IBM zBX (System z BladeCenter Extension) HMC (Hardware Management Console) Hardware & Operational Management

March 1, 2011

SHARE in Anaheim

Brian Valentine
HMC Development
bdvalent@us.ibm.com
File Updated: 2-24-11

IBM Systems

SHARE Session 9026

Topics

Topics (cont.)

Introduction

► Hardware/Operational Management

- zBX Integration will attempt to provide the System z value propositions of each of the Management disciplines covered today by HMC and SE
  - Concurrency
  - Security
  - Automatic configuration

► **zBX blades truly integrated into system**

- Not seen as an external control unit
- Logically seen as processor, but more like a Network Attached service device.
- From a packaging perspective, the analogy is that Blade Centers should be considered like an I/O Cage in System z, and blades are similar to channels within that I/O cage.
- 95 % target of task via GUI or API function is for CPC (system)
- 5 % (or less) uses a specific target of z Blade Extension object

► **z Blade Extension** Types

- Acceleration:
  - **ISAOPT (IBM Smart Analytics Optimizer)**
    - ♦ DB2 assist offload processing
  - **DataPower XI50z (IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise)**
    - ♦ XML offload processing
- Virtualization Workloads:
  - **POWER Blade**
    - ♦ Virtualized Image applications having strong affinity to System z workloads

zBX Hardware Integration

► zBX blades integrated into System z via Blade Centers (BladeCenter H)

  ● Can have up to 14 blades in BC (BladeCenter)

► Up to 2 Blade Centers per additional zBX rack

  ● **zBX racks(s) physically next to System z frame(s) (for service reasons)**
    – 25 meter cable limit
  ● zBX Blades network attach to SE internal mgmt network (HMC/SE Mgmt)
  ● zBX Blades also have separate physical network attachment for functional connection to System z operating systems
  ● No additional cooling for racks containing Blade Centers

► **1 to 4 additional racks (max of 8 BCs) per system (z196)**

  ● ISAOPT Limits:
    – Lower: 0 or 7 blades and Upper 56 blades
    – Multiple Config Offerings: blade number/intended to handle x amount of DB2 data
      ♦ XS: 7/0.5 TB, S: 14/1 TB, M: 28/2 TB, L: 42/3 TB, XL: 56/4 TB
  ● POWER Blade Limits: 0 to 112
  ● DataPower XI50z Limits: 0 to 28 (Double wide blade)
  ● ISAO homogeneous within BladeCenter
  ● POWER Blade and DataPower XI50z heterogeneous within BladeCenter

zBX Hardware Integration (cont.)

► **Blade Center power not integrated into system power**
  - Blade Center power comes off wall power and should always be on
  - **Blade power is associated with System z power (or to Repair or MES scenario)**
    – Default is blade power tied to system power.
    – Configuration option to allow CPC and Blade power to be disjoint (shared CEC support).
      ♦ Single System z system owns/manages zBX hardware in shared CEC environment.

► zBX hardware is defined for redundancy (n+1)

► HMC Console: used for both System z Hardware/Images, and zBX hardware/Virtual Servers
  - Generally, actions taken to zBX blades are done by targeting System z system object (zBX blades just another component of the system).
    – Not a blade server farm
  - Some initial customer concern for increased number of users of HMC
    – Two new Ensemble default userids: **ENSADMIN** and **ENSOPERATOR**
    – New zManager Task Roles and Resource roles
    – Details in Appendix A of IBM SC27-2606: *zEnterprise System Hardware Management Console Operations Guide for Ensembles*
  - **Discussions with customers on security and audit ability of HMC console**
    – No major issues found
      ♦ Enhancements in area of data offload/audit and userid template definitions (HMC 2.11.0)
    – HMC Security Whitepaper available on IBM Resource Link Tech Notes section
      ♦ See Additional Materials section for abbreviated presentation

System z196 and zBX Hardware Components

System z

zBX Infrastructure

Blades

Rack

Top-of-Rack Switch

BladeCenter Chassis

Ethernet & FC Cables

Switches (ESM, FC)

Power Dist. Units

Opt: Heat Exchanger, Power cord types

HS22 Blade (ISAOPT)

DataPower XI50z Blade

POWER Blade

Change Management

► **Same Base Functions as System z**

- View Firmware Information (Blade Center and Blades)
- Retrieve Firmware Changes
- Change Firmware Levels
- Backup/Restore Critical Data (zBX configuration data backed up as part of System z SE backup and restored on replacement of zBX)

► Benefits of zBX Firmware packaged with System z Firmware

- Tested together with System z Firmware GA and MCL/fix bundle releases
- Retrieve code as same integrated process of System z (IBM RETAIN or media)
  - No need to use separate tools and connect to websites to obtain code
- Utilize System z firmware features such as Digitally Signed Firmware
- Infrastructure incorporates System z concurrency controls where possible.
  - BC Firmware update fully concurrent, blades similar to Config Off/On controls
- Audit trail of all code changes in security log
- Automatic back out of changes to previous working level on code apply failures.

