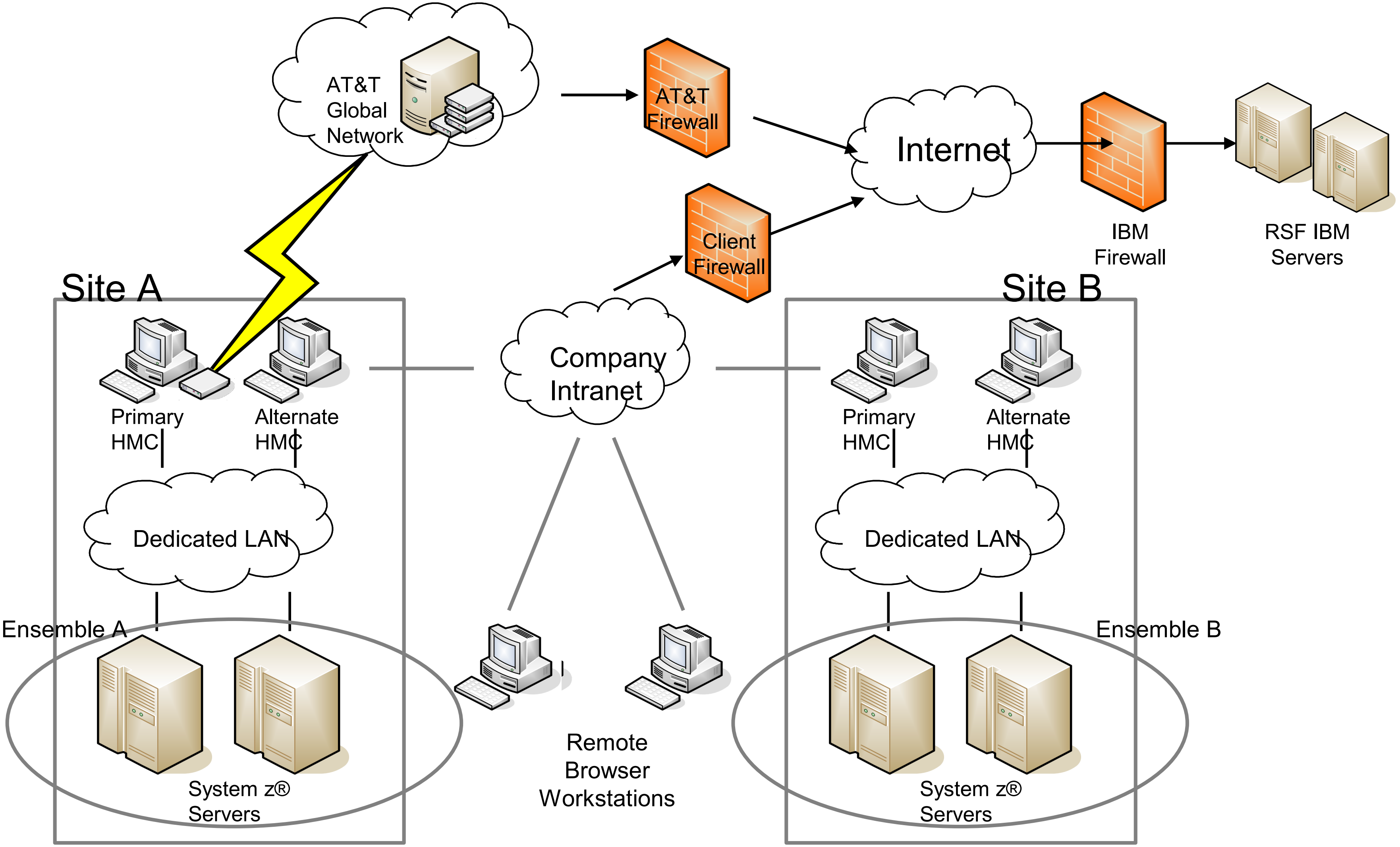
Example Single Sysplex Network Topology



Example Single Sysplex Topology (cont.)

- Systemz servers at 2 locations; Site A and Site B
  - SYSPLEX can span both sites
- Dedicated LAN at both sites
  - Could be physical subnet
  - Could be accomplished via VLANS
  - Only requirement is local (from a network point of view) HMC for service
  - Dedicate LAN now includes a router that allows cross site connectivity
- All HMCs have connectivity to Systemz servers at both sites
  - These HMCs can be defined as “Change Management” HMCs since they have global scope
  - HMC-A1 and HMC-B1 have redundant paths to reach machines at the other site
  - HMC-A1 is a call home HMC using dial up connectivity
  - HMC-B1 is a call home server using internet connectivity

Example Multiple Ensemble Topology



Example Multiple Ensemble Topology (continued)

- System z servers at 2 locations; Site A and Site B
  - Ensembles do not span both sites

- Dedicated LAN at both sites
  - Could be physical subnet
  - Could be accomplished via VLANS
  - Only requirement is local (from a network point of view) HMC for service

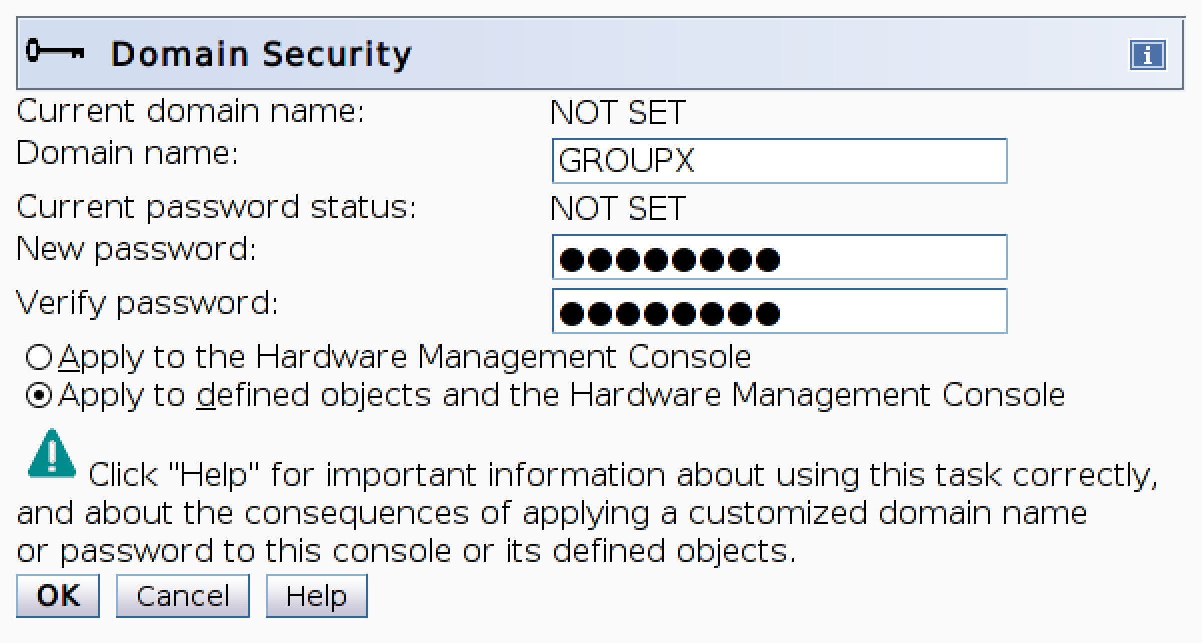
- All HMCs only have connectivity to System z servers at their respective local site
  - Site A Primary HMC is a call home HMC using dial up connectivity
  - Site B Primary HMC is a call home server using internet connectivity

Internal Firewall

- Full function embedded firewall on HMC and SE
- Completely closed by default; services opened as enabled (with the exception of discover port on SE)
- HMC to SE communications ports opened as CPCs are defined to the HMC
- Other ports on HMC/SE opened when enabled; i.e. SNMP, Web Services, Remote Access
- No ability for customer to control the internal firewall other than through enabling HMC/SE features

Domain Security

- Allows for partitioning HMCs and System z server into logical groupings
  - System z servers only allow communications from HMC in the same with the same domain information



Domain Security

Current domain name:	NOT SET
Domain name:	GROUPX
Current password status:	NOT SET
New password:	●●●●●●●●●
Verify password:	●●●●●●●●●

○ Apply to the Hardware Management Console

● Apply to defined objects and the Hardware Management Console

Click "Help" for important information about using this task correctly, and about the consequences of applying a customized domain name or password to this console or its defined objects.

- Easiest way to change is to change all values from the HMC at a single time
- Access administrator can use the “Domain Security” task to define a:
  - Domain name
  - Domain password
- HMCs and System z server have a “default” domain name and password even if not specified by the customer
  - shown as “NOT SET”

What are the benefits of RSF (Remote Security Facility)?

What are the security aspects of RSF?

Should you insert a RSF proxy box?

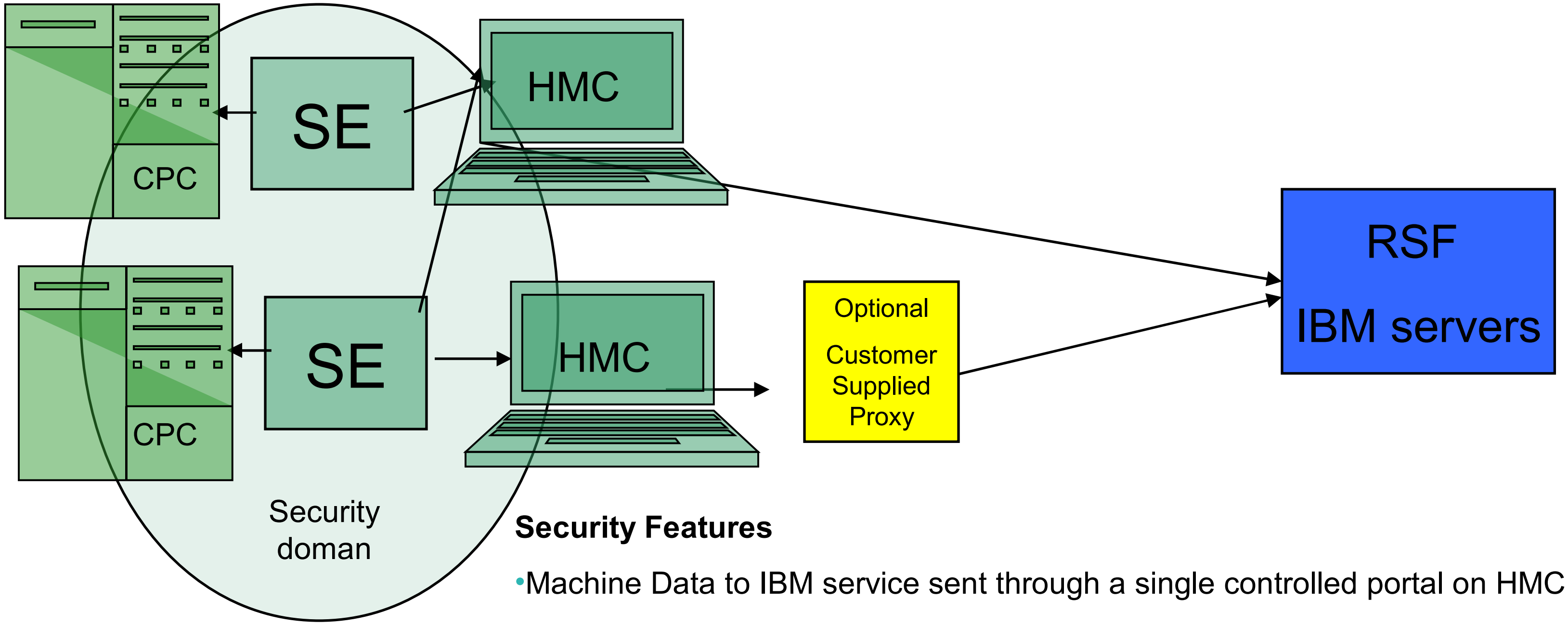
Benefits of configuring HMC connectivity to IBM using Remote Support Facility

- Report failures with recommended parts and/or FFDC information to expedite service
  - 24x7 monitoring by IBM
  - Customer interaction not required
- Expedites Customer Initiated Upgrade processing
- Provide ability for automatic scheduled fix downloads
- Provide IBM with specific hardware configuration, installed firmware levels to enable customized recommendations for preventive maintenance
- Prime system usage information for viewing using IBM Resource Link portal

Remote Support Functions at a Glance

- **Problem Management**
  - Automatic Problem Reporting
  - Support electronic transmission of additional diagnostic data for problem diagnosis
  - Repair information
- **On Demand**
  - Permanent and Temporary upgrades
  - Capacity Backup
- **Fix Management**
  - Download microcode fixes from IBM
  - Enable clone of system configurations
- **Hardware data for IBM analysis**
  - Vital Product Data
  - System Availability Data, performance and usage

Hardware communications to IBM



Security Features

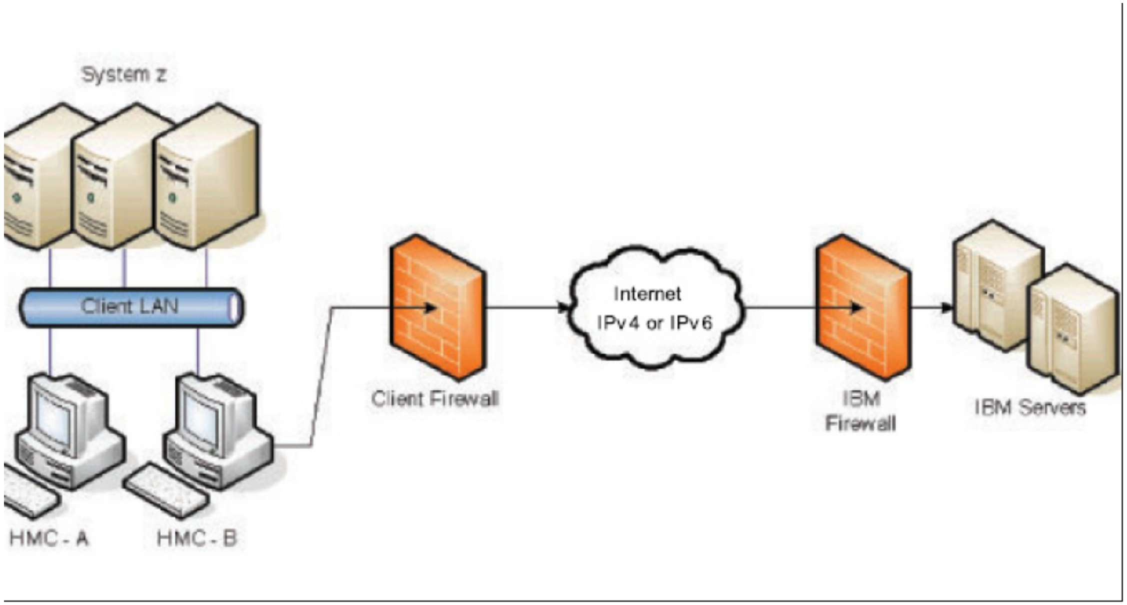
- Machine Data to IBM service sent through a single controlled portal on HMC
- Call home support is disabled by default
- HMC and SE record all outbound connections in event logs
- No NIC connection from Support Element or CEC to internet
- Separate ethernet adaptors to isolate interactions …
  - Private network from SE to CEC
  - HMC to SE
  - HMC to internet

RSF connectivity attributes

- Only HMC outbound connections are initiated. The HMC firewall prohibits the inbound connection
- IPv4 and/or IPv6 customer networks are supported
- SSL used to encrypt all data going over the wire, and to verify that the digital certificate of that the target destination is the IBM support site.
- All connections are routed to RSF IBM servers that are designed for high redundancy.

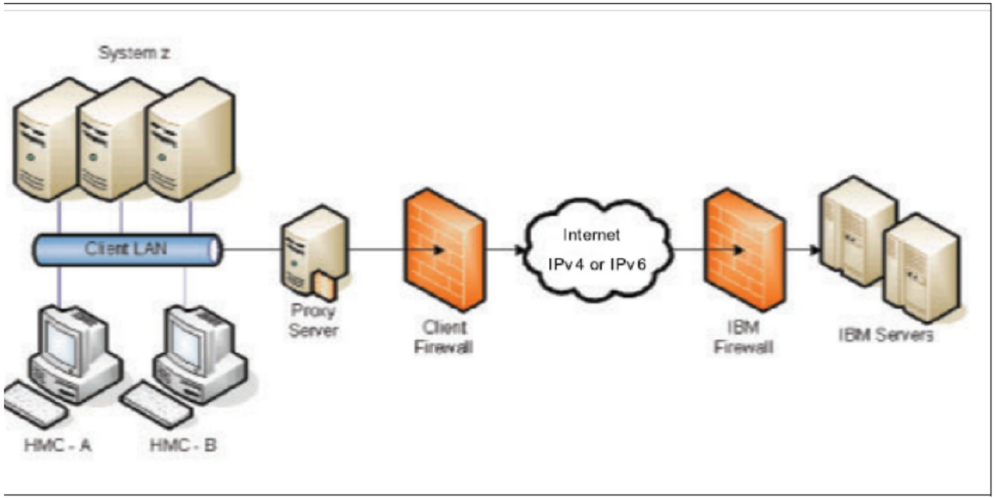
Direct Internet connection

- Recommend placing behind customer firewall
- HMC firewall ports automatically Customer firewall ports must open to documented addresses
- HTTPS connection
- SNAT (source net address translation) supported

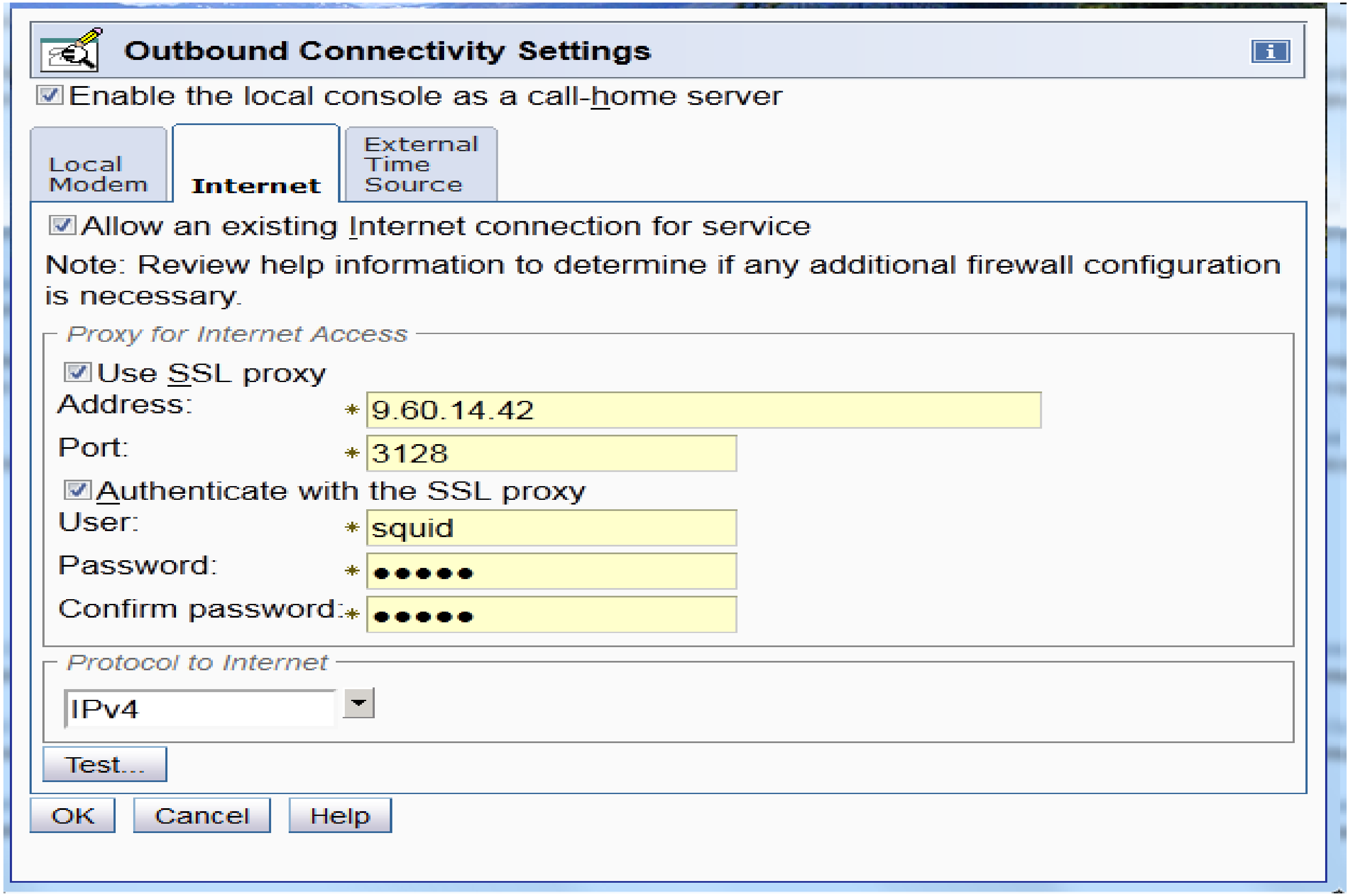


Proxy (indirect) Internet connection

- Customer provided proxy forwards requests to IBM
- Customer proxy can provide additional functions like audit, address translation .
- Customer HTTP proxy and/or firewall must be configured allow port 443 outbound. Connect Method on proxy uses documented ip addresses
- Data is encrypted by the HMC prior to transmission through the proxy
- HMC connects through Proxy to IBM using HTTP CONNECT method (per RFC 2616)
- Optional basic authentication from the HMC through proxy is supported (RFC 2617)



Configuring Outbound Connectivity using Proxy



Outbound Connectivity Settings

☑ Enable the local console as a call-home server

☑ Allow an existing Internet connection for service

Note: Review help information to determine if any additional firewall configuration is necessary.

Proxy for Internet Access

☑ Use SSL proxy

Address: * 9.60.14.42

Port: * 3128

☑ Authenticate with the SSL proxy

User: * squid

Password: * ●●●●●

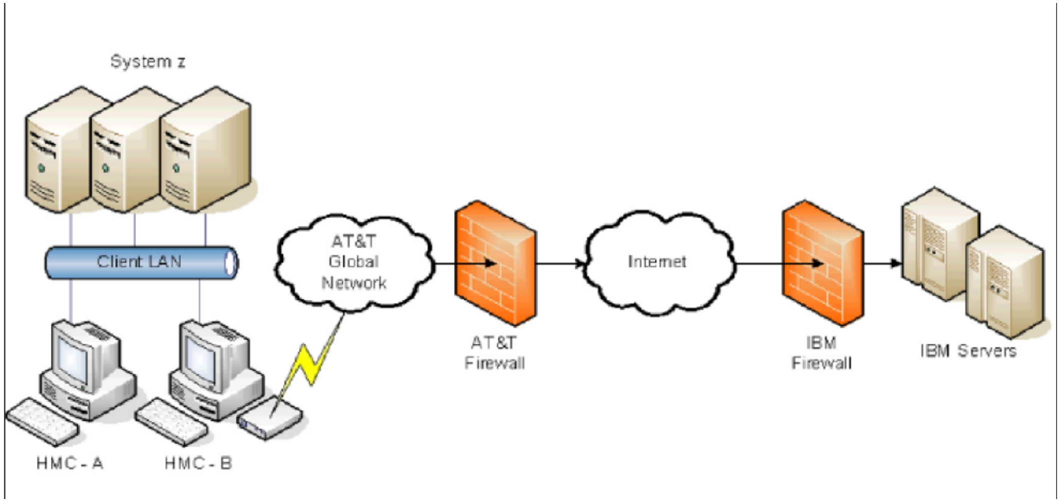
Confirm password: * ●●●●●

Protocol to Internet

IPv4

Dial Support – support

- Slowest and least reliable connection
- Actual connection to IBM is done using a “fenced internet connection”
  - Special account code provide limited access to IBM defined addresses
- Modem (internal or external) shipped with each HMC
  - Modem configuration done at customer shop
- Set of phone numbers to IBM for each country maintained by IBM, can be customized.
- Customers configure 1 to 5 phone numbers per callhome server



If you choose to enable Remote Browser user communication to the HMC,

-- What should you be aware of in regards to
---- browser security
---- type of security certificates/controls

-- Can you isolate remote browsing capability on a per user basis?

Enabling Remote Communications

1) Configure HMC Network Settings
   - including the specification of the IP address and host name

2) Ensure remote users are using supported browsers with latest security fixes applied

3) Configure the certificate used by the HMC (if changing to use a certificate signed by a CA instead of a self-signed certificate)

4) Enable remote communications for HMC

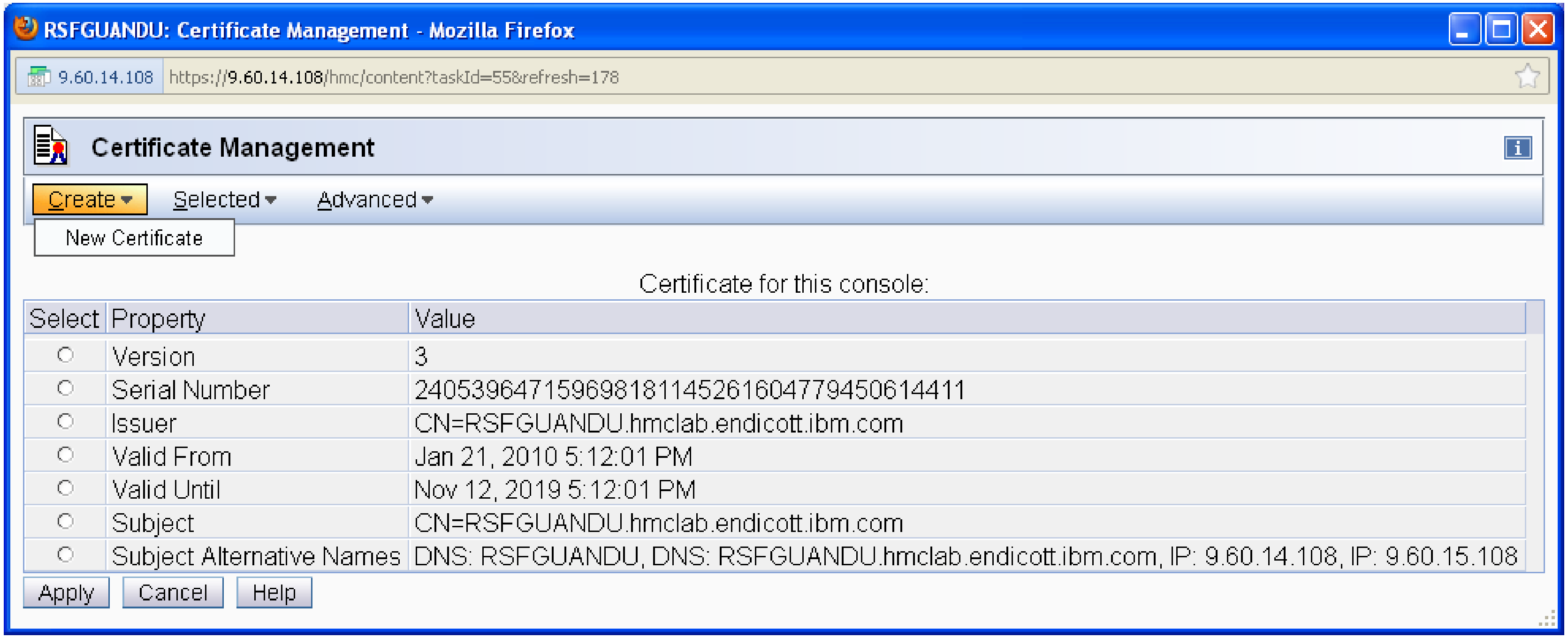
5) Enable specific users for remote access
   - Authorize only users who really need it

HMC Certificate Management

- Self-signed certificate created at the time of HMC installation
  - Not used until remote communications enabled
- If the remote users using a network which potentially isn't absolutely secure,
  - Recommendation => replace self-signed certificate with one signed by a Certificate Authority (CA)
  - If the self-signed certificate not replaced,
    - If user uses a browser and adds the certificate as an exception,
      - risk of being spoofed with HMC user ID and password given to the spoofing server
- If your company does not have its own CA,
  - a CA that has a certificate shipped with the browsers normally used by the users should be used
  - Check your browser for the list of CA certificates already installed and trusted

HMC Certificate Management (cont.)

- Use the “New Certificate” action of the Certificate Management task to change the self-signed certificate created when the HMC was installed

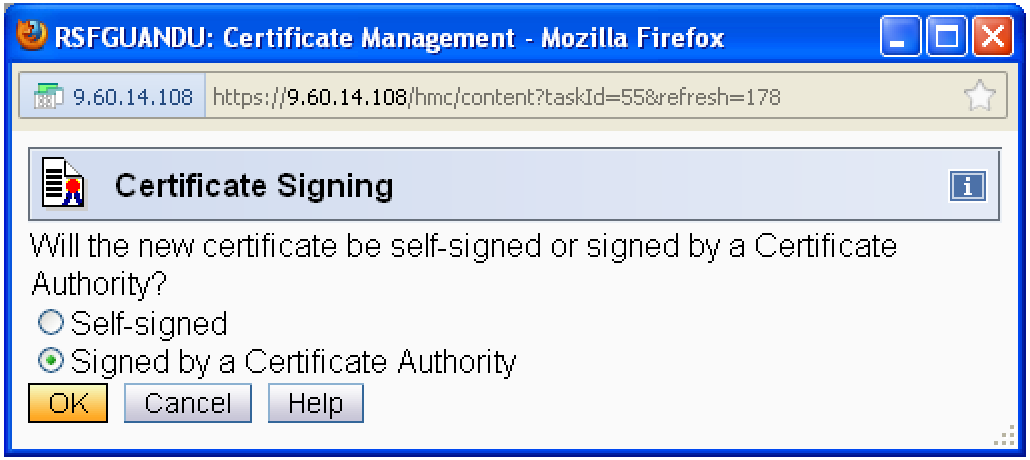

RSFGUANDU: Certificate Management - Mozilla Firefox
9.60.14.108
https://9.60.14.108/hmc/content?taskId=55&refresh=178
Certificate Management
Create
Selected
Advanced
New Certificate
Apply
Cancel
Help

Certificate for this console:

Select	Property	Value
○	Version	3
○	Serial Number	240539647159698181145261604779450614411
○	Issuer	CN=RSFGUANDU.hmclab.endicott.ibm.com
○	Valid From	Jan 21, 2010 5:12:01 PM
○	Valid Until	Nov 12, 2019 5:12:01 PM
○	Subject	CN=RSFGUANDU.hmclab.endicott.ibm.com
○	Subject Alternative Names	DNS: RSFGUANDU, DNS: RSFGUANDU.hmclab.endicott.ibm.com, IP: 9.60.14.108, IP: 9.60.15.108

HMC Certificate Management (cont.)

