

# IBM System z Hardware Management Console (HMC) Security

February 5, 2013

*SHARE in San Francisco*

**Brian Valentine**  
HMC Development  
[bdvalent@us.ibm.com](mailto:bdvalent@us.ibm.com)

**Kurt Schroeder**  
HMC Development  
[schroedk@us.ibm.com](mailto:schroedk@us.ibm.com)

**Patrick Callaghan**  
HMC Development  
[patrickc@us.ibm.com](mailto:patrickc@us.ibm.com)

*File Updated: 02-05-13*

# Topics

- ▶ **HMC System Support** Page: 5
  
- ▶ **Objectives** Page: 6
  
- ▶ **Initial State of the Console** Page: 7
  
- ▶ **Networking** Page: 8
  - Topology Page: 10
  - Firewall Page: 16
  - Domain Security Page: 17
  
- ▶ **Remote Support Facility** Page: 18
  
- ▶ **Enabling Remote Communications** Page: 27
  - HMC Certificate Management Page: 29
  - Customize Console Services Page: 36

## Topics (cont.)

- ▶ **Defining Users and Roles** Page: 38
  - Users, Roles, Resources, Passwords, User Properties Page: 39
  - LDAP Authentication Page: 48
  - User Templates and Patterns Page: 54
  
- ▶ **Enabling APIs** Page: 60
  - SNMP Page: 61
  - Web Services API Page: 63
  
- ▶ **Operating System HMC Considerations** Page: 64
  - Operating System Messages Page: 65
  - BCPii Page: 68
  
- ▶ **HMC Protection Against Malware** Page: 69
  - Digitally Signed Firmware Page: 70
  - Secure FTP Page: 71
  
- ▶ **Auditing** Page: 75
  - Security Event Notification Page: 76
  - Audit Reports Page: 78

## Topics (cont.)

- ▶ **Summary - Best Practices** Page: 87
  
- ▶ **Appendix** Page: 90
  - Removing Default User IDs Page: 91
  - External Firewall Ports Page: 93
  - RSF Connectivity Attributes Page: 96
  - Cipher Suites Page: 97
  - HMC Data Replication Page: 100
  - Default User Password Rules Page: 102
  - View Only User IDs Page: 103
  - BCPii Networking Page: 105
  - IBM Common Criteria EAL5 Configuration Page: 107
  - z/OS NIP Console Config for HMC on Startup Page: 111
  
- ▶ **Additional Materials** Page: 112
  - Other SHARE Sessions of Related Interest Page: 113
  - Registering for IBM Resource Link Access Page: 115
  - Notable HMC/SE Publications Page: 116

## HMC System support

- The HMC Version 2.12.0 supports the systems/SE (Support Element) versions shown in the table.
  - ▶ 9672 G5/G6 (Driver 26, SE version 1.6.2) systems are no longer supported.
- Both Classic and Tree UI Styles supported

Machine Family	Machine Type	Firmware Driver	SE Version
zEC12	zEC12	12	2.12.0
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

# 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?***

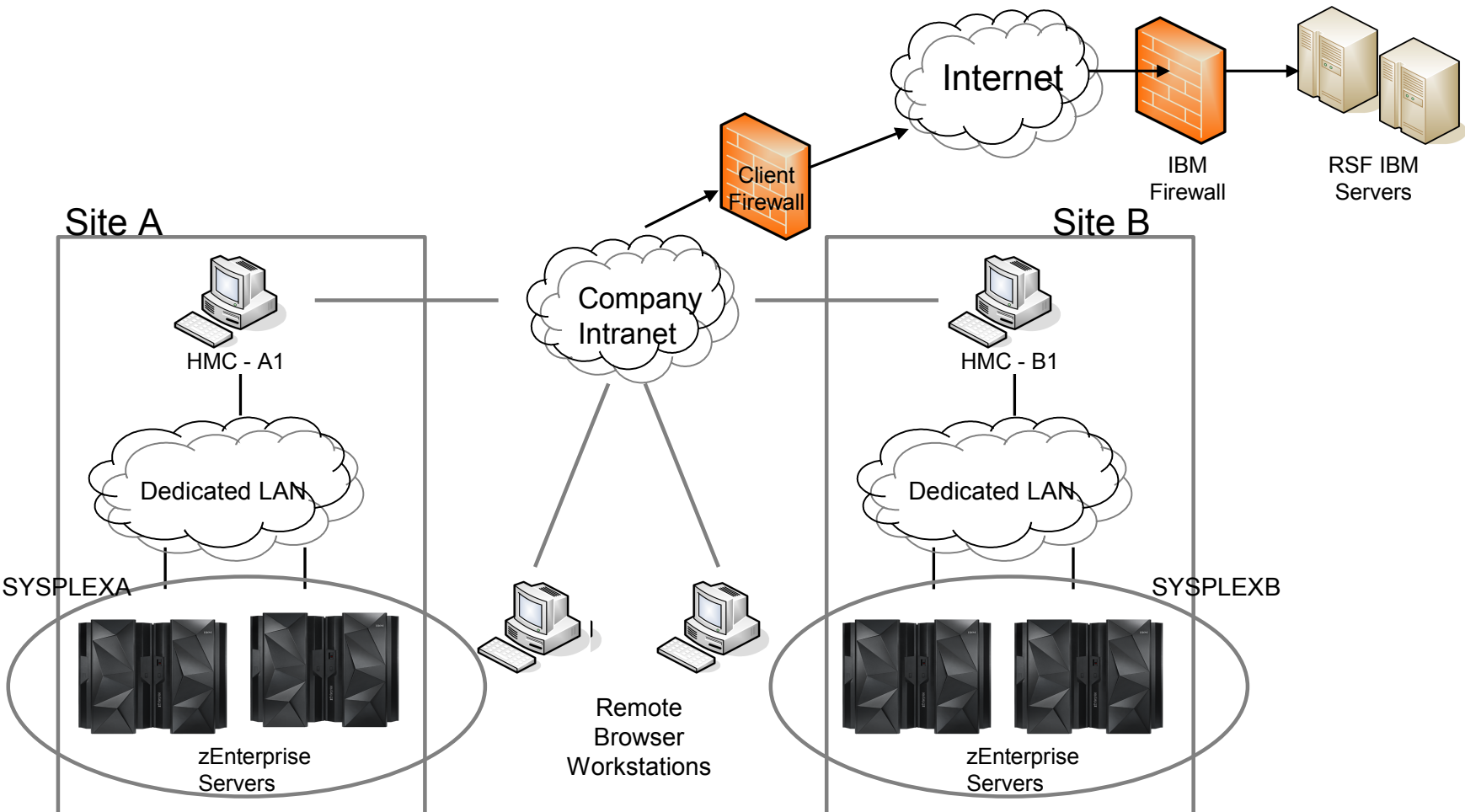
***New HMC 2.12.0 STP NTP External Time Source Authentication***



## 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

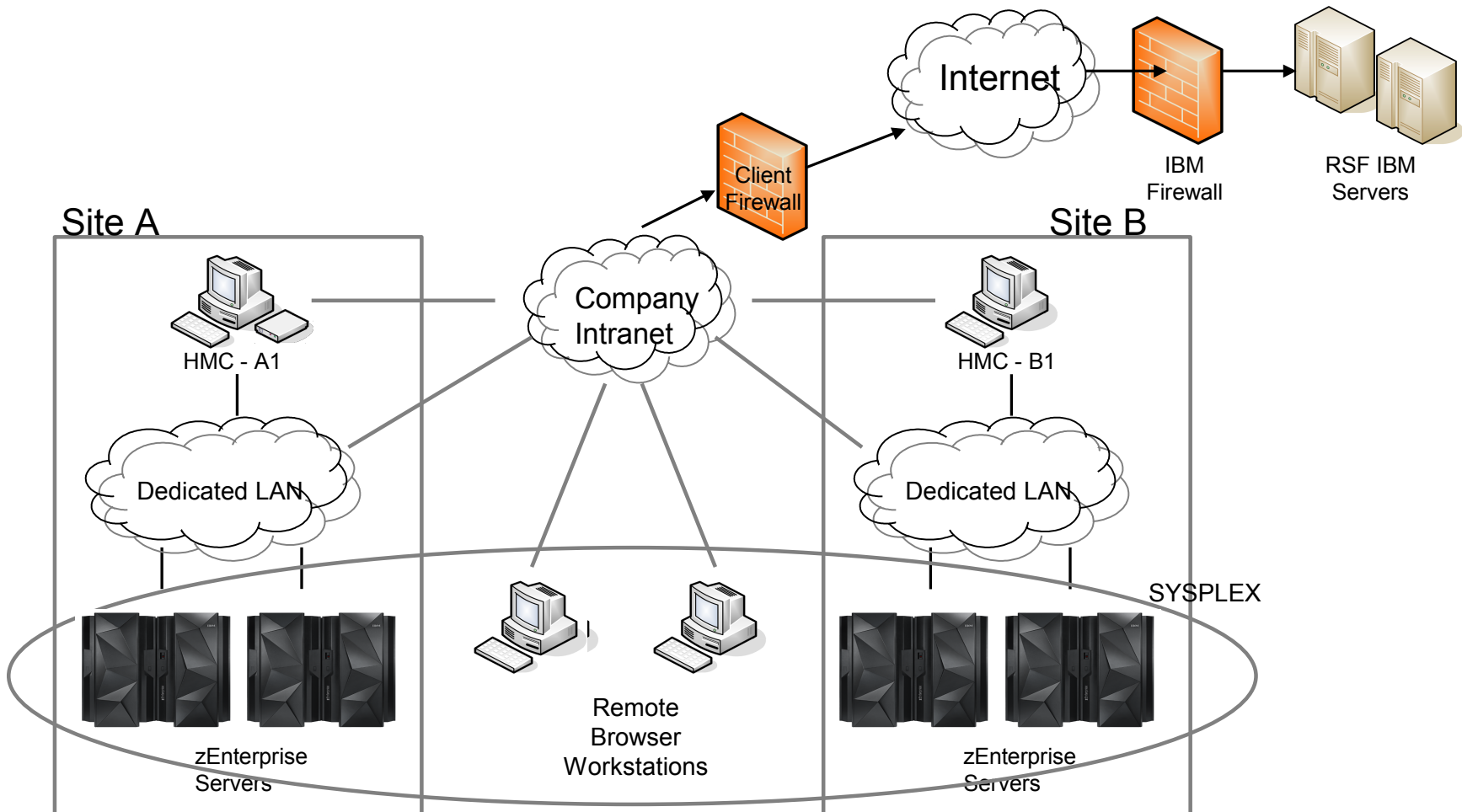
# Example Multiple Sysplex Network Topology



## Example Multiple Sysplex Topology (continued)

- zEnterprise 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 zEnterprise servers at their respective local site
  - ▶ Note: Both HMCs => call home servers using internet connectivity
    - Modem/Dial RSF no longer supported in 2.12.0

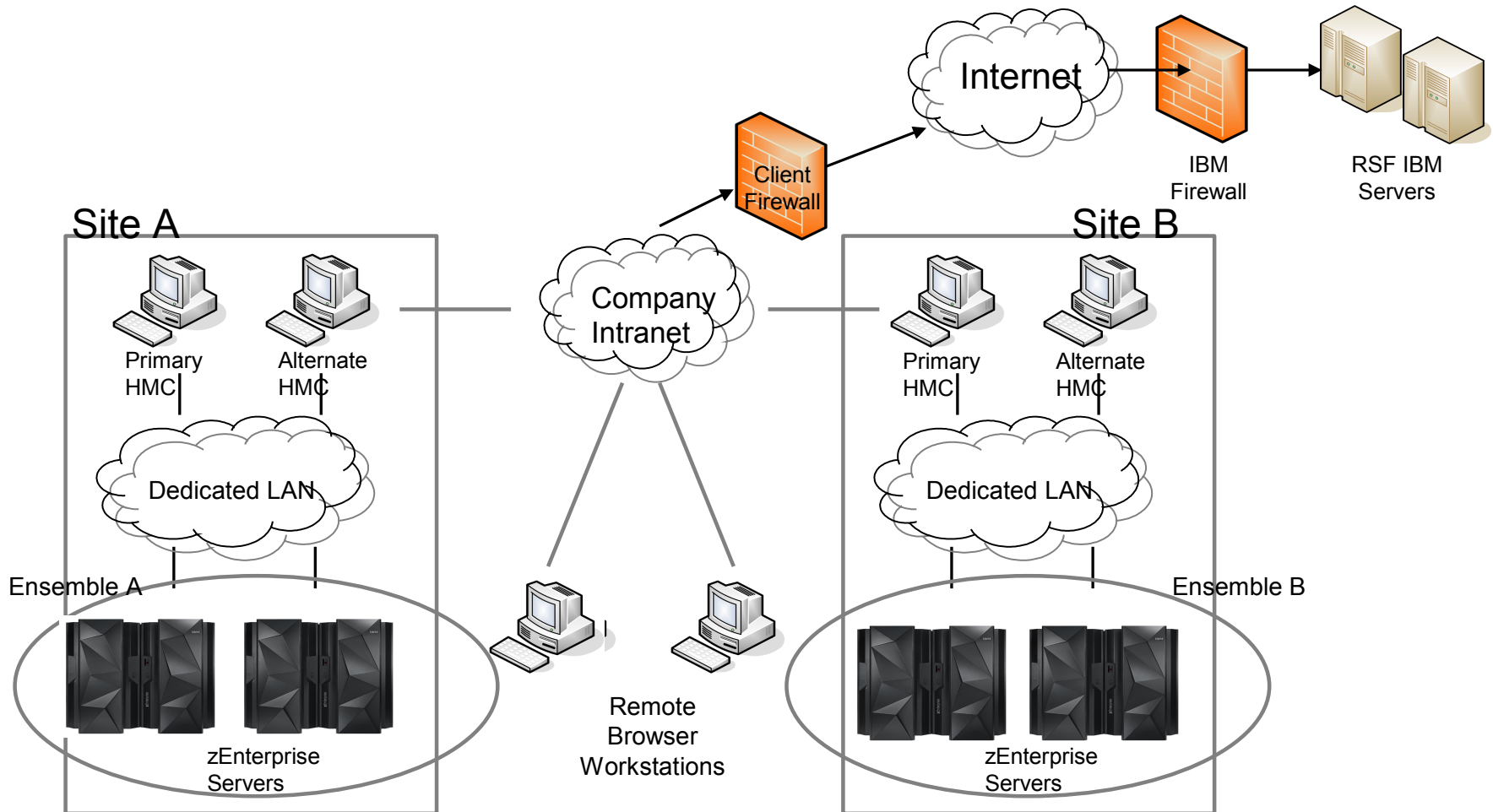
# Example Single Sysplex Network Topology



## Example Single Sysplex Topology (cont.)

- zEnterprise 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 zEnterprise 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
  - ▶ Both HMCs => call home servers using internet connectivity

# Example Multiple Ensemble Topology



## Example Multiple Ensemble Topology (continued)

- zEnterprise 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 zEnterprise servers at their respective local site
  - ▶ Both HMCs => call home servers 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
- 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”

🔑 **Domain Security** i

Current domain name:	NOT SET
Domain name:	<input style="width: 100%;" type="text" value="GROUPX"/>
Current password status:	NOT SET
New password:	<input style="width: 100%;" type="password" value="●●●●●●●●"/>
Verify password:	<input style="width: 100%;" type="password" value="●●●●●●●●"/>

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.