► **zBX Firmware**

- All zBX 'Firmware' repackaged as System z Firmware
- Blade Center: all code for BC chassis (Mgmt Module, power controls, fans, etc.) is firmware
- ISAOPT (zBX Blade FW example):
  - HS22 Subcomponents: BIOS (uEFI), IMM, I/O Adapter FW, Diagnostics
  - SE Management Agent
  - ISAOPT operating system (SLES) and ISAOPT application released as SW
    - ♦ 1st entitlement from SE media, subsequent download from DS5020 DASD
    - ♦ Exception to architecture: usually base zBX Blade OS is considered as System z FW
- External (Top Of Rack) Switches & BC Switches: vendor code in switches (Juniper, BNT, Q-Logic)
- **System z technical analysis of when and what to include with System z Base GA/Fixes**

Additional Firmware Details

- ► POWER Blade

  - Must have **PowerVM Enterprise Edition feature preloaded including license**
  - Lower Layer FW: PHYP, Partition FW, FSP, I/O Adapter
  - Image FW: VIOS (Virtual I/O Server) (AIX, Virtualization, IVM)
  - Component FW: SE Agent, HPM, FFDC, Auth, RAS, Tools, Surveillance Daemon
  - VIOS (4 GB) will drive a new media only MCL release for new release
    - Hopefully, only one per GA, if any
  - Other components are expected to be managed by MCLs via RETAIN or media
  - OSes running in Virtual Servers considered SW

- ► DataPower XI50z

  - 4 Loads (completely considered as FW)
    - Base
    - Base + DataDirect (Database Connectivity (ODBC) feature from DataDirect)
    - Base + Tibco (Tibco-EMS feature)
    - Base + DataDirect + Tibco
  - Loads consist of
    - Lower Layer FW: uEFI, IMM, I/O Adapter, Diagnostics
    - MCP
    - AMP Server
    - DP Application

Additional Firmware Details (cont.)

► Separation of MCL EC streams

- zBX Firmware: separate EC streams from zEnterprise legacy firmware (CFCC, LPAR, channels, etc.)

- zEnterprise FW (legacy & zBX) MCLs: recommend apply all
  – Controls allow separate apply if desired or exception
    ♦ Provided no dependency (generally the case)
  – zBX FW download/apply shouldn't gate zEnterprise legacy FW

- zBX Firmware EC streams hidden until Ensemble Management feature (w & wo zBX) applied
  – zEnterprise systems won't be downloading zBX FW until the system is included in an Ensemble
  – zBX FW towers in HMC and SE won't be started until configured for Ensemble Management

► zBX Blade Disruptive FW requires specific action by user to truly apply

- Manage zBX Blade Internal Code task
  – Similar to Channel Config Off/On exception
  – Quiesce request always part of action
  – Can try on one or more blades first/then apply to rest later

- zBX Concurrent FW applies to all hardware at time of install (no different than other zEnterprise FW)

SHARE Session 9026

System Information Change Management EC streams

SHARE Session 9026

System Information Change Management EC streams

R15: System Information - Mozilla Firefox: IBM Edition

9.60.15.114 https://9.60.15.114:9950/hmc/content?taskId=4&refresh=3

System Information - R15

Machine Information

EC number: N29802	LIC control level: 0009	Engineering Changes AROM
Type: 2817	Model number: M15	Serial number: 000020040C75
Version: 2.11.0		

Internal Code Change Information

Select	EC Number	Retrieved Level	Installable Concurrent	Activated Level	Accepted Level	Description
○	N29789					CHANNEL DIAGS
○	N29790	2	2	2	2	PCX LIC
○	N29791	1	1	1		OSA Express3 ICC
○	N29792	3	3	3	2	OSA Express3 Networking
○	N29793					OSA Express3 CDLC
○	N29794	12	12	12	11	FCS Ficon Express4 LIC
○	N29795	12	12	12	11	FCS Ficon Express8 LIC
○	N29796	5	5	5	5	CFCC LIC
○	N29797	7	7	7	6	LPAR HV LIC
○	N29798	1	1	1	1	ESCON CHANNEL CODE LIC
○	N29799	71	71	71	71	I390/PU-ML LIC
○	N29800					SE LIC Alert

EC Details...