- Select “Signed by a Certificate Authority” to replace the current certificate



RSFGUANDU: Certificate Management - Mozilla Firefox
9.60.14.108
https://9.60.14.108/hmc/content?taskId=55&refresh=178
Certificate Signing

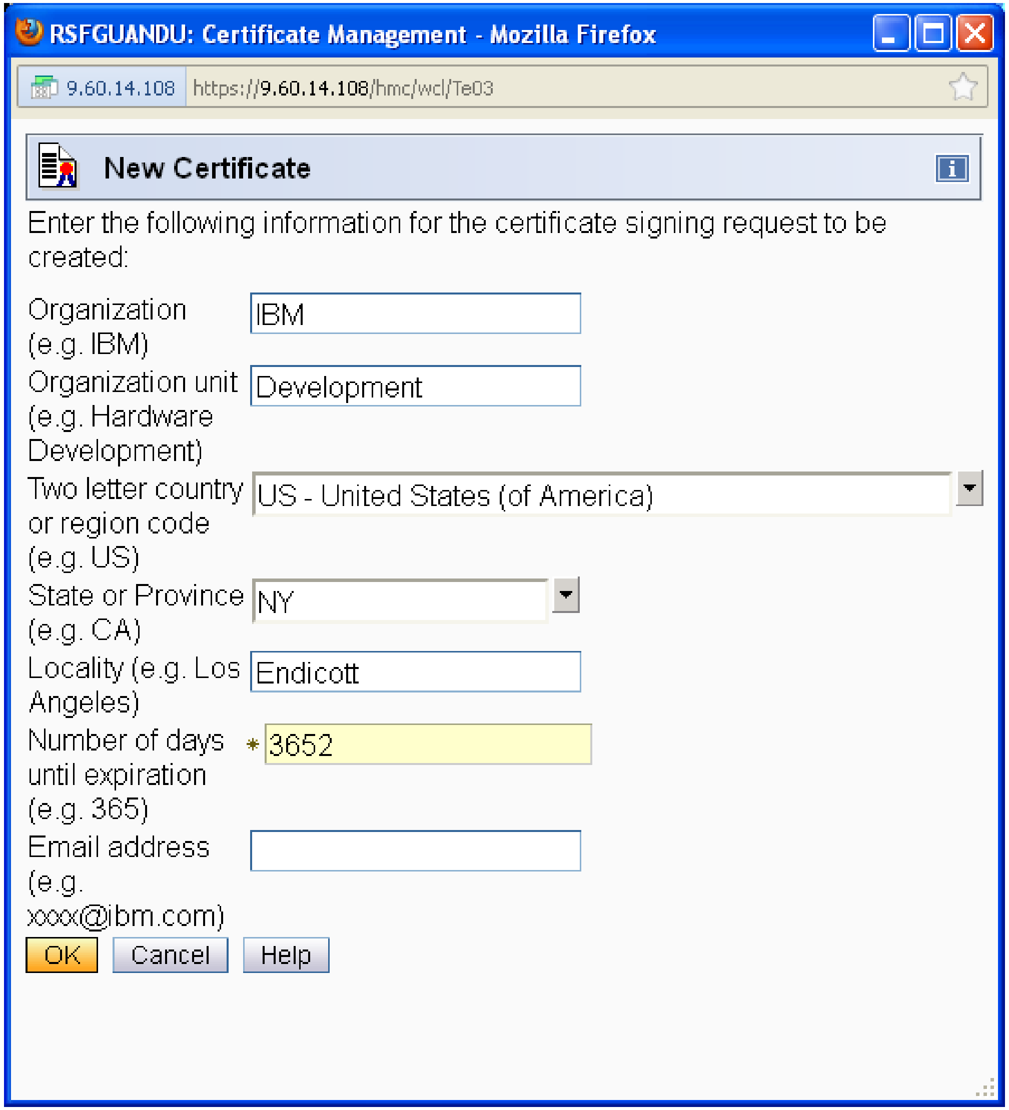
Will the new certificate be self-signed or signed by a Certificate Authority?

○ Self-signed

● 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 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)


RSFGUANDU: Certificate Management - Mozilla Firefox
9.60.14.108
https://9.60.14.108/hmc/wcl/Te03

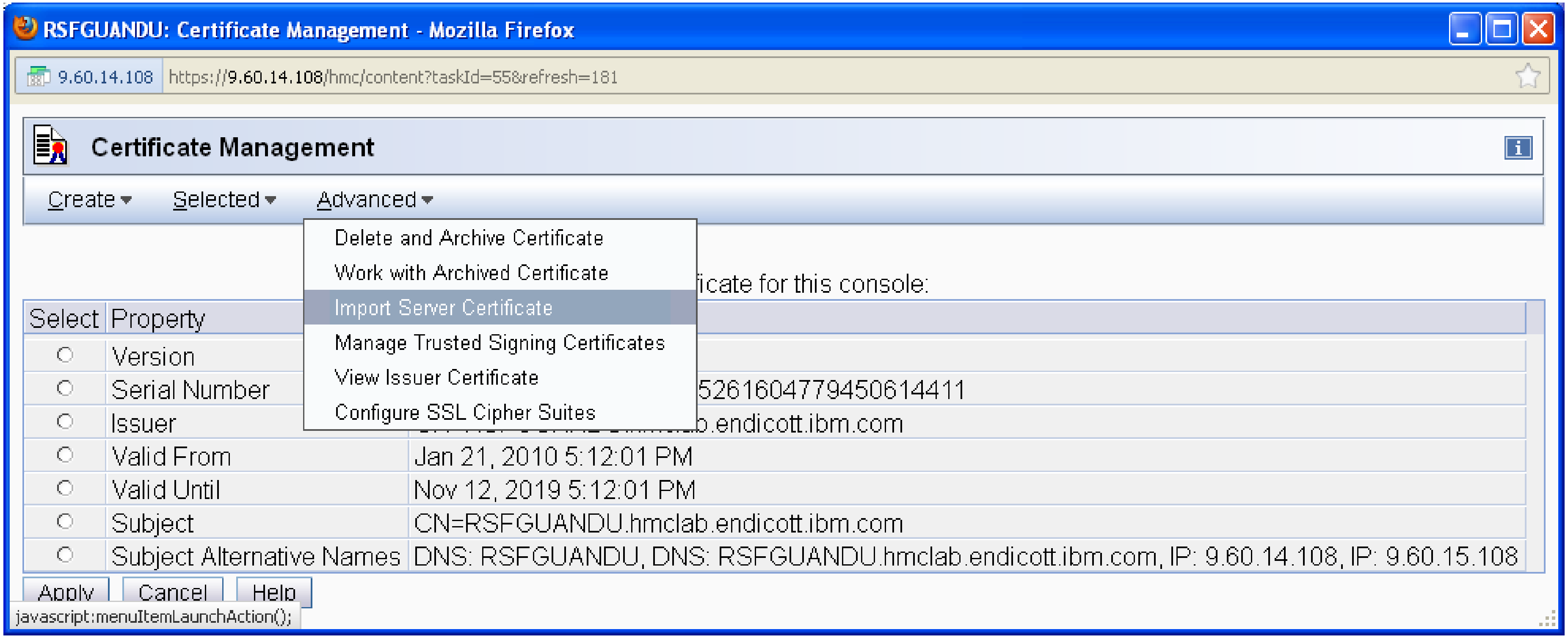
New Certificate

Enter the following information for the certificate signing request to be created:

Organization (e.g. IBM)	IBM
Organization unit (e.g. Hardware Development)	Development
Two letter country or region code (e.g. US)	US - United States (of America)
State or Province (e.g. CA)	NY
Locality (e.g. Los Angeles)	Endicott
Number of days until expiration (e.g. 365)	* 3652
Email address (e.g. xxxx@ibm.com)	

HMC Certificate Management (cont.)

- After sending the CSR to your company CA or well known CA, use "Import Server Certificate" to import the received "signed" certificate for use by the HMC

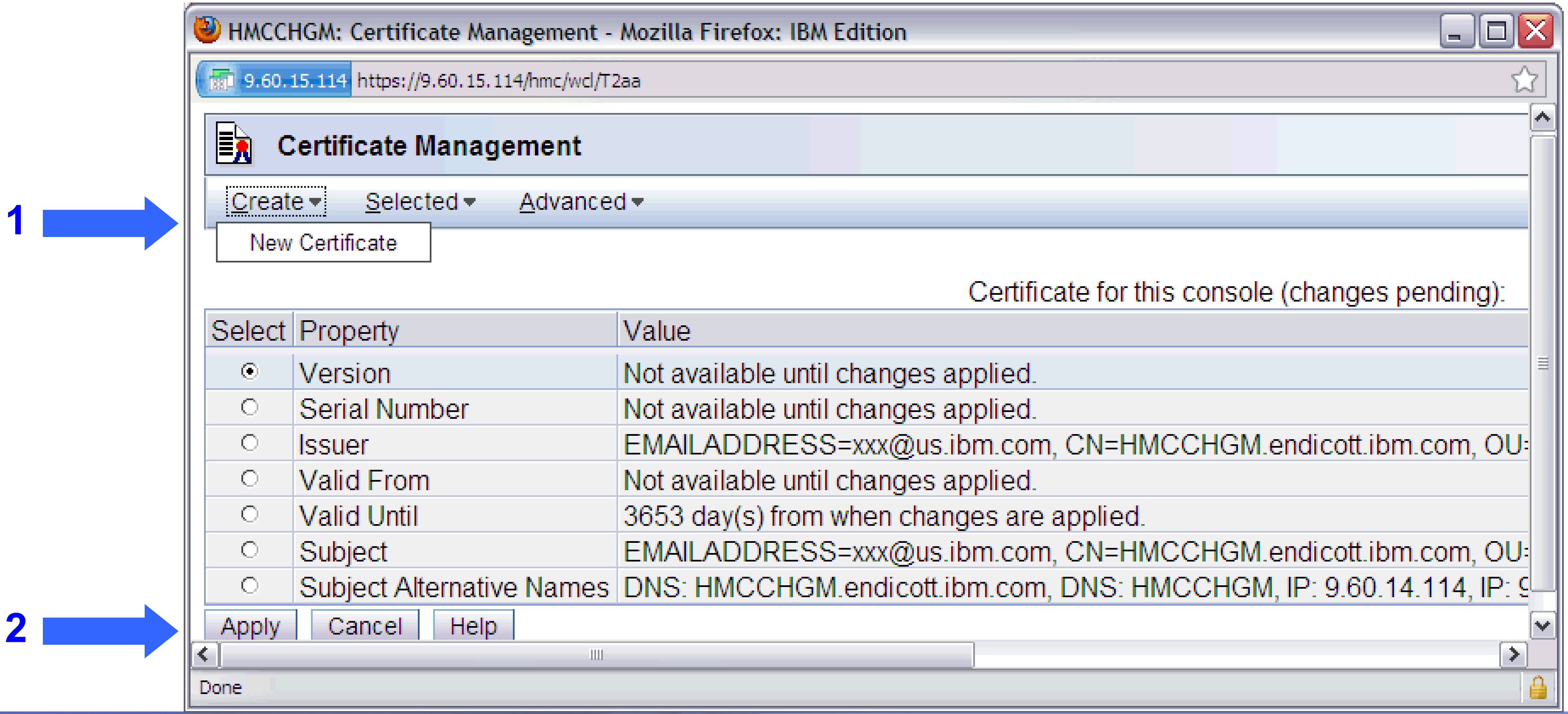

RSFGUANDU: Certificate Management - Mozilla Firefox
9.60.14.108
https://9.60.14.108/hmc/content?taskId=55&refresh=181
Certificate Management
Create
Selected
Advanced
Delete and Archive Certificate
Work with Archived Certificate
Import Server Certificate
Manage Trusted Signing Certificates
View Issuer Certificate
Configure SSL Cipher Suites
Apply
Cancel
Help
javascript:menuItemLaunchAction();

icate for this console:

Select	Property	
○	Version	
○	Serial Number	526160477945061441 1
○	Issuer	b.endicott.ibm.com
○	Valid From	Jan 21, 2010 5:12:01 PM
○	Valid Until	Nov 12, 2019 5:12:01 PM
○	Subject	CN=RSFGUANDU.hmclab.endicott.ibm.com
○	Subject Alternative Names	DNS: RSFGUANDU, DNS: RSFGUANDU.hmclab.endicott.ibm.com, IP: 9.60.14.108, IP: 9.60.15.108

HMC Certificate Management (cont.)

- HMC 2.11.0 and prior use 1024 bit network certificates.
- HMC 2.11.1 uses 2048 bit certificates when
  - new certificates are **Created**
  - and then **Applied**
  - **Otherwise,** existing certificates carried forward on upgrade to 2.11.1 remain at 1024 bit.



https://9.60.15.114/hmc/wcl/T2aa

Certificate Management

Certificate for this console (changes pending):

Select	Property	Value
●	Version	Not available until changes applied.
○	Serial Number	Not available until changes applied.
○	Issuer	EMAILADDRESS=xxx@us.ibm.com, CN=HMCCHGM.endicott.ibm.com, OU=
○	Valid From	Not available until changes applied.
○	Valid Until	3653 day(s) from when changes are applied.
○	Subject	EMAILADDRESS=xxx@us.ibm.com, CN=HMCCHGM.endicott.ibm.com, OU=
○	Subject Alternative Names	DNS: HMCCHGM.endicott.ibm.com, DNS: HMCCHGM, IP: 9.60.14.114, IP: 9

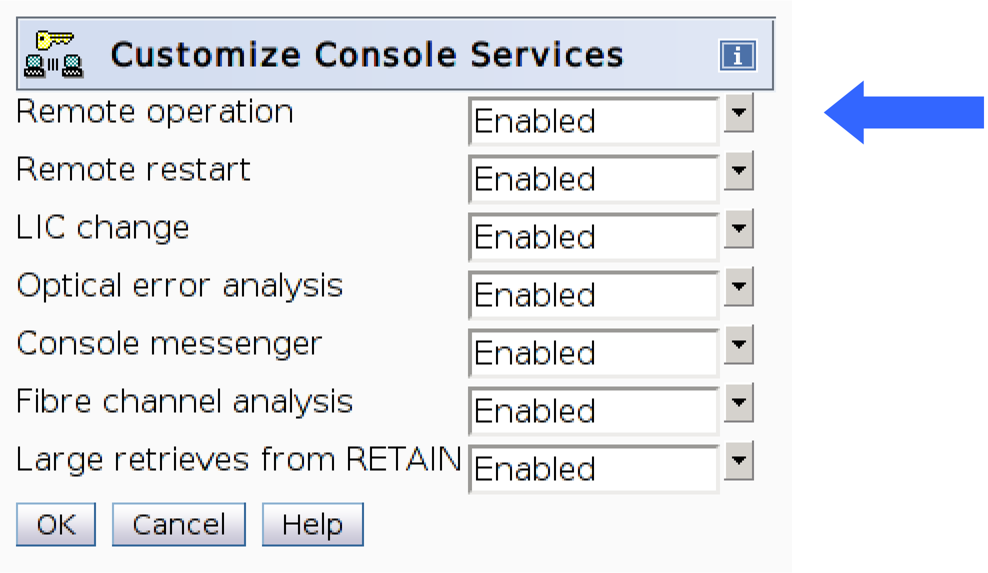
Cipher Suites

- Create policy that all users update browsers with latest security fixes
  - And stay relatively current in browser versions

- Above policy ensures SSL Cipher Suites of High strength are supported
  - Configure HMC to use Browser Remote Communication Cipher Suites of High Strength
  - See Appendix for more details on how to configure HMC

Customize Console Services

- **From the local HMC console, invoke the “Customize Console Services” task and enable the “Remote operation” service**

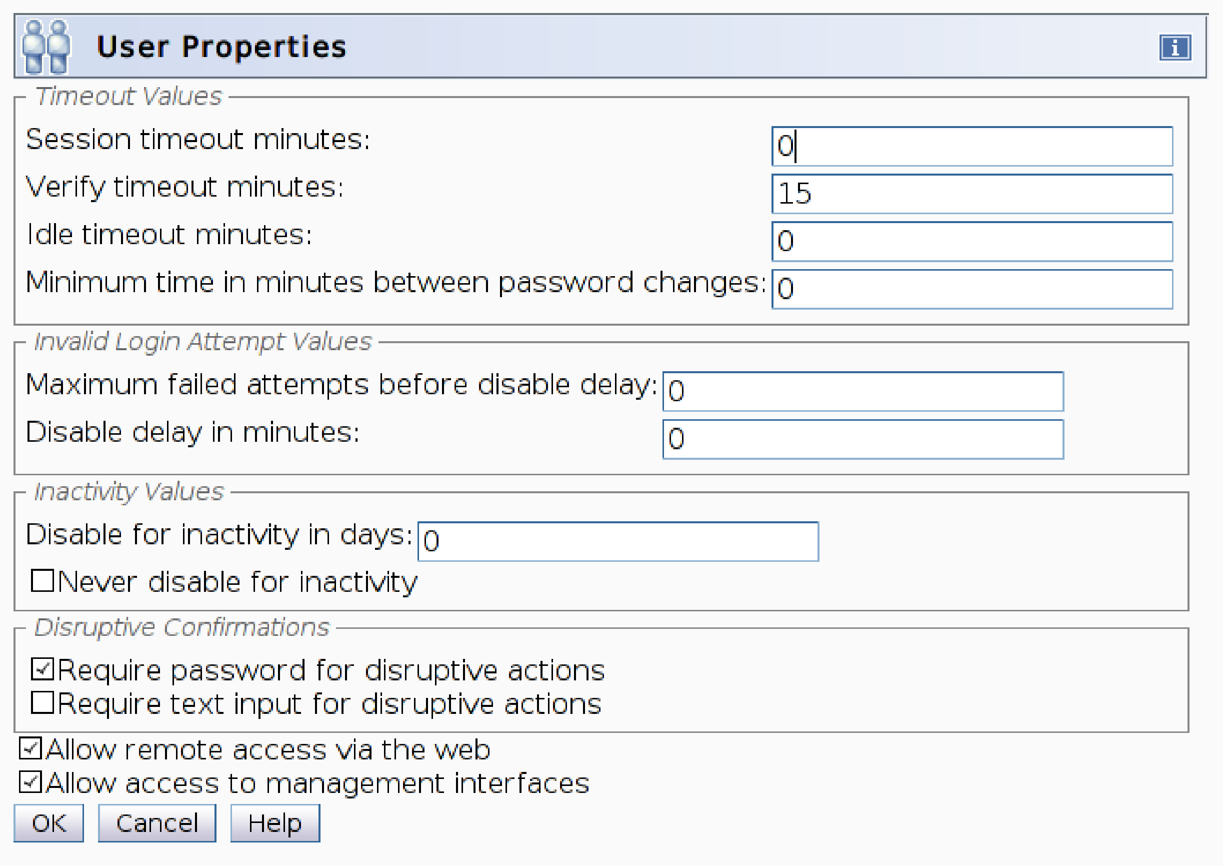


Customize Console Services

Remote operation	Enabled
Remote restart	Enabled
LIC change	Enabled
Optical error analysis	Enabled
Console messenger	Enabled
Fibre channel analysis	Enabled
Large retrieves from RETAIN	Enabled

User Properties

- **Enable specific users for remote access**
  - **Use the “Manage Users Wizard” task and select “Allow remove access via the web” or**
  - **Use the “User Properties” option within the “User Profiles” task (shown to the right)**



User Properties

Timeout Values

Session timeout minutes: 0

Verify timeout minutes: 15

Idle timeout minutes: 0

Minimum time in minutes between password changes: 0

Invalid Login Attempt Values

Maximum failed attempts before disable delay: 0

Disable delay in minutes: 0

Inactivity Values

Disable for inactivity in days: 0

□Never disable for inactivity

Disruptive Confirmations

☑Require password for disruptive actions

□Require text input for disruptive actions

☑Allow remote access via the web

☑Allow access to management interfaces

How many users do you want to have access to the HMC?

Which objects & tasks should be available to each user?

Do you want to create users which only have monitoring capability (Read only tasks & severely limit other tasks)?

Where do you want user/password authentication?
-- local at HMC console
-- at LDAP server

Are user policies that users only exist for short periods of time?
-- If so, HMC User Templates

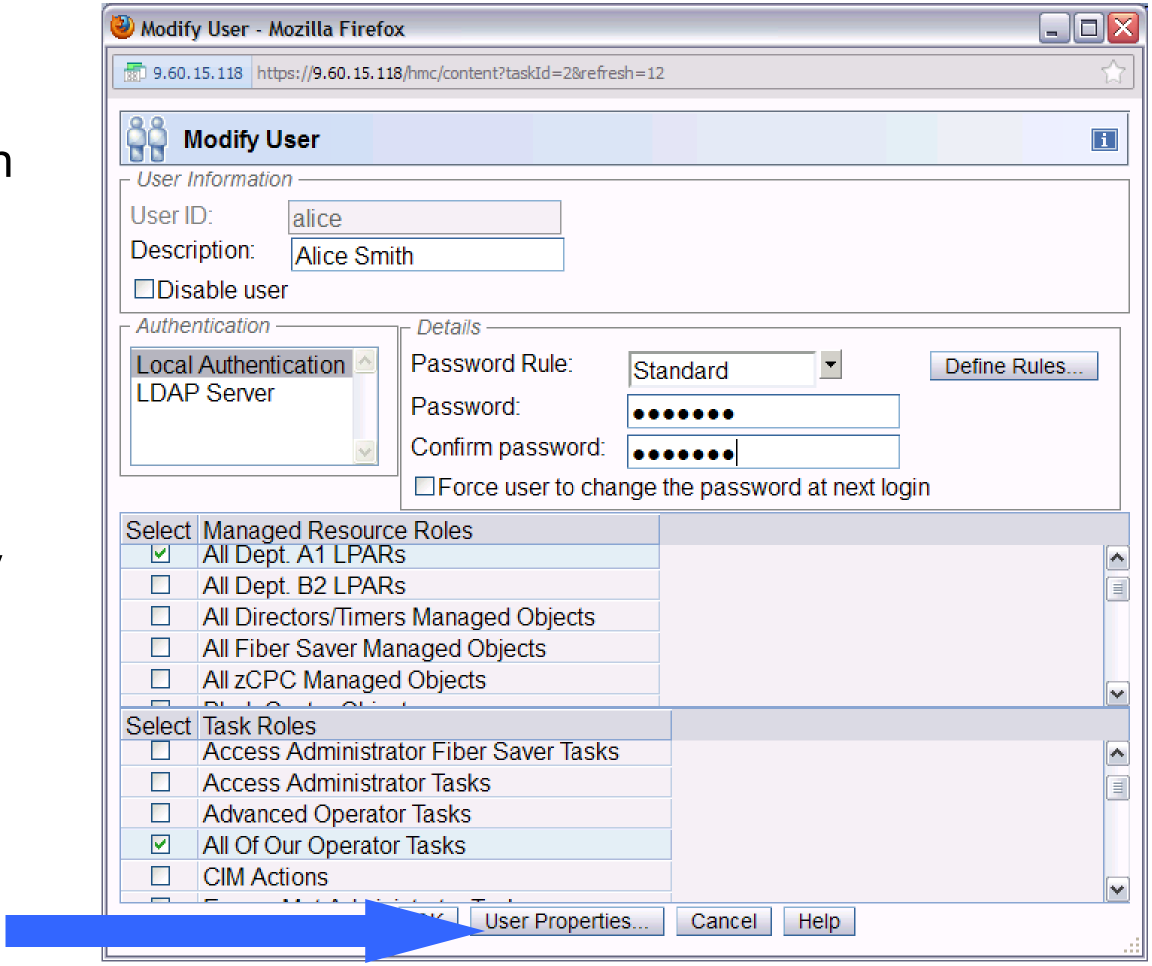
HMC Data Replication to keep all HMCs in sync with User Controls (See Appendix)

Defining Users and Roles

- Decide if the HMC or an LDAP server will be used to verify the user ID and password of the HMC user
- If an LDAP Server
  - Decide if User Patterns/Templates will be used or not
    - User Patterns/Templates useful if you have groups of users that require the same permissions but at least the auditing of unique user Ids is important
    - Useful if you want users where the user settings are not retained for long (i.e. the retention period)
- **Do not share user IDs among users**
  - Can clone customized user roles

Defining Users and Roles (cont.)

- A user is given permission to objects and tasks through one or more roles associated with the user
  - Each role contains a list of objects or a list of tasks
    - the pre-defined roles can contain all objects of a given type (existing currently or in the future)
  - Use the “Manage Users Wizard” task or the User Profiles” task to create, modify or delete users
  - Use the “User Properties” button to configure other properties such as session timeout values, etc. (page 37)



Modify User - Mozilla Firefox
9.60.15.118
https://9.60.15.118/hmc/content?taskId=2&refresh=12

Modify User

User Information

User ID: alice

Description: Alice Smith

□ Disable user

Authentication

Local Authentication
LDAP Server

Details

Password Rule: Standard

Password: ●●●●●●●

Confirm password: ●●●●●●●

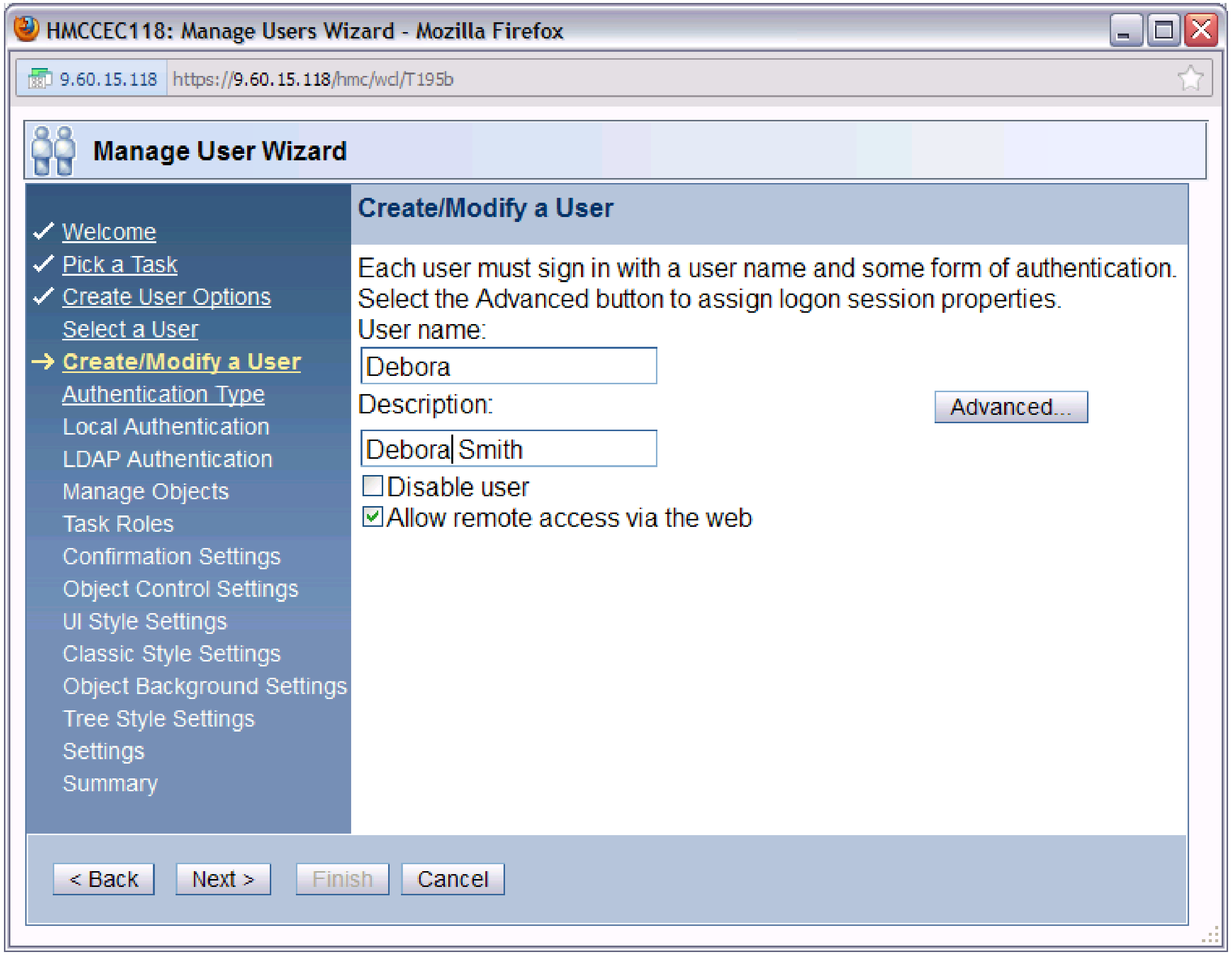
□ Force user to change the password at next login

Select	Managed Resource Roles
☑	All Dept. A1 LPARs
□	All Dept. B2 LPARs
□	All Directors/Timers Managed Objects
□	All Fiber Saver Managed Objects
□	All zCPC Managed Objects

Select	Task Roles
□	Access Administrator Fiber Saver Tasks
□	Access Administrator Tasks
□	Advanced Operator Tasks
☑	All Of Our Operator Tasks
□	CIM Actions

Defining Users and Roles (cont.)

- Use the Manage User Wizard task from the ACSADMIN user ID to create a user



Create/Modify a User

Each user must sign in with a user name and some form of authentication. Select the Advanced button to assign logon session properties.