OK
Cancel
Help

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

***What are the security aspects of RSF?***

***Should you insert a RSF proxy box?***

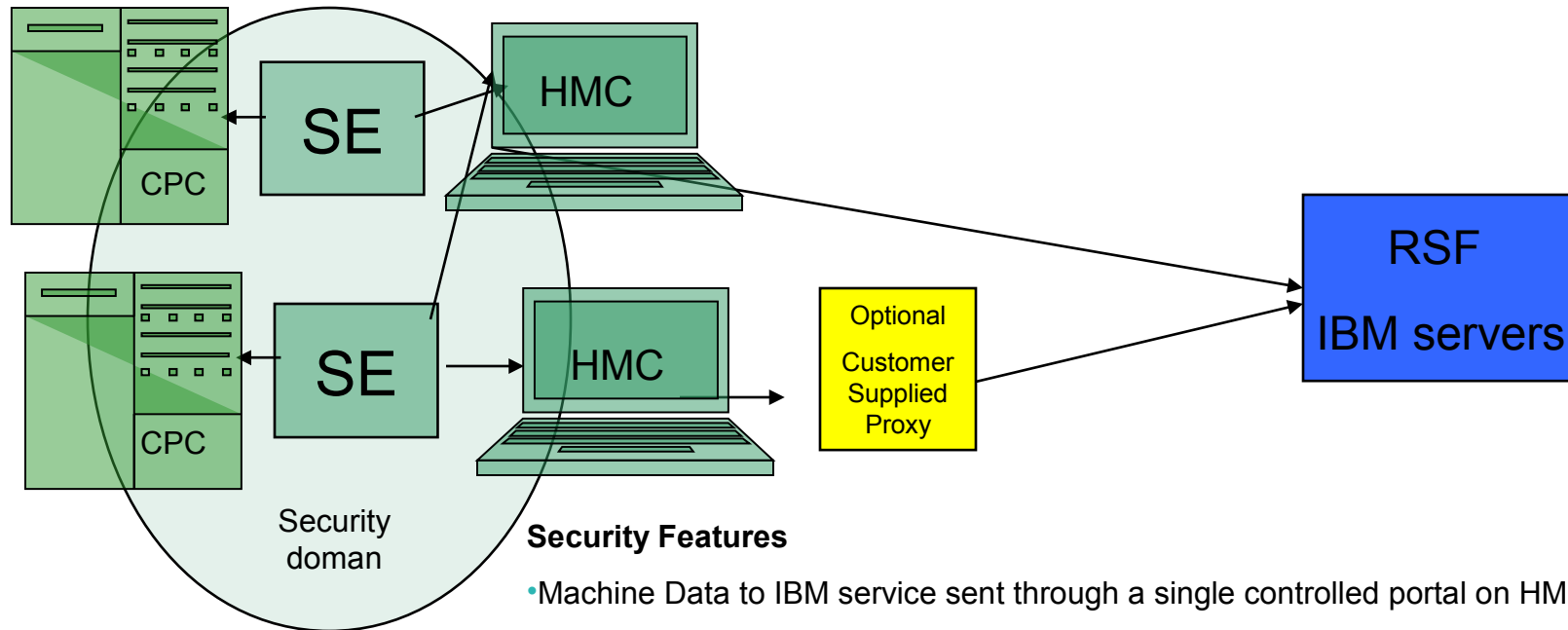
## Benefits of configuring HMC connectivity to IBM using Remote Support Facility

- **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

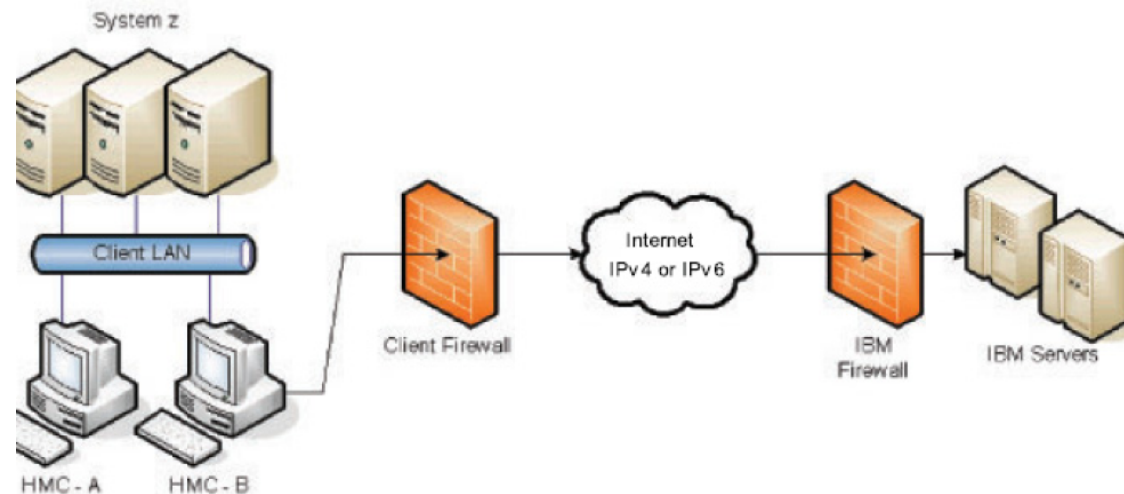
- Machine Data to IBM service sent through a single controlled portal on HMC
- Call home support is disabled by default
- HMC and SE record all outbound connections in event logs
- No NIC connection from Support Element or CEC to internet
- Separate ethernet adaptors to isolate interactions ...
  - Private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

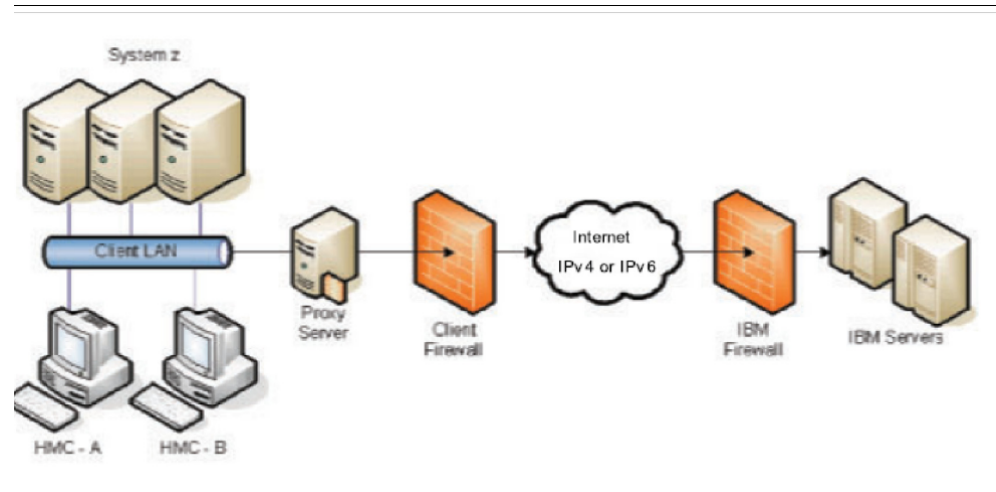
## Direct Internet connection

- 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

Local Modem    **Internet**    External Time Source

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*

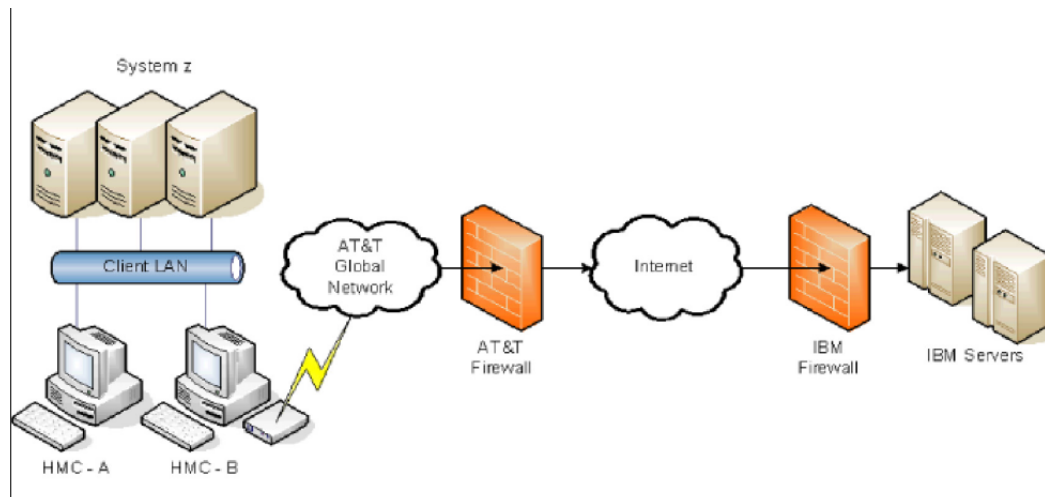
IPv4

Test...

OK    Cancel    Help

## Dial Support – Removed

- **Removed for HMC 2.12.0 (this slide only applies if on older HMC version)**
- 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

Certificate for this console:

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

Apply Cancel Help

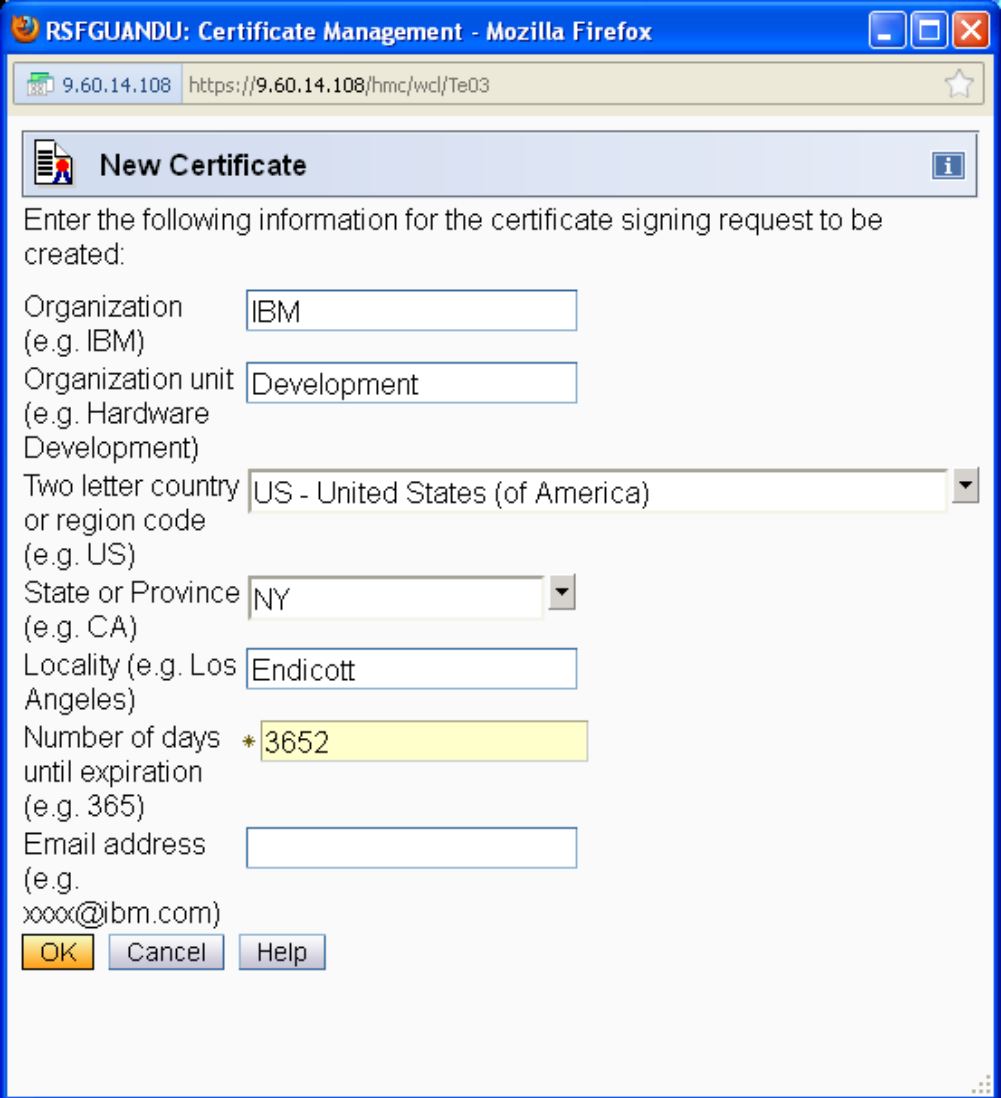
## HMC Certificate Management (cont.)