Pending Actions

There may be some pending actions. Click "Query Additional Actions..." for more information.

Query Additional Actions...

OK   Help

Done

System Information Change Management EC streams

R15: System Information - Mozilla Firefox: IBM Edition

9.60.15.52 https://9.60.15.52:9950/hmc/content?taskId=63&refresh=182

System Information - R15

Machine Information

EC number: N29802 LIC control level: 0009 Engineering Changes AROM
Type: 2817 Model number: M15 Serial number: 000020040C75
Version: 2.11.0

Internal Code Change Information

Select	EC Number	Retrieved Level	Installable Concurrent	Activated Level	Accepted Level	Description
○	N29802	314	314	314	262	SE Framework
○	N29766	21	21	21	21	CRYPTO EXPRESS3
○	N29767	2	2	2		DataPower XI50z Base + SQL-ODBC + TIBCO-EMS
○	N29768	2	2	2		DataPower XI50z Base + TIBCO-EMS
○	N29769	2	2	2		DataPower XI50z Base + SQL-ODBC
○	N29770	2	2	2		DataPower XI50z Base
○	N29771	56	56	56	45	zVM Management Guest Firmware
○	N29772	6	6	6	5	POWER Blade Disruptive Components
○	N29773	59	59	59	46	POWER Blade Concurrent Components
○	N29774	11	11	11	10	POWER Blade Operating System
○	N29777	3	3	3	3	BladeCenter Enablement
○	N29778	6	6	6	6	BladeCenter Switches

EC Details...

Pending Actions

There may be some pending actions. Click "Query Additional Actions..." for more information.

Query Additional Actions...

OK Help

Done

Problem Management

► **Automatic Error Logging and FFDC Data Collection**

- Registering for traps and messages from BladeCenters, Switches, & zBX blades
- SE analysis of that information
- FFDC (First Failure Data Capture) automatic for errors
- Translation to System z SRCs (which may be displayed as Hardware Messages)

► Problem Analysis and Call Home Reporting

- **Electronically open a problem**
- **CE Dispatch with FRUs**

► **View Hardware Messages**

► **View Open Problems**

- Problems opened for zBX hardware
- Same view for any other zEnterprise hardware

► Manual Problem Reporting and Data Collection

- User perceived problems can also be reported manually
  - HMC/SE Report a Problem task selecting zBX entry
  - HMC/SE Transmit Service Data task

Serviceability Management

► **Guided Repair and Verification**

- SSR (Support Services Representative) driven**, not customer service**

► Process

- SSR arrives on site with FRUs in hand prior to service action
- Prepare for Service
    - Quisece operator request and SE validation, Power Off blade(s) if required
- SE Graphical Online Guided Mechanical Replacement
    - All under System z SE direction
- Validate after Service
    - If required, Power On blade(s), Load zBX blade code, Restore config data (DP)
    - Specific automatic verification depending on which FRUs serviced
- Infrastructure incorporates System z concurrency controls where possible.

Problem Management Example

SHARE Session 9026

Problem Management Example

Problem Management Example

Hardware Messages - P00MAUI7

P00MAUI7

Select	Date	Time	Message Text
☐	February 15, 2011	12:40:34 PM	zBX Problem [Problem # 15]

Details... | Delete | Select All | Deselect All | Cancel | Help

Problem Analysis - P00MAUI7

System name:	Local
Date:	Feb 15, 2011
Time:	12:37:32 PM
Blade Center Location:	C10B
Source:	POWER_O1

Problem Description

A DC fault has occurred in the specified power module, and the power module is shut down. Power module 01 is off. DC fault.

Corrective Actions

Service is required.

Impact of Repair

The repair of this problem can most likely be performed concurrent with CPC operations.

Request Service... | No Service | Display Sense Data | Delete | Cancel | Help

Problem Management Example

Hardware Messages - P00MAUI7

P00MAUI7

Select	Date	Time	Message Text
☐	February 15, 2011	12:43:33 PM	Service authorization complete

Details...   Delete   Select All   Deselect All   Cancel   Help

Problem Analysis - P00MAUI7

System name: P00MAUI7
Date: Feb 15, 2011
Time: 12:37:32 PM

Service information was transmitted successfully. The following information is associated with this problem.