User name: Debora

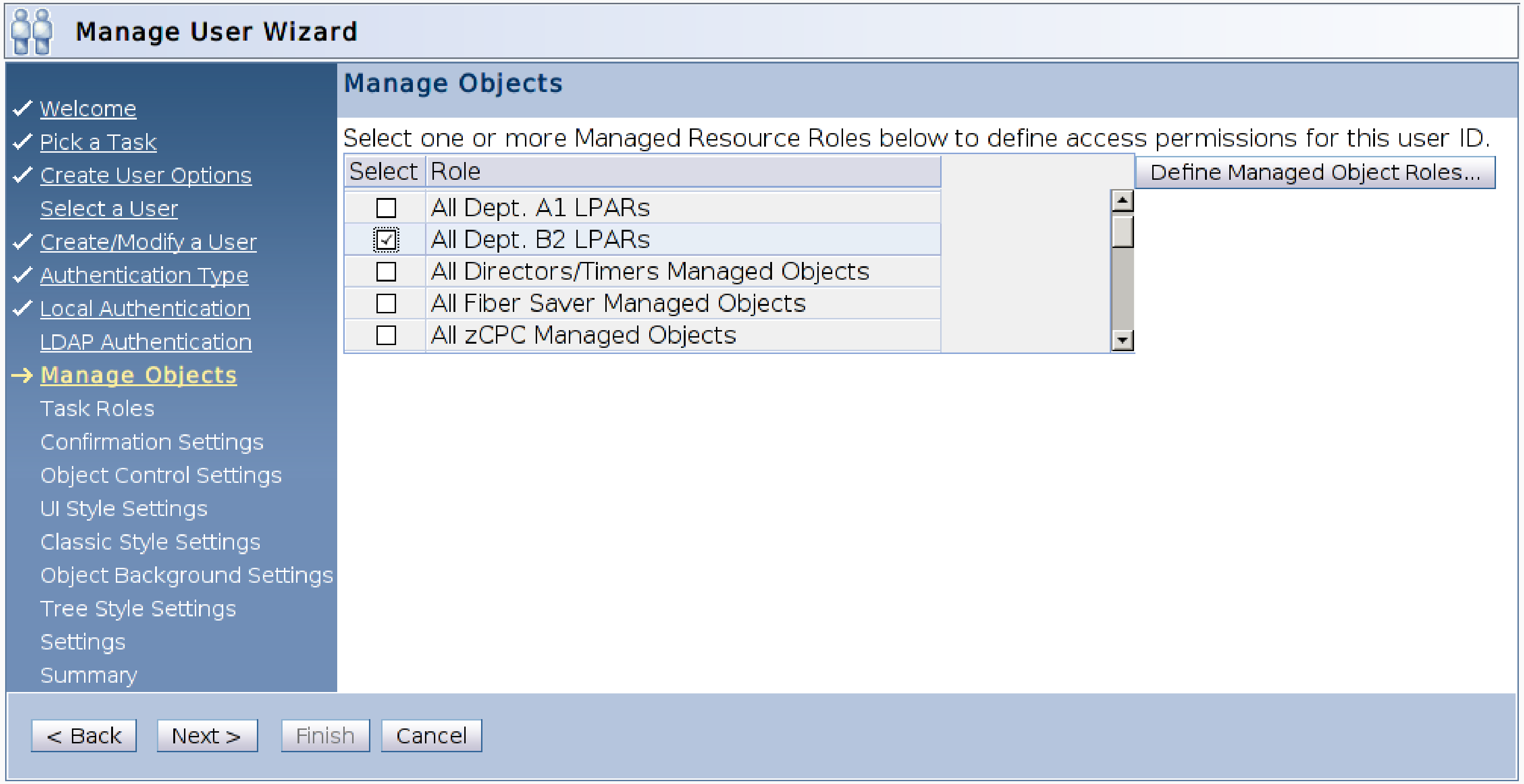
Description: Debora Smith

☐ Disable user

☑ Allow remote access via the web

Defining Users and Roles (cont.)

- Decide what objects/resources this user will have access to
  - Consider using your own Managed Resource Roles with specific objects instead of the “All...Objects” default roles



Manage User Wizard

- ✓ Welcome
- ✓ Pick a Task
- ✓ Create User Options
- Select a User
- ✓ Create/Modify a User
- ✓ Authentication Type
- ✓ Local Authentication
- LDAP Authentication
- → Manage Objects
- Task Roles
- Confirmation Settings
- Object Control Settings
- UI Style Settings
- Classic Style Settings
- Object Background Settings
- Tree Style Settings
- Settings
- Summary

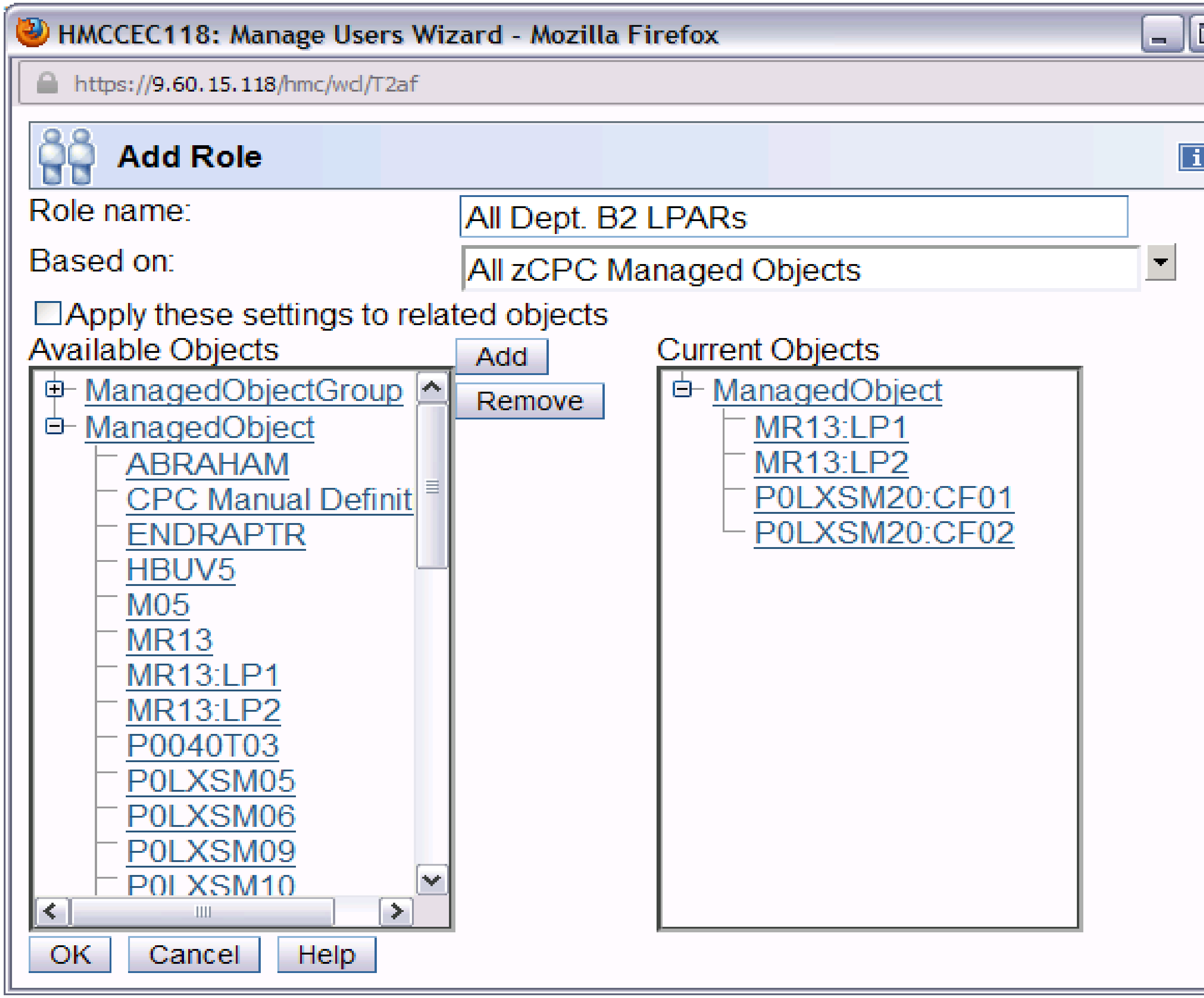
Manage Objects

Select one or more Managed Resource Roles below to define access permissions for this user ID.

Select	Role
□	All Dept. A1 LPARs
☑	All Dept. B2 LPARs
□	All Directors/Timers Managed Objects
□	All Fiber Saver Managed Objects
□	All zCPC Managed Objects

Defining Users and Roles (cont.)

- Build up the list of objects on the right by selecting objects on the left and pressing the Add button



HMCCEC118: Manage Users Wizard - Mozilla Firefox

https://9.60.15.118/hmc/wcl/T2af

Add Role

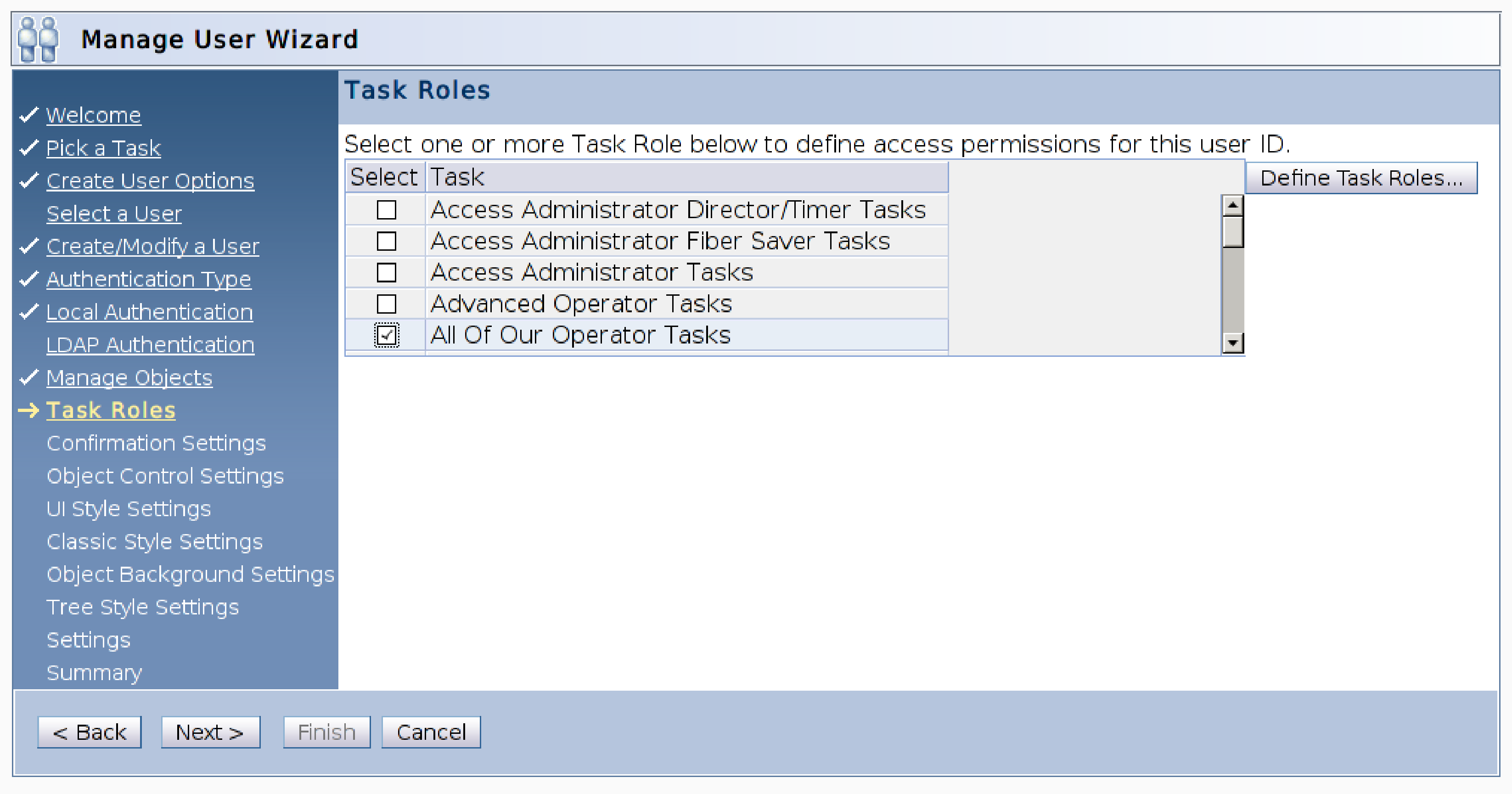
Role name: All Dept. B2 LPARs

Based on: All zCPC Managed Objects

□ Apply these settings to related objects

Defining Users and Roles (cont.)

- Decide what tasks this user can perform
  - Consider using your own Task Roles with specific tasks instead of the “All...Tasks” default roles



Manage User Wizard

✓ Welcome
✓ Pick a Task
✓ Create User Options
Select a User
✓ Create/Modify a User
✓ Authentication Type
✓ Local Authentication
LDAP Authentication
✓ Manage Objects
→ Task Roles
Confirmation Settings
Object Control Settings
UI Style Settings
Classic Style Settings
Object Background Settings
Tree Style Settings
Settings
Summary

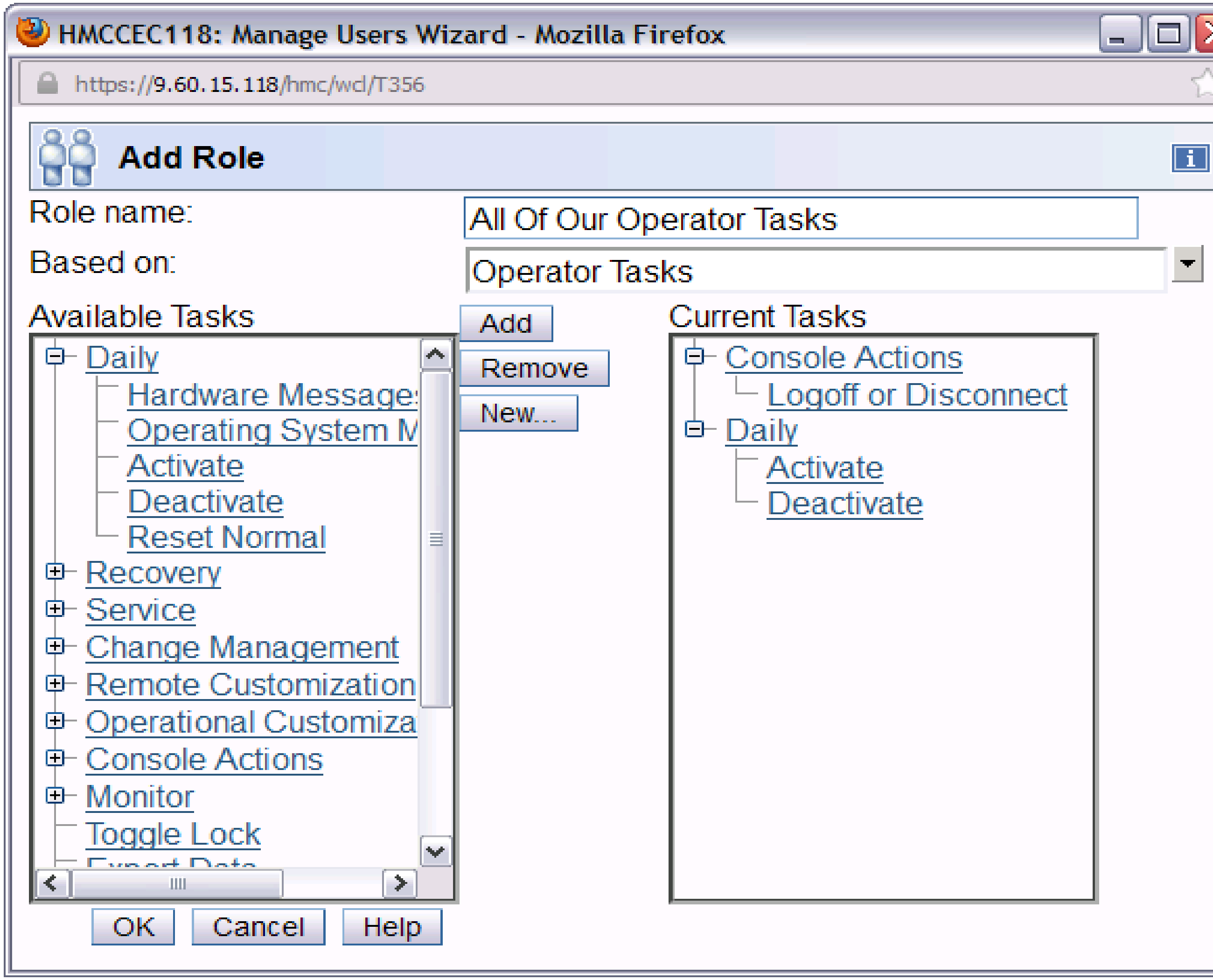
Task Roles

Select one or more Task Role below to define access permissions for this user ID.

Select	Task
□	Access Administrator Director/Timer Tasks
□	Access Administrator Fiber Saver Tasks
□	Access Administrator Tasks
□	Advanced Operator Tasks
☑	All Of Our Operator Tasks

Defining Users and Roles (cont.)

- Build up the list of tasks on the right by selecting tasks on the left and pressing the Add button

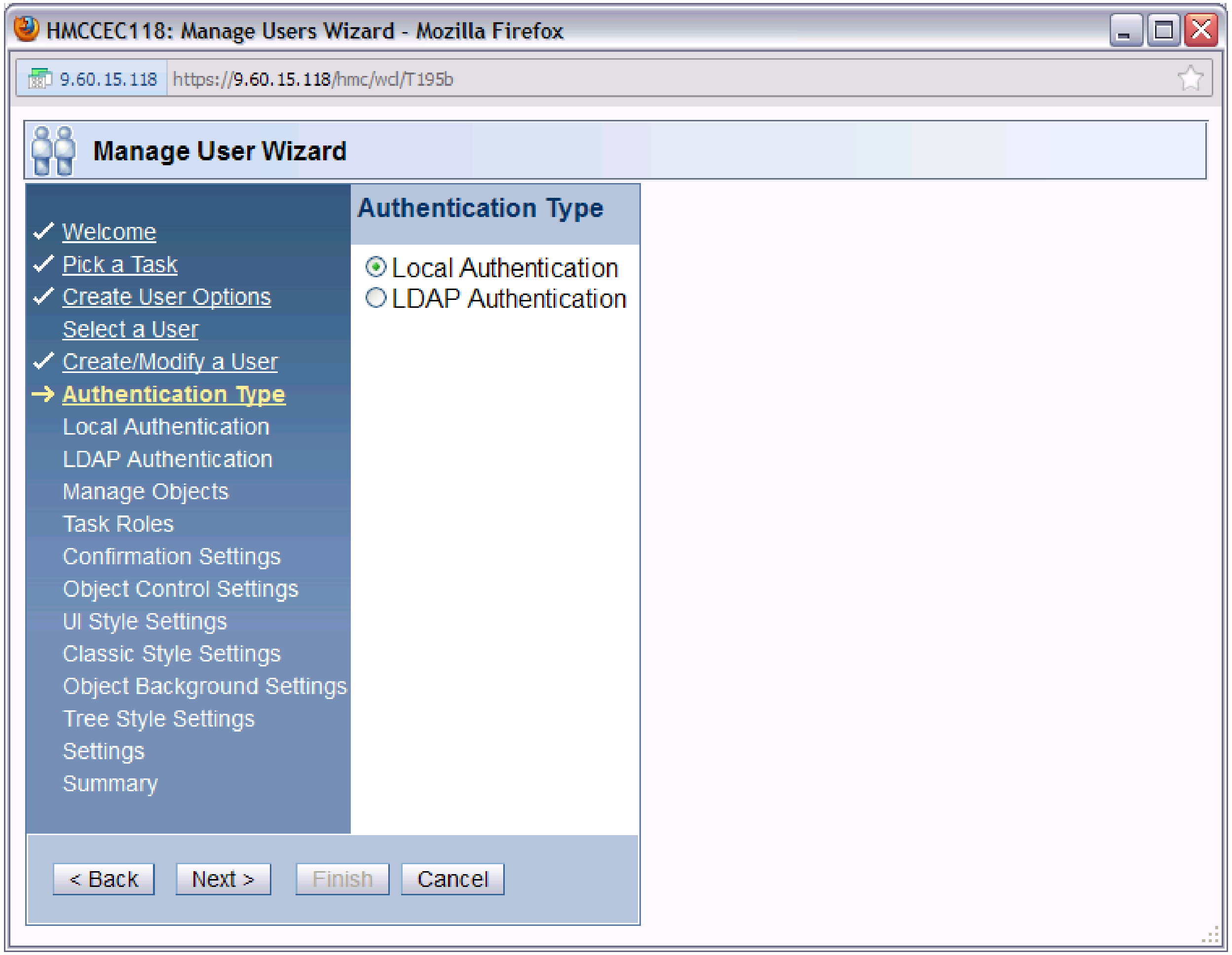

HMCCEC118: Manage Users Wizard - Mozilla Firefox
https://9.60.15.118/hmc/wcl/T356
Add Role

Role name: All Of Our Operator Tasks

Based on: Operator Tasks

Defining Users and Roles (cont.)

- Decide if the HMC or an LDAP server will be used for authenticating the user. Assuming local (HMC) authentication...



HMCCEC118: Manage Users Wizard - Mozilla Firefox

9.60.15.118 https://9.60.15.118/hmc/wcl/T195b

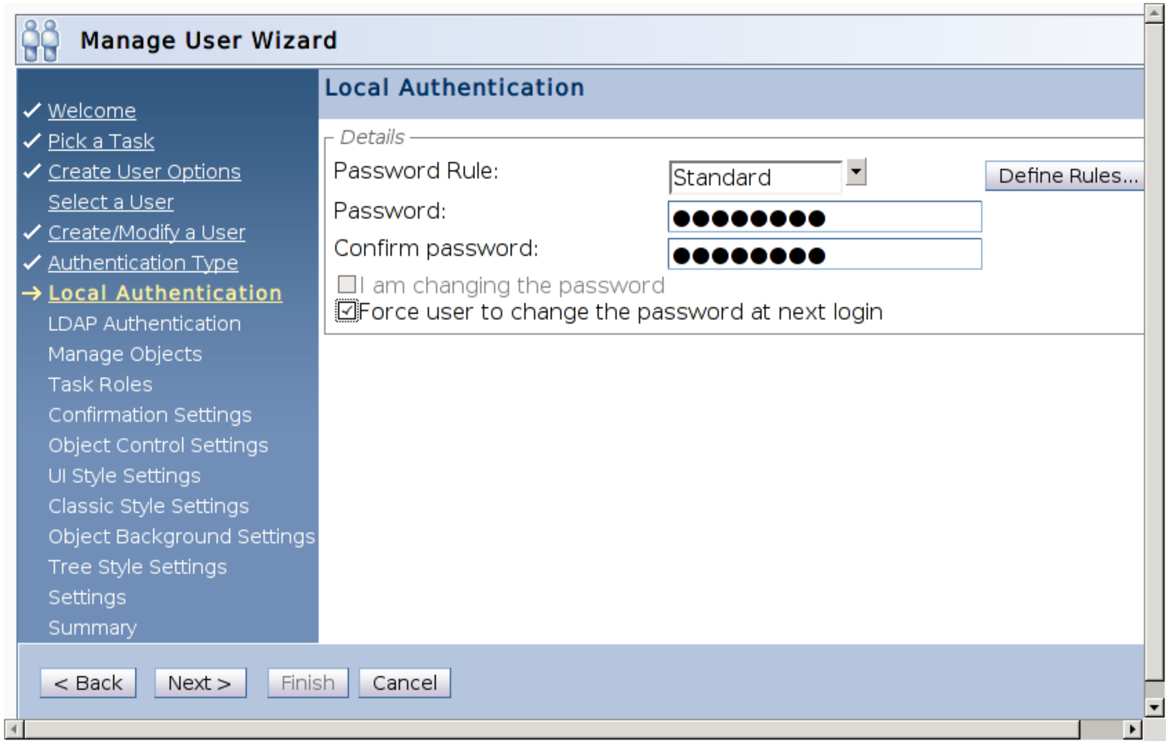
Manage User Wizard

Authentication Type

● Local Authentication
○ LDAP Authentication

Defining Users and Roles (cont.)

- Decide what password rules will be enforced for this new user
- See the Appendix for the meaning of the default password rules
- Optionally, configure new password rules enforced for all your users which adhere to your corporate guidelines



Manage User Wizard

Local Authentication

Details

Password Rule: Standard

Password: ●●●●●●●●

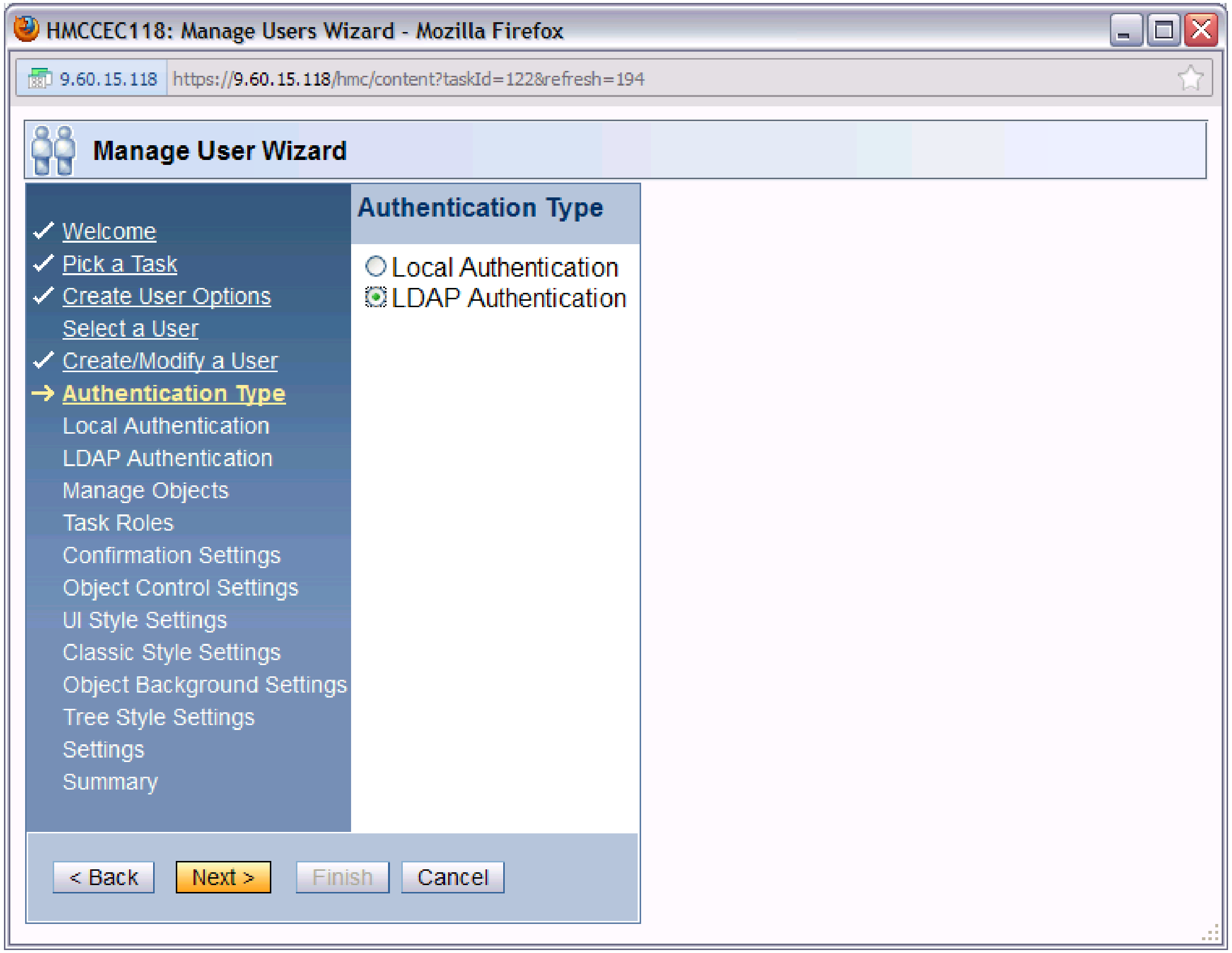
Confirm password: ●●●●●●●●

□ I am changing the password

☑ Force user to change the password at next login

Defining Users and Roles (cont.)

- An LDAP server can be used to authenticate the identity of the user



HMCCEC118: Manage Users Wizard - Mozilla Firefox

9.60.15.118 https://9.60.15.118/hmc/content?taskId=122&refresh=194

Manage User Wizard

✓ Welcome
✓ Pick a Task
✓ Create User Options
Select a User
✓ Create/Modify a User
→ Authentication Type
Local Authentication
LDAP Authentication
Manage Objects
Task Roles
Confirmation Settings
Object Control Settings
UI Style Settings
Classic Style Settings
Object Background Settings
Tree Style Settings
Settings
Summary

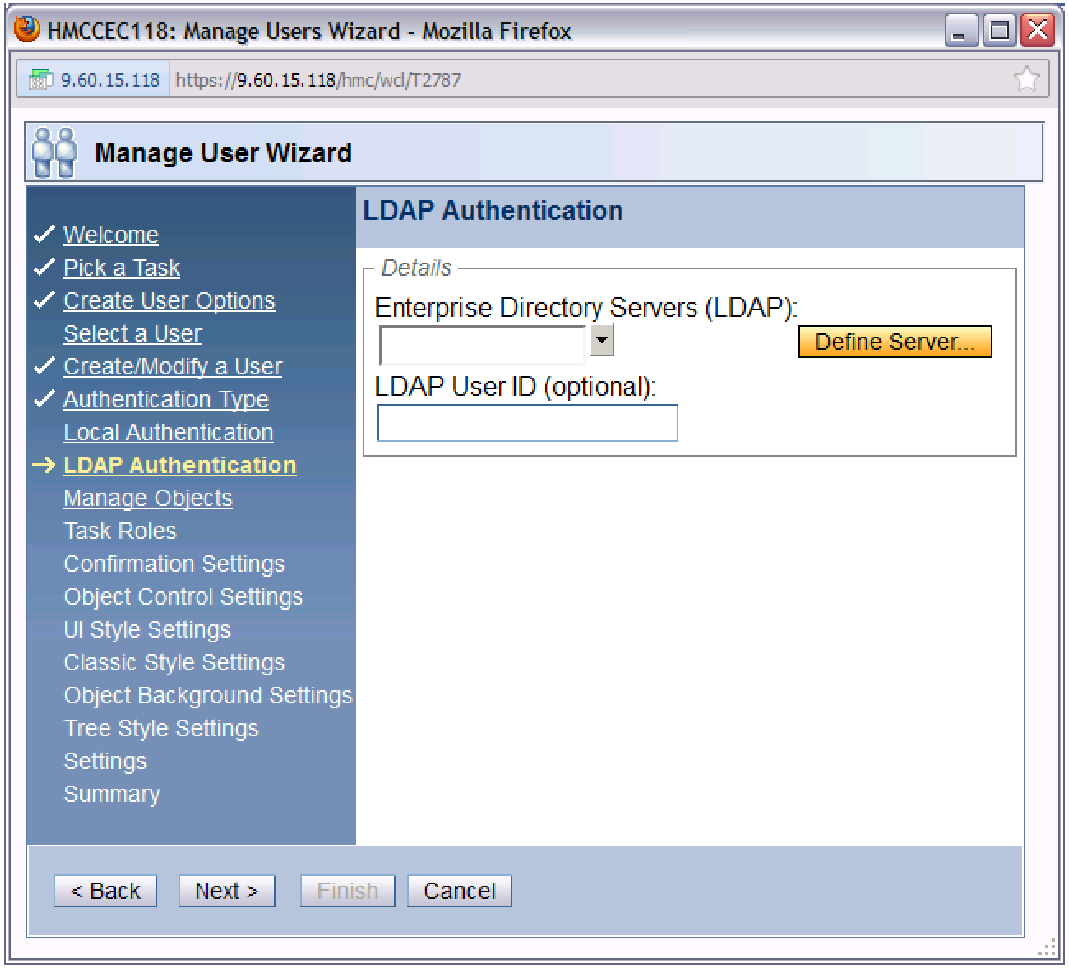
Authentication Type

○ Local Authentication
● LDAP Authentication

< Back | Next > | Finish | Cancel

Defining Users and Roles (cont.)