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



## 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)



**RSGUANDU: 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)

Organization unit   
(e.g. Hardware Development)

Two letter country or region code   
(e.g. US)

State or Province   
(e.g. CA)

Locality (e.g. Los Angeles)

Number of days \*   
until expiration  
(e.g. 365)

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

Select	Property
<input type="radio"/>	Version
<input type="radio"/>	Serial Number
<input type="radio"/>	Issuer
<input type="radio"/>	Valid From
<input type="radio"/>	Valid Until
<input type="radio"/>	Subject
<input type="radio"/>	Subject Alternative Names

Apply Cancel Help

javascript:menuItemLaunchAction();

## HMC Certificate Management (cont.)

- HMC 2.11.0 and prior use 1024 bit network certificates.
- HMC 2.11.1 and newer releases use 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.

1 →

2 →

HMCCHGM: Certificate Management - Mozilla Firefox: IBM Edition

9.60.15.114 https://9.60.15.114/hmc/wcd/T2aa

**Certificate Management**

Create Selected Advanced

New Certificate

Certificate for this console (changes pending):

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

Apply Cancel Help

Done

## 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

Service	Status
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

OK Cancel Help

# 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:	<input type="text" value="0"/>
Verify timeout minutes:	<input type="text" value="15"/>
Idle timeout minutes:	<input type="text" value="0"/>
Minimum time in minutes between password changes:	<input type="text" value="0"/>

*Invalid Login Attempt Values*

Maximum failed attempts before disable delay:	<input type="text" value="0"/>
Disable delay in minutes:	<input type="text" value="0"/>

*Inactivity Values*

Disable for inactivity in days:	<input type="text" value="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:

Description:

Disable user

*Authentication*

Local Authentication

LDAP Server

*Details*

Password Rule:  [Define Rules...](#)

Password:

Confirm password:

Force user to change the password at next login

Select	Managed Resource Roles
<input checked="" type="checkbox"/>	All Dept. A1 LPARs
<input type="checkbox"/>	All Dept. B2 LPARs
<input type="checkbox"/>	All Directors/Timers Managed Objects
<input type="checkbox"/>	All Fiber Saver Managed Objects
<input type="checkbox"/>	All zCPC Managed Objects

Select	Task Roles
<input type="checkbox"/>	Access Administrator Fiber Saver Tasks
<input type="checkbox"/>	Access Administrator Tasks
<input type="checkbox"/>	Advanced Operator Tasks
<input checked="" type="checkbox"/>	All Of Our Operator Tasks
<input type="checkbox"/>	CIM Actions



## Defining Users and Roles (cont.)

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

HMCCEC118: Manage Users Wizard - Mozilla Firefox

9.60.15.118 https://9.60.15.118/hmc/wd/T195b

### Manage User Wizard

#### 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:

Description:

Disable user

Allow remote access via the web

< Back   Next >   Finish   Cancel

## 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**

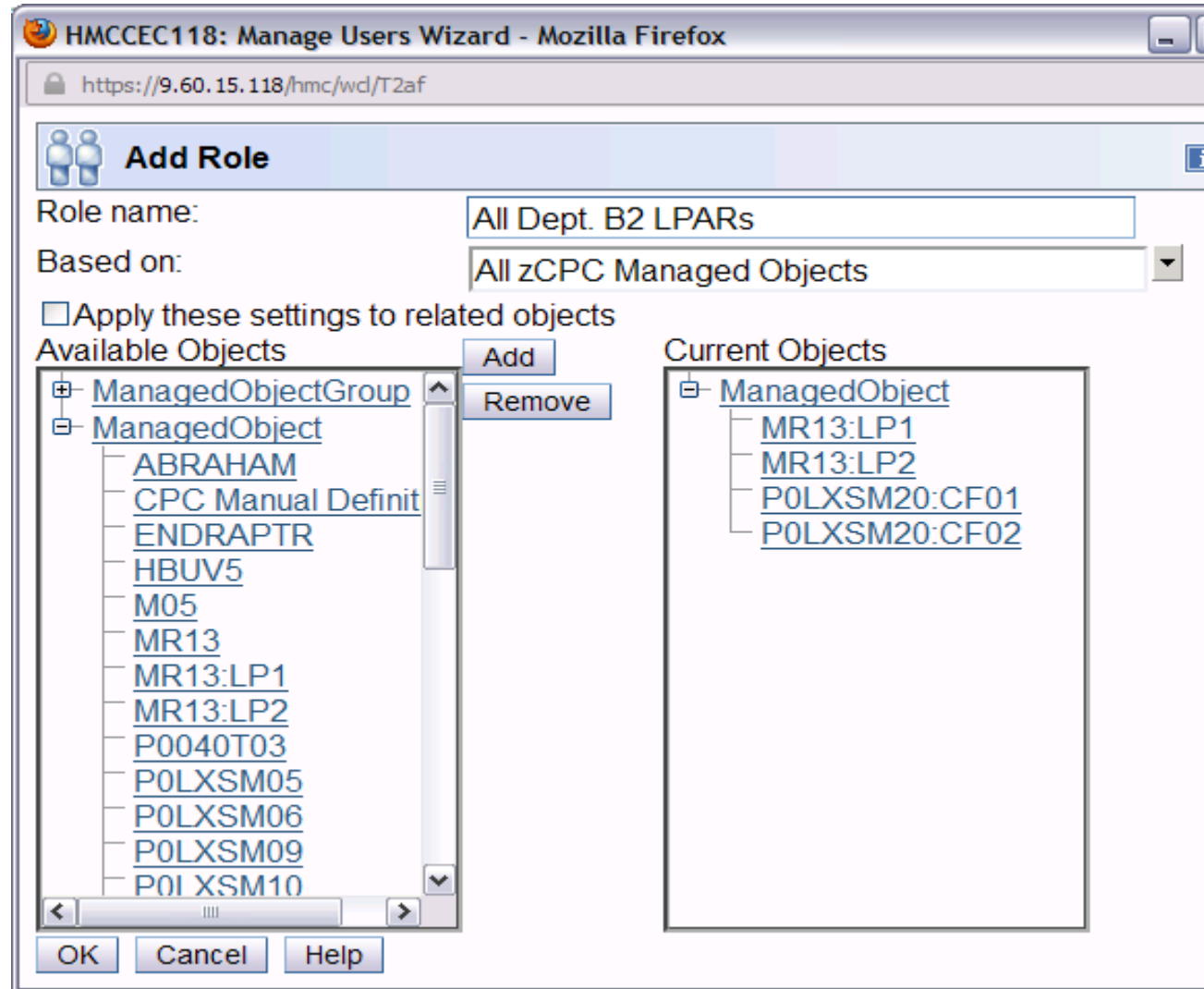
Select one or more Managed Resource Roles below to define access permissions for this user ID.

Select	Role
<input type="checkbox"/>	All Dept. A1 LPARs
<input checked="" type="checkbox"/>	All Dept. B2 LPARs
<input type="checkbox"/>	All Directors/Timers Managed Objects
<input type="checkbox"/>	All Fiber Saver Managed Objects
<input type="checkbox"/>	All zCPC Managed Objects

< Back
Next >
Finish
Cancel


## 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



## 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**

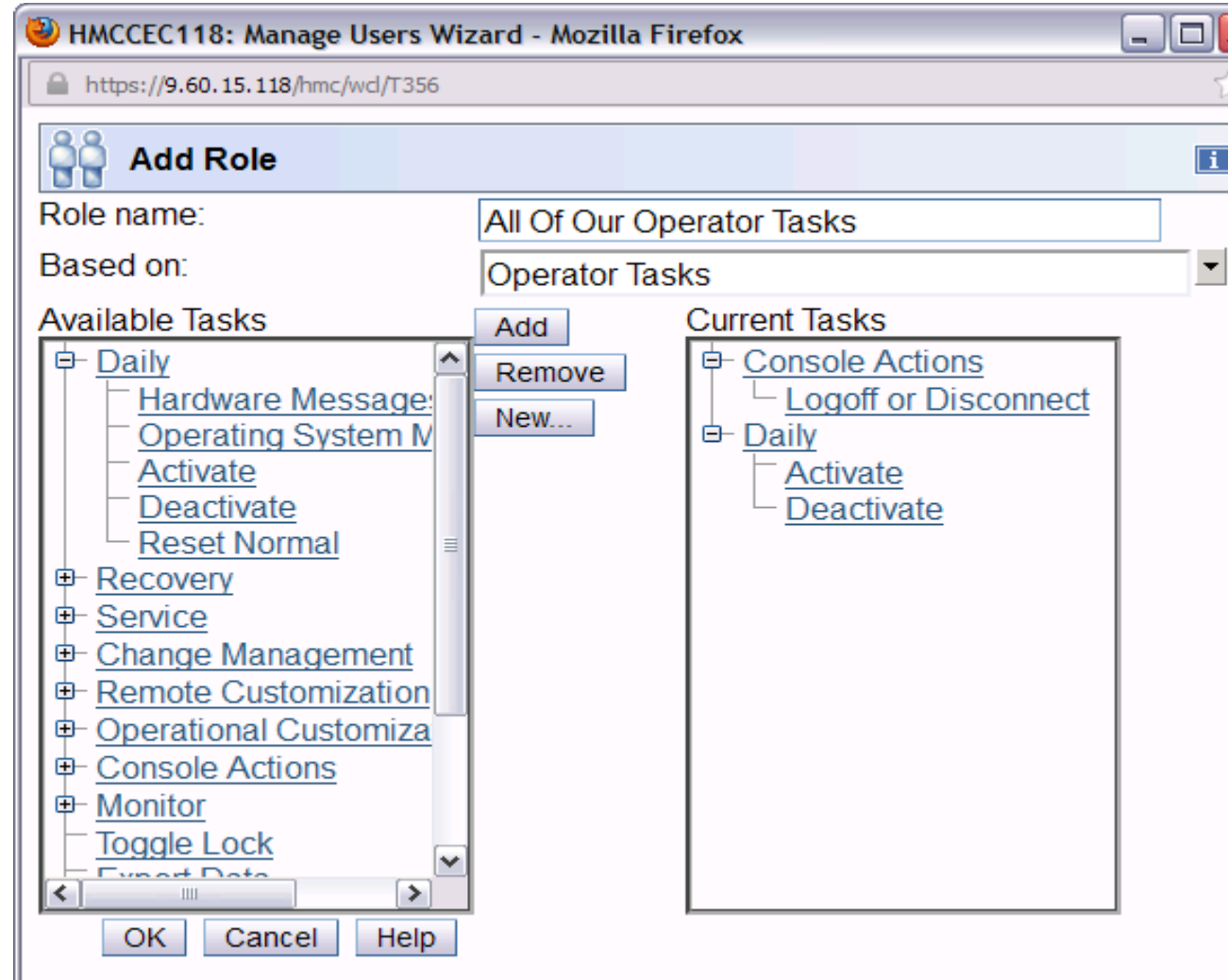
Select one or more Task Role below to define access permissions for this user ID.

Select	Task	
<input type="checkbox"/>	Access Administrator Director/Timer Tasks	<div style="border: 1px solid gray; padding: 2px; width: 100px; margin: 0 auto;">Define Task Roles...</div>
<input type="checkbox"/>	Access Administrator Fiber Saver Tasks	
<input type="checkbox"/>	Access Administrator Tasks	
<input type="checkbox"/>	Advanced Operator Tasks	
<input checked="" type="checkbox"/>	All Of Our Operator Tasks	

[< Back](#)
[Next >](#)
[Finish](#)
[Cancel](#)

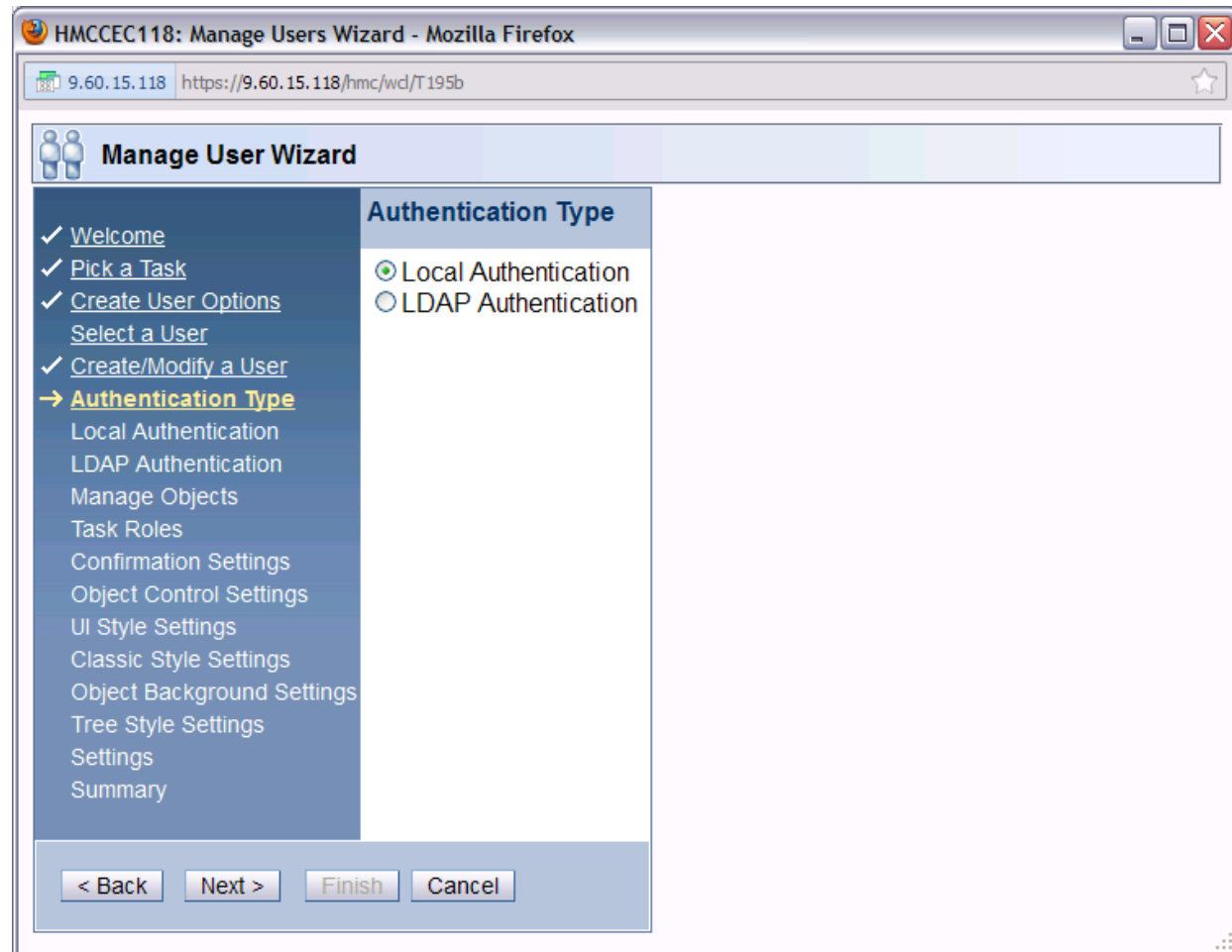
## Defining Users and Roles (cont.)