Problem number: 15.

Problem management hardware number: 25743.

OK   Delete Message   Cancel   Help

Problem Management Example

Service History - P00MAUI7

View ▾   Close ▾   Sort ▾   Help ▾

Select	Date	Time	System Name	Problem Number	Status	Description
○	Feb 15, 2011	12:37:32 PM	P00MAUI7	15	Open	zBX Problem
○	Feb 15, 2011	12:03:21 PM	P00MAUI7	14	Open	Licensed internal code has detected a problem.

Service History - P00MAUI7

System name: P00MAUI7
Machine type: 2458
Machine model: 002
Machine serial number: 00000MNXK4BC
Problem management hardware (PMH) number: 25743
Problem number: 15
Problem type: 1
Problem data: 39Y7349,1, 34F3991,1

Date	Time	Problem State
Feb 15, 2011	12:40:34 PM	Problem detected
Feb 15, 2011	12:40:34 PM	Customer notified

OK   Help

Problem Management Example

Problem Analysis - P00MAUI7

Due to the user mode that you are currently logged on as, service cannot be requested for this problem.

Machine type:	2458	Refcode:	28BC0274
Machine model:	002	Extension:	7BB00001
Machine serial number:	00000MNXK4BC	Secondary Extension:	FF000000
Problem number:	15	Status:	

Problem Data

39Y7349,1, 34F3991,1

Parts List

Part Location	Part Number	Fix Percentage	Serial Number	Quantity
C10BPM01	39Y7349	70.0	K143400B001	1
C06ZPDUC	34F3991	20.0		1
C10BJ.P1-C06ZJ.01	26R0001	10.0		1

OK | Cancel | Help

Configuration Management

- ► VPD (Vital Product Data)
  - Physical configuration of Blade Center and Blades
  - **Stored into System z VPD records (for each FRU)**

- ► Edit Frame Layout (Configuration controls for unsensed hardware location)
  - Racks, switches, Blade Centers (identification of location for Service reasons)
  - Add/Remove of physical blades via 'Manage zBX Hardware' task
  - Separate controls for which blades to enable (see below)

- ► MES Support
  - Fully populate BladeCenter consecutive blade slot plugging strategy
  - No known issues with power, cooling, and availability

- ► **zBX Blade per Type Management Enablement paid feature**
  - Definition of maximum number of blades per zBX blade type
  - HMC/SE 'Perform Model Conversion' task 'Manage zBX Blade Entitlement' option allows SSR/Customer to define which blades should be managed up to the defined maximums
    - LICCC controls define high water marks

- ► Capacity On Demand
  - LICCC asset control approach (same as system processors)
  - CIU (Customer Initiated Upgrade) permanent
  - Temporary processor upgrade currently not seen as requirement

Operations Management

► Power On and Power Off Blades

- On system power off/on, all blades powered off/on
  - **Individual blade power controls for service**
  - **Optional Disjoint power control for system power off**

► Upstream SNMP/CIM API Automation Management

► Event Notification (based on logged events or state change)

- Pager, email, etc.

► Scheduled Operations (Firmware Update, Activate, Deactivate, etc.)

► Time Synchronization

- BC/zBX Blade sync time with SE/System z

► Network Settings for Operational Network

- GUI for setting TCP/IP address, Group Name, etc.

► Launch Full Device Console

- "Launch in Context" zBX blade GUI
  - Similar to HMC Single Object Operations of SE GUI
  - Example is DataPower XI50z GUI for editing XML Style sheets
  - Provided as a convenience feature for single console entry point to zBX blade
- **"Launch in Context" Blade Center Management Module GUI (Service)**