- Specify the LDAP server used if not already done so...



HMCCEC118: Manage Users Wizard - Mozilla Firefox

9.60.15.118 https://9.60.15.118/hmc/wcl/T2787

Manage User Wizard

- ✓ Welcome
- ✓ Pick a Task
- ✓ Create User Options
- Select a User
- ✓ Create/Modify a User
- ✓ Authentication Type
- Local Authentication
- → LDAP Authentication
- Manage Objects
- Task Roles
- Confirmation Settings
- Object Control Settings
- UI Style Settings
- Classic Style Settings
- Object Background Settings
- Tree Style Settings
- Settings
- Summary

LDAP Authentication

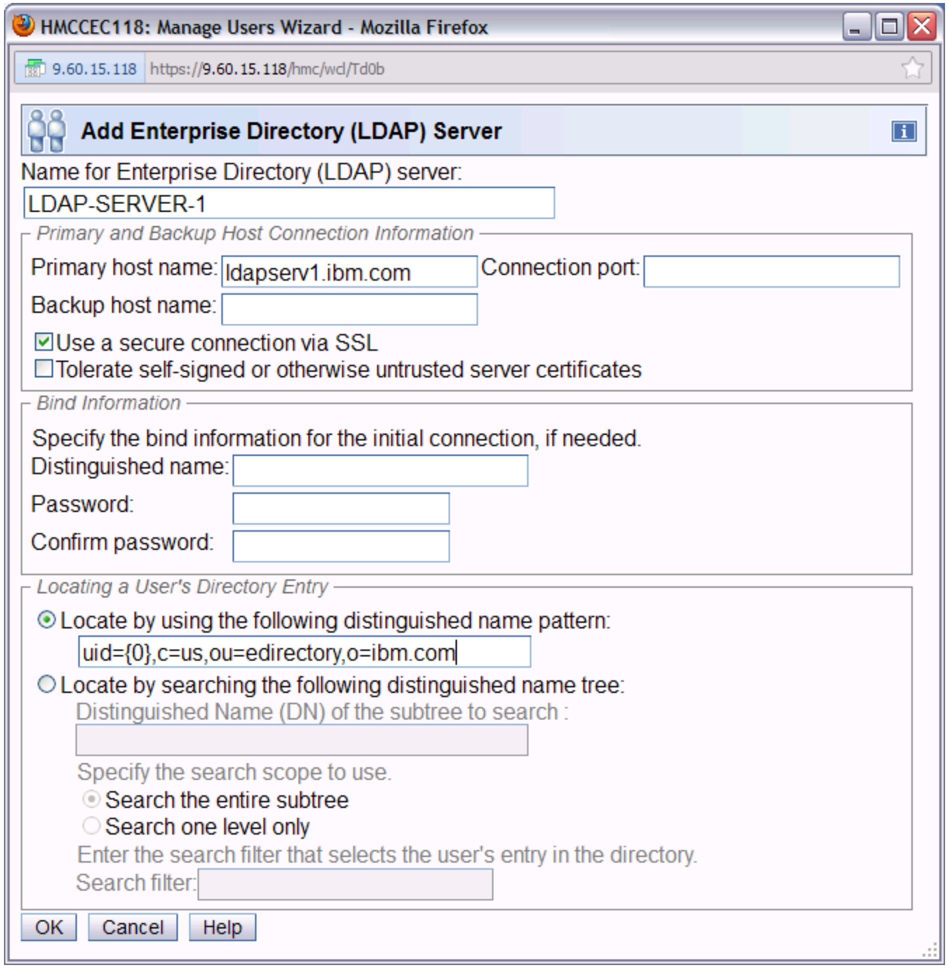
Details

Enterprise Directory Servers (LDAP):

LDAP User ID (optional):

Defining Users and Roles (cont.)

- Specify the host name and the distinguished name pattern to match
- In this example, a search is performed for the directory entry with a "uid=" value that matches that specified as the HMC user at the HMC logon



HMCCEC118: Manage Users Wizard - Mozilla Firefox

9.60.15.118 https://9.60.15.118/hmc/wcl/Td0b

Add Enterprise Directory (LDAP) Server

Name for Enterprise Directory (LDAP) server: LDAP-SERVER-1

Primary and Backup Host Connection Information

Primary host name: ldapserv1.ibm.com Connection port:

Backup host name:

☑ Use a secure connection via SSL

☐ Tolerate self-signed or otherwise untrusted server certificates

Bind Information

Specify the bind information for the initial connection, if needed.

Distinguished name:

Password:

Confirm password:

Locating a User's Directory Entry

● Locate by using the following distinguished name pattern:

uid={0},c=us,ou=edirectory,o=ibm.com

○ Locate by searching the following distinguished name tree:

Distinguished Name (DN) of the subtree to search :

Specify the search scope to use.

● Search the entire subtree

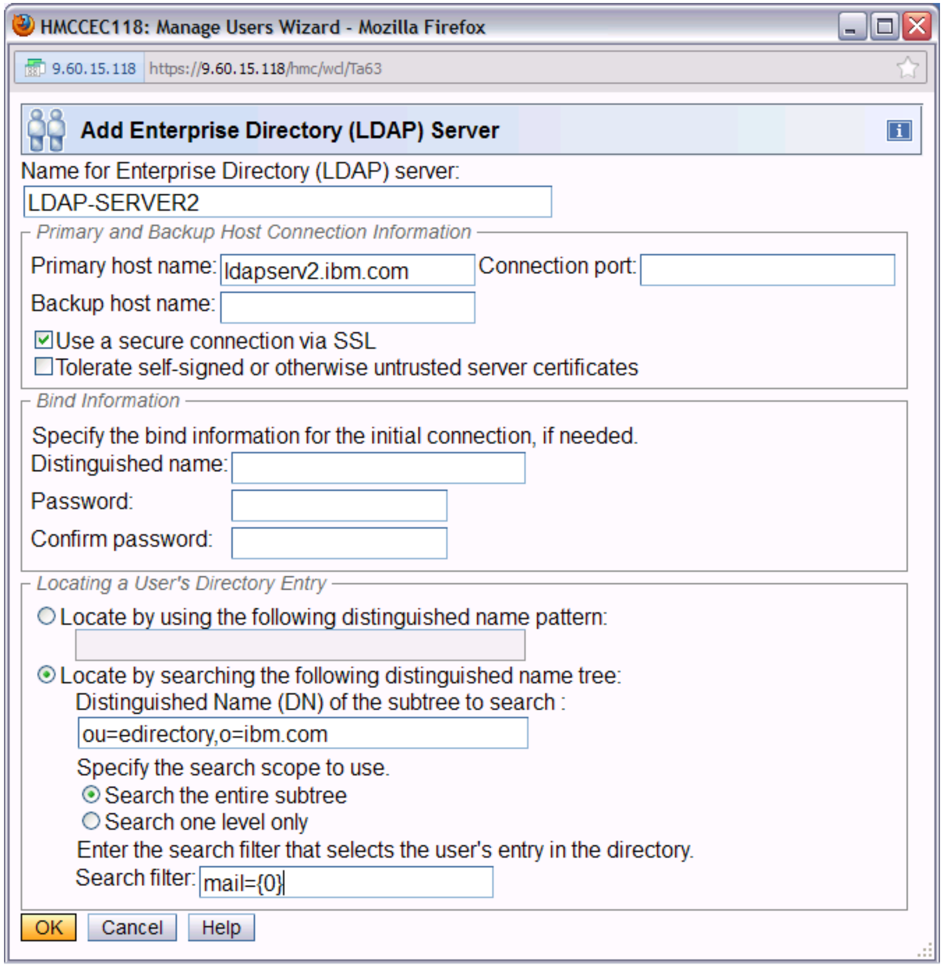
○ Search one level only

Enter the search filter that selects the user's entry in the directory.

Search filter:

Defining Users and Roles (cont.)

- Alternatively, find a user's directory by searching a Distinguished Name (DN) tree
- In this example, a search is performed for the directory entry with a “mail=” value that matches that specified as the HMC user at the HMC logon


HMCCEC118: Manage Users Wizard - Mozilla Firefox
9.60.15.118 https://9.60.15.118/hmc/wcl/Ta63

Add Enterprise Directory (LDAP) Server

Name for Enterprise Directory (LDAP) server: LDAP-SERVER2

Primary and Backup Host Connection Information

Primary host name: ldapserv2.ibm.com Connection port:

Backup host name:

☑ Use a secure connection via SSL

☐ Tolerate self-signed or otherwise untrusted server certificates

Bind Information

Specify the bind information for the initial connection, if needed.

Distinguished name:

Password:

Confirm password:

Locating a User's Directory Entry

○ Locate by using the following distinguished name pattern:

● Locate by searching the following distinguished name tree:

Distinguished Name (DN) of the subtree to search : ou=edirectory,o=ibm.com

Specify the search scope to use.

● Search the entire subtree

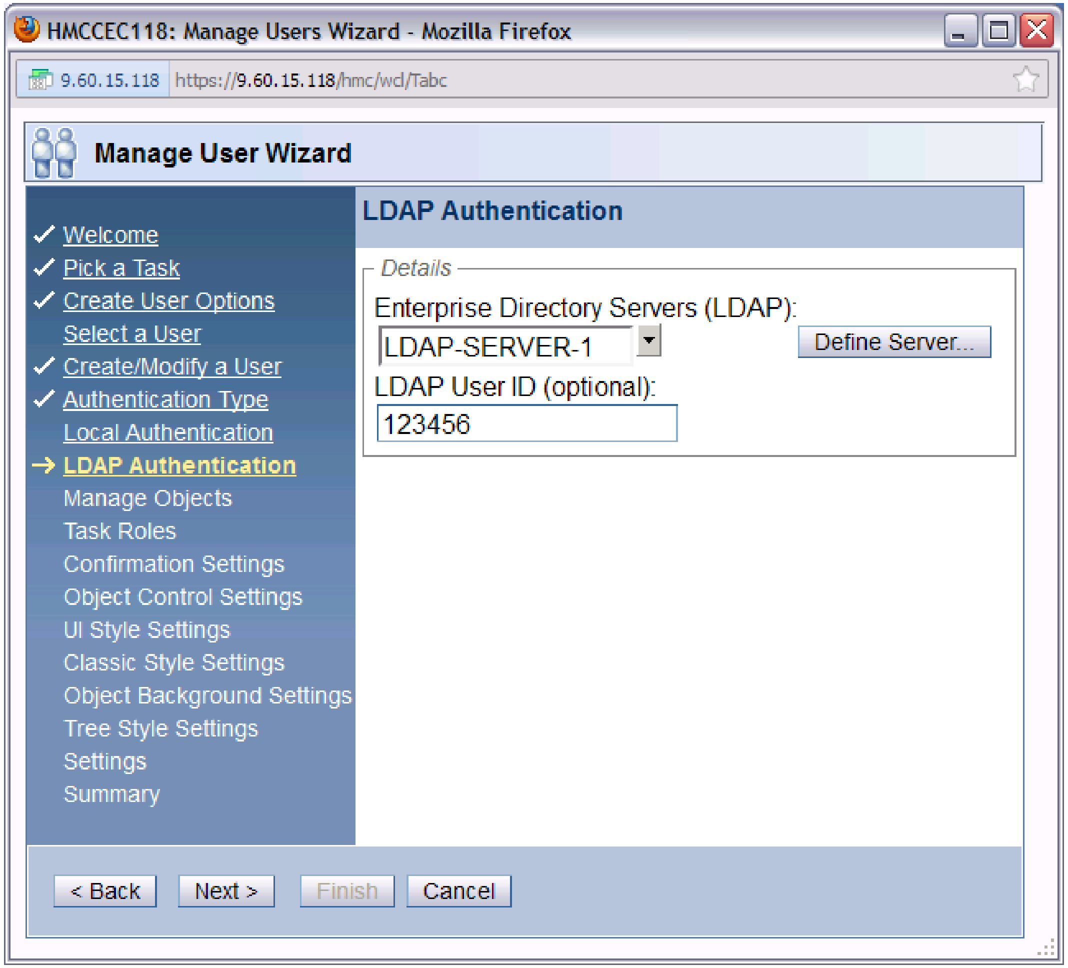
○ Search one level only

Enter the search filter that selects the user's entry in the directory.

Search filter: mail={0}

Defining Users and Roles (cont.)

- Now that the LDAP server has been configured, indicate that this user will be authenticated using the server using their UID or …



LDAP Authentication

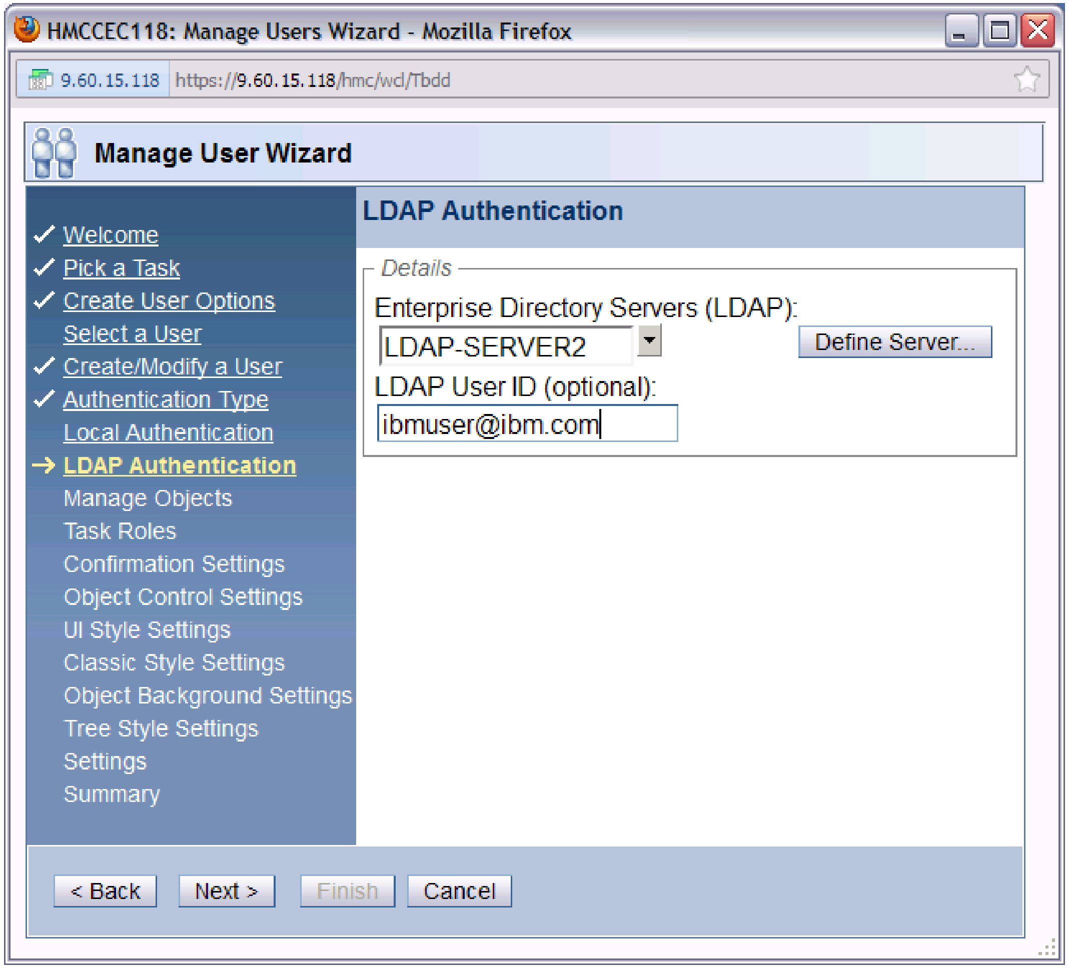
Details

Enterprise Directory Servers (LDAP): LDAP-SERVER-1

LDAP User ID (optional): 123456

Defining Users and Roles (cont.)

- that this user will be authenticated using the server using their email address



HMCCEC118: Manage Users Wizard - Mozilla Firefox

9.60.15.118 https://9.60.15.118/hmc/wcl/Tbdd

Manage User Wizard

LDAP Authentication

Details

Enterprise Directory Servers (LDAP): LDAP-SERVER2

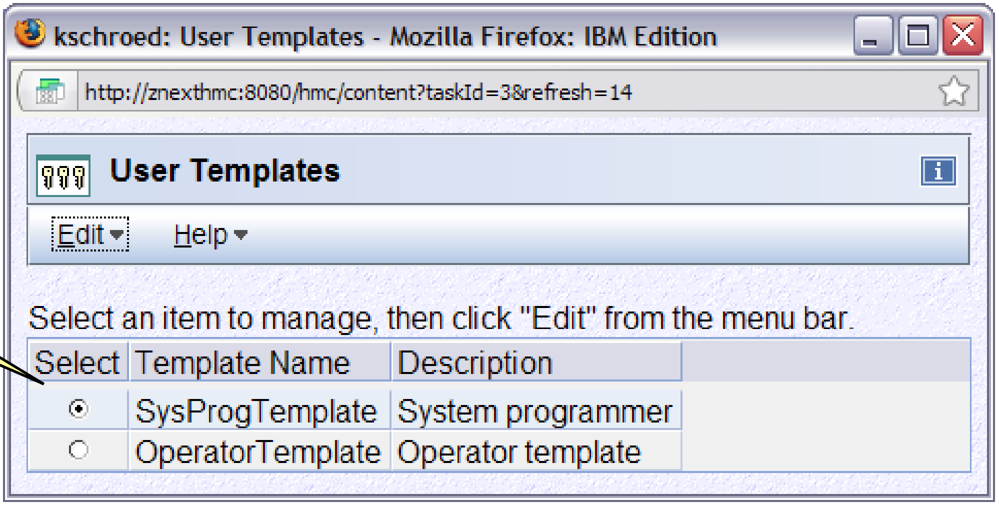
LDAP User ID (optional): ibmuser@ibm.com

User Templates and Patterns

- **User template**
  - Defines all the same characteristics that would normally be defined for a user
  - Restricted to LDAP authentication
- **User pattern**
  - Defines the pattern to be used to try and match “unknown” user ids with a template
  - Defines a default template to be used for matching user ids
  - Defines the retention time (in days) for modified user setting information
  - Optionally defines LDAP attributes used to determine:
    - User template to be used
    - “Domains” where the pattern is valid
- **Note: LDAP server used for authentication can be different from the one used to specify the template and domain names**

User Templates task

Selected the template to be modified, removed, etc.



kschroed: User Templates - Mozilla Firefox: IBM Edition

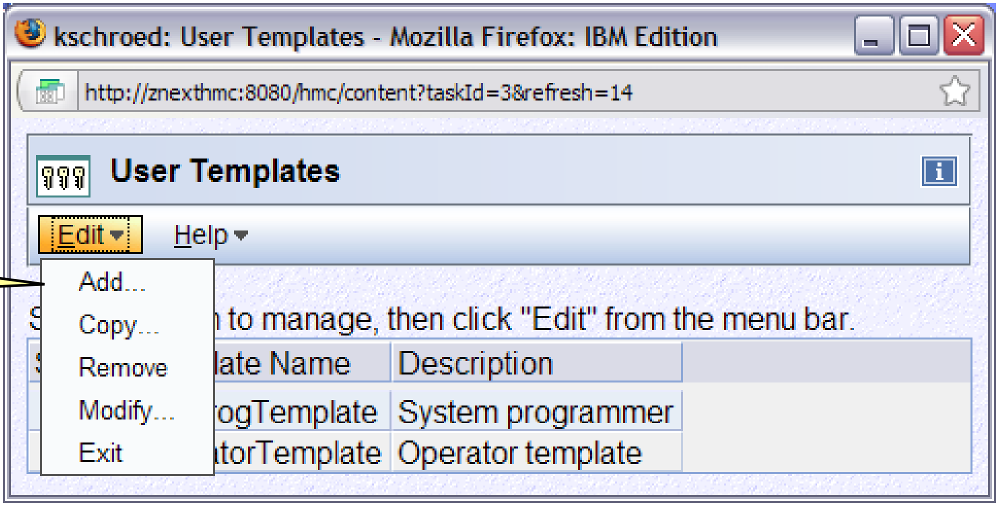
http://znexthmc:8080/hmc/content?taskId=3&refresh=14

User Templates

Select an item to manage, then click "Edit" from the menu bar.

Select	Template Name	Description
●	SysProgTemplate	System programmer
○	OperatorTemplate	Operator template

Drop down menu to choose the action to be performed



kschroed: User Templates - Mozilla Firefox: IBM Edition

http://znexthmc:8080/hmc/content?taskId=3&refresh=14

User Templates

S to manage, then click "Edit" from the menu bar.

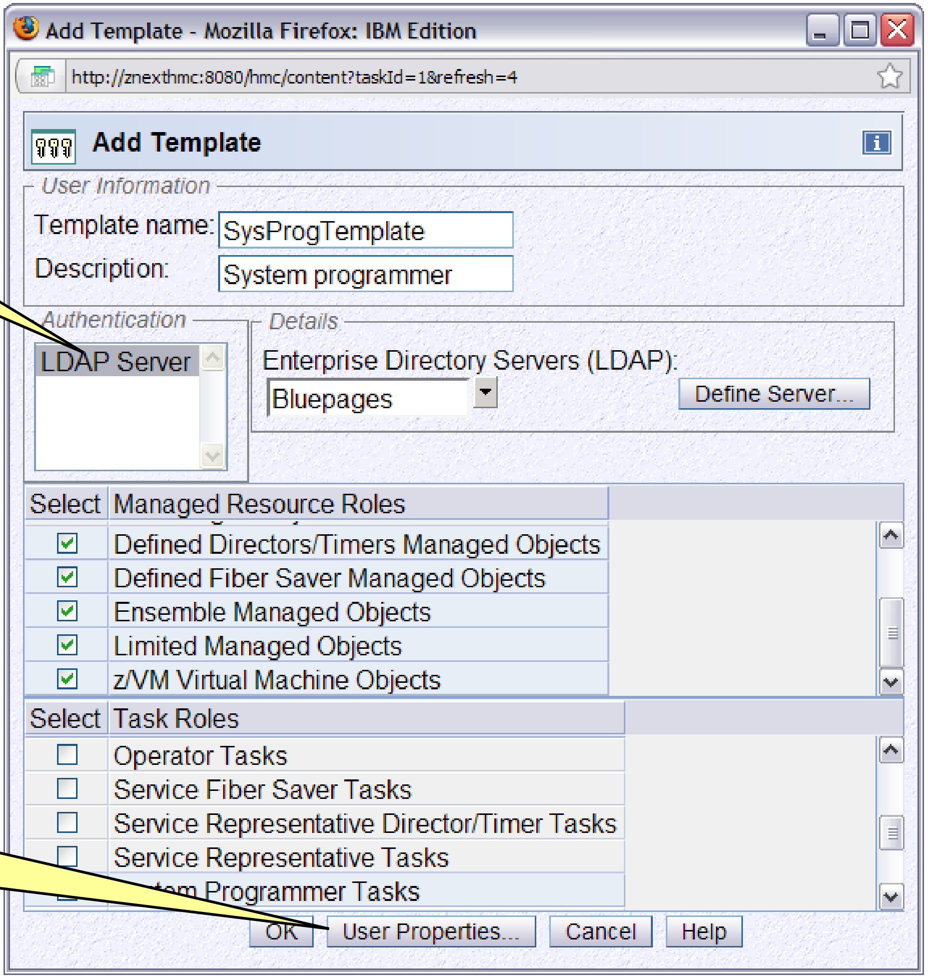
S	late Name	Description
	ogTemplate	System programmer
	torTemplate	Operator template

User Templates

Restricted to LDAP authentication; no password defined

Defines which roles a dynamic user based on this template will have

Additional user properties for user template is the same as for real users



Add Template - Mozilla Firefox: IBM Edition

http://znexthmc:8080/hmc/content?taskId=1&refresh=4

Add Template

User Information

Template name: SysProgTemplate

Description: System programmer

Authentication

LDAP Server

Details

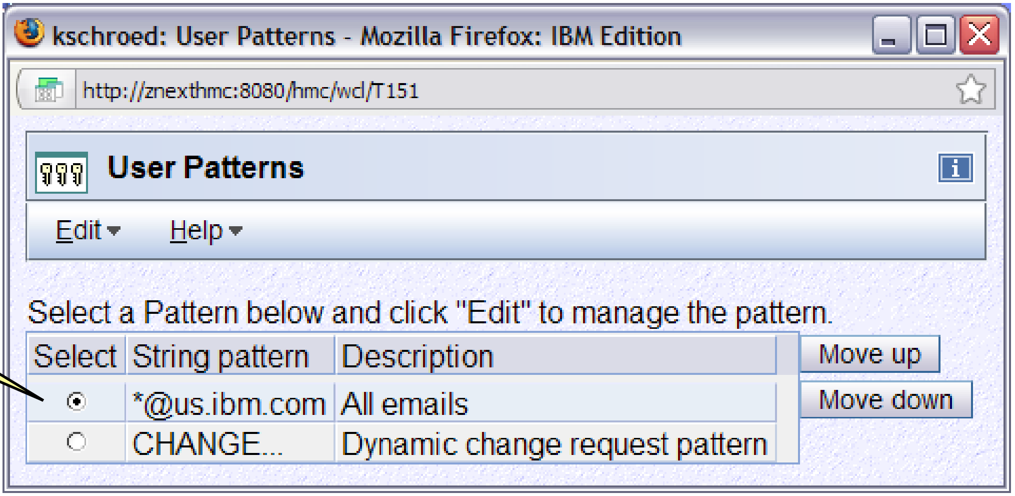
Enterprise Directory Servers (LDAP): Bluepages

Select	Managed Resource Roles
☑	Defined Directors/Timers Managed Objects
☑	Defined Fiber Saver Managed Objects
☑	Ensemble Managed Objects
☑	Limited Managed Objects
☑	z/VM Virtual Machine Objects

Select	Task Roles
□	Operator Tasks
□	Service Fiber Saver Tasks
□	Service Representative Director/Timer Tasks
□	Service Representative Tasks
	tem Programmer Tasks

User Patterns task

Selected the pattern to be modified, removed, etc.



kschroed: User Patterns - Mozilla Firefox: IBM Edition

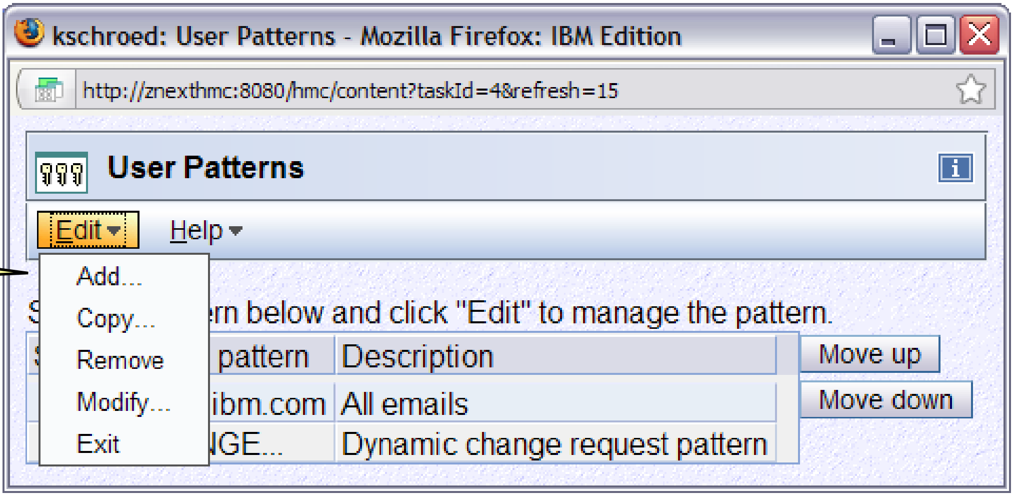
http://znexthmc:8080/hmc/wcl/T151

User Patterns

Select a Pattern below and click "Edit" to manage the pattern.

Select	String pattern	Description
●	*@us.ibm.com	All emails
○	CHANGE...	Dynamic change request pattern

Drop down menu to choose the action to be performed



kschroed: User Patterns - Mozilla Firefox: IBM Edition

http://znexthmc:8080/hmc/content?taskId=4&refresh=15

User Patterns

S rn below and click "Edit" to manage the pattern.