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



## Defining Users and Roles (cont.)

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

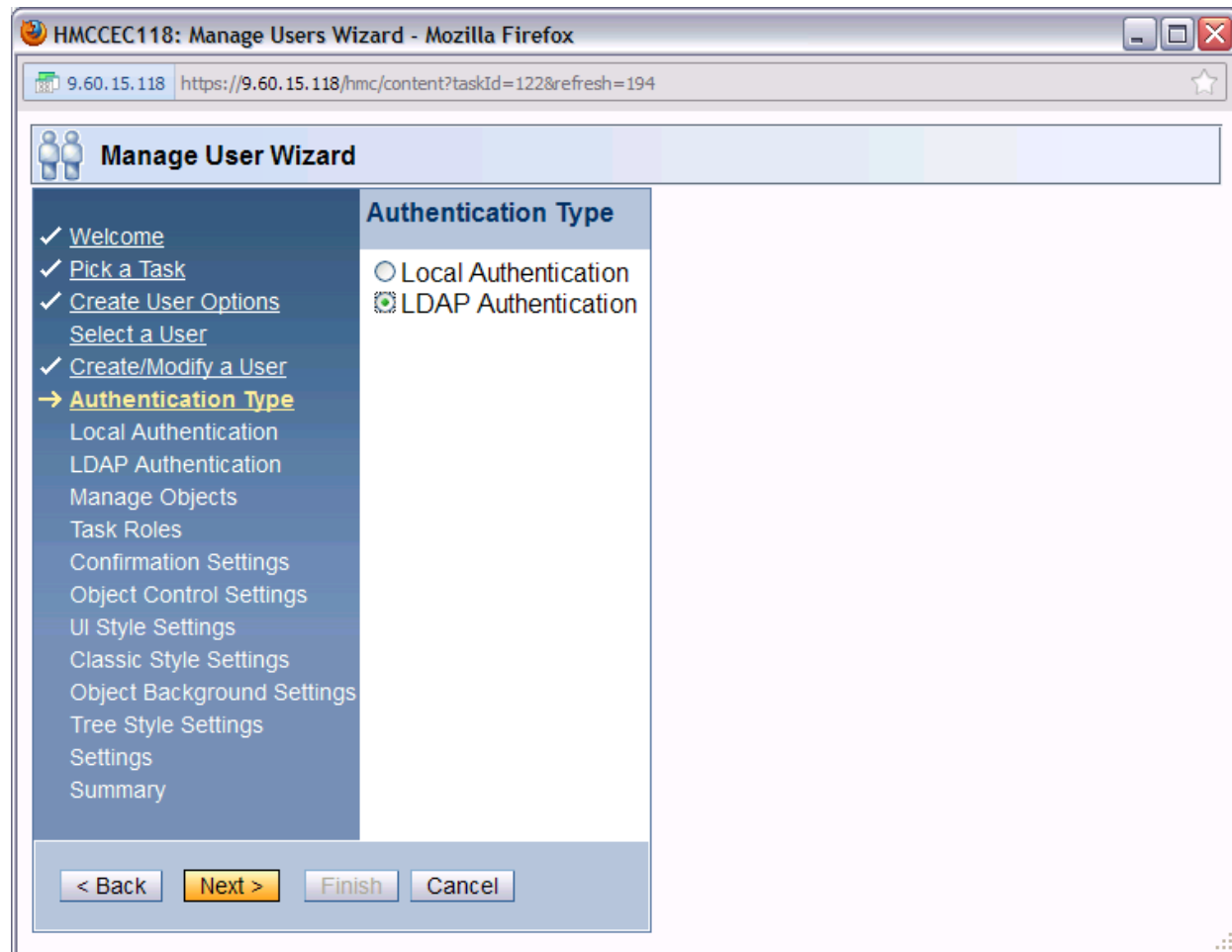
The screenshot shows the 'Manage User Wizard' window with the 'Local Authentication' tab selected. The left sidebar contains a navigation tree with the following items: Welcome, Pick a Task, Create User Options, Select a User, Create/Modify a User, Authentication Type, Local Authentication (highlighted with a yellow arrow), LDAP Authentication, Manage Objects, Task Roles, Confirmation Settings, Object Control Settings, UI Style Settings, Classic Style Settings, Object Background Settings, Tree Style Settings, Settings, and Summary. The main content area is titled 'Local Authentication' and includes a 'Details' section with the following fields and options:

- Password Rule: Standard (dropdown menu) with a 'Define Rules...' button.
- Password: [Masked input field]
- Confirm password: [Masked input field]
- I am changing the password
- Force user to change the password at next login

At the bottom of the wizard, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

## Defining Users and Roles (cont.)

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





## Defining Users and Roles (cont.)

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



## 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/wd/Td0b

### Add Enterprise Directory (LDAP) Server

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

*Primary and Backup Host Connection Information*

Primary host name: ldapsevr1.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:

OK Cancel Help

## 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/wd/Ta63

### Add Enterprise Directory (LDAP) Server

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

*Primary and Backup Host Connection Information*

Primary host name: ldaperv2.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.

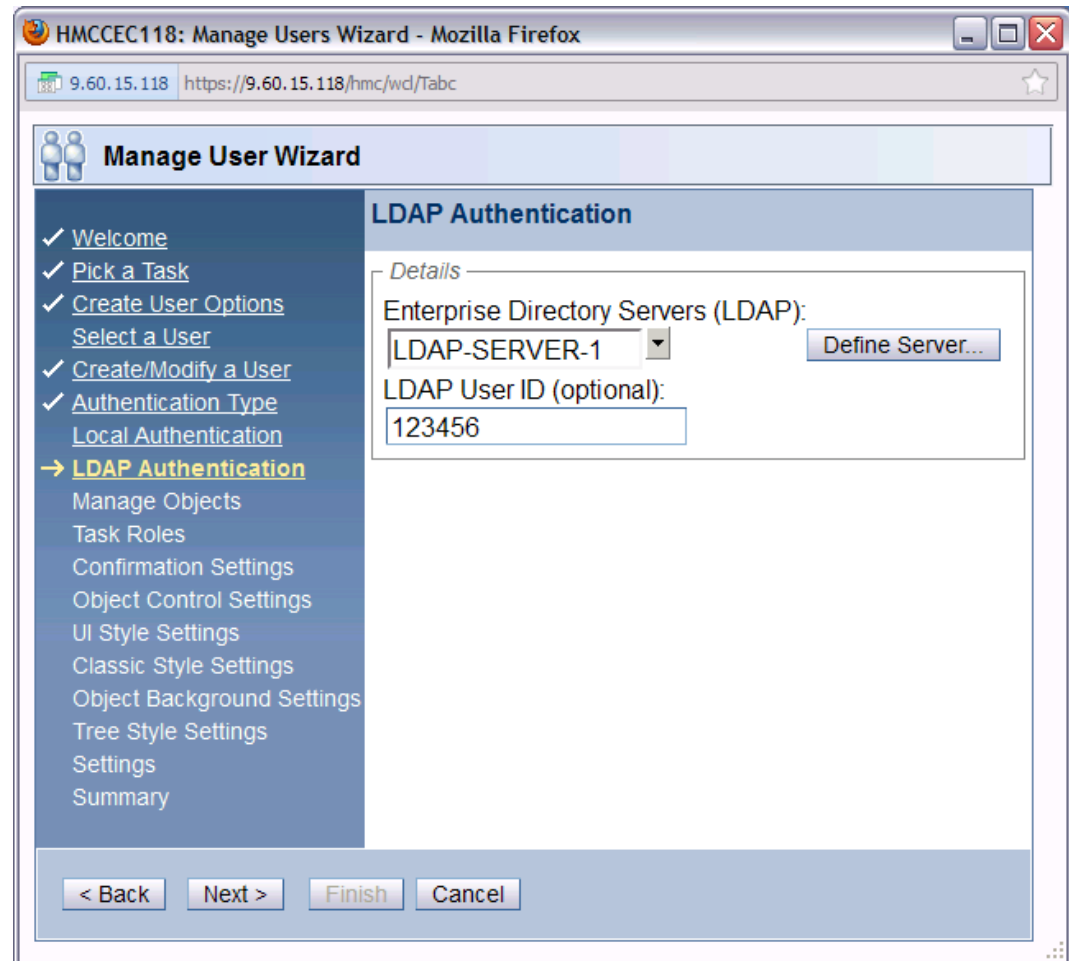
Search the entire subtree  
 Search one level only

Enter the search filter that selects the user's entry in the directory.  
Search filter: mail={0}

OK Cancel Help

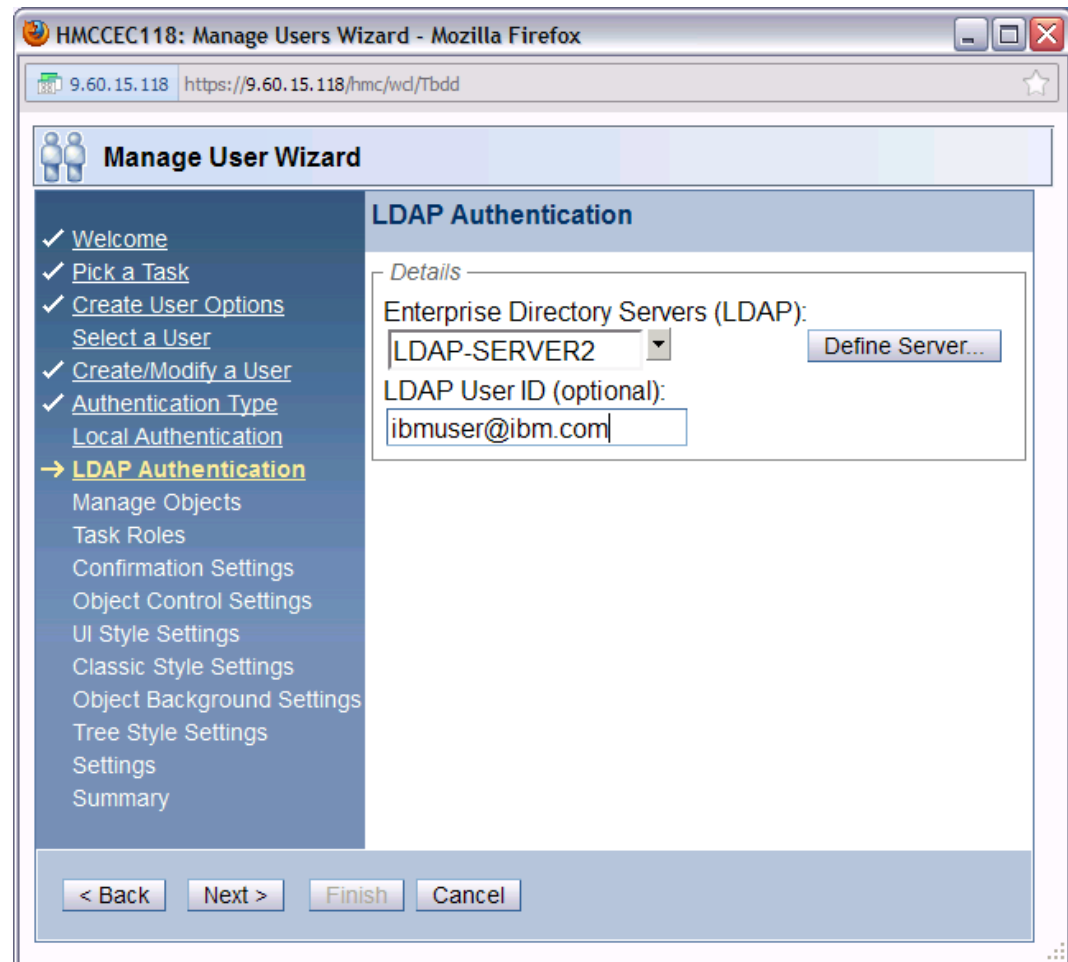
## Defining Users and Roles (cont.)