DataPower WebGUI Launch

CPC Configuration -> Manage DataPower XI50z

DataPower WebGUI
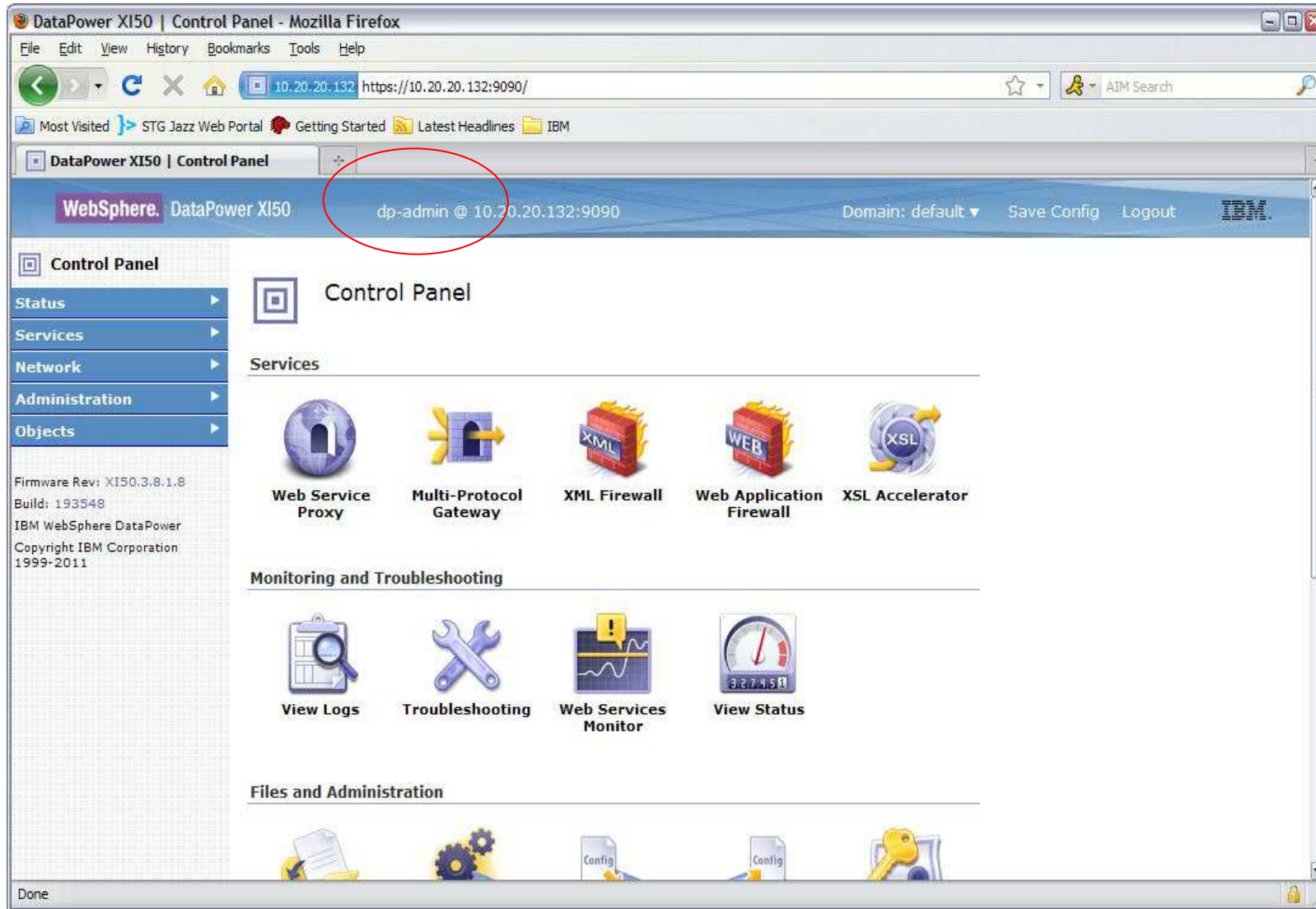
Performance Management

► SAD (System Activity Display):

- Performance data for zBX blades:
  - CPU usage
  - Memory usage
  - Storage I/O usage
  - Networking usage

► Energy Monitoring of Consumption and Temperature

- Blade Center information
- Also shown on SAD
- Aggregate data to IBM Director AEM (Active Energy Manager)

► Reporting Performance Data to IBM, TSAD (Transmit System Availability Data)

- Include energy information
- Include performance information
- Include firmware levels
- IBM Resource Link to provide
  - Alternative customer display of data
  - any alert notifications based on analysis

Monitoring ISAOPT, DataPower XI50z, Power Blades

Monitors Processor and Memory usage, POWER Blade also monitors Network & Storage

Business Management

► User Management

- automatically creates/manages userid and passwords for Service Network connectivity
- Launch in context GUI password validation as part of SE validation
  - Strong password rules supported
  - LDAP Server User Authentication
- DataPower XI50z customer defined users/passwords