S pattern	Description
ibm.com	All emails
IGE...	Dynamic change request pattern

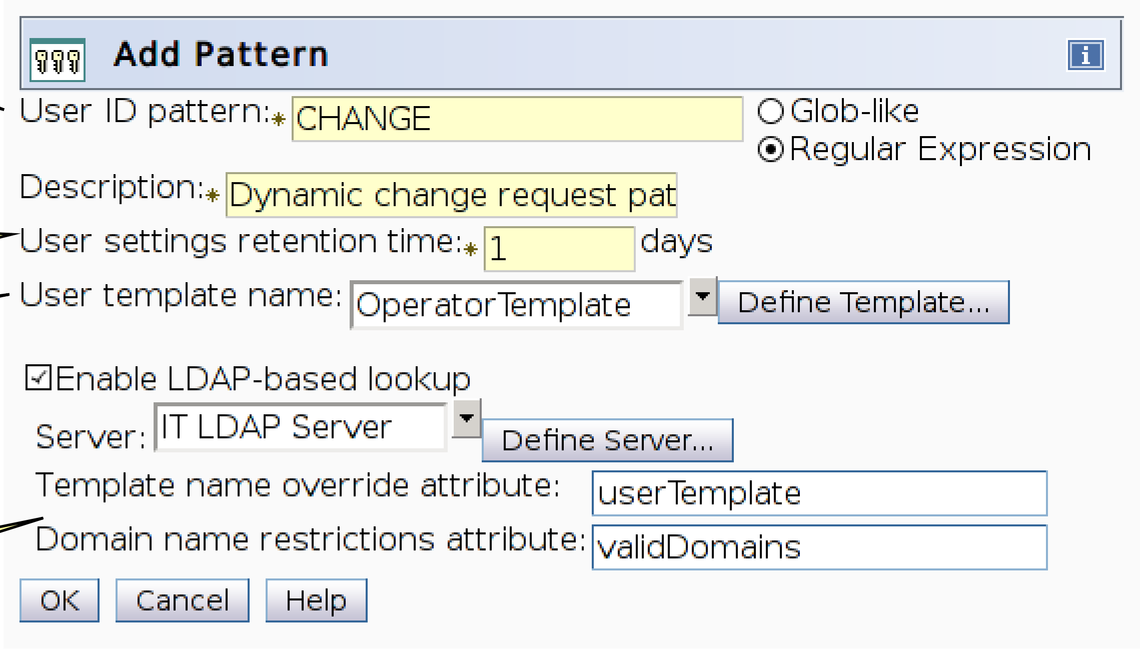
User Patterns

Patterns allow for 2 different types of expressions

Number of days user settings data for dynamic users is retained

Default template to use if template not specified via LDAP

Optional LDAP attributes used to determine template and valid domains



Add Pattern

User ID pattern:* CHANGE

○ Glob-like
● Regular Expression

Description:* Dynamic change request pat

User settings retention time:* 1 days

User template name: OperatorTemplate

☑ Enable LDAP-based lookup

Server: IT LDAP Server

Template name override attribute: userTemplate

Domain name restrictions attribute: validDomains

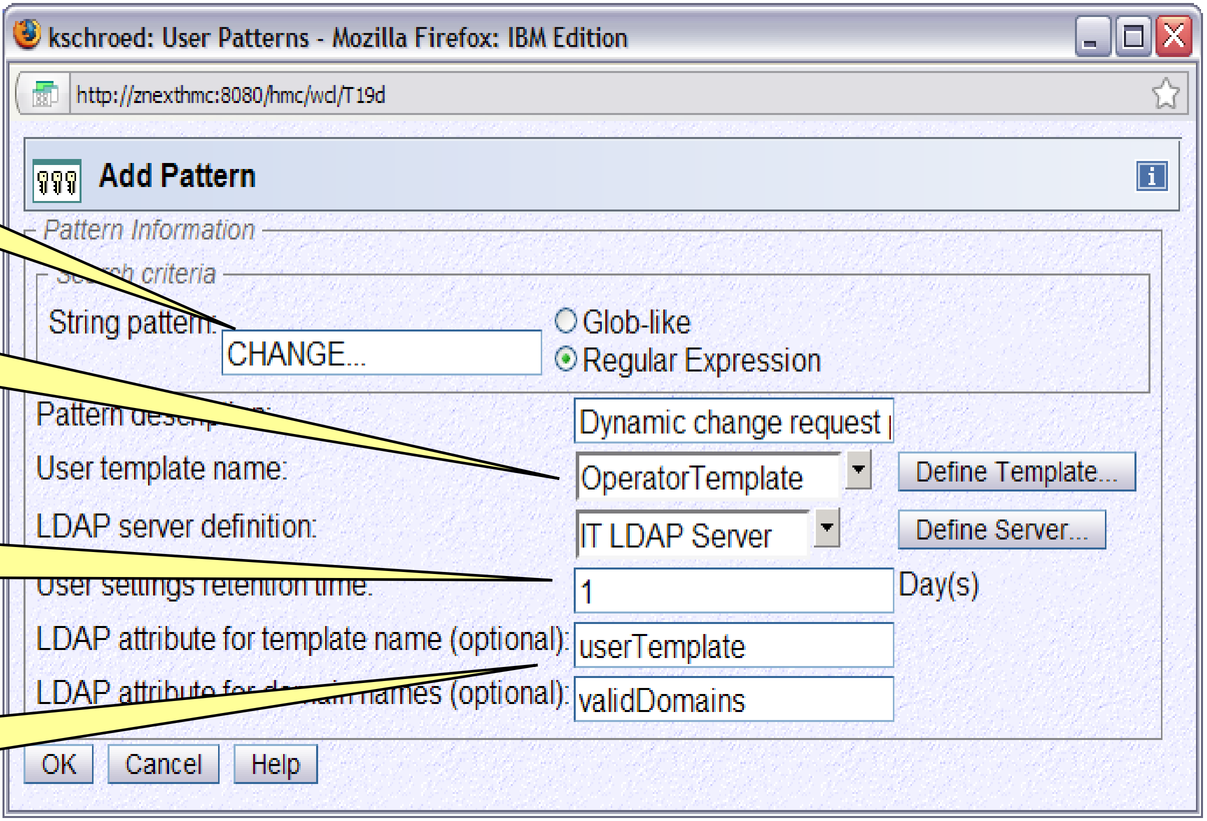
User Patterns

Patterns allow for 2 different types of expressions

Default template to use if template not specified via LDAP

Number of days user settings data for dynamic users is retained

Optional LDAP attributes used to determine template and valid domains



kschroed: User Patterns - Mozilla Firefox: IBM Edition

http://znexthmc:8080/hmc/wcl/T19d

Add Pattern

Pattern Information

Search criteria

String pattern: CHANGE...

○ Glob-like

● Regular Expression

Pattern description: Dynamic change request

User template name: OperatorTemplate

LDAP server definition: IT LDAP Server

User settings retention time: 1 Day(s)

LDAP attribute for template name (optional): userTemplate

LDAP attribute for domain names (optional): validDomains

Do you want to enable for Automation Controls (APIs) access to the HMC?

Is this automation driven over an internal network?

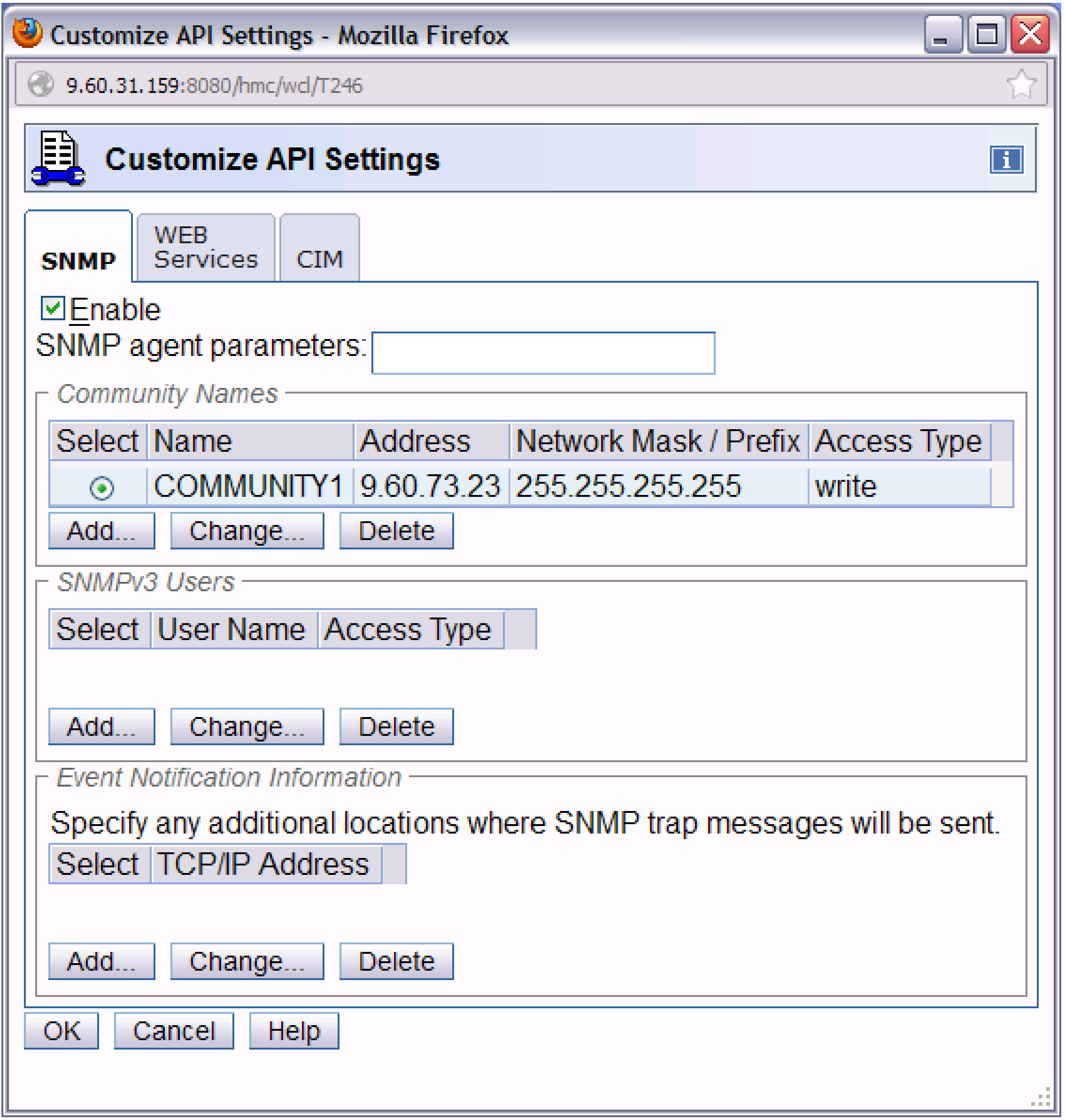
Do you want to restrict access to tasks/objects or additionally from which IP sources and/or users?

If already have an investment in one type of APIs (ie. SNMP),
-- answers to above questions will validate to stay there
-- or potentially make an investment to WebServices APIs

Enabling APIs

SNMP V1 and V2

- Authentication based on the community name and IP address configured on the HMC
  - Discussed in RFCs 1157 and 1901
- Use within a network that is secure; for example within your intranet


Customize API Settings - Mozilla Firefox

9.60.31.159:8080/hmc/wcl/T246

Customize API Settings

☑ Enable

SNMP agent parameters:

Community Names

Select	Name	Address	Network Mask / Prefix	Access Type
●	COMMUNITY1	9.60.73.23	255.255.255.255	write

SNMPv3 Users

Select	User Name	Access Type

Event Notification Information

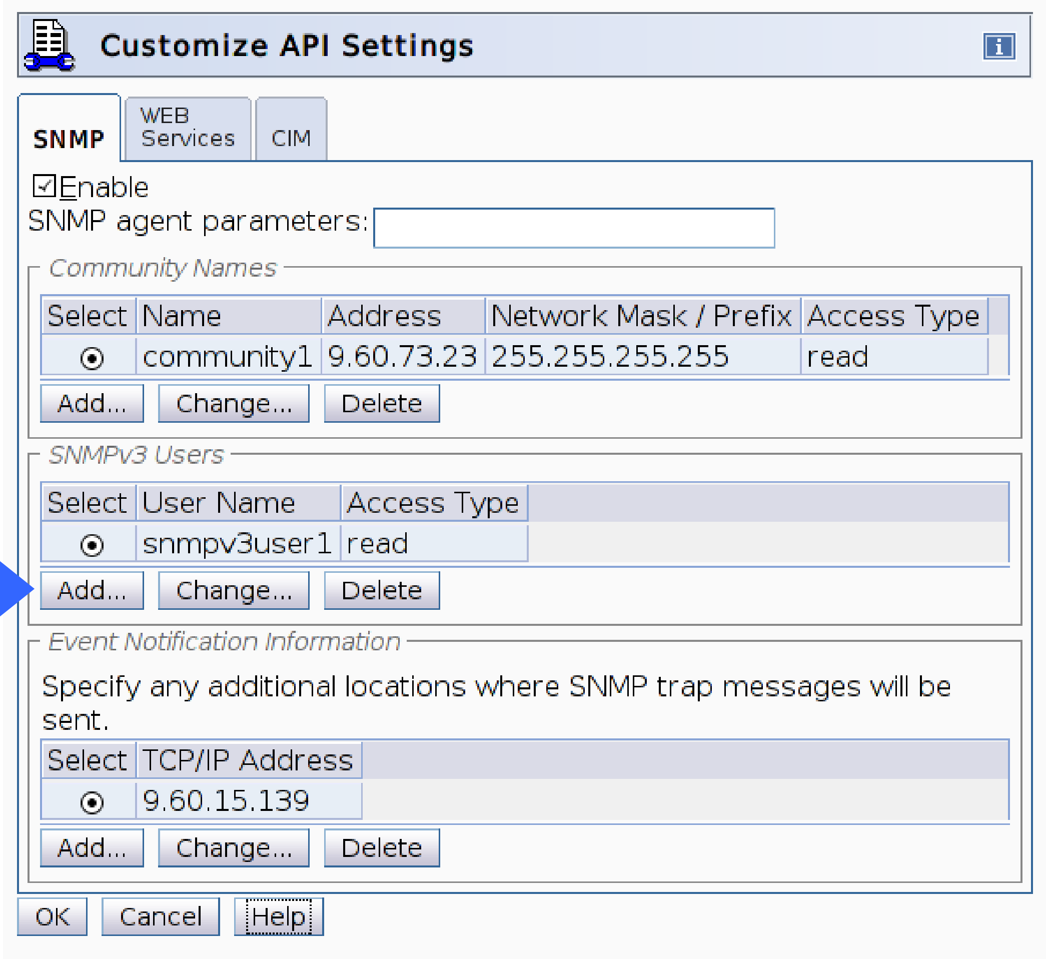
Specify any additional locations where SNMP trap messages will be sent.

Select	TCP/IP Address

Enabling APIs (cont.)

SNMP V3

- User and password configured on both sides and used for authentication
  - RFC 3414 discusses the User Based Security Model (USM)
  - User configured is not an HMC user (password not shown)
- Messages are encrypted
- More secure than V1 or V2



Customize API Settings

☑ Enable

SNMP agent parameters:

Community Names

Select	Name	Address	Network Mask / Prefix	Access Type
●	community1	9.60.73.23	255.255.255.255	read

SNMPv3 Users

Select	User Name	Access Type
●	snmpv3user1	read

Event Notification Information

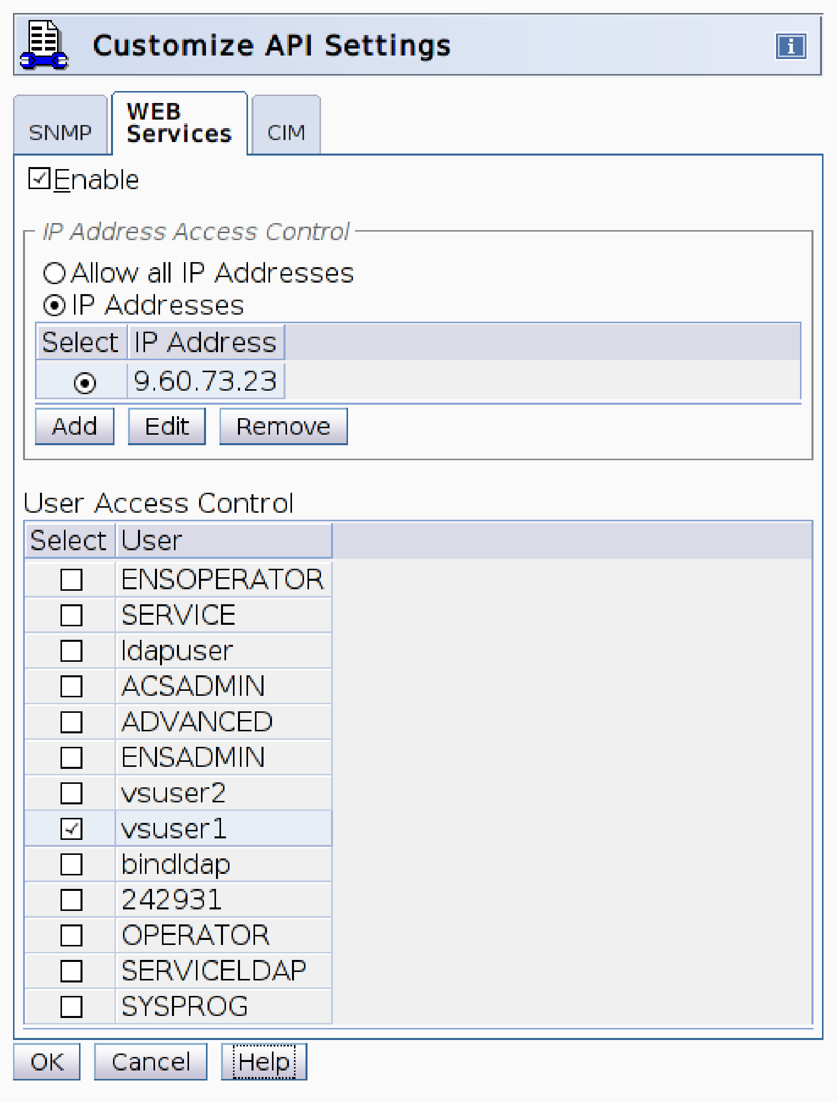
Specify any additional locations where SNMP trap messages will be sent.

Select	TCP/IP Address
●	9.60.15.139

Enabling APIs (cont.)

Web Services APIs

- Client connections use HMC certificates and encryption
  - Same benefits as discussed in the HMC Certificates section
- Clients authenticated as HMC users
  - Normal user access controls apply
- Can restrict to specific IP addresses
- Can restrict to specific HMC users



Customize API Settings

☑ Enable

IP Address Access Control

○ Allow all IP Addresses
● IP Addresses

Select	IP Address
●	9.60.73.23

User Access Control

Select	User
□	ENSOPERATOR
□	SERVICE
□	ldapuser
□	ACSADMIN
□	ADVANCED
□	ENSADMIN
□	vsuser2
☑	vsuser1
□	bindldap
□	242931
□	OPERATOR
□	SERVICELDAP
□	SYSPROG

Many customers have very strict controls with z/OS controlling which users have access to which z/OS commands?

Do you know that enabling Operating Systems Messages on the HMC enables it for all HMCs which manage that system/LPAR?

How should you manage Operating Systems Messages enablement?
-- limit users, LPARs, Read Only vs. Read Write?

Operating System HMC Considerations

- Operating System Messages
  - For z/VM and z/Linux consoles accessed from the HMC,
    - Required to logon via an OS user ID
  - Setup on z/OS
    - Using the Operating System Messages task targeted to an LPAR, issue (to activate problem determination mode)

      ```
      VARY CN(*),ACTIVATE
      ```

      to allow the the Operating System Messages task on the HMC or any current or future HMC managing the targeted LPAR, to issue z/OS commands
    - To deactivate problem determination mode and the ability of issuing z/OS commands from the HMC(s), issue

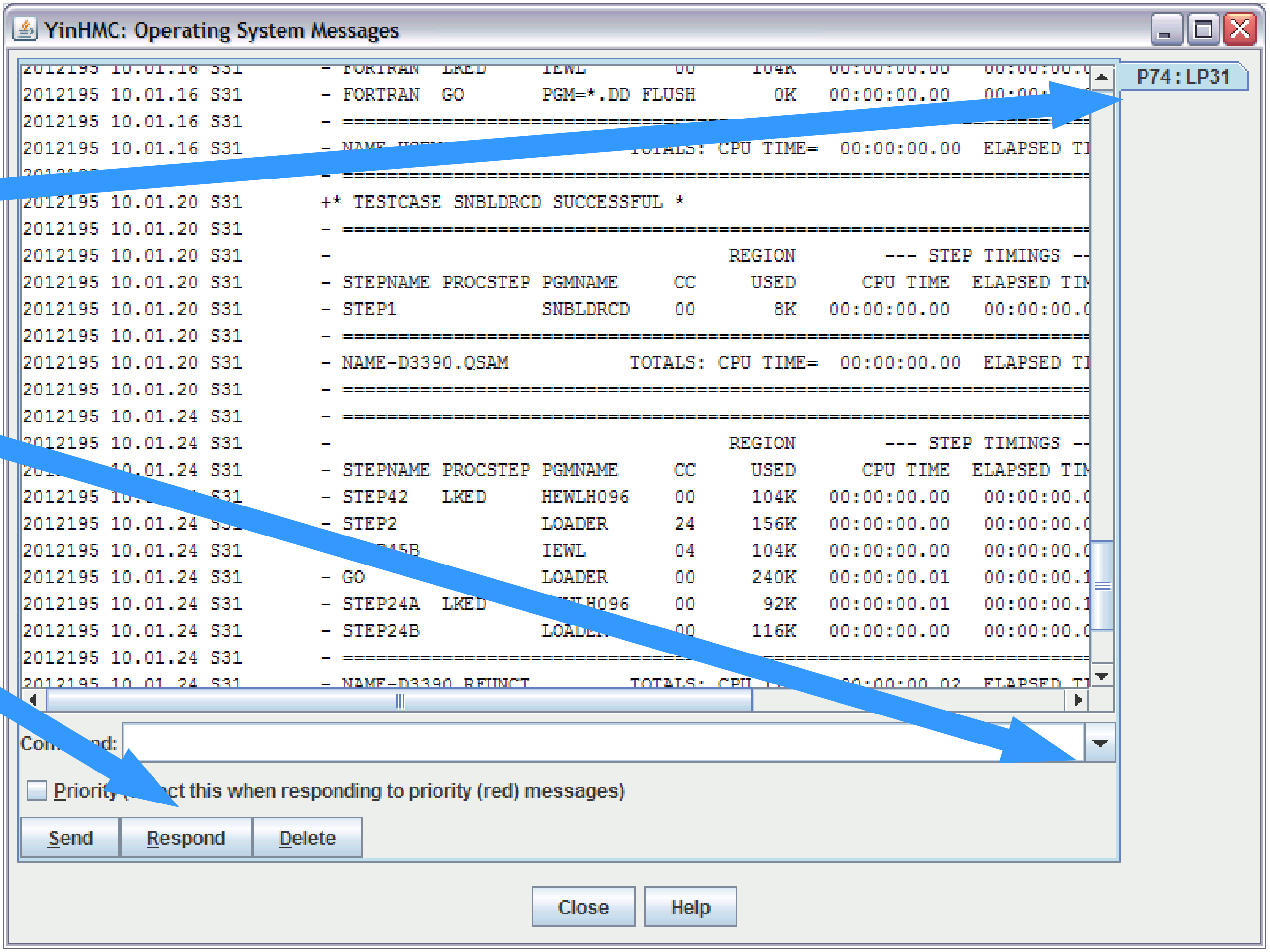
      ```
      VARY CN(*),DEACT
      ```

Operating System HMC Considerations (cont.)

- Operating System Messages (cont.)
  - Depending on your requirements:
    - Limit what HMCs can manage the CEC
    - Limit access to which HMC users can access the LPAR
    - Limit access to which HMC users can run the Operating System Messages task
      - Limit to read-only if read-write is not required
    - For z/OS, use RACF profiles to limit which commands can be issued by the **system console**
      - Operating System Messages commands issued as if from the system console

Operating System HMC Considerations (cont.)

- Operating System Messages (cont.)
  - One tab per LPAR
  - Command history maintained with reissue capability
  - Respond to a specific selected message



YinHMC: Operating System Messages

```
2012195 10.01.16 S31       - FORTRAN  LKED     IEWL          00      104K   00:00:00.00    00:00:00.0
2012195 10.01.16 S31       - FORTRAN  GO       PGM=*.DD FLUSH         0K   00:00:00.00    00:00:0
2012195 10.01.16 S31       - =====================================================================
2012195 10.01.16 S31       - NAME-USTWN              TOTALS: CPU TIME=  00:00:00.00   ELAPSED TI
2012195                    - =====================================================================
2012195 10.01.20 S31       +* TESTCASE SNBLDRCD SUCCESSFUL *
2012195 10.01.20 S31       - =====================================================================
2012195 10.01.20 S31       -                                 REGION         --- STEP TIMINGS --
2012195 10.01.20 S31       - STEPNAME PROCSTEP PGMNAME     CC      USED       CPU TIME  ELAPSED TIM
2012195 10.01.20 S31       - STEP1             SNBLDRCD    00        8K   00:00:00.00    00:00:00.0
2012195 10.01.20 S31       - =====================================================================
2012195 10.01.20 S31       - NAME-D3390.QSAM         TOTALS: CPU TIME=  00:00:00.00   ELAPSED TI
2012195 10.01.20 S31       - =====================================================================
2012195 10.01.24 S31       - =====================================================================
2012195 10.01.24 S31       -                                 REGION         --- STEP TIMINGS --
2012195 10.01.24 S31       - STEPNAME PROCSTEP PGMNAME     CC      USED       CPU TIME  ELAPSED TIM
2012195 10.01.24 S31       - STEP42   LKED     HEWLH096    00      104K   00:00:00.00    00:00:00.0
2012195 10.01.24 S31       - STEP2             LOADER      24      156K   00:00:00.00    00:00:00.0
2012195 10.01.24 S31       - STEP45B           IEWL        04      104K   00:00:00.00    00:00:00.0
2012195 10.01.24 S31       - GO                LOADER      00      240K   00:00:00.01    00:00:00.1
2012195 10.01.24 S31       - STEP24A  LKED     HEWLH096    00       92K   00:00:00.01    00:00:00.1
2012195 10.01.24 S31       - STEP24B           LOADER      00      116K   00:00:00.00    00:00:00.0
2012195 10.01.24 S31       - =====================================================================
2012195 10.01.24 S31       - NAME-D3390.REFUNCT      TOTALS: CPU TIME=  00:00:00.02   ELAPSED TI
```

Command:

□ Priority (select this when responding to priority (red) messages)

Operating System HMC Considerations (cont.)

- BCPii from OS
  - Used for Sysplex Monitoring and Recovery controls and Graphically Dispersed Parallel Sysplex (GDPS)
    - All systems in the Sysplex must be defined to the Change Management HMC
    - Add 127.0.0.1/255.255.255.255 as a write access community name entry within the Customize APIs task on the SE
    - See the BCPii presentation in the “Additional Materials” section for more details on configuring BCPii

What considerations are there for protection against Malware getting onto HMC or SE?

What does IBM do?

What should you do? (Secure FTP)

Besides all HMC provided security/networking controls, should you consider any physical access restriction to local HMCs/SEs?

HMC Protection Against Malware

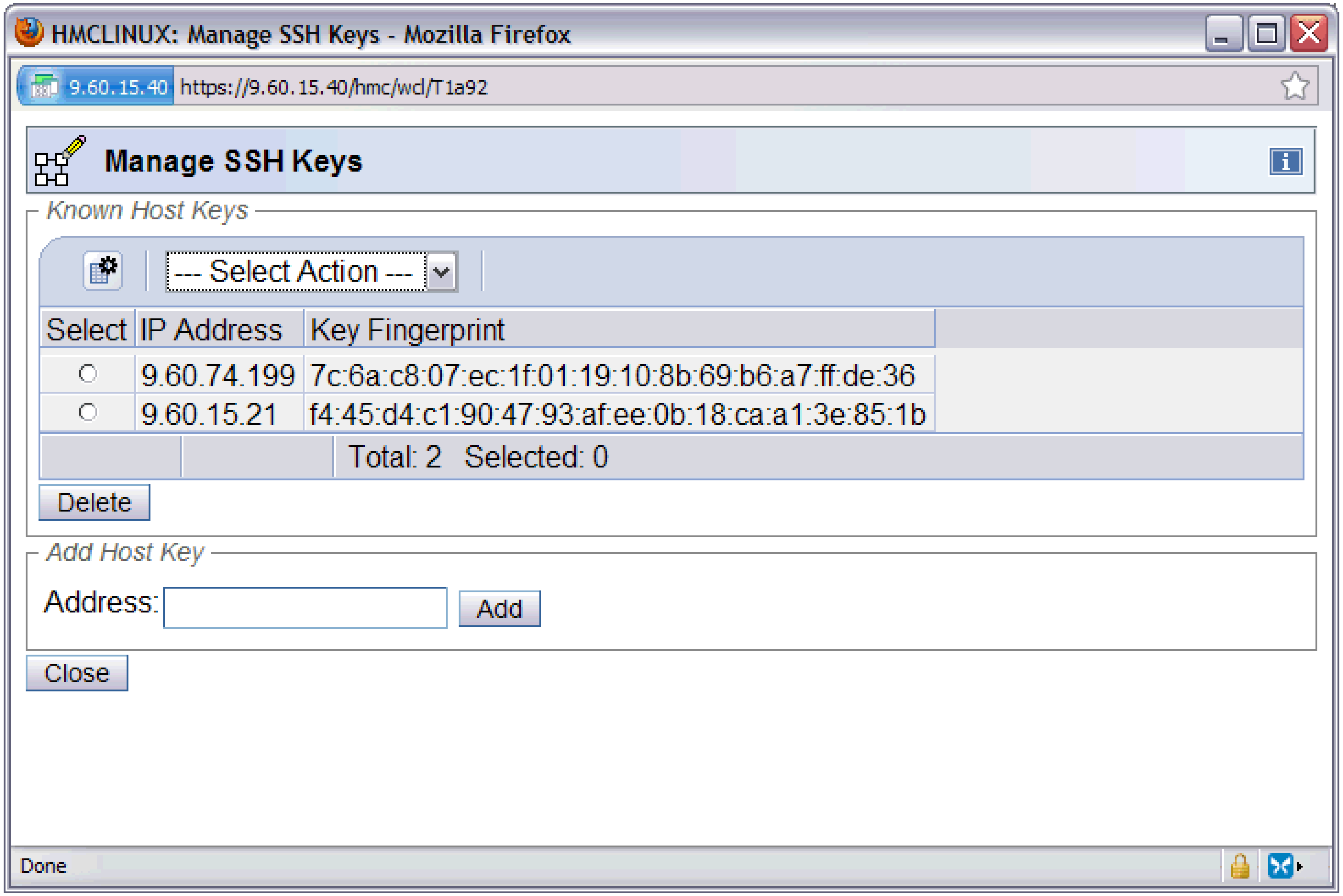
- HMC provides protection of all Firmware updates by using digitally signed Firmware (FW)
  - Also used by Backup Critical Data and Harddisk Restore in case of Harddisk failures.
  - Base code signed with private key; includes disk image files and individual firmware modules
  - MCLs/MCFs (fixes) signed with private key and validated during retrieval
  - Symmetric key used during backups to allow validation when performing a hard disk restore
  - Compliance with Federal Information Processing Standard (FIPS) 140-2 Level 1 for crypto LIC changes.