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



## Defining Users and Roles (cont.)

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

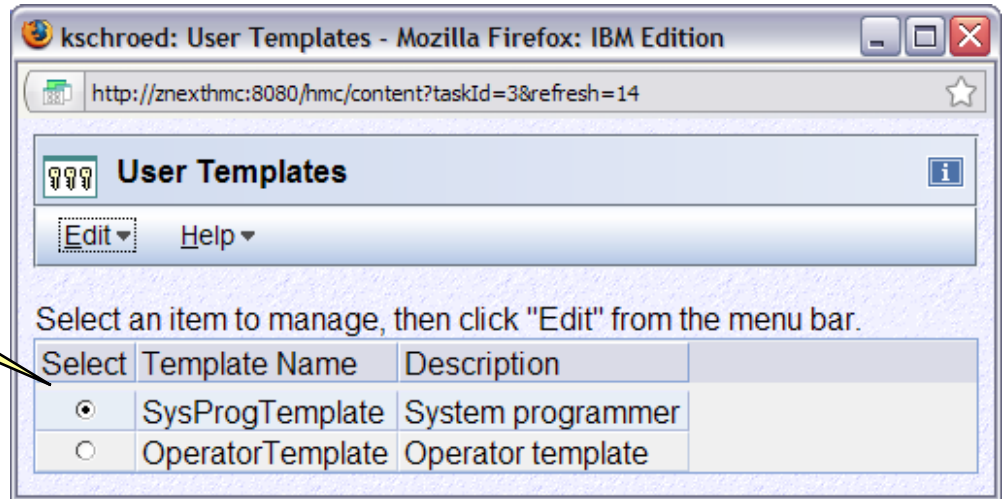


## User Templates and Patterns

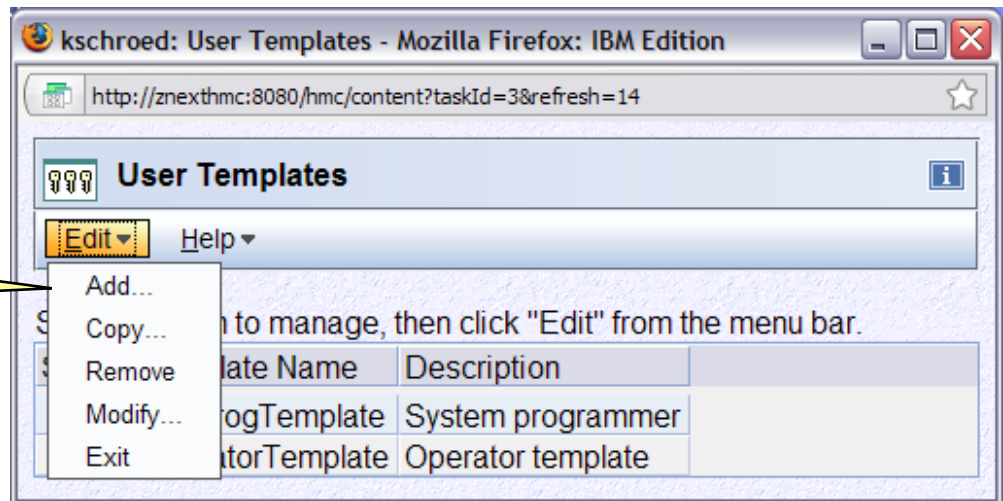
- **User template**
  - ▶ Defines all the same characteristics that would normally be defined for a user
  - ▶ Restricted to LDAP authentication
- **User pattern**
  - ▶ Defines the pattern to be used to try and match “unknown” user ids with a template
  - ▶ Defines a default template to be used for 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.



Drop down menu to choose the action to be performed



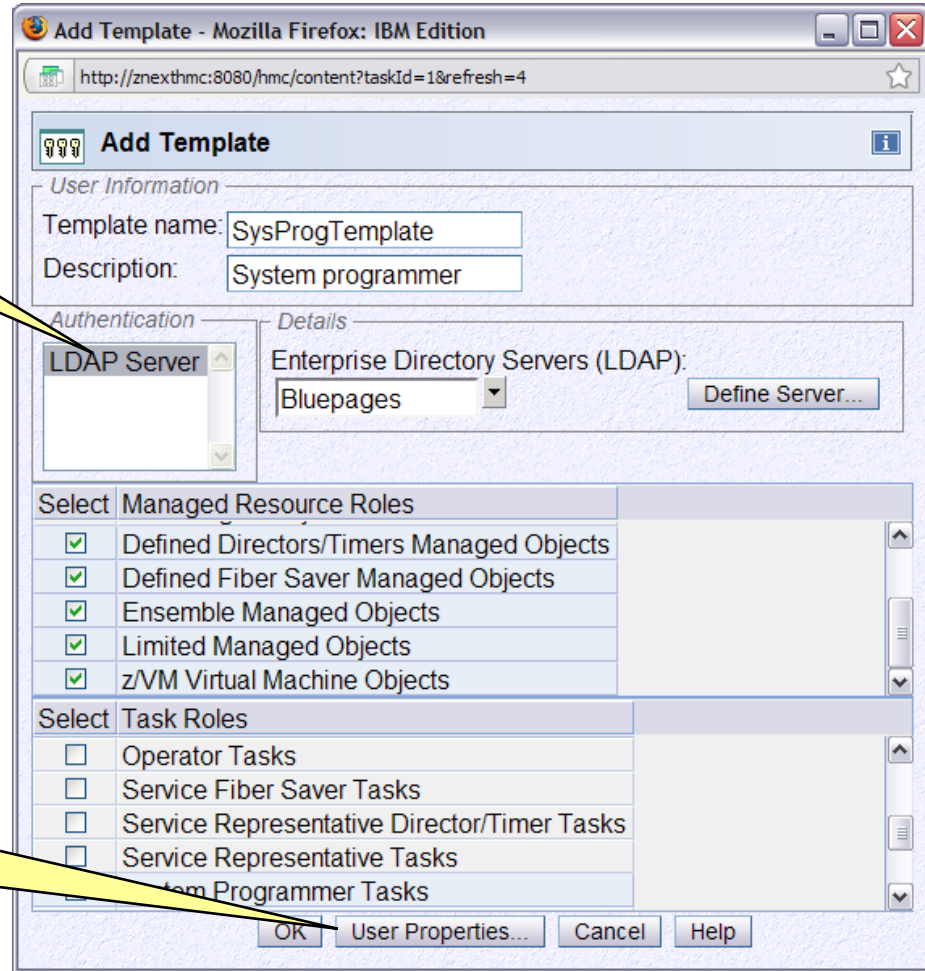


# User Templates

Restricted to LDAP authentication; no password defined

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

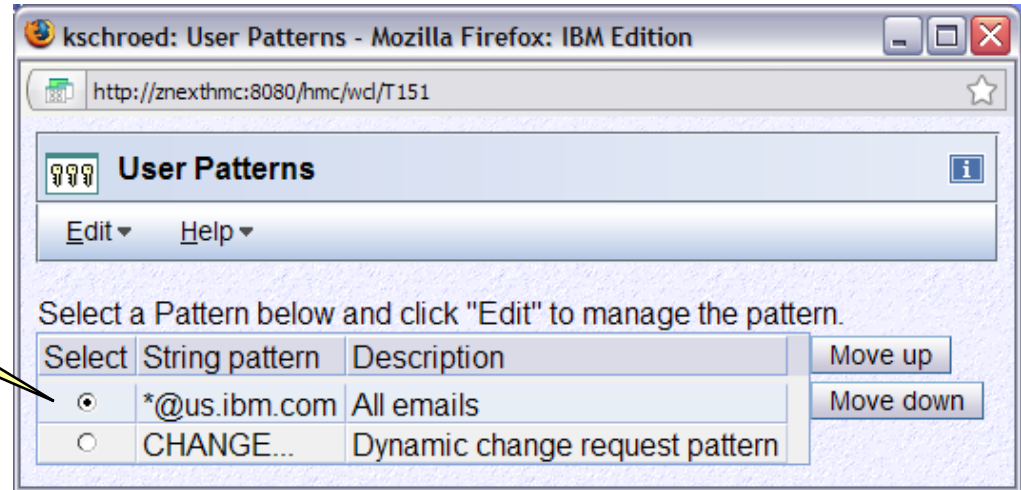
Additional user properties for user template is the same as for real users



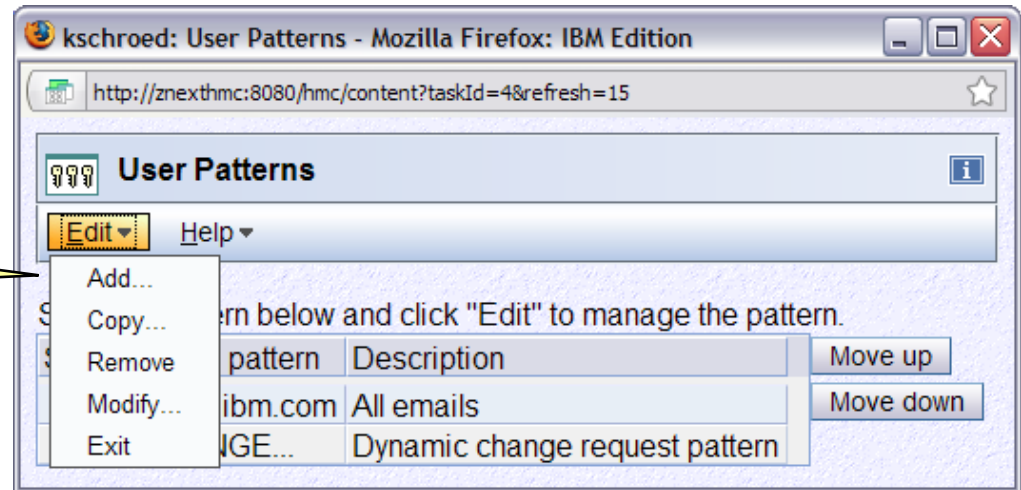


# User Patterns task

Selected the pattern to be modified, removed, etc.



Drop down menu to choose the action to be performed



# 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** i

User ID pattern: \*  
 Glob-like  
 Regular Expression

Description: \*

User settings retention time: \*  days

User template name:  Define Template...

Enable LDAP-based lookup

Server:  Define Server...

Template name override attribute:

Domain name restrictions attribute:

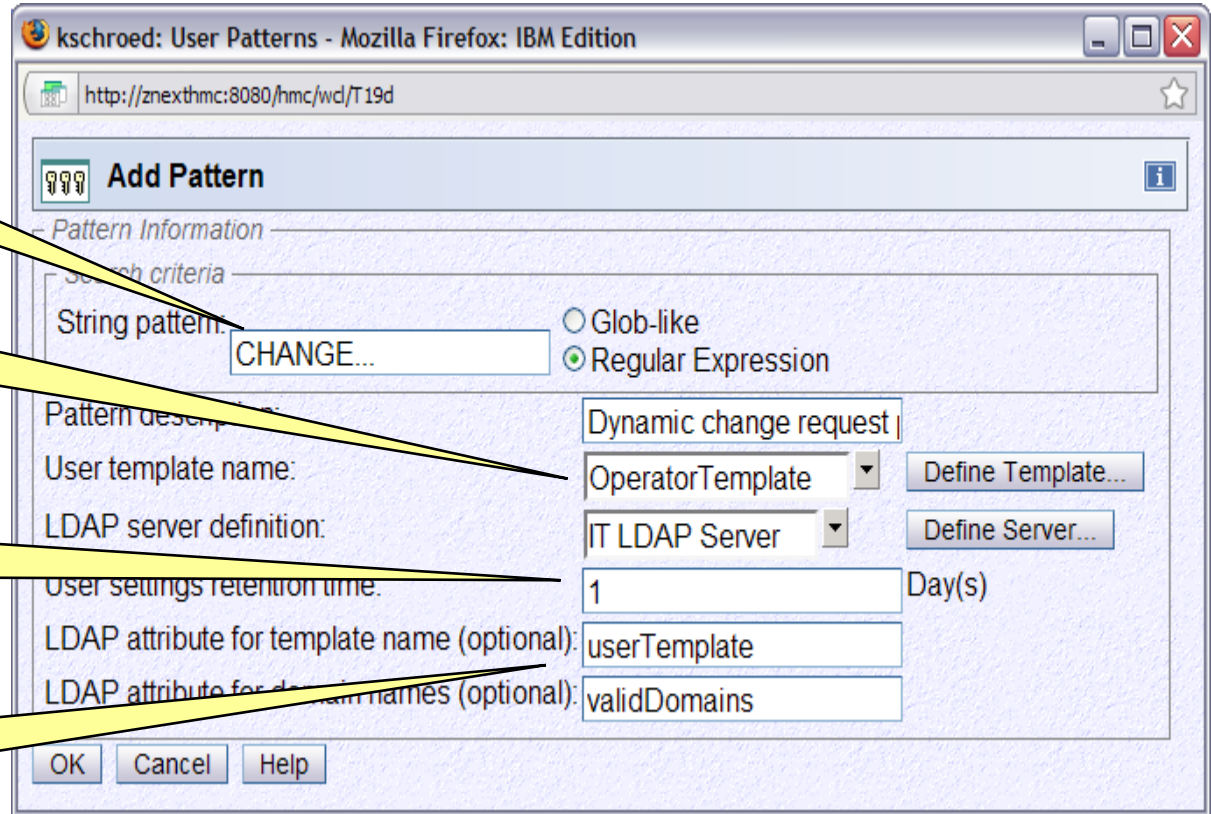
# User Patterns

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



***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/wd/T246

**Customize API Settings**

SNMP WEB Services CIM

Enable

SNMP agent parameters:

Community Names

Select	Name	Address	Network Mask / Prefix	Access Type
<input checked="" type="radio"/>	COMMUNITY1	9.60.73.23	255.255.255.255	write