► Security Auditing

- Audit trail of important changes (ie., firmware, configuration, etc.)
- Same infrastructure of security logs as is used for Common Criteria EAL6
  - More investigation needed to understand where zBX stands with EAL6

► Device Status and Details

- Showing BladeCenter and zBX blade Objects and status (power, quiesce, operational, error)
- Objects for launching specific actions to zBX blades
- New zBX Blades view (similar to processors, channels, cryptos)

► **Service Network Automatically configured/managed**

- More to come on zBX Networks

► Legal

- Copyright, license agreements included on HMC

► Documentation

- Physical planning, installation , operation and service

BladeCenters along with Processors, Channels, Cryptos, z Images

SHARE Session 9026

Blades view within the BladeCenters

SHARE Session 9026

Details of POWER Blade

Details of POWER Blade

Details of DataPower XI50z Blade

Details of ISAOPT Blade

R15: zBX Blade Details - Mozilla Firefox: IBM Edition

9.60.15.52 | https://9.60.15.52:9950/hmc/content?taskId=59&refresh=171

B.2.01 Details - B.2.01

| **Instance Information** | Acceptable Status | Product Information | Energy Management Information |

Status: Operating
Node type: Coordinator
Number of processors: 2
Memory size: 49152 MB

[Apply] [Cancel] [Help]

Done

R15: zBX Blade Details - Mozilla Firefox: IBM Edition

9.60.15.52 | https://9.60.15.52:9950/hmc/wcl/T3bb3

B.2.01 Details - B.2.01

| Instance Information | Acceptable Status | **Product Information** | Energy Management Information |

Type: IBM Smart Analytics Optimizer
Name: B.2.01
Machine type - model: 7870 - PEL
Serial number: KQWALGX
Location: B01BBS01

[Apply] [Cancel] [Help]

Done

Blades View with Unsorted Power Usage

Blades View with Sorted Power Usage

SHARE Session 9026

Blades View with Type Field Added (User Customized Views)

Tasks for ISAOPT Blades

Tightly Integrated/Loosely Coupled

- **Tightly Integrated** (zBX Infrastructure, ISAOPT, DataPower XI50z)
  - ▶ **System z Order Process and Mfg**
  - ▶ HMC/SE Managed Code
  - ▶ HMC/SE Call Problem Call Home and Guided Repair
  - ▶ Treated like all other System z integrated hardware

- **Loosely Coupled** (POWER Blade)
  - ▶ No System z Order Process and Mfg
    - ● **Customer obtains POWER Blade hardware by own means**
  - ▶ **Tightly Integrated after HMC/SE validation**
    - ● Validation step for correct hardware config and no functional hardware problems found during entitlement
    - ● Other 3 Tightly Integrated points apply
  - ▶ Created for potential of pricing discounts by Mass Distributors

POWER Blade Required Configurations

- *ftp://public.dhe.ibm.com/common/ssi/ecm/en/zsy03019usen/ZSY03019USEN.PDF*

PS701 Express blade	Feature Code	Config 1	Config 2	Config 3
Processor 3.0 GHz@150W		1	1	1
Processor Activations	8411	4	4	4
(quantity should equal 8 total)	8412	4	4	4
Memory kits		32 GB	64 GB	128 GB
8 GB (2 x 4GB)	8208	4	8	0
16 GB (2 x 8GB)	8209	0	0	8
HDD 300GB	8274	1	1	1
CFFh 10Gb Ethernet	8275	1	1	1
CIOv 8Gb FiberChannel	8242	1	1	1
PowerVM™ Enterprise Edition	5228	8	8	8
Required SW PID	**Feature Code**	**Config 1**	**Config 2**	**Config 3**
SW License PID 5765-PVE	0001	8	8	8
1 YR SWMA PID (5771-PVE) or	1191	Choose quantity of eight for either one year or three year (8 equates to one per activated processor)		
3 YR SWMA PID (5773-PVE)	0999			

2458 zBx Machine Type

► System z current hardware under System z MTM/SN (Machine Type Model/Serial Number) Service Contract

► zBX hardware under separate zBX MTM/SN (Machine Type (2458)/Model/Serial Number) Service Contract

- Single contract for all zBX hardware
  - Exception for DataPower XI50z blade
  - Own warranty under 2462 Service Contract per blade
- Order Process generated zBX MTM/SN delivered via VPDC media process.
- OEM field updated to System z unique identifier for BC, Blade, & Switch
  - System z Mfg process
  - Loosely Coupled Validation
  - System x field stock updated during System z Field Repair/Replacement