HMC/SE Secure FTP support

- New support was added in 2.11.1 to allow a secure FTP connection from a HMC/SE FTP client to a customer FTP server location
  - Implemented using the SSH File Transfer Protocol which is an extension of the Secure Shell protocol (SSH)
  - A new Manage SSH Keys console action allows the customer import public keys associated with a host address – added to both HMC and SE.
  - Secure FTP infrastructure allows HMC/SE applications to query if a public key is associated with a host address as well as to utilize the Secure FTP interface with the appropriate public key for a given host.
  - Tasks utilizing FTP now provide a selection for the Secure Host connection.
    - When selected they verify that a public key is associated with the specified host name, and if none is provided they put up a message box to point them to the Manage SSH Keys task to input one. Tasks that provide this support include:
      - Input/Output (I/O) Configuration -> Import/Export Source File ->FTP Location
      - Customize Scheduled Operations (Audit and Log Management only)
      - Retrieve Internal Code -> Retrieve code changes from FTP site to the selected objects
      - Change Console Internal Code -> Retrieve Internal Code Changes ->Retrieve code changes from FTP site to the HMC
      - Advanced Facilities->Card Specific Advanced Facilities->Manual Configuration Options->Import/Export source file by FTP (For OSA-ICC PCHIDS only – Channel Type=OSC)

HMC/SE Secure FTP support (cont.)

- Manage SSH Keys console action



HMCLINUX: Manage SSH Keys - Mozilla Firefox

9.60.15.40 https://9.60.15.40/hmc/wcl/T1a92

Manage SSH Keys

Known Host Keys

--- Select Action ---

Select	IP Address	Key Fingerprint
○	9.60.74.199	7c:6a:c8:07:ec:1f:01:19:10:8b:69:b6:a7:ff:de:36
○	9.60.15.21	f4:45:d4:c1:90:47:93:af:ee:0b:18:ca:a1:3e:85:1b

Total: 2 Selected: 0

Delete

Add Host Key

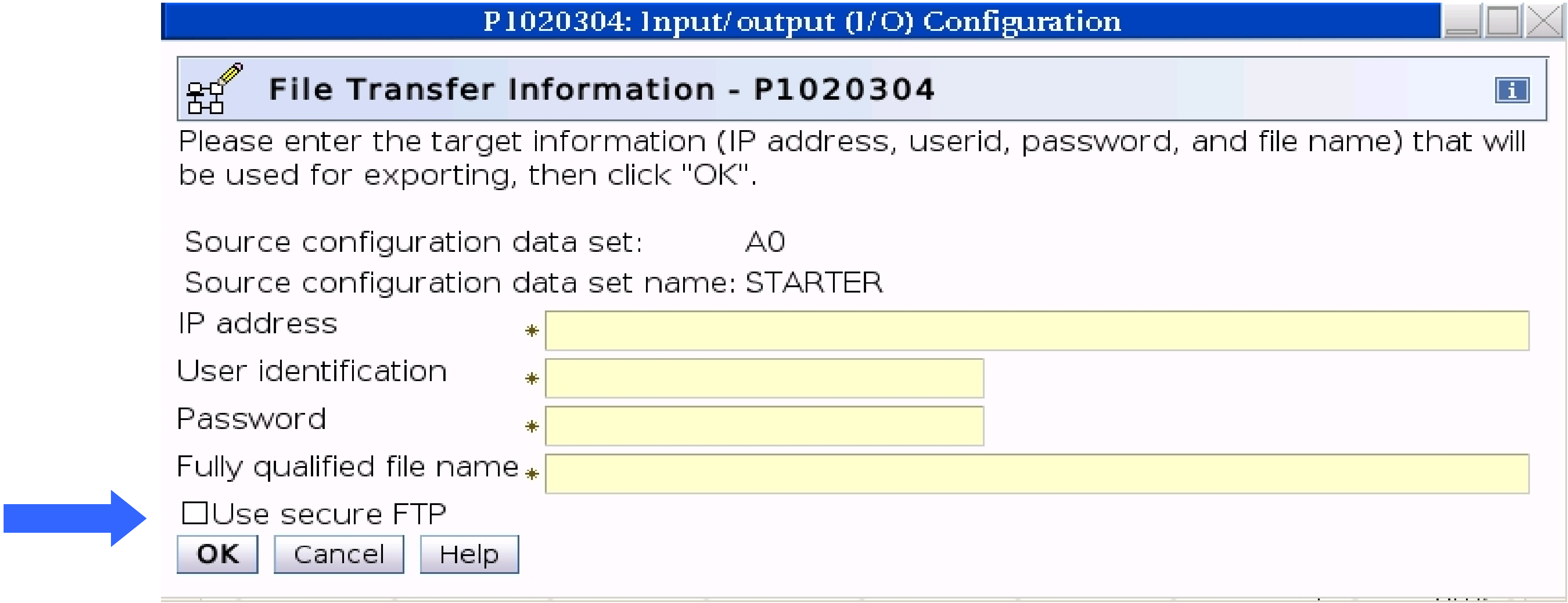
Address: Add

Close

Done

HMC Secure FTP support (cont.)

- Export IOCDS Panel showing the new “Use secure FTP” checkbox



P1020304: Input/output (I/O) Configuration

File Transfer Information - P1020304

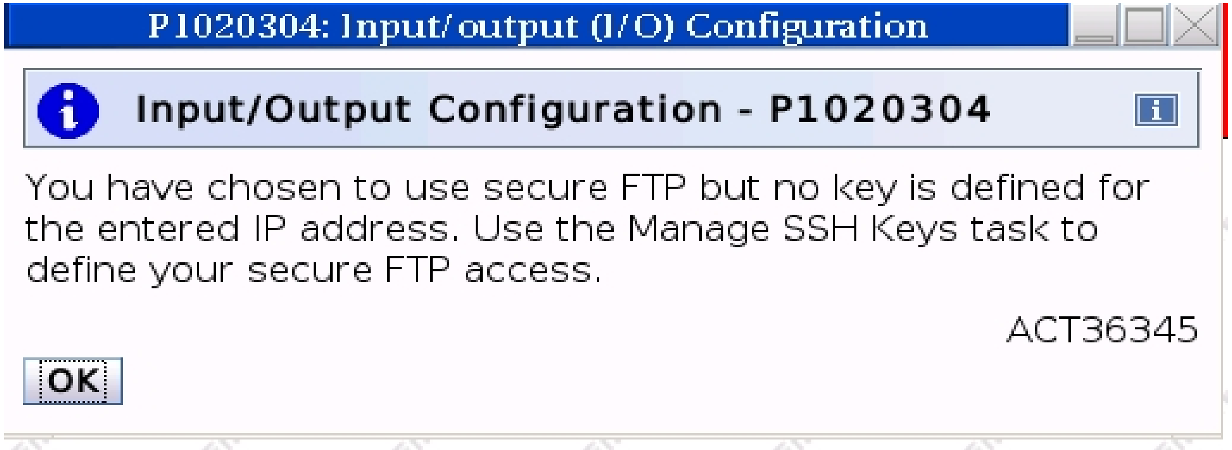
Please enter the target information (IP address, userid, password, and file name) that will be used for exporting, then click "OK".

Source configuration data set: A0
Source configuration data set name: STARTER
IP address *
User identification *
Password *
Fully qualified file name *

□Use secure FTP

HMC Secure FTP support (cont.)

- Export IOCDS Panel showing message display if the “Use secure FTP” checkbox is selected but no SSH keys exist for the specified address.


P1020304: Input/output (I/O) Configuration
Input/Output Configuration - P1020304

You have chosen to use secure FTP but no key is defined for the entered IP address. Use the Manage SSH Keys task to define your secure FTP access.

ACT36345

What Auditing information/processes does the HMC provide?

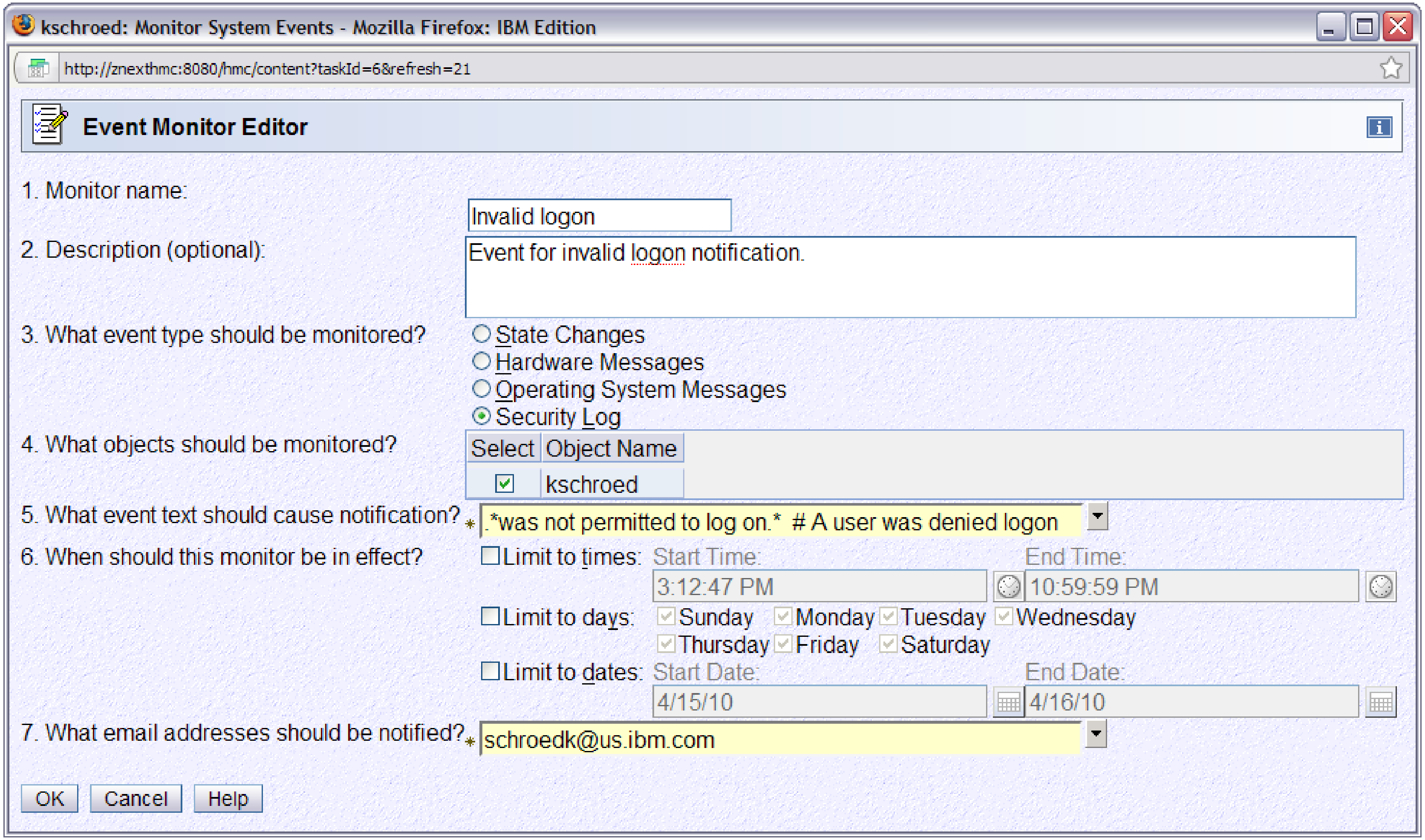
Have you established policies to utilize it?

Security Event Notification

- **Email notification of security events**
  - **Monitor System Events task supports creating event monitors for security logs**
  - **Any number of users can get an email when a matching security log occurs**

Security Event Notification (cont.)

- **Configuring a security event monitor**



kschroed: Monitor System Events - Mozilla Firefox: IBM Edition
http://znexthmc:8080/hmc/content?taskId=6&refresh=21

Event Monitor Editor

1. Monitor name: Invalid logon

2. Description (optional): Event for invalid logon notification.

3. What event type should be monitored?
○ State Changes
○ Hardware Messages
○ Operating System Messages
● Security Log

4. What objects should be monitored?

Select	Object Name
☑	kschroed

5. What event text should cause notification? .*was not permitted to log on.* # A user was denied logon

6. When should this monitor be in effect?
□ Limit to times: Start Time: 3:12:47 PM End Time: 10:59:59 PM
□ Limit to days: ☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday
□ Limit to dates: Start Date: 4/15/10 End Date: 4/16/10

7. What email addresses should be notified? schroedk@us.ibm.com

Audit reporting capabilities

- **Provide scheduled and manual methods to obtain audit reports which include:**
  - **All user related data (user ids, user settings, roles, password rules, LDAP servers, automatic logon, etc.)**
  - **Configuration details (remote access, automation parameters, data replication, network settings, etc.)**
  - **Operational data (custom group definitions, associated activation profile settings, managed resources)**
  - **SSL certificate information**

- **The offloading can be manually initiated via the Audit & Log Management task or scheduled via the Scheduled Operations task.**

Audit reporting capabilities (cont.)

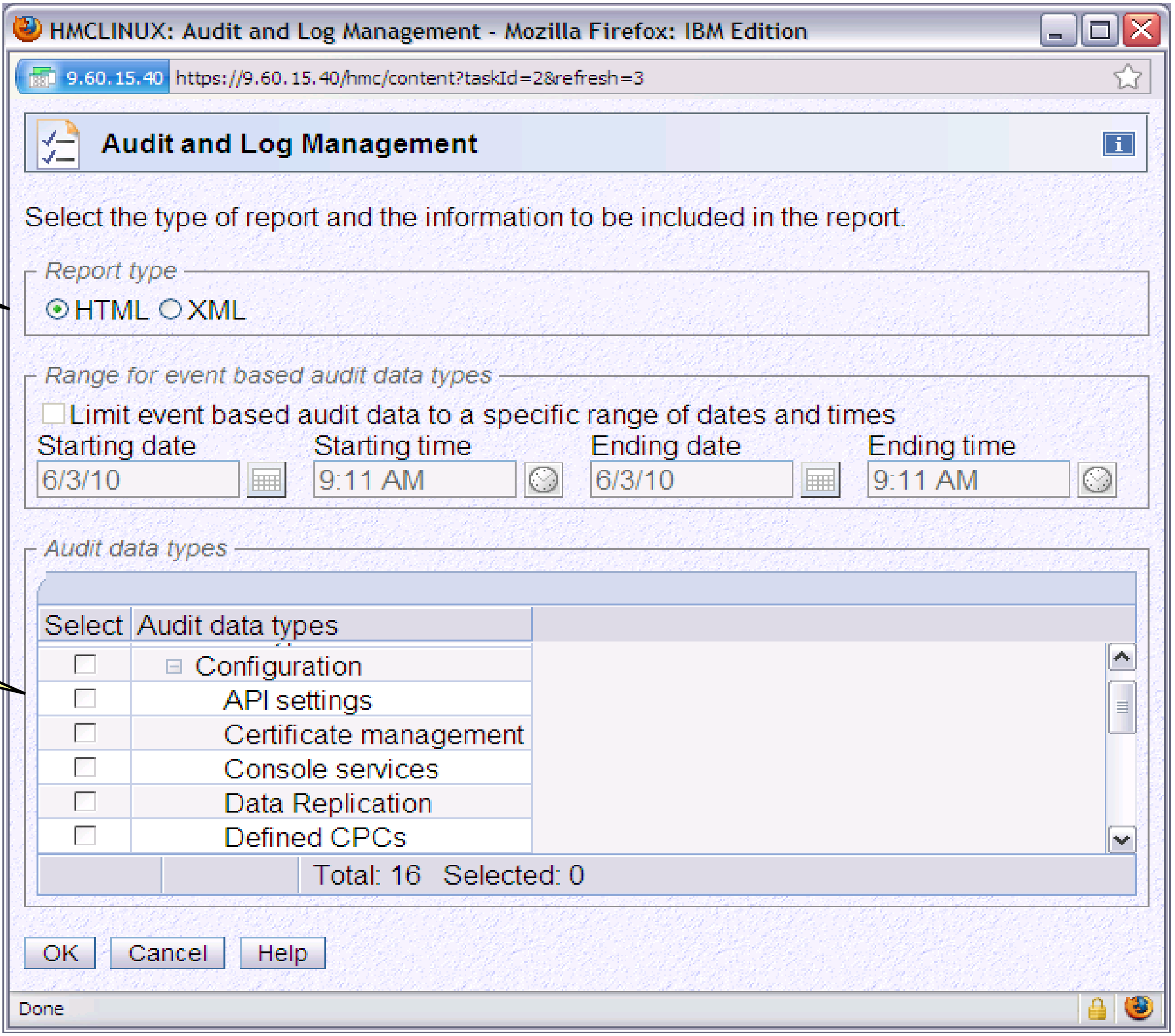
- **Provide scheduled and manual methods to obtain audit reports**
- **Auditable types of information broken in to 3 categories**

Configuration	Logs	User Profiles
API settings Certificate management Console services Data replication Defined CPCs Domain security Grouping Monitor system events Object locking Product engineering access Welcome text	Console events Security log Audit log Service history Tasks performed log	Default user settings LDAP server definitions Password profiles User roles Users User templates User patterns

Manual Audit Report Generation

Human consumable (HTML) and program consumable (XML) formats available

Entire categories or individual types of data can be selected for inclusion



HMCLINUX: Audit and Log Management - Mozilla Firefox: IBM Edition

9.60.15.40 https://9.60.15.40/hmc/content?taskId=2&refresh=3

Audit and Log Management

Select the type of report and the information to be included in the report.

Report type

● HTML ○ XML

Range for event based audit data types

□ Limit event based audit data to a specific range of dates and times

Starting date	Starting time	Ending date	Ending time
6/3/10	9:11 AM	6/3/10	9:11 AM

Audit data types

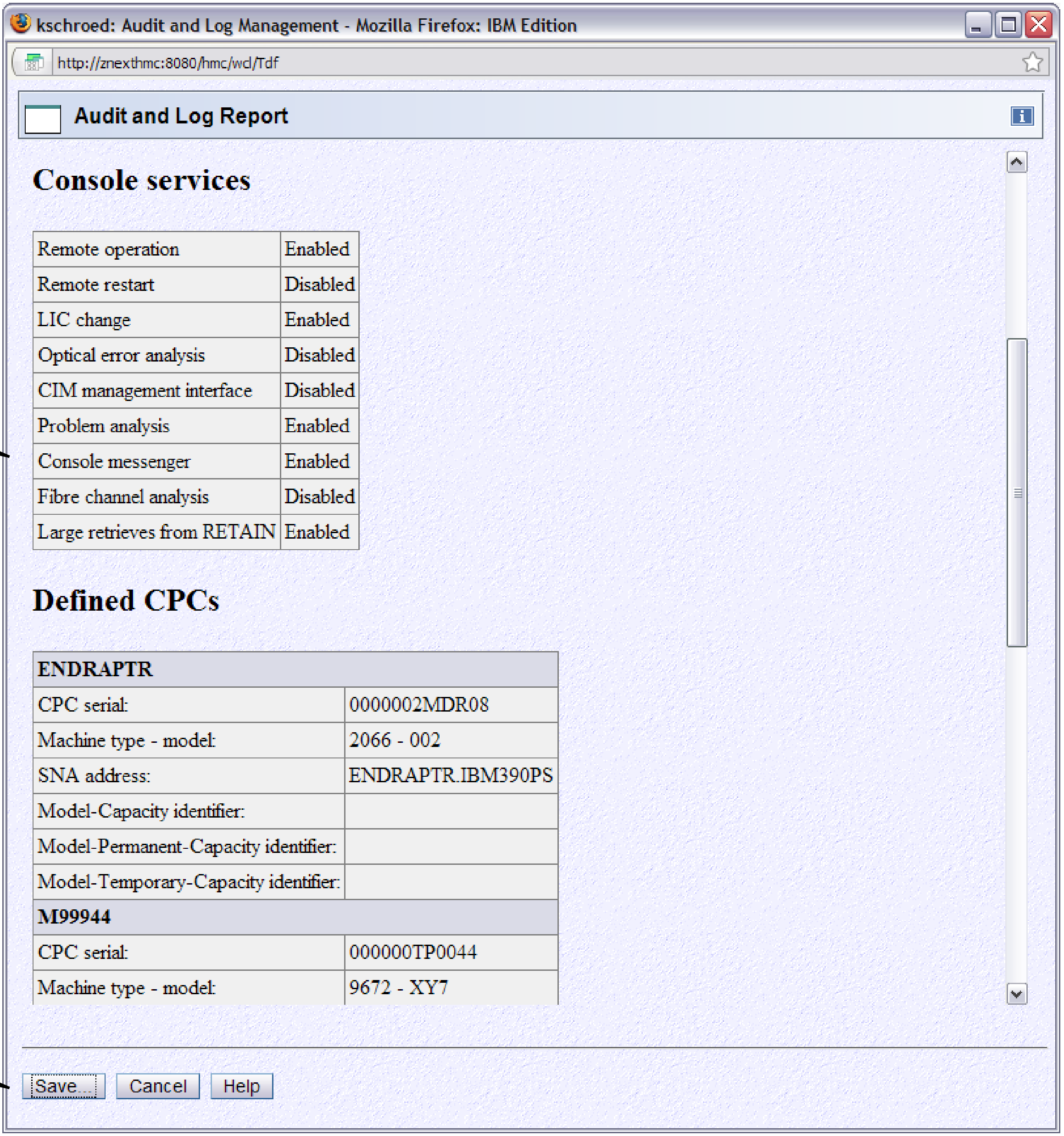
Select	Audit data types
□	⊟ Configuration
□	API settings
□	Certificate management
□	Console services
□	Data Replication
□	Defined CPCs

Total: 16 Selected: 0

Example Audit Report

Report contains the up to date configuration data for the selected types of data

Report can be saved remotely using the normal browser “Save as…” or locally to removable media


kschroed: Audit and Log Management - Mozilla Firefox: IBM Edition
http://znexthmc:8080/hmc/wcl/Tdf
Audit and Log Report
Save...
Cancel
Help

Console services

Remote operation	Enabled
Remote restart	Disabled
LIC change	Enabled
Optical error analysis	Disabled
CIM management interface	Disabled
Problem analysis	Enabled
Console messenger	Enabled
Fibre channel analysis	Disabled
Large retrieves from RETAIN	Enabled

Defined CPCs

ENDRAPTR	
CPC serial:	0000002MDR08
Machine type - model:	2066 - 002
SNA address:	ENDRAPTR.IBM390PS
Model-Capacity identifier:	
Model-Permanent-Capacity identifier:	
Model-Temporary-Capacity identifier:	
M99944	
CPC serial:	000000TP0044
Machine type - model:	9672 - XY7

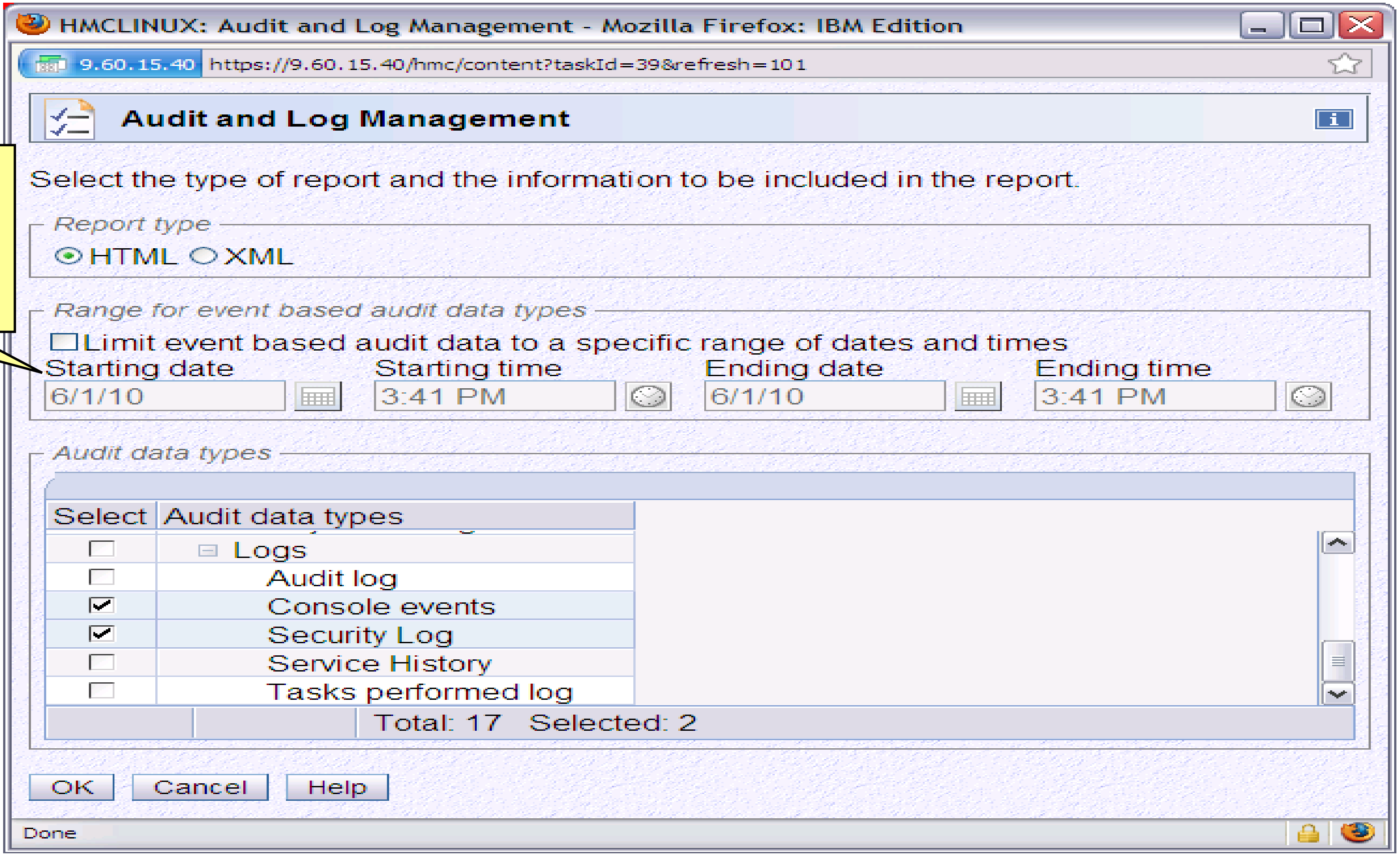
Offloading of security and event logs

- **Provide scheduled and manual methods to offload which include:**
  - **Security related events (log on/off, configuration changes, disruptive actions, etc.)**
  - **System events (scheduled operations definition, time sync, retrieval of Licensed Internal Code (firmware) fixes, etc.)**
  - **Recent task history including task, targets and user**
  - **Service history log**

- **The offloading can be manually initiated via the new Audit & Log Management task or scheduled via the Scheduled Operations task.**

- **The Format Security Logs to DVD-RAM task was removed from the HMC since it was redundant with the support above.**

Manual Audit Report Generation (logs)



HMCLINUX: Audit and Log Management - Mozilla Firefox: IBM Edition
9.60.15.40
https://9.60.15.40/hmc/content?taskId=39&refresh=101

Audit and Log Management

Select the type of report and the information to be included in the report.