Add... Change... Delete

SNMPv3 Users

Select	User Name	Access Type
--------	-----------	-------------

Add... Change... Delete

Event Notification Information

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


Select	TCP/IP Address
--------	----------------

Add... Change... Delete

OK Cancel Help

## 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** ?

SNMP

WEB Services

CIM

Enable

SNMP agent parameters:

*Community Names*

Select	Name	Address	Network Mask / Prefix	Access Type
<input checked="" type="radio"/>	community1	9.60.73.23	255.255.255.255	read

Add...
Change...
Delete

*SNMPv3 Users*

Select	User Name	Access Type
<input checked="" type="radio"/>	snmpv3user1	read

Add...
Change...
Delete

*Event Notification Information*

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

Select	TCP/IP Address
<input checked="" type="radio"/>	9.60.15.139

Add...
Change...
Delete

OK
Cancel
Help

## 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 i

SNMP
**WEB Services**
CIM

Enable

*IP Address Access Control*

Allow all IP Addresses

IP Addresses

Select	IP Address
<input checked="" type="radio"/>	9.60.73.23

Add
Edit
Remove

User Access Control

Select	User
<input type="checkbox"/>	ENSOPERATOR
<input type="checkbox"/>	SERVICE
<input type="checkbox"/>	ldapuser
<input type="checkbox"/>	ACSADMIN
<input type="checkbox"/>	ADVANCED
<input type="checkbox"/>	ENSADMIN
<input type="checkbox"/>	vsuser2
<input checked="" type="checkbox"/>	vsuser1
<input type="checkbox"/>	bindldap
<input type="checkbox"/>	242931
<input type="checkbox"/>	OPERATOR
<input type="checkbox"/>	SERVICELDAP
<input type="checkbox"/>	SYSPROG

OK
Cancel
Help



***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

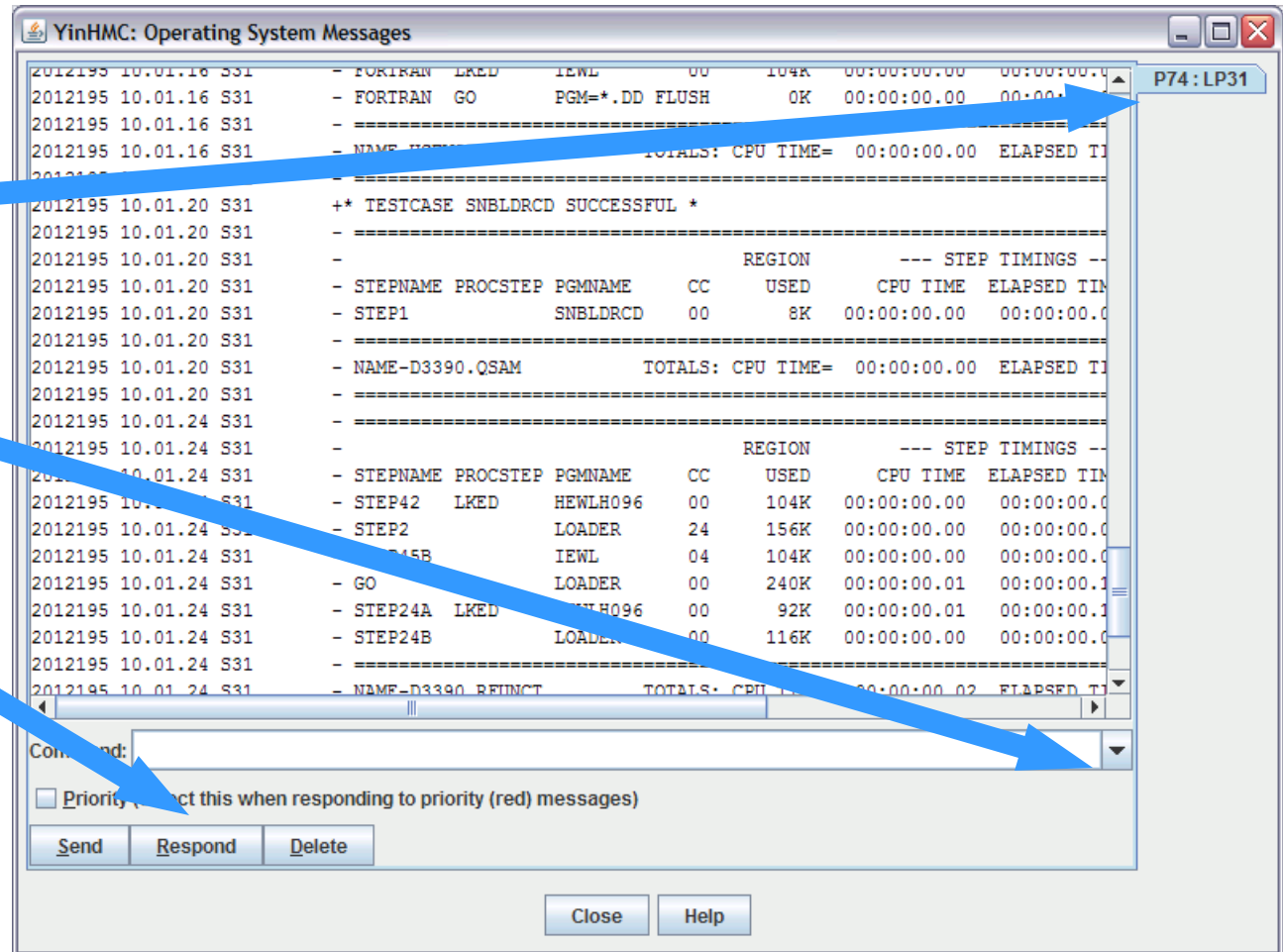
## Operating System HMC Considerations (cont.)

- 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



## 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/wd/T1a92

### Manage SSH Keys

*Known Host Keys*

--- Select Action ---

Select	IP Address	Key Fingerprint
<input type="radio"/>	9.60.74.199	7c:6a:c8:07:ec:1f:01:19:10:8b:69:b6:a7:ff:de:36
<input type="radio"/>	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 \*

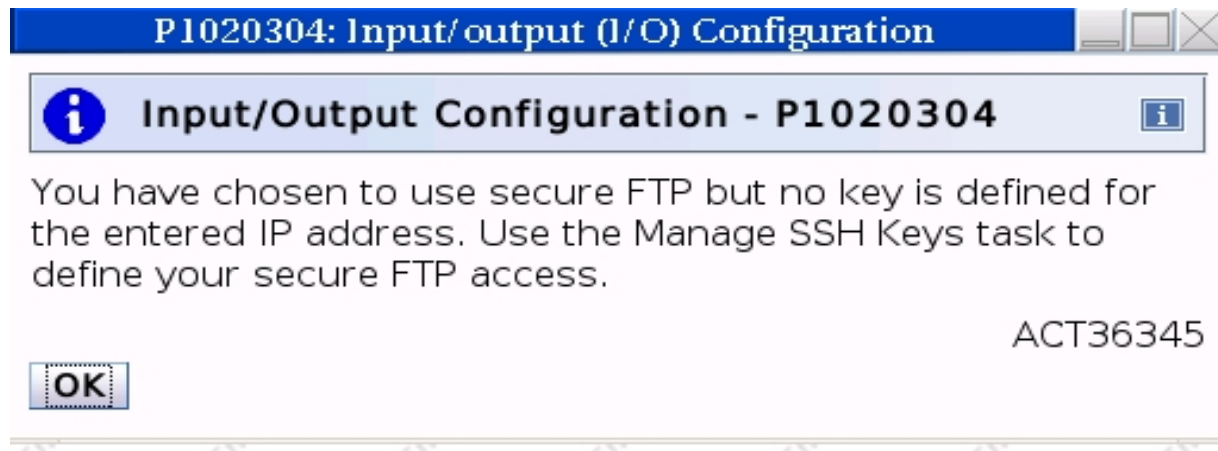
Fully qualified file name \*

Use secure FTP

**OK** **Cancel** **Help**

## 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.



***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:
2. Description (optional):
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
<input checked="" type="checkbox"/>	kschroed
5. What event text should cause notification? \*
6. When should this monitor be in effect?
  - Limit to times: Start Time:  End Time:
  - Limit to days:  Sunday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday
  - Limit to dates: Start Date:  End Date:
7. What email addresses should be notified? \*

OK Cancel Help

## 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

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



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

Audit data types

Select	Audit data types
<input type="checkbox"/>	Configuration
<input type="checkbox"/>	API settings
<input type="checkbox"/>	Certificate management
<input type="checkbox"/>	Console services
<input type="checkbox"/>	Data Replication
<input type="checkbox"/>	Defined CPCs

Total: 16 Selected: 0

OK Cancel Help

Done



# 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

### 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

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

Save... Cancel Help

## 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)

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

*Audit data types*

Select	Audit data types
<input type="checkbox"/>	Logs
<input type="checkbox"/>	Audit log
<input checked="" type="checkbox"/>	Console events
<input checked="" type="checkbox"/>	Security Log
<input type="checkbox"/>	Service History
<input type="checkbox"/>	Tasks performed log

Total: 17 Selected: 2

OK Cancel Help

Done

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/wcd/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.

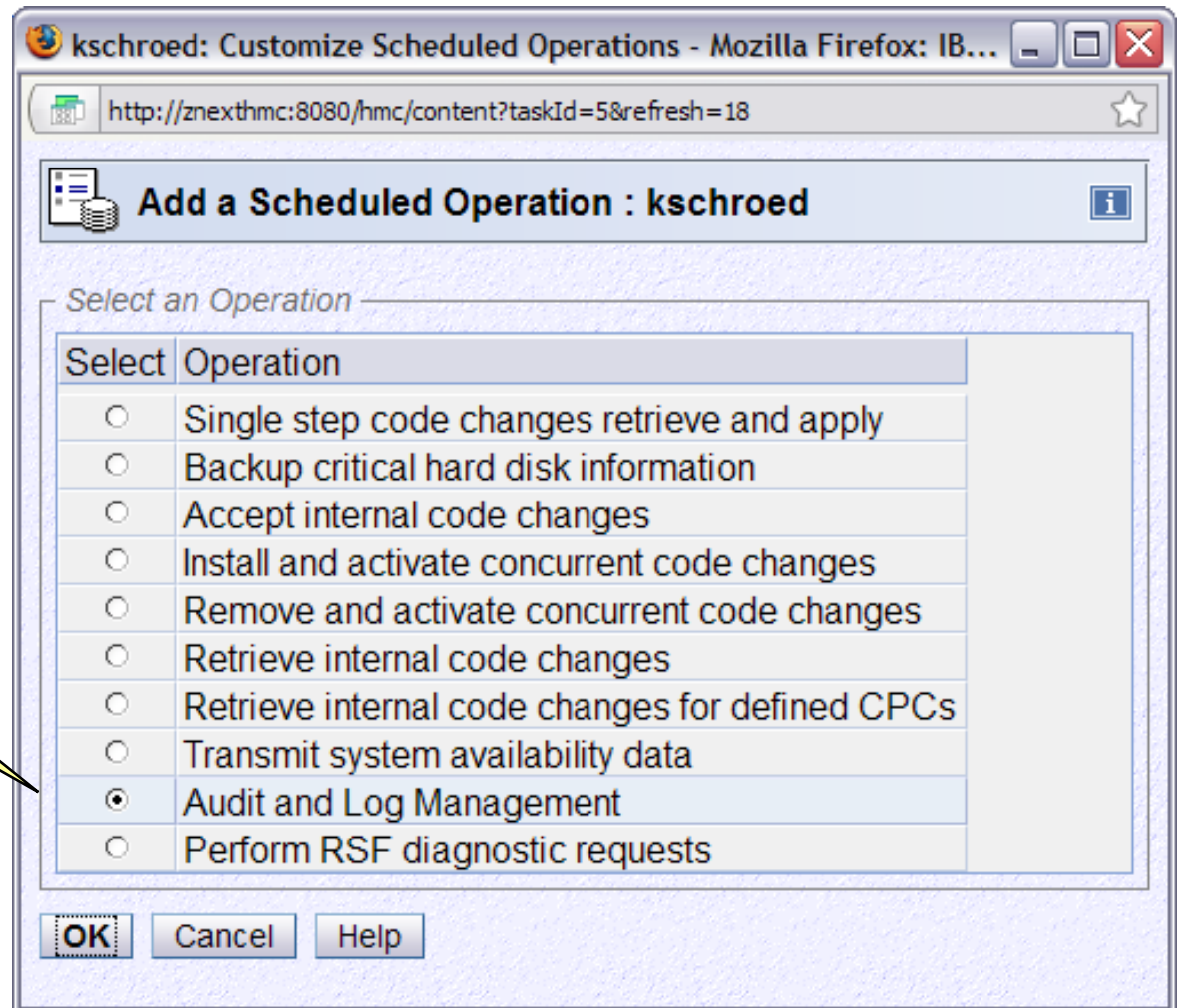
Save... Cancel Help

Done



## Scheduled generation of reports

Scheduled operation  
for generating audit  
reports



# 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**

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:

Offload information

Host or address:  User name:   
 File name:  Password:

Audit data types

Select	Audit data types
<input type="checkbox"/>	<input type="checkbox"/> All data types
<input type="checkbox"/>	<input type="checkbox"/> Configuration
<input type="checkbox"/>	API settings
<input type="checkbox"/>	Certificate management
<input type="checkbox"/>	Console services
<input type="checkbox"/>	Data Replication
Total: 17 Selected: 0	