► Hardware validation/guidelines

- Only predefined hardware configs and OEM System z IDs are supported
- Only given System z Blade Extension types can execute in that hardware
- Only user enabled blades not exceeding LICCC high watermark per type will execute
- Otherwise, powered off
- zBX is **not** a Blade Server farm

zBX Networks Overview

► zBX Automatically Configured/Managed Networks

- **IEDN (Intra Ensemble Data Network)**
  - Functional Data network
    - ♦ Connections from System z OS to accelerator type zBX blades (ie., ISAOPT)
    - ♦ Connections between Virtual Servers within zBX blades to System z OS
  - Can span multiple zBXes
  - 10 Gb Ethernet network
- **INMN (Intra Node Management Network)**
  - System z Unified Resource Manager Management network
    - ♦ Hardware and Operational Management
    - ♦ Virtualization Life Cycle Management
    - ♦ Platform Performance
  - Limited to single zBX
  - 1 Gb Ethernet network

► See additional materials section for other SHARE sessions that go into more detail on zBX networks

zBX Networks Overview

Customer managed
Management Networks

HMC

Intra Node
Management Network

Management
Interfaces

Intra Ensemble
Data Network

Customer managed
Data Networks

SHARE Session 9026

zBX Switch Interconnection

- ► IEDN
    - Physical Separation of network switches from INMN
        - – TORs (Top Of Rack switches)
        - – ESMs (IBM BladeCenter Electronic Switching Modules)
    - Automatic detection and configuration of switches
    - New CHPID type (OSX) when connecting from LPAR in CPC for DataNetwork connections to zBX
    - See red network on next chart
        - – OSX to 10 Gb TOR switch to 10 Gb ESM to blade
- ► INMN
    - Physical Separation of network switches from IEDN
    - Automatic detection and configuration of switches
    - New CHPID type (OSM) when connecting to Virtual Server in CPC (ie, zVM) for Unified Resource Management purposes
    - See yellow network on next chart
        - – HMC to SE to BPH
        - – BPH to OSM
        - – BPH to 1 Gb TOR switch to 1 Gb ESM to blade
- ► Next chart notes:
    - Omits redundancy
    - Only shows one node in Ensemble