Report type

● HTML ○ XML

Range for event based audit data types

□ Limit event based audit data to a specific range of dates and times

Starting date	Starting time	Ending date	Ending time
6/1/10	3:41 PM	6/1/10	3:41 PM

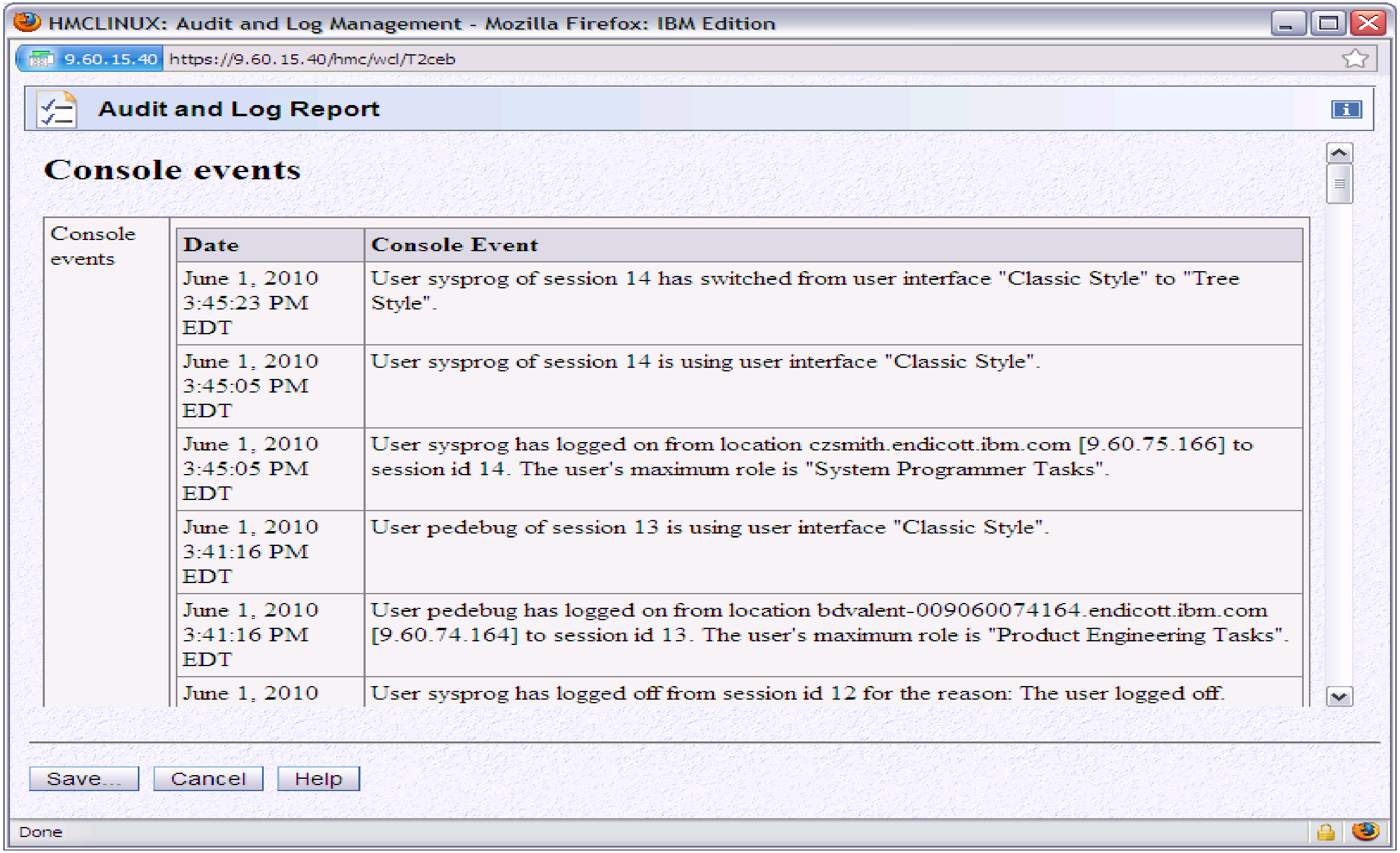
Audit data types

Select	Audit data types
□	⊟ Logs
□	Audit log
☑	Console events
☑	Security Log
□	Service History
□	Tasks performed log

Total: 17 Selected: 2

Event based data can be limited to a specific time period

Log Data Display/Save



HMCLINUX: Audit and Log Management - Mozilla Firefox: IBM Edition
9.60.15.40 https://9.60.15.40/hmc/wcl/T2ceb

Audit and Log Report

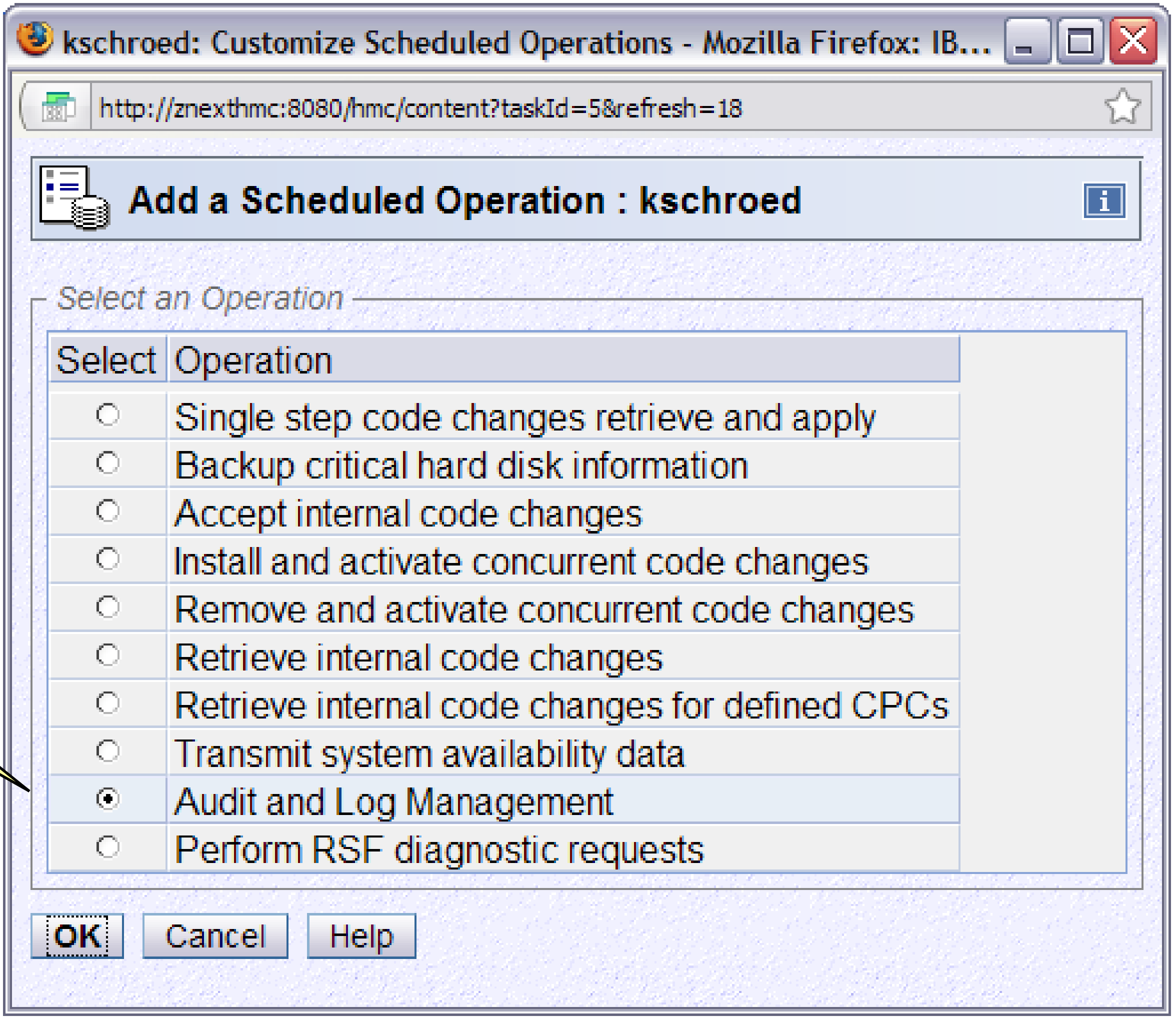
Console events

Console events

Date	Console Event
June 1, 2010 3:45:23 PM EDT	User sysprog of session 14 has switched from user interface "Classic Style" to "Tree Style".
June 1, 2010 3:45:05 PM EDT	User sysprog of session 14 is using user interface "Classic Style".
June 1, 2010 3:45:05 PM EDT	User sysprog has logged on from location czsmith.endicott.ibm.com [9.60.75.166] to session id 14. The user's maximum role is "System Programmer Tasks".
June 1, 2010 3:41:16 PM EDT	User pedebug of session 13 is using user interface "Classic Style".
June 1, 2010 3:41:16 PM EDT	User pedebug has logged on from location bdvalent-009060074164.endicott.ibm.com [9.60.74.164] to session id 13. The user's maximum role is "Product Engineering Tasks".
June 1, 2010	User sysprog has logged off from session id 12 for the reason: The user logged off.

Scheduled generation of reports

Scheduled operation for generating audit reports



kschroed: Customize Scheduled Operations - Mozilla Firefox: IB...

http://znexthmc:8080/hmc/content?taskId=5&refresh=18

Add a Scheduled Operation : kschroed

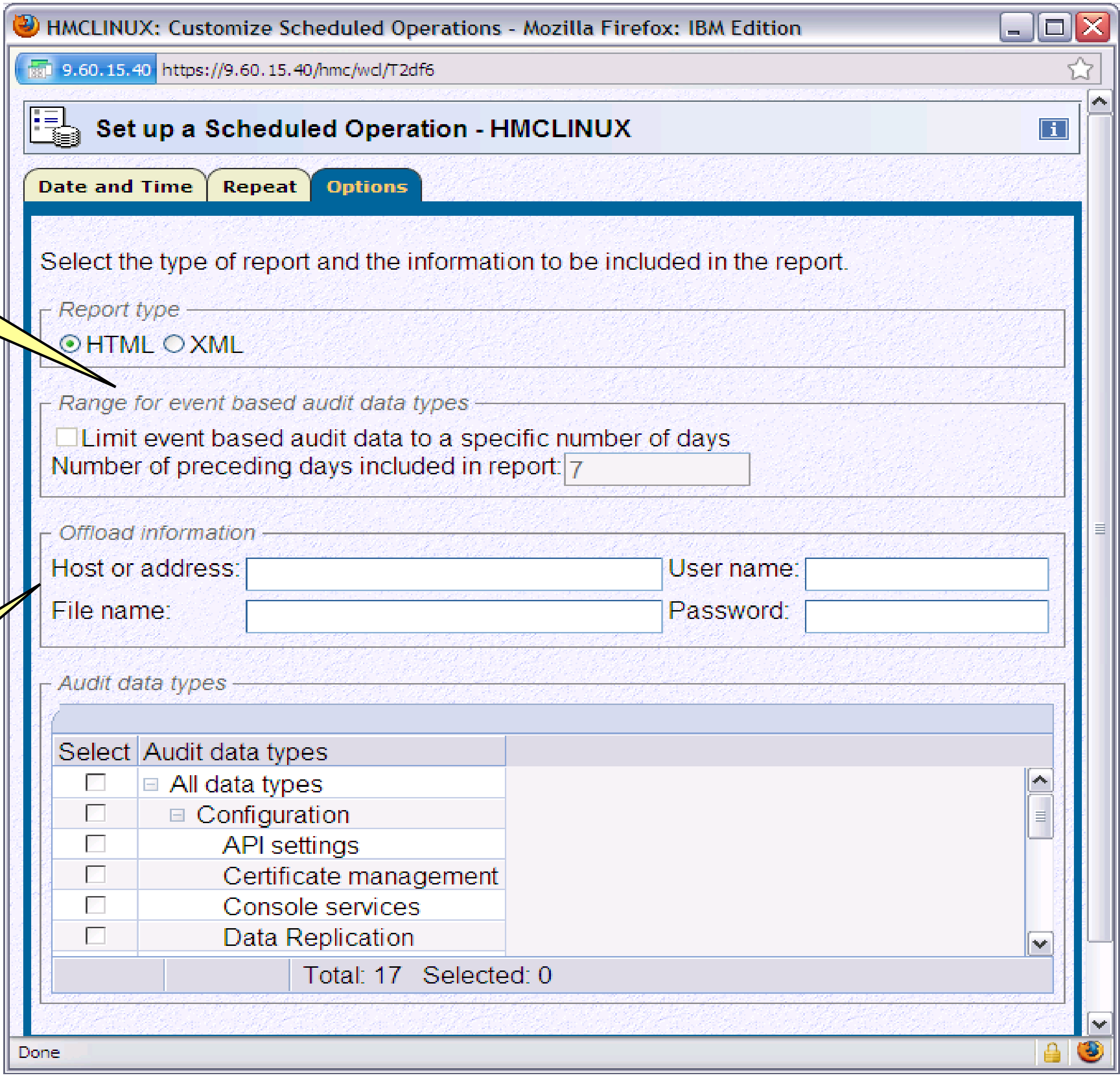
Select an Operation

Select	Operation
○	Single step code changes retrieve and apply
○	Backup critical hard disk information
○	Accept internal code changes
○	Install and activate concurrent code changes
○	Remove and activate concurrent code changes
○	Retrieve internal code changes
○	Retrieve internal code changes for defined CPCs
○	Transmit system availability data
●	Audit and Log Management
○	Perform RSF diagnostic requests

Scheduled Audit Report Generation

Scheduled Event based data limiting uses days rather than a time period

Generated report is offloaded via FTP


HMCLINUX: Customize Scheduled Operations - Mozilla Firefox: IBM Edition
9.60.15.40 https://9.60.15.40/hmc/wcl/T2df6
Set up a Scheduled Operation - HMCLINUX
Date and Time
Repeat
Options
Done

Select the type of report and the information to be included in the report.

Report type

● HTML ○ XML

Range for event based audit data types

□ Limit event based audit data to a specific number of days

Number of preceding days included in report: 7

Offload information

Host or address: ______ User name: ______

File name: ______ Password: ______

Audit data types

Select	Audit data types
□	⊟ All data types
□	⊟ Configuration
□	API settings
□	Certificate management
□	Console services
□	Data Replication

Total: 17 Selected: 0

Summary - Best Practices

- Install your physical HMC hardware in same type of physically secure environment as your System z servers
  - Located in a secure location
  - Preferably an area that has physical access control and monitoring
    - ie., Raised Floor

- Connect HMC to your System z servers resources using a dedicated or trusted separate network
  - If using Browser Remote communications or RSF Broadband,
    - use second HMC network adapter to the appropriate customer network

- Connect to RSF Broadband through customer firewall
  - Optionally, utilize Proxy Box (auditing/additional security)
  - RSF Benefits
    - Efficient Problem Reporting, Firmware Update, & Customer Initiated Upgrade

Summary - Best Practices (cont.)

- If remote access browser is required,
  - Enable remote access only for the specific userids that require it
  - Use CA Signed Certificates
  - Use SSL Cipher Suites of High strength
  - Ensure browser levels are kept up to date and security fixes applied
- Minimally, change the passwords for all the default HMC userids
  - Recommend removing all of the default userids
  - Define a userid for each individual user of the HMC using task and resource roles
  - Do not share HMC userids among multiple people!
- Ensure each userid is only permitted access to the tasks and managed resources needed to perform their job responsibilities.
  - For Operating System Messages,
    - Limit access, Read Only for most access, Write Access very limited

Summary - Best Practices (cont.)

- Use HMC data replication to ensure that User Profile information (userids, roles, password rules, etc.) are automatically kept in sync among all HMC installed in the enterprise.

- If automation is required,
  - If using SNMP, utilize SNMP V3
  - Consider WebServices APIs for more granular access controls

- Utilize Secure FTP for HMC offload/import options

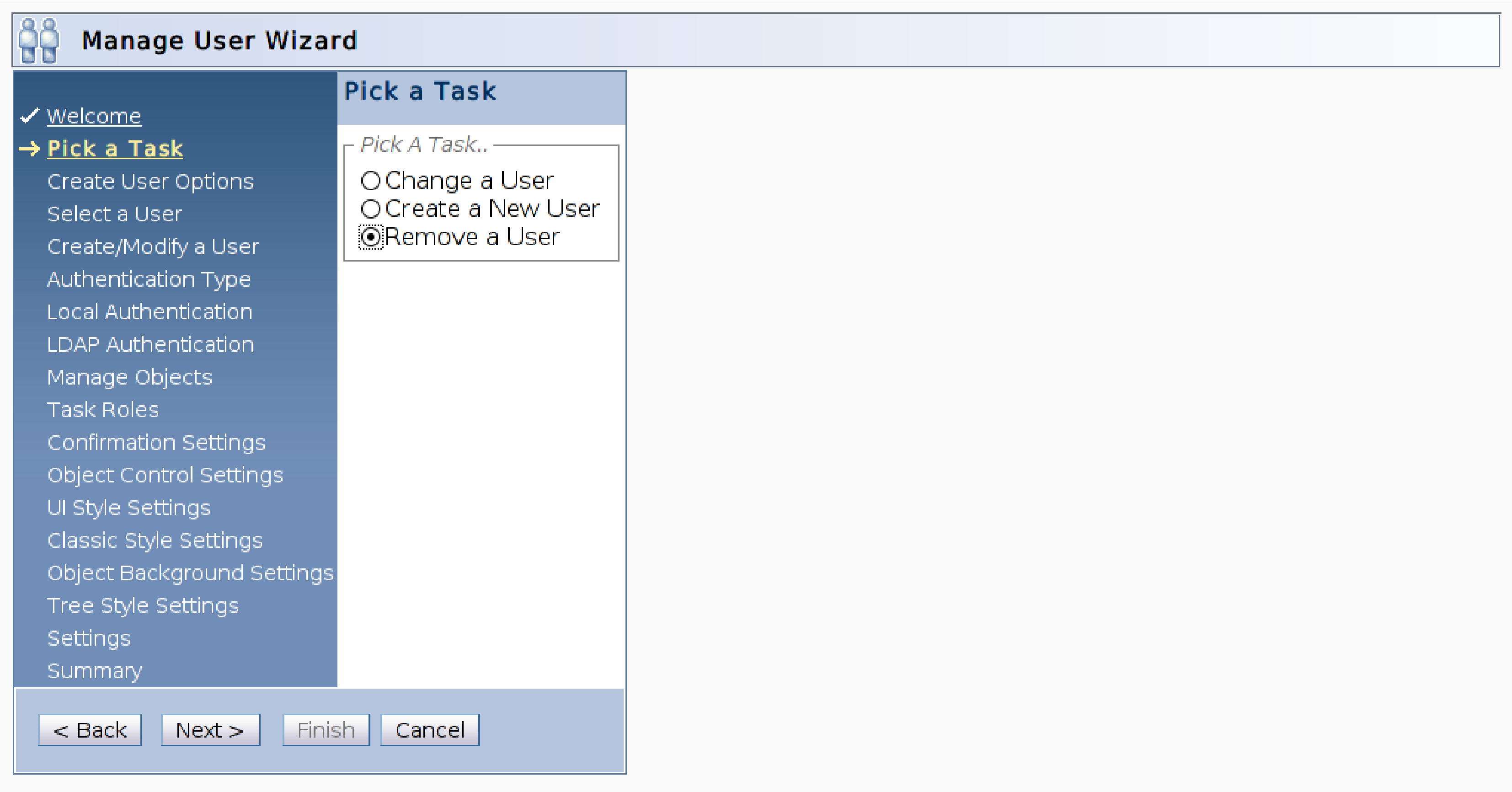
- Implement procedures that offload and analyze the HMC security logs for any suspicious activity.
  - When feasible, automate notification of security log events for the HMC.

Appendix

- Removing Default User Ids
- External Firewall Ports
- RSF Connectivity Attributes
- Cipher Suites
- HMC Data Replication
- Default User Password Rules
- View Only User IDs
- BCPii Networking
- IBM Common Criteria Evaluation Assurance Level (EAL) 5+

Removing Default User IDs

- **Consider using the Manage User Wizard task from ACSADMIN to remove the shipped default user Ids other than ACSADMIN.**



Manage User Wizard

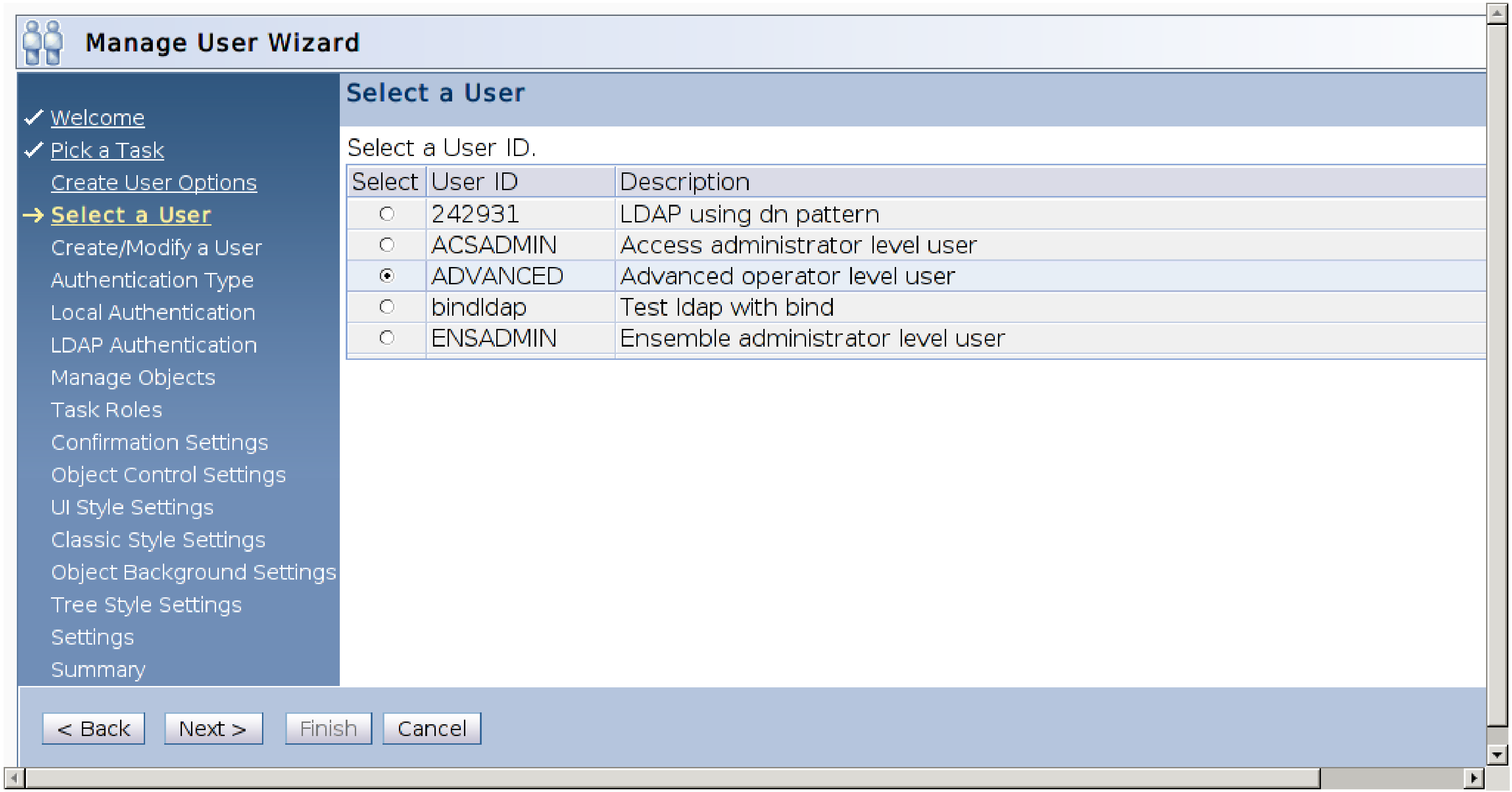
Pick a Task

Pick A Task..

○ Change a User
○ Create a New User
● Remove a User

Removing Default User IDs (cont.)

- **Select a shipped/default user ID**



Select a User

Select a User ID.

Select	User ID	Description
○	242931	LDAP using dn pattern
○	ACSADMIN	Access administrator level user
●	ADVANCED	Advanced operator level user
○	bindldap	Test ldap with bind
○	ENSADMIN	Ensemble administrator level user

HMC "Inbound" Network Traffic

TCP/IP Source Port	Usage
ICMP Type 8	Used to "ping" to and from the HMC and the System z® resources being managed by the HMC.
tcp 58787	Used for automatic discovery of System z® servers.
tcp 4455	Used for automatic discovery of Director/Timer console.
udp 9900	Used for HMC to HMC automatic discovery.
tcp 55555	Used for SSL encrypted communications to and from System z® servers. The internal firewall only allows inbound traffic from the System z® servers that are defined to the HMC.
tcp 9920	Used for HMC to HMC communications.
tcp 443	Used for remote user access to the HMC. Inbound traffic for this port is only allowed if remote access has been enabled for the HMC.
tcp 9950-9954	Used to proxy ***Single Object Operations*** sessions for a System z® server.
tcp 9960	Used for remote user applet based tasks. Inbound traffic for this port is only allowed if remote access has been enabled for the HMC.
tcp 21	Used for inbound FTP requests. This is **ONLY** enabled when Electronic Service Agent or the ***Enable FTP Access to Hardware Management Console Mass Storage Media*** task is being used. FTP is an unencrypted protocol, so for maximum security these tasks should not be used on the HMC.
udp/tcp 161	Used for SNMP automation. Inbound traffic for these ports is only allowed when SNMP automation is enabled.

HMC “Inbound” Network Traffic (cont.)

TCP/IP Source Port	Usage
tcp 5988 tcp 5989	Used for CIM automation. Inbound traffic for these ports is only allowed when CIM automation is enabled.
tcp 6794	Web services SSL encrypted automation traffic. Inbound traffic for this port is allowed only when Web Services automation is enabled.

HMC “Outbound” Network Traffic

TCP/IP Destination Port	Usage
ICMP Type 8	Used to “ping” to and from the HMC and the System z® resources being managed by the HMC.
udp 9900	Used for HMC to HMC automatic discovery.
tcp/udp 58787	Used for automatic discovery and establishing communications with System z® servers.
tcp 55555	Used for SSL encrypted communications to and from System z® servers. The internal firewall only allows inbound traffic from the System z® servers that are defined to the HMC.
tcp 9920	Used for HMC to HMC communications.
tcp 443	Used for Single Object Operations to a System z® server console.
tcp 9960	Used when proxying remote user applet based tasks during a ***Single Object Operations*** session for a System z® server console.
tcp 25345	Used for ***Single Object Operations*** session to legacy System z® server console.
tcp 4455	Used for communications with Director/Timer consoles being managed by the HMC.
udp 161	Used for communications with IBM Fiber Saver managed by the HMC.
tcp 25	Used when the HMC is configured, using the ***Monitor System Events*** task, to send email events to an SMTP server for delivery. (This may be a port other than 25, but this is the default SMTP port used by most SMTP servers.)

RSF Connectivity Attributes

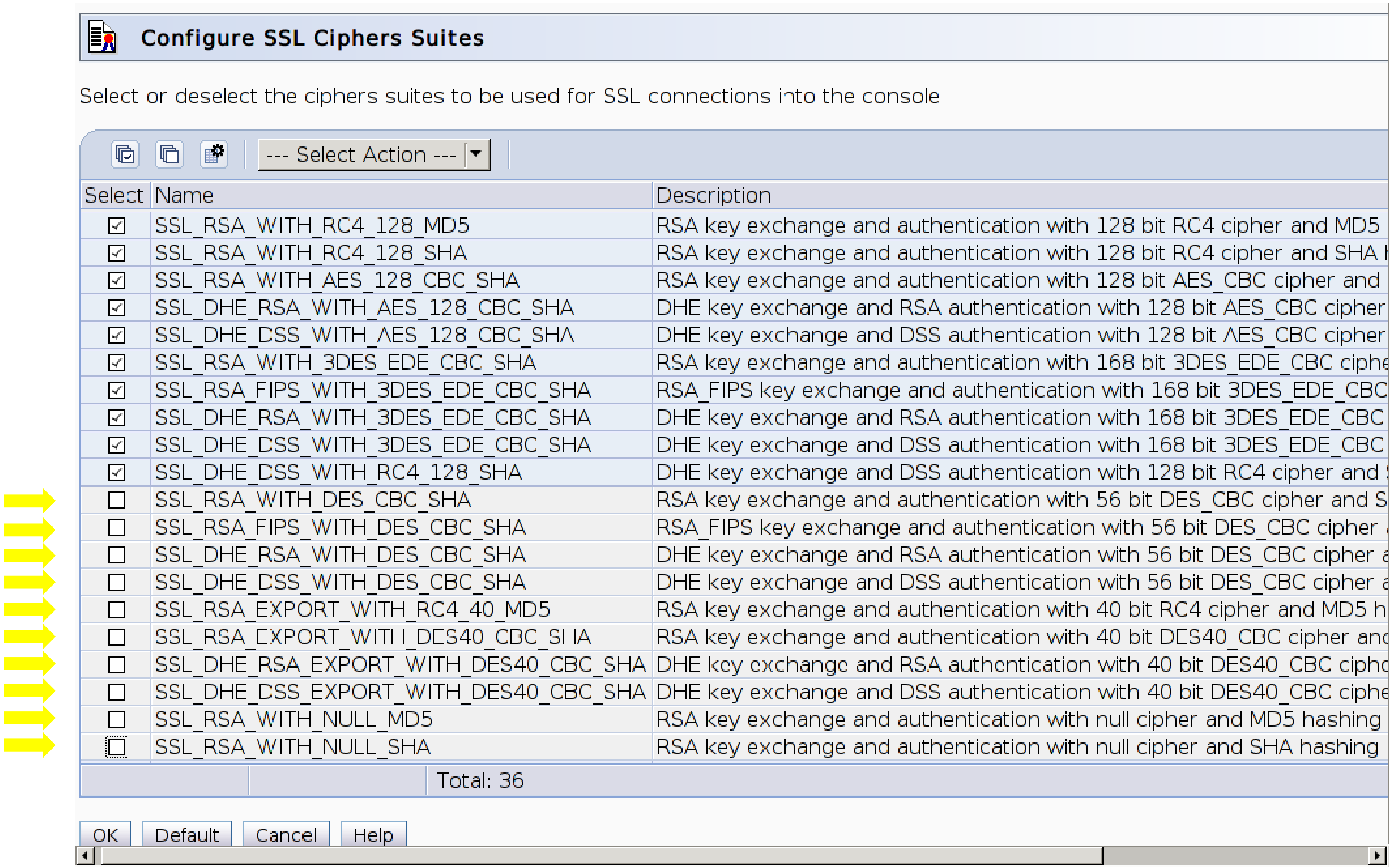
- An internet connection is **TCP/IP socket** that flows over the Hardware Management Console's default gateway to the internet
- The destination port is always 443, and ip addresses are following:
  - **ipv4 internet**
    - **129.42.26.224**
    - **129.42.34.224**
    - **129.42.42.224**
  - **Ipv6 internet**
    - **2620:0:6C0:1::1000**
    - **2620:0:6C1:1::1000**
    - **2620:0:6C2:1::1000**

Cipher Suites

- If the browsers used by your users can tolerate it (for example, are up to date versions of the supported browsers), use the Advanced action of “Configure SSL Cipher Suites” within the Certificate Management task to remove cipher suites that do not use authentication or are of medium strength (currently defined as at least 56 bits but less than 112 bits)
  - Cipher Suites stronger than medium strength are, given current technology, extremely difficult to break

Cipher Suites (cont.)