Done

## 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.)

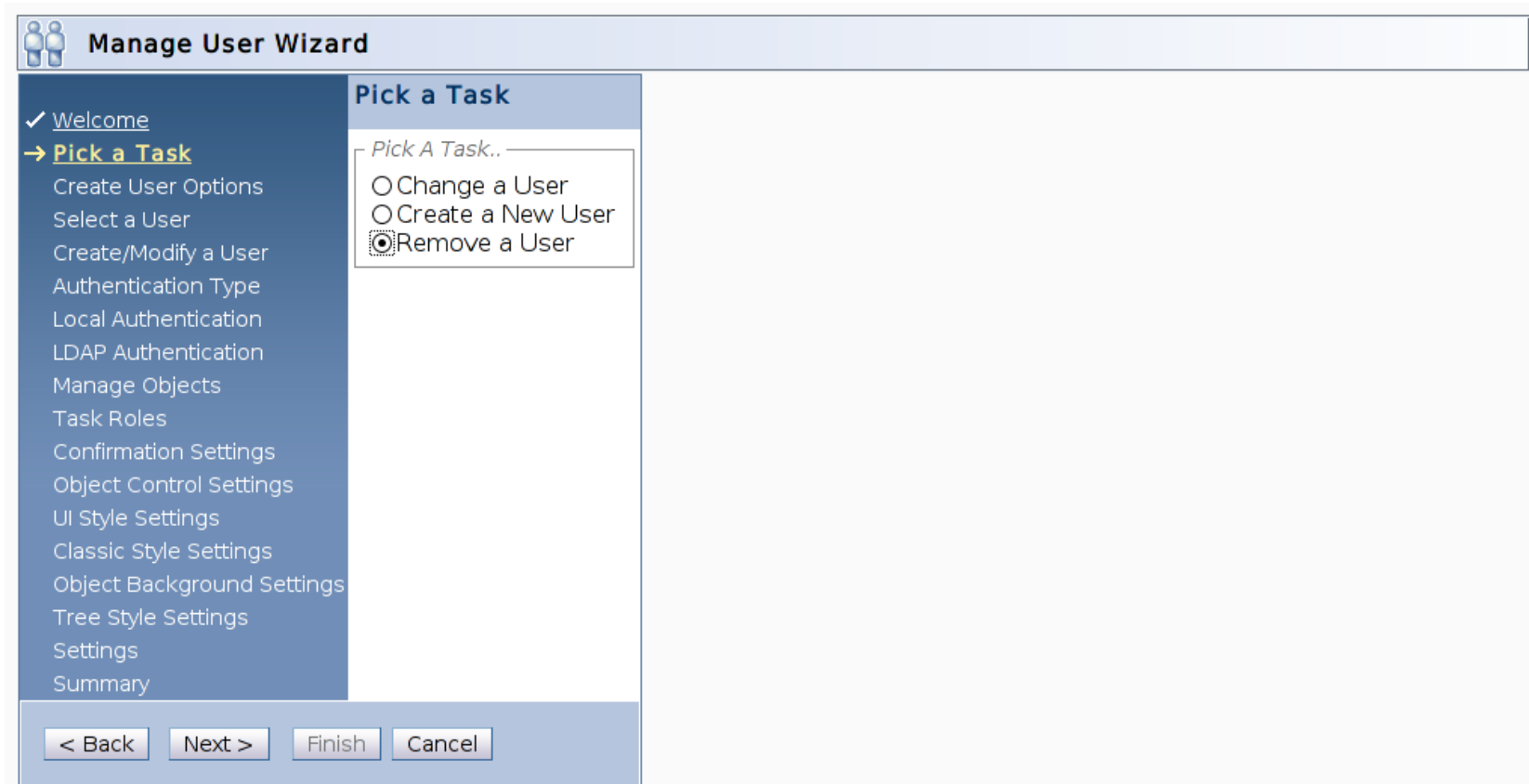
- Use HMC data replication to ensure that User Profile information (userids, roles, password rules, etc.) are automatically kept in sync among all HMC installed in the enterprise.
  
- If automation is required,
  - ▶ If using SNMP, utilize SNMP V3
  - ▶ Consider WebServices APIs for more granular access 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+
- z/OS NIP Console Config for HMC on Startup

## Removing Default User IDs

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



## Removing Default User IDs (cont.)

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

**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

**Select a User**

Select a User ID.

Select	User ID	Description
<input type="radio"/>	242931	LDAP using dn pattern
<input type="radio"/>	ACSADMIN	Access administrator level user
<input checked="" type="radio"/>	ADVANCED	Advanced operator level user
<input type="radio"/>	bindldap	Test ldap with bind
<input type="radio"/>	ENSADMIN	Ensemble administrator level user

< Back   Next >   Finish   Cancel

## 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 9950-9959	Used to proxy <b>Single Object Operations</b> 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 <b>ONLY</b> enabled when Electronic Service Agent or the <b>Enable FTP Access to Hardware Management Console Mass Storage Media</b> 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.)

<b>TCP/IP Source Port</b>	<b>Usage</b>
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.
tcp 61612	Used for connecting to the Web Services API message broker and flowing Streaming Text Oriented Messaging Protocol (STOMP) over the connection when the Web Services API is enabled.
tcp 61617	Used for connecting to the Web Services API message broker and flowing OpenWire over the connection when the Web Services API is enabled.
tcp 123	Used to set the time of the Support Element (SE) and any blades of a zEnterprise BladeCenter® Extension (zBX).

## 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 <b>Single Object Operations</b> session for a System z® server console.
tcp 25345	Used for <b>Single Object Operations</b> 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 <b>Monitor System Events</b> 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)

**Configure SSL Ciphers Suites**

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

--- Select Action ---

Select	Name	Description
<input checked="" type="checkbox"/>	SSL_RSA_WITH_RC4_128_MD5	RSA key exchange and authentication with 128 bit RC4 cipher and MD5
<input checked="" type="checkbox"/>	SSL_RSA_WITH_RC4_128_SHA	RSA key exchange and authentication with 128 bit RC4 cipher and SHA
<input checked="" type="checkbox"/>	SSL_RSA_WITH_AES_128_CBC_SHA	RSA key exchange and authentication with 128 bit AES_CBC cipher and
<input checked="" type="checkbox"/>	SSL_DHE_RSA_WITH_AES_128_CBC_SHA	DHE key exchange and RSA authentication with 128 bit AES_CBC cipher
<input checked="" type="checkbox"/>	SSL_DHE_DSS_WITH_AES_128_CBC_SHA	DHE key exchange and DSS authentication with 128 bit AES_CBC cipher
<input checked="" type="checkbox"/>	SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA key exchange and authentication with 168 bit 3DES_EDE_CBC cipher
<input checked="" type="checkbox"/>	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	RSA_FIPS key exchange and authentication with 168 bit 3DES_EDE_CBC
<input checked="" type="checkbox"/>	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	DHE key exchange and RSA authentication with 168 bit 3DES_EDE_CBC
<input checked="" type="checkbox"/>	SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DHE key exchange and DSS authentication with 168 bit 3DES_EDE_CBC
<input checked="" type="checkbox"/>	SSL_DHE_DSS_WITH_RC4_128_SHA	DHE key exchange and DSS authentication with 128 bit RC4 cipher and
<input type="checkbox"/>	SSL_RSA_WITH_DES_CBC_SHA	RSA key exchange and authentication with 56 bit DES_CBC cipher and S
<input type="checkbox"/>	SSL_RSA_FIPS_WITH_DES_CBC_SHA	RSA_FIPS key exchange and authentication with 56 bit DES_CBC cipher
<input type="checkbox"/>	SSL_DHE_RSA_WITH_DES_CBC_SHA	DHE key exchange and RSA authentication with 56 bit DES_CBC cipher a
<input type="checkbox"/>	SSL_DHE_DSS_WITH_DES_CBC_SHA	DHE key exchange and DSS authentication with 56 bit DES_CBC cipher a
<input type="checkbox"/>	SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA key exchange and authentication with 40 bit RC4 cipher and MD5 h
<input type="checkbox"/>	SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA key exchange and authentication with 40 bit DES40_CBC cipher and
<input type="checkbox"/>	SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	DHE key exchange and RSA authentication with 40 bit DES40_CBC cipher
<input type="checkbox"/>	SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	DHE key exchange and DSS authentication with 40 bit DES40_CBC cipher
<input type="checkbox"/>	SSL_RSA_WITH_NULL_MD5	RSA key exchange and authentication with null cipher and MD5 hashing
<input type="checkbox"/>	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 Action ---

Select	Name	Description
<input type="checkbox"/>	SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	DHE key exchange and RSA authentication with 40 bit DES40_CBC cipher
<input type="checkbox"/>	SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	DHE key exchange and DSS authentication with 40 bit DES40_CBC cipher
<input type="checkbox"/>	SSL_RSA_WITH_NULL_MD5	RSA key exchange and authentication with null cipher and MD5 hashing
<input type="checkbox"/>	SSL_RSA_WITH_NULL_SHA	RSA key exchange and authentication with null cipher and SHA hashing
<input type="checkbox"/>	SSL_DH_anon_WITH_AES_128_CBC_SHA	DH key exchange and no authentication with 128 bit AES_CBC cipher and
<input type="checkbox"/>	SSL_DH_anon_WITH_RC4_128_MD5	DH key exchange and no authentication with 128 bit RC4 cipher and MD
<input type="checkbox"/>	SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	DH key exchange and no authentication with 168 bit 3DES_EDE_CBC cip
<input type="checkbox"/>	SSL_DH_anon_WITH_DES_CBC_SHA	DH key exchange and no authentication with 56 bit DES_CBC cipher and
<input type="checkbox"/>	SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	DH key exchange and no authentication with 40 bit RC4_40 cipher and M
<input type="checkbox"/>	SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	DH key exchange and no authentication with 40 bit DES40_CBC cipher a
<input checked="" type="checkbox"/>	SSL_KRB5_WITH_RC4_128_SHA	KRB5 key exchange and authentication with 128 bit RC4 cipher and SHA
<input checked="" type="checkbox"/>	SSL_KRB5_WITH_RC4_128_MD5	KRB5 key exchange and authentication with 128 bit RC4 cipher and MD5
<input checked="" type="checkbox"/>	SSL_KRB5_WITH_3DES_EDE_CBC_SHA	KRB5 key exchange and authentication with 168 bit 3DES_EDE_CBC ciph
<input checked="" type="checkbox"/>	SSL_KRB5_WITH_3DES_EDE_CBC_MD5	KRB5 key exchange and authentication with 168 bit 3DES_EDE_CBC ciph
<input type="checkbox"/>	SSL_KRB5_WITH_DES_CBC_SHA	KRB5 key exchange and authentication with 56 bit DES_CBC cipher and
<input type="checkbox"/>	SSL_KRB5_WITH_DES_CBC_MD5	KRB5 key exchange and authentication with 56 bit DES_CBC cipher and
<input type="checkbox"/>	SSL_KRB5_EXPORT_WITH_RC4_40_SHA	KRB5 key exchange and authentication with 40 bit RC4_40 cipher and St
<input type="checkbox"/>	SSL_KRB5_EXPORT_WITH_RC4_40_MD5	KRB5 key exchange and authentication with 40 bit RC4_40 cipher and M
<input type="checkbox"/>	SSL_KRB5_EXPORT_WITH_DES_CBC_40_SHA	KRB5 key exchange and authentication with 40 bit DES_CBC_40 cipher a
<input type="checkbox"/>	SSL_KRB5_EXPORT_WITH_DES_CBC_40_MD5	KRB5 key exchange and authentication with 40 bit DES_CBC_40 cipher a
		Total: 36