SHARE Session 9026

zBX Networks Overview
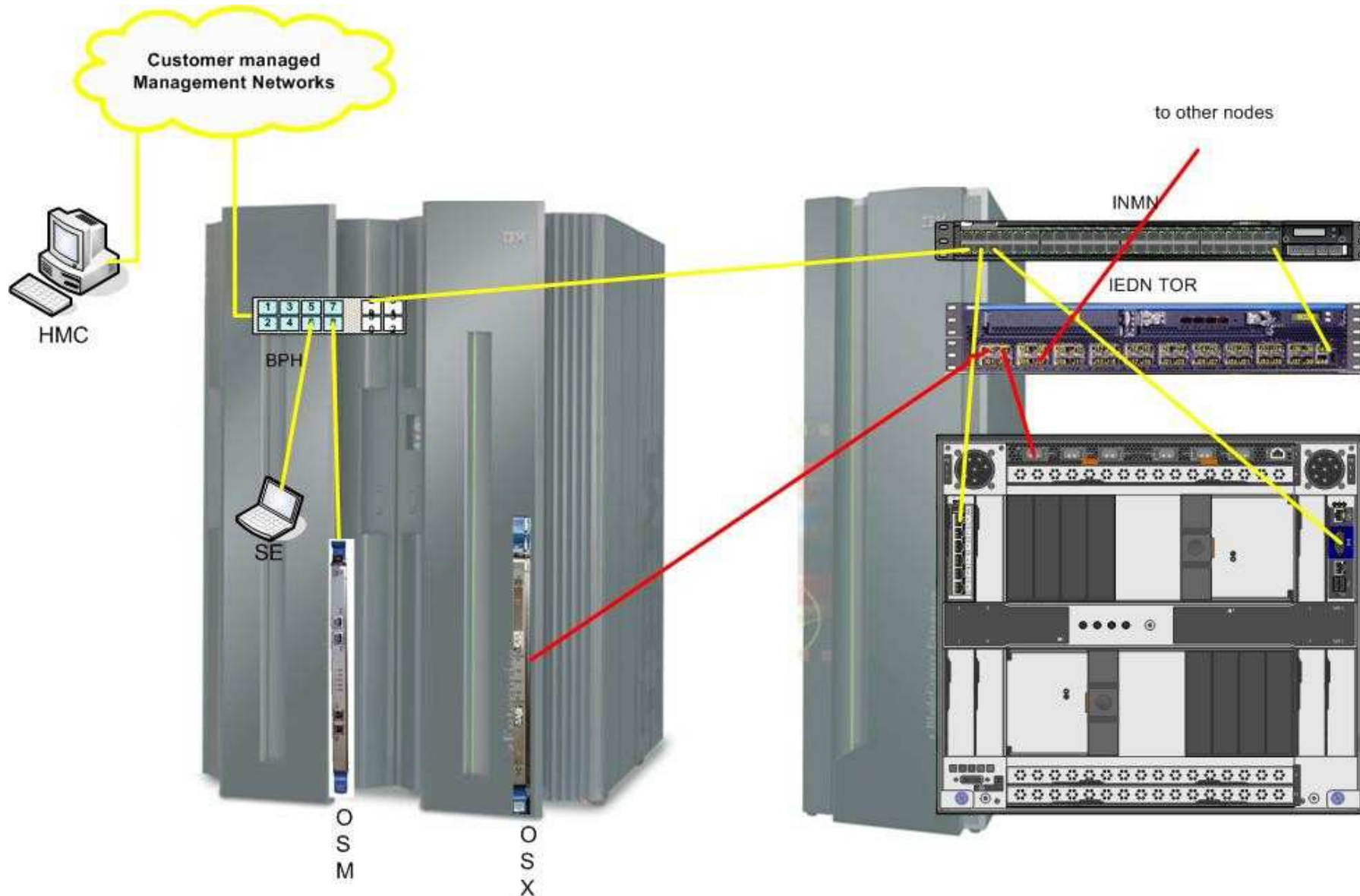
Summary

► zBX Integration to provide the **System z value propositions** of each of the Management disciplines covered today by HMC/SE

- Concurrency
- Security
- Automatic configuration

► zBX Hardware truly integrated into System z

- Generally not to be managed as individual objects
- Just another component in the system

Thank you for your time and consideration….

Brian Valentine

HMC/SE Team

Contact for any Questions:

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

Additional Materials (Backup)

- **Other SHARE Sessions of Related Interest**

- **HMC Security**

- **Registering for IBM Resource Link Access**

- **Notable HMC/SE Publications**

Additional Materials (Backup)

- **Other SHARE Sessions of Related Interest**

- **HMC Security**

- **Registering for IBM Resource Link Access**

- **Notable HMC/SE Publications**

SHARE Session 9026

Other SHARE Sessions of Related Interest

► March 1st, 9:30 - 10:30 AM

- **8316**: zEnterprise System – Network Architecture and Virtualization Overview (Part 1)

► March 1st, 11:00 AM - 12:00 PM

- **8317**: zEnterprise System – z/OS IEDN network design and implementation (Part 2)

► March 1st, 3:00 PM – 4:00 PM

- **9031**: IBM System z Hardware Management Console (HMC) 2.11.0

► **March 1st, 6:00 PM – 7:00 PM**

- **9071**: Roundtable: Shaping the Future of Mainframe Professionals Discussion

► March 2nd, 11:00 AM - 12:00 PM

- **8686**: System x Platform Performance Management

Other SHARE Sessions of Related Interest (cont.)

► March 2nd, 3:00 PM – 4:00 PM

- **9074**: Unified Resource Manager Hands-On-Lab

► March 2nd, 3:00 PM – 4:00 PM

- **8669**: Energy Management for zEnterprise

► March 3rd, 8:00 AM - 9:00 AM

- **8316**: zEnterprise Unified Resource Manager

Additional Materials (Backup)

- **Other SHARE Sessions of Related Interest**

- **HMC Security**

- **Registering for IBM Resource Link Access**

- **Notable HMC/SE Publications**

What is the HMC?

- **Is** an orderable feature of a System z® server consisting of a standard PC hardware platform

- **Is** a closed platform

- **Is** intended and required to be a network attached device

- **Is** serviced by IBM service personnel

- **Is not** an open operating platform

- Should be considered an **appliance,** not a server

Connectivity Options

AT&T
Global
Network

AT&T
Firewall

Internet

IBM
Firewall

IBM Servers

HMC -
A

HMC -
B

WAN

Client
Firewall

Private LAN

System z® Servers

Client
Workstations