De-selected below are the current cipher suites that do not support Authentication (red arrow) or are of medium strength (yellow arrow)



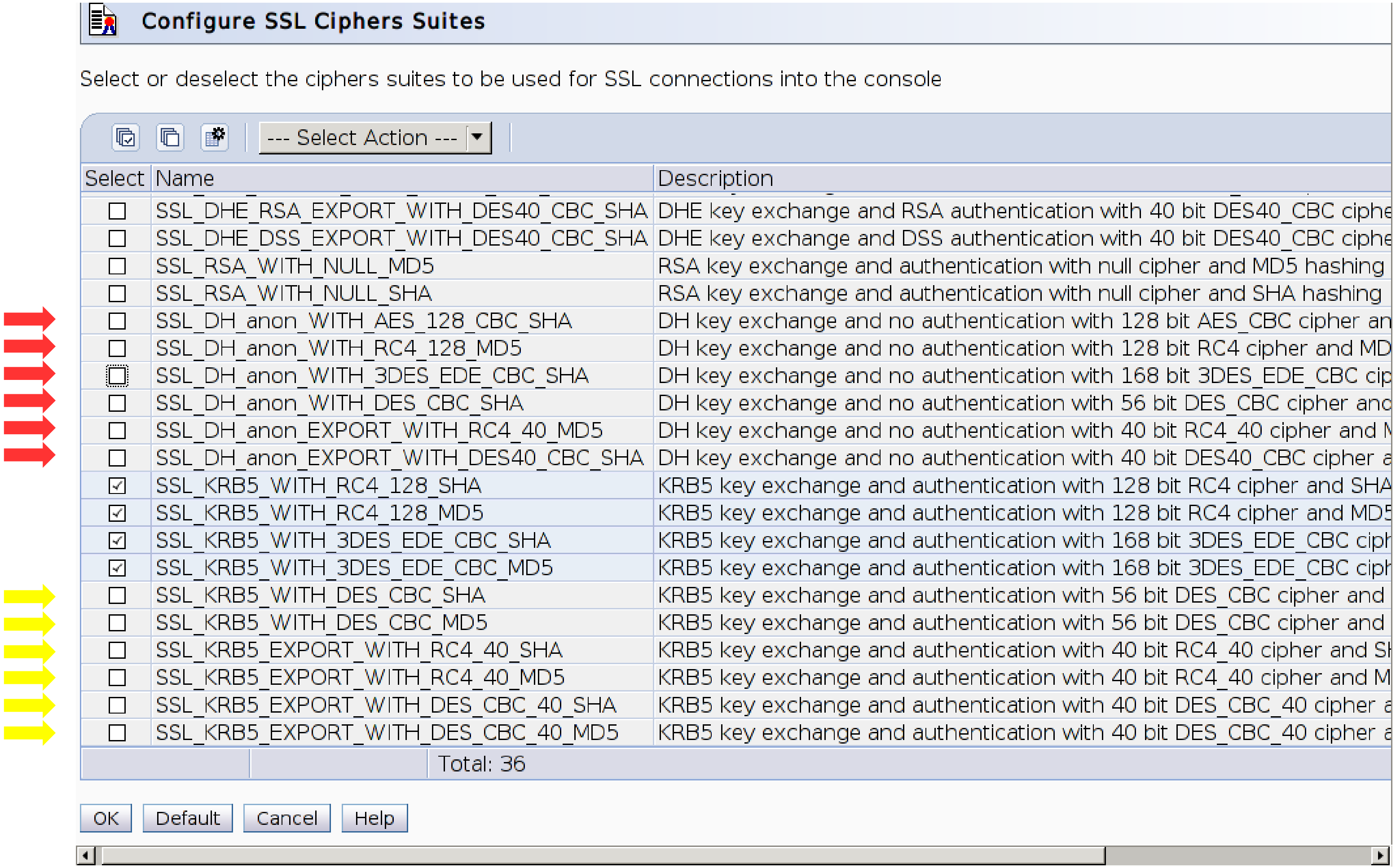
Select or deselect the ciphers suites to be used for SSL connections into the console

Select	Name	Description
☑	SSL_RSA_WITH_RC4_128_MD5	RSA key exchange and authentication with 128 bit RC4 cipher and MD5
☑	SSL_RSA_WITH_RC4_128_SHA	RSA key exchange and authentication with 128 bit RC4 cipher and SHA h
☑	SSL_RSA_WITH_AES_128_CBC_SHA	RSA key exchange and authentication with 128 bit AES_CBC cipher and
☑	SSL_DHE_RSA_WITH_AES_128_CBC_SHA	DHE key exchange and RSA authentication with 128 bit AES_CBC cipher
☑	SSL_DHE_DSS_WITH_AES_128_CBC_SHA	DHE key exchange and DSS authentication with 128 bit AES_CBC cipher
☑	SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA key exchange and authentication with 168 bit 3DES_EDE_CBC ciphe
☑	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	RSA_FIPS key exchange and authentication with 168 bit 3DES_EDE_CBC
☑	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	DHE key exchange and RSA authentication with 168 bit 3DES_EDE_CBC
☑	SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DHE key exchange and DSS authentication with 168 bit 3DES_EDE_CBC
☑	SSL_DHE_DSS_WITH_RC4_128_SHA	DHE key exchange and DSS authentication with 128 bit RC4 cipher and S
□	SSL_RSA_WITH_DES_CBC_SHA	RSA key exchange and authentication with 56 bit DES_CBC cipher and S
□	SSL_RSA_FIPS_WITH_DES_CBC_SHA	RSA_FIPS key exchange and authentication with 56 bit DES_CBC cipher a
□	SSL_DHE_RSA_WITH_DES_CBC_SHA	DHE key exchange and RSA authentication with 56 bit DES_CBC cipher a
□	SSL_DHE_DSS_WITH_DES_CBC_SHA	DHE key exchange and DSS authentication with 56 bit DES_CBC cipher a
□	SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA key exchange and authentication with 40 bit RC4 cipher and MD5 h
□	SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA key exchange and authentication with 40 bit DES40_CBC cipher and
□	SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	DHE key exchange and RSA authentication with 40 bit DES40_CBC ciphe
□	SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	DHE key exchange and DSS authentication with 40 bit DES40_CBC ciphe
□	SSL_RSA_WITH_NULL_MD5	RSA key exchange and authentication with null cipher and MD5 hashing
□	SSL_RSA_WITH_NULL_SHA	RSA key exchange and authentication with null cipher and SHA hashing

Total: 36

Cipher Suites (cont.)

De-selected below are the current cipher suites that do not support Authentication (red arrow) or are of medium strength (yellow arrow)



Configure SSL Ciphers Suites

Select or deselect the ciphers suites to be used for SSL connections into the console

Select	Name	Description
□	SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	DHE key exchange and RSA authentication with 40 bit DES40_CBC ciphe
□	SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	DHE key exchange and DSS authentication with 40 bit DES40_CBC ciphe
□	SSL_RSA_WITH_NULL_MD5	RSA key exchange and authentication with null cipher and MD5 hashing
□	SSL_RSA_WITH_NULL_SHA	RSA key exchange and authentication with null cipher and SHA hashing
□	SSL_DH_anon_WITH_AES_128_CBC_SHA	DH key exchange and no authentication with 128 bit AES_CBC cipher an
□	SSL_DH_anon_WITH_RC4_128_MD5	DH key exchange and no authentication with 128 bit RC4 cipher and MD
□	SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	DH key exchange and no authentication with 168 bit 3DES_EDE_CBC cip
□	SSL_DH_anon_WITH_DES_CBC_SHA	DH key exchange and no authentication with 56 bit DES_CBC cipher and
□	SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	DH key exchange and no authentication with 40 bit RC4_40 cipher and M
□	SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	DH key exchange and no authentication with 40 bit DES40_CBC cipher a
☑	SSL_KRB5_WITH_RC4_128_SHA	KRB5 key exchange and authentication with 128 bit RC4 cipher and SHA
☑	SSL_KRB5_WITH_RC4_128_MD5	KRB5 key exchange and authentication with 128 bit RC4 cipher and MD5
☑	SSL_KRB5_WITH_3DES_EDE_CBC_SHA	KRB5 key exchange and authentication with 168 bit 3DES_EDE_CBC ciph
☑	SSL_KRB5_WITH_3DES_EDE_CBC_MD5	KRB5 key exchange and authentication with 168 bit 3DES_EDE_CBC ciph
□	SSL_KRB5_WITH_DES_CBC_SHA	KRB5 key exchange and authentication with 56 bit DES_CBC cipher and
□	SSL_KRB5_WITH_DES_CBC_MD5	KRB5 key exchange and authentication with 56 bit DES_CBC cipher and
□	SSL_KRB5_EXPORT_WITH_RC4_40_SHA	KRB5 key exchange and authentication with 40 bit RC4_40 cipher and SH
□	SSL_KRB5_EXPORT_WITH_RC4_40_MD5	KRB5 key exchange and authentication with 40 bit RC4_40 cipher and M
□	SSL_KRB5_EXPORT_WITH_DES_CBC_40_SHA	KRB5 key exchange and authentication with 40 bit DES_CBC_40 cipher a
□	SSL_KRB5_EXPORT_WITH_DES_CBC_40_MD5	KRB5 key exchange and authentication with 40 bit DES_CBC_40 cipher a

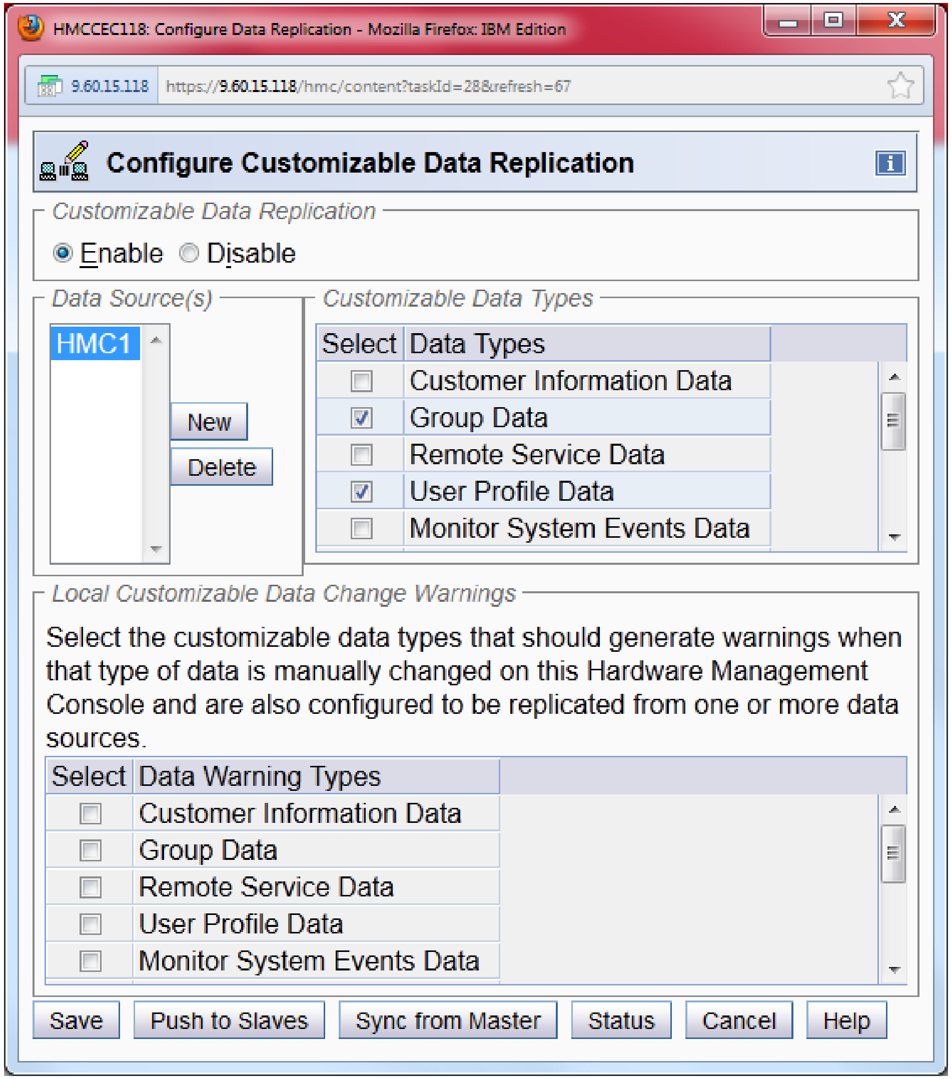
Total: 36

HMC Data Replication

- Allows for multiple HMCs to keep certain types of data synchronized
- Type of data include user profiles and roles, grouping, remote service, call home, acceptable status, monitor system events, etc.
- Support multiple different topologies
  - Peer to peer
  - Master – slave
  - Any combination of peer to peer and master – slave
- When selected data is changed on a peer/master HMC it is automatically sent to any interested peer/slave HMC
  - Peer/slave HMCs also resync themselves when restarted
  - A resync can also be manually forced via the GUI
- Users can be warned when changes made to data configured to be replicated from another HMC

HMC Data Replication (cont.)

- Multiple sources can be defined for redundancy
- Can select the type of data to be received from each source
- Can choose to warn users when locally changing data configured to be obtained from a different source
- Resync can be forced from either the master or the slave



HMCCEC118: Configure Data Replication - Mozilla Firefox: IBM Edition
9.60.15.118
https://9.60.15.118/hmc/content?taskId=28&refresh=67

Configure Customizable Data Replication

Customizable Data Replication

● Enable ○ Disable

Data Source(s)

HMC1

Customizable Data Types

Select	Data Types
☐	Customer Information Data
☑	Group Data
☐	Remote Service Data
☑	User Profile Data
☐	Monitor System Events Data

Local Customizable Data Change Warnings

Select the customizable data types that should generate warnings when that type of data is manually changed on this Hardware Management Console and are also configured to be replicated from one or more data sources.

Select	Data Warning Types
☐	Customer Information Data
☐	Group Data
☐	Remote Service Data
☐	User Profile Data
☐	Monitor System Events Data

Default User Password Rules

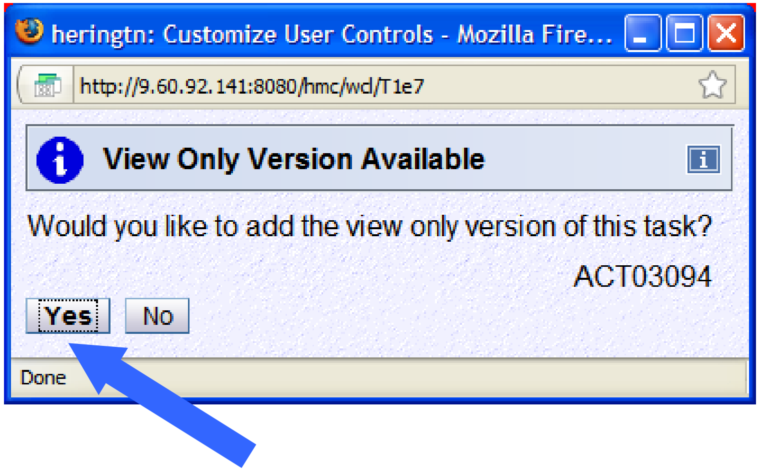
- Basic
  - A password must be a minimum of four characters and a maximum of eight characters long.
  - These characters include A-Z, a-z, 0-9.
- Strict
  - Password expires in 180 days.
  - A password must be a minimum of six characters and a maximum of eight characters long.
  - A password must contain both letters and numbers.
  - The first and last character in a password must be alphabetic.
  - No character can repeat more than twice.
- Standard
  - Password expires in 186 days.
  - A password must be a minimum of six characters and a maximum of 30 characters long.
  - The first and last character in a password can be alphabetic or special.
  - A password can contain letters, numbers, and special characters.
  - No character can repeat more than twice.
  - A password can only match three characters from the previous password.
  - You can repeat a password after using four unique passwords.

View Only User IDs

- **View Only User IDs/Access for HMC/SE**
  - The HMC and SE User ID support added the ability to create users who have View Only access to select tasks.
  - The View Only tasks are simply the full function tasks with minor modifications to their GUI controls which prevent any actions from being taken. The following subset support a View Only user ID.
    - Hardware Messages
    - Operating System Messages
    - Customize/Delete Activation Profiles
    - Advanced Facilities
    - Configure On/Off
  - To support View Only user IDs:
    - When adding tasks into a new Task Role the option of adding the View Only version of that task is provided.
    - The Access Administrator can then specify these Task Roles to create View Only user IDs if desired.

View Only User Ids (cont.)

- **View Only User IDs/Access for HMC/SE**



heringtn: Customize User Controls - Mozilla Fire...

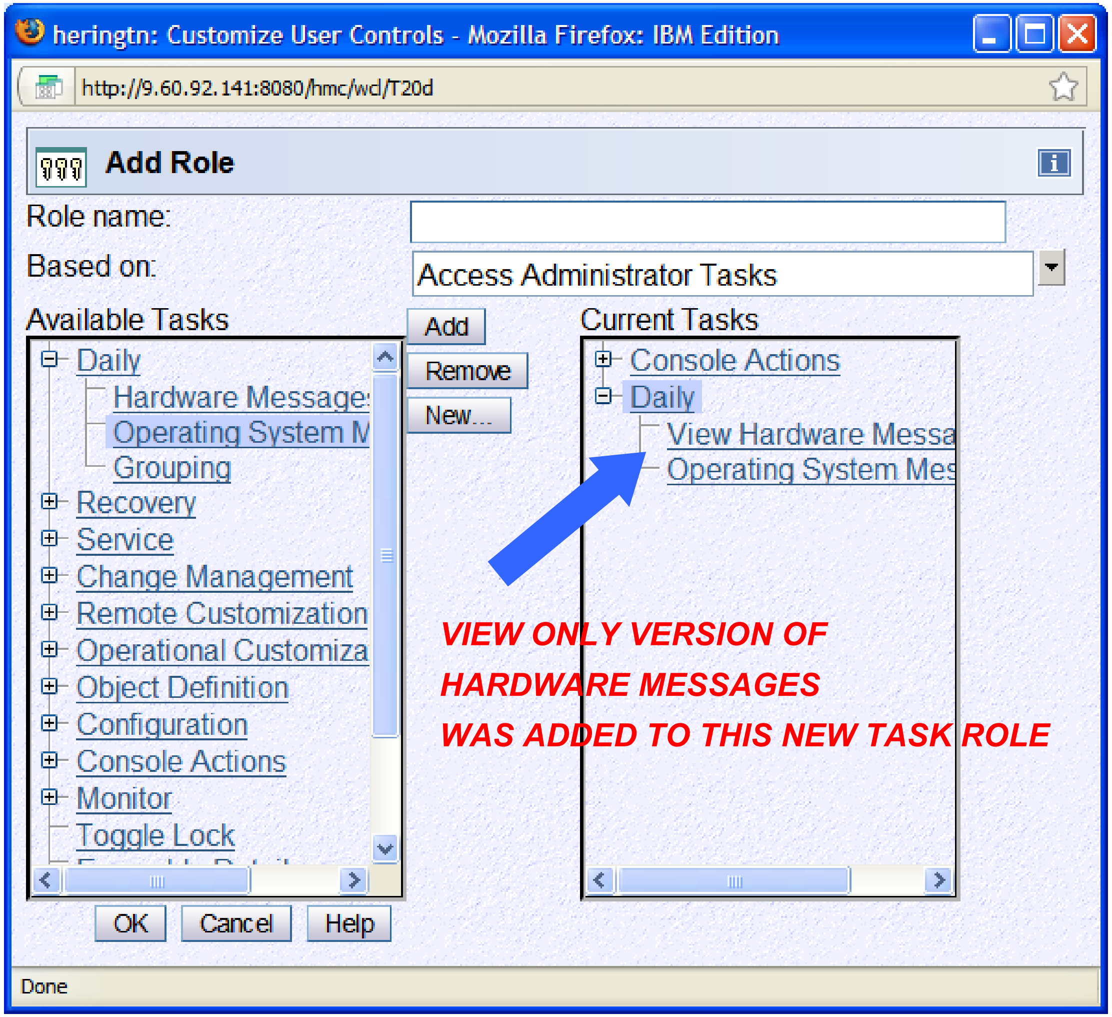
http://9.60.92.141:8080/hmc/wcl/T1e7

View Only Version Available

Would you like to add the view only version of this task?

ACT03094

CLICK-YES



heringtn: Customize User Controls - Mozilla Firefox: IBM Edition

http://9.60.92.141:8080/hmc/wcl/T20d

Add Role

Role name:

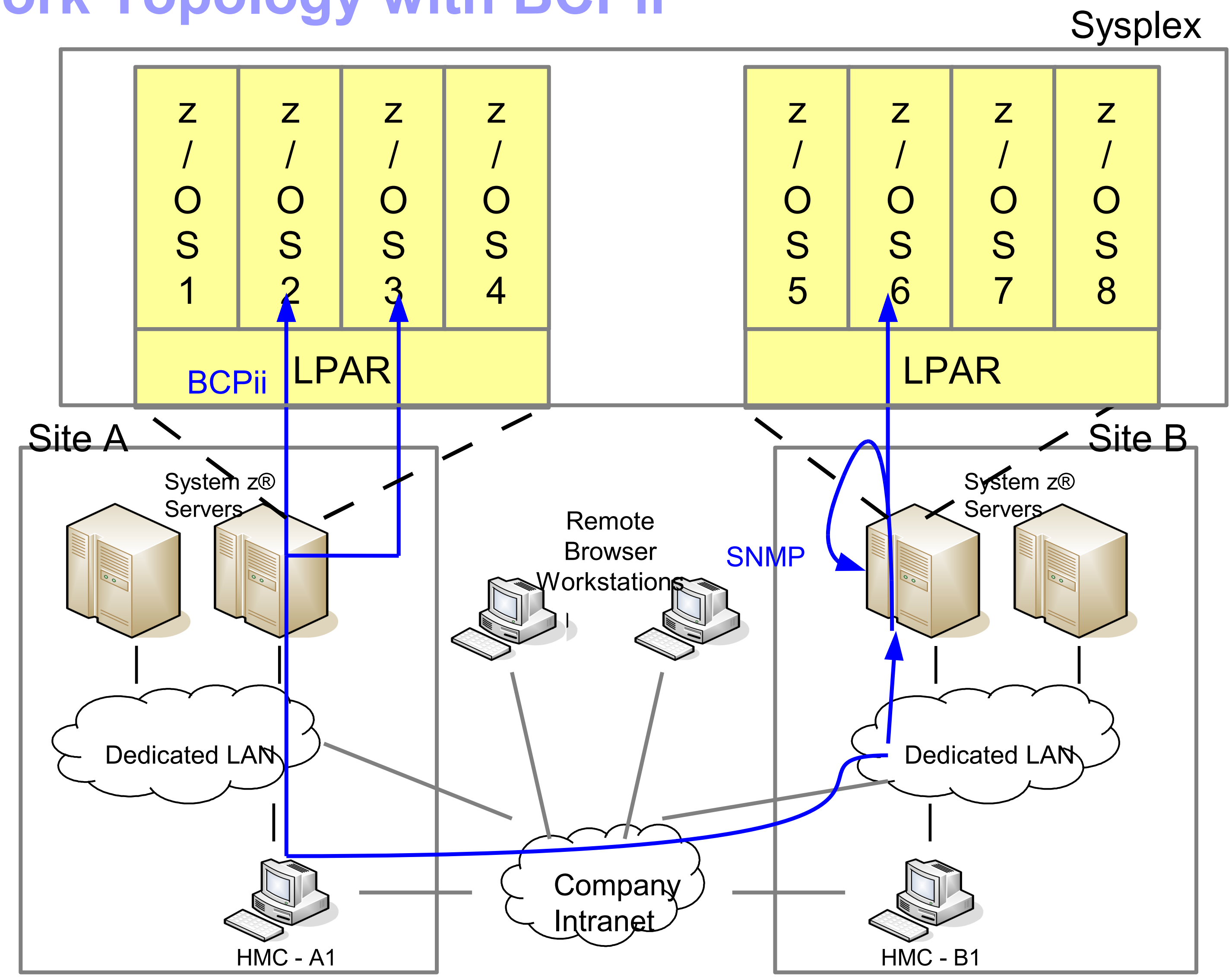
Based on: Access Administrator Tasks

Available Tasks
- Daily
  - Hardware Message:
  - Operating System M
  - Grouping
- Recovery
- Service
- Change Management
- Remote Customization
- Operational Customiza
- Object Definition
- Configuration
- Console Actions
- Monitor
- Toggle Lock

Current Tasks
- Console Actions
- Daily
  - View Hardware Messa
  - Operating System Mes

VIEW ONLY VERSION OF HARDWARE MESSAGES WAS ADDED TO THIS NEW TASK ROLE

Network Topology with BCPii



Network Topology with BCPii (continued)

- BCPii (Base control Program Internal Interface) communications within a CPC
  - Request sent from z/OS2 to z/OS3
  - Both must have cross partition authority enabled or request rejected
  - Request/response flows from the OS to the SE to the target OS and back again
  - Nothing ever flows on any networks
- BCPii communications between CPCs
  - Request sent from z/OS2 to z/OS6
  - Both must have cross partition authority enabled or request rejected
  - Request flows from z/OS2 to the SE, then to one of the Change Management HMCs.
    - The HMC to SE flow is proprietary and encrypted and flows over the customer network
  - HMC forwards request onto target CPC
  - Target CPC sends wrapped SNMP request to itself over loopback.
    - SNMP request never leaves the SE
    - Community names used to authenticate SNMP request over loopback
  - Response flows back in basically the reverse with the exception of SNMP

Evaluated Secure Configuration

- To help secure sensitive data and business transactions, the zSeries is designed for Common Criteria Evaluation Assurance Level 5+ (EAL5+) certification for security of logical partitions. This means that the zSeries is designed to prevent an application running on one operating system on one LPAR from accessing application data running on a different operating system image on another LPAR on the server.
- Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. The evaluation is performed by an independent lab (evaluation facility).
- The evaluation facility is accredited with a certification body, typically a government institution. Assurance is gained through:
  - Analysis of development processes and procedures
  - Checking that processes and procedures are applied
  - Analysis of the correspondence between product design representations
  - Analysis of the product design representations against the requirements
  - Analysis of the source code
  - Analysis of guidance documents
  - Analysis of functional tests and results
  - Independent functional testing
  - Analysis for flaws
  - Penetration testing

Evaluated Secure Configuration (cont.)

- Although only portions of the HMC and SE support are included in the Common Criteria evaluation the development processes and procedures are used throughout the product and help to assure that all the security functions are effective. **Features excluded do not imply a security issue but instead were just excluded to limit the scope and cost of the evaluation**

- The configuration evaluated is as follows:

  Physical

  - Hardware and the networks used to connect the hardware must be physically secure
  - Access to I/O devices must be restricted to authorized personnel
  - The HMC must be physically protected from access other than by authorized system administrators

  IO

  - HMC/SE communications network should be physically separate from the logical partition data networks
  - Control Units and Devices should be allocated to only one Isolated logical partition

Evaluated Secure Configuration (cont.)

I/O (cont.)

- No channel paths may be shared between an Isolated partition and any other partition(s).
- An Isolated partition must not be configured to enable hipersockets (Internal Queued Direct I/O).
- No Isolated partition may have coupling facility channels
- Dynamic I/O Configuration changes must be disabled.
- Workload Manager must be disabled for Isolated partitions so that CPU and I/O resources are not managed across partitions.
- Global Performance Data Control Authority and Cross-partition Control Authority must be disabled
- The ’Use dynamically changed address’ and ’Use dynamically changed parameter’ checkboxes (Image/Load Profile) must be disabled.
- No Isolated partition should have the following Counter Facility Security Options enabled:
  - Crypto activity counter set authorization control
  - Coprocessor group counter sets authorization control
- Limited Restrictions
  - At most one partition can have I/O Configuration Control Authority
  - write access is disabled for each IOCDS

Evaluated Secure Configuration (cont.)

HMC

- No Enterprise Directory Server (LDAP) Definitions should be created on the Hardware Management Console or the Support Element.
- Disable the following:
  - HMC Customizable Data Replication service
  - Remote HMC access by IBM Product Engineering (PE)
  - Simple Network Management Protocol (SNMP) API
  - Common Information Model (CIM) Management Interface
  - Web Services API

Additional Materials

- Other SHARE Sessions of Related Interest
- Registering for IBM Resource Link Access
- Notable HMC/SE Publications
- Trademarks

Other SHARE Sessions of Related Interest

- August 6th, 2012, 1:30 – 2:30 PM
  - ***"The HMC Is a Fantastic Feature of the zEnterprise, but What Mistakes Are You Making Securing It? (Session Number 11198)"* – Barry Schrager and Paul Robichaux**
- August 7th, 2012, 9:30 – 10:30 AM
  - ***"zEverything You Always Needed to Know About zEnterprise Server Firmware Support and Maintenance (Session Number 11786)"* – Harv Emery**
- August 7th, 2012, 4:30 – 5:30 PM
  - ***"zEnterprise System – Secure Networking with zEnterprise Ensemble (Session Number 11901)"* – Gwen Dente**
- August 7th, 2012, 4:30 – 5:30 PM
  - ***"zBX x86 Blade Integration and Unified Resource Manager Virtualization (Session Number 11724)"* – Romney White**
- August 8th, 2012, 1:30 – 2:30 PM
  - ***"BUnified Resource Manager: HMC Ensemble navigation and Virtual Server Hands-on Lab (Session Number 11571)"* – Hiren Shah**
- August 9th, 2012, 8:00 – 9:00 AM
  - ***"zBCPii Programming Beyond the Basics for the z/OS System Programmer (Session Number 11713)"* – Steve Warren**

Previous SHARE Conference Sessions of Related Interest

- August 2011 SHARE Conference in Orlando
  - **"*IBM System z Hardware Management Console (HMC) 2.11.0 (including some 2.11 Updates)*" - Brian Valentine**
    - **http:/www.share.org/d/do/4297**
- August 2011 SHARE Conference in Orlando
  - **"*IBM zBX (System z BladeCenter Extension) HMC (Hardware Management Console) Hardware & Operational Management*" - Brian Valentine**
    - **http:/www.share.org/d/do/4218**
- March 2011 SHARE Conference in Anaheim
  - **"*BCPii for Dummies: Start to finish installation, setup and usage*" – Steve Warren**
    - **http:/www.share.org/d/do/1420**

Registering for IBM Resource Link Access

- **To view the documents on the Resource Link Web site. you need to register your IBM Registration ID (IBM ID) and password with Resource Link.**

- **To register:**
  - **Open the Resource Link sign-in page:** http://www.ibm.com/servers/resourcelink/
  - **You need an IBM ID to get access to Resource Link.**
    - **If you do not have an IBM ID and password, select the "Register for an IBM ID" link in the "Your IBM Registration" menu. Return to the Resource Link sign-in page after you get your IBM ID and password.**
    - Note: **If you're an IBM employee, your IBM intranet ID is not an IBM ID.**
  - **Sign in with your IBM ID and password.**
  - **Follow the instructions on the subsequent page.**

Reference Documentation

- Available from “Books” group of Classic Style UI and the Welcome page of the Tree Style UI (& IBM Resource Link: Library->z196->Publications)
  - **IBM SC28-6905: Hardware Management Console Operations Guide (**Version 2.11.1)
  - **IBM SC28-6906: Support Element Operations Guide** (Version 2.11.1)
  - **IBM SB10-7030: Application Programming Interfaces**

- Available from IBM Resource Link: Library->z196->Technical Notes
  - **System z Hardware Management Console Security**
  - **System z Hardware Management Console Broadband Remote Support Facility**

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

APPN*
CICS*
DB2*
DB2 Connect
e-business logo*
Enterprise Storage Server*
ESCON*
FICON
FICON Express
GDPS*
Geographically Dispersed Parallel Sysplex
HiperSockets
HyperSwap
IBM
IBM eServer
IBM ^*
IBM logo*
IMS
Infoprint*
Language Environment*
MQSeries*
Multiprise*
NetView*
On demand business logo
OS/2*
OS/390*
Parallel Sysplex*
POWER
PR/SM
Processor Resource/Systems Manager
pSeries*
RACF*
Resource Link
RMF
S/390*
S/390 Parallel Enterprise Server
Sysplex Timer*
TotalStorage*
VM/ESA*
VSE/ESA
VTAM*
WebSphere*
z/Architecture
z/OS*
z/VM*
zSeries*
zSeries Entry License Charge

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

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

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

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