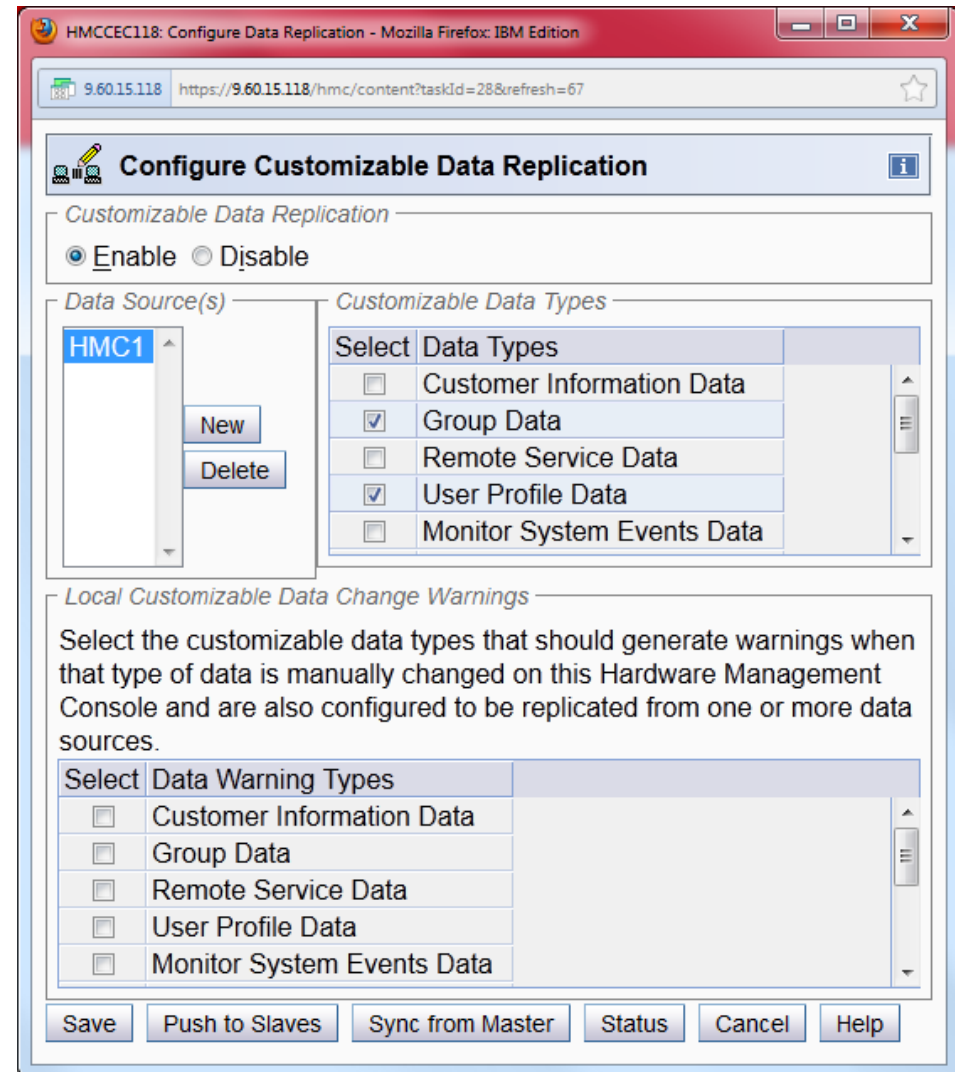
OK Default Cancel Help

## 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



## 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**

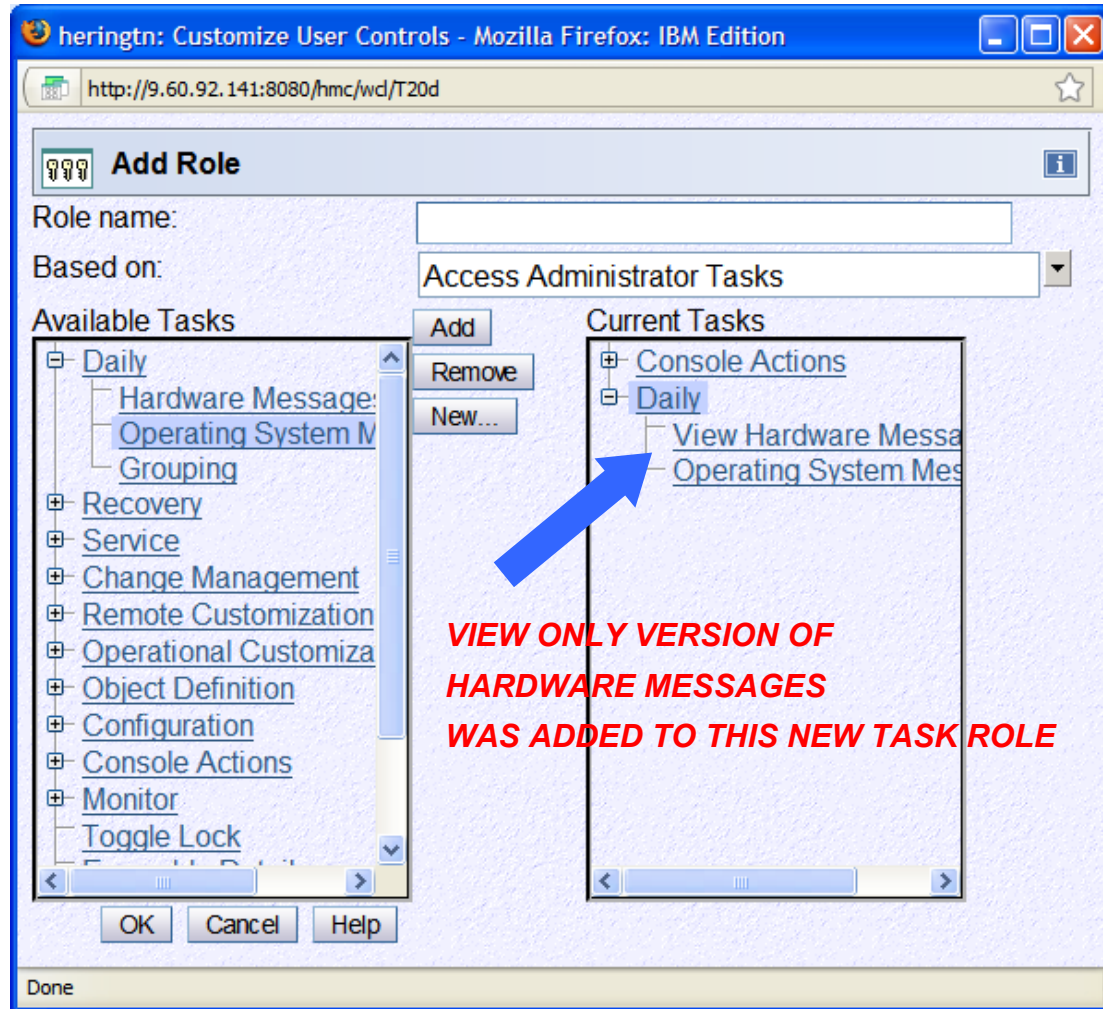
- ▶ The HMC and SE User ID support added the ability to create users who have View Only access to select tasks.
- ▶ The View Only tasks are simply the full function tasks with minor modifications to their GUI controls which prevent any actions from being taken. The following subset support a View Only 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



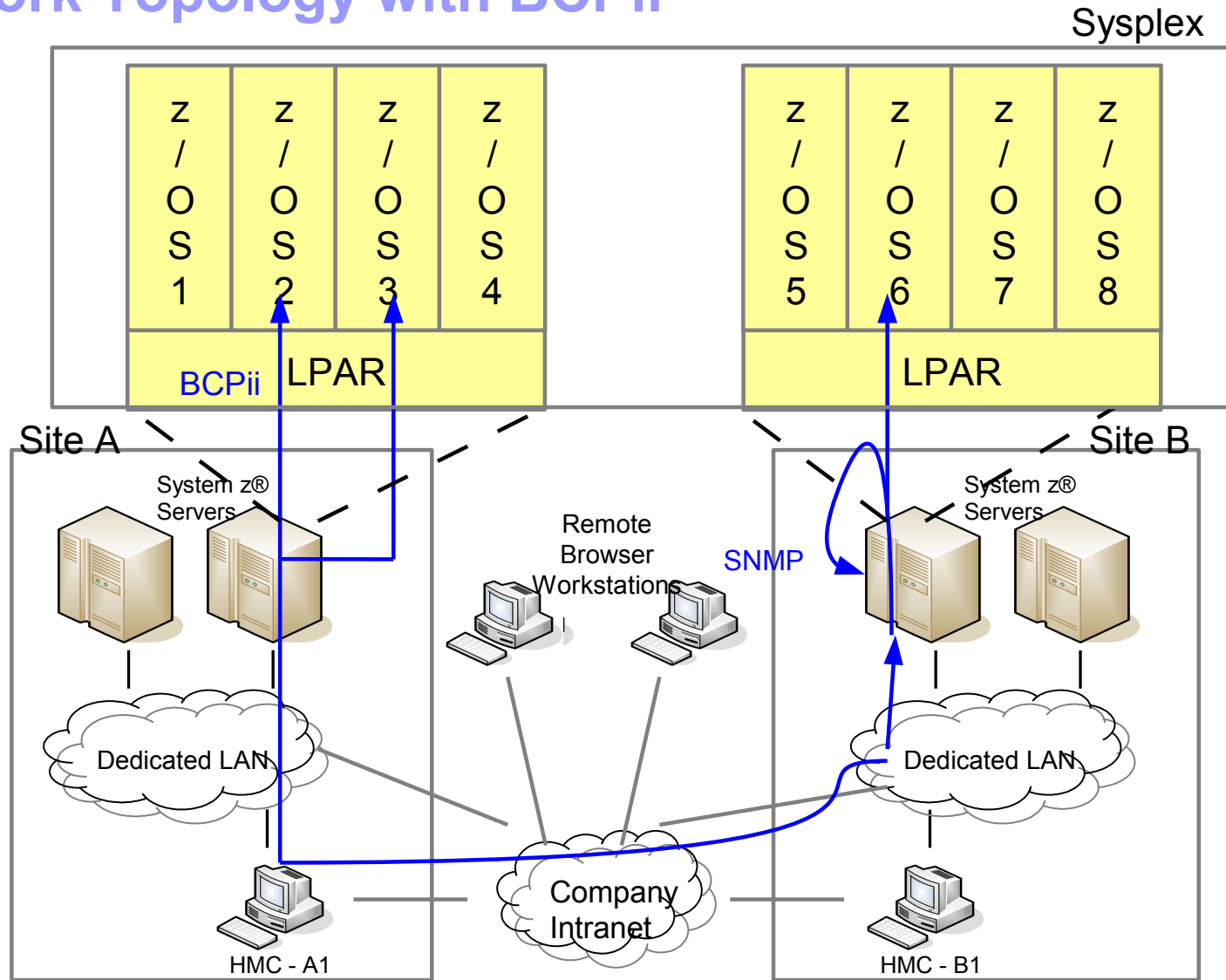
**CLICK-YES**



**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

## z/OS NIP Console Config for HMC on Startup

- **Configuration setup for HMC to be NIP (Nucleus Initialization Program) console (one example scenario):**
  - ▶ **When directed to Operating System messages and choose to only have the NIP console on the HMC Operating Systems Messages**
  - ▶ If there are no NIP (i.e. OSA, or 3274 control unit devices) consoles specified in the IODF or all of those NIP consoles are offline,
    - z/OS will automatically use the "system" console (Operating System Messages) to receive z/OS IPL messages.
    - A V CN(\*),ACTIVATE is not needed.
    - Once IPL is over (going green screen), if there are z/OS operator consoles defined and online, z/OS will use them and the "system" console will be deactivated.
    - To continue use of the "system" console HMC OS Msgs, the V CN(\*),ACTIVATE command will be required.
    - If there are no z/OS operator consoles available, the "system" console will continue to be used.
    - Note: The CONSOLxx parmlib member specification of AUTOACT is used to determine when the "system" console should be automatically activated or kept active after IPL. AUTOACT accepts a list of console names that when a console is active will cause the "system" console to deactivate. If all consoles in the AUTOACT list are offline, z/OS will automatically activate the "system" console.
  - ▶ More details in *z/OS V1R13 MVS Planning Operations* publication (Chapter 6, section "Initializing the System")

## 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

- ▶ February 4<sup>th</sup>, 4:30 – 5:30 PM
  - **12808**: *IBM System z Hardware Management Console (HMC) 2.12.0*
- ▶ February 5<sup>th</sup>, 11:00 AM – 12:00 PM
  - **13035**: *BCPii Programing Beyond the Basics for the z/OS System Programmer*
- ▶ February 5<sup>th</sup>, 12:15 – 1:15 PM
  - **12255**: *The HMC Is a Fantastic Feature of the zEnterprise, but What Mistakes Are You Making Securing It?*
- ▶ February 5<sup>th</sup>, 1:30 – 2:30 PM
  - **13086**: *zFlash Introduction, Uses, and Benefits*
- ▶ February 5<sup>th</sup>, 3:00 – 4:00 PM
  - **13057**: *zFlash Setup, Management and Configuration*
- ▶ February 6<sup>th</sup>, 9:30 – 10:30 AM
  - **13063**: *IBM zAware – Using Analytics to Improve System z Availability*
- ▶ February 6<sup>th</sup>, 11:00 AM – 12:15 PM
  - **13066**: *Setting up IBM zAware – Step by Step*

## Other SHARE Sessions of Related Interest

- ▶ February 6<sup>th</sup>, 3:00 – 4:00 PM
  - **12749 & 12750**: *Unified Resource Manager: HMC Ensemble Hands-on Labs*
- ▶ February 7<sup>th</sup>, 3:00 – 4:00 PM
  - **12948**: *z/OS Tuning Basics: Exploring the World of Hybrid, Blades, and the zManager*
- ▶ February 7<sup>th</sup>, 3:00 – 4:00 PM
  - **12859**: *zEnterprise System - z/OS IEDN Network Design & Implementation*
- ▶ February 7<sup>th</sup>, 4:30 – 5:30 PM
  - **13091**: *zBX Capacity Sizing using IBM zBladeSizer and IBM zBladeEXTR*

## Registering for IBM Resource Link Access

- **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->zEC12->Publications)
  - ▶ IBM SC28-6919: Hardware Management Console Operations Guide (Version 2.12.0)
  - ▶ IBM SC28-6920: Support Element Operations Guide (Version 2.12.0)
  - ▶ IBM SB10-7030: Application Programming Interfaces
  - ▶ IBM SC28-2605: Capacity on Demand User’s Guide
  - ▶ IBM SB10-7154: Common Information Model (CIM) Management Interfaces
  - ▶ IBM SB10-7156: PR/SM Planning Guide
  - ▶ IBM SA22-1088: System Overview
  - ▶ IBM SC27-2623 Advanced Workload Analysis Reporter (IBM zAware) Guide
- Available from IBM Resource Link: Library->zEC12->Technical Notes
  - ▶ System z Hardware Management Console Security
  - ▶ System z Hardware Management Console Broadband Remote Support Facility
  - ▶ System z Activation Profile Update and Processor Rules

## Reference Documentation (cont.)

- SHARE Conference in Orlando, August 2011
  - ▶ ***“IBM System z Hardware Management Console (HMC) 2.11.0 (including some 2.11.1 Updates)”***
  - ▶ Presenter: Brian Valentine
  - ▶ Presentation url:
    - <http://www.share.org/d/do/4297>
  
- SHARE Conference in Orlando, August 2011
  - ▶ ***“IBM zBX (System z BladeCenter Extension) HMC (Hardware Management Console) Hardware & Operational Management”***
  - ▶ Presenter: Brian Valentine
  - ▶ Presentation url:
    - <http://www.share.org/d/do/4218>

# Trademarks

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

DS8000	PR/SM	Z9*
ECKD	Redbooks*	z10
FICON*	System x*	z10 Business Class
GDPS*	System z*	z10 EC
GPFS	System z9*	z/OS*
HiperSockets	System z10*	z/VM*
IBM*	Tivoli	zEnterprise
IBM (logo)*	WebSphere*	
InfiniBand*		
Parallel Sysplex*		

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries. Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. UNIX is a registered trademark of The Open Group in the United States and other countries. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

\* 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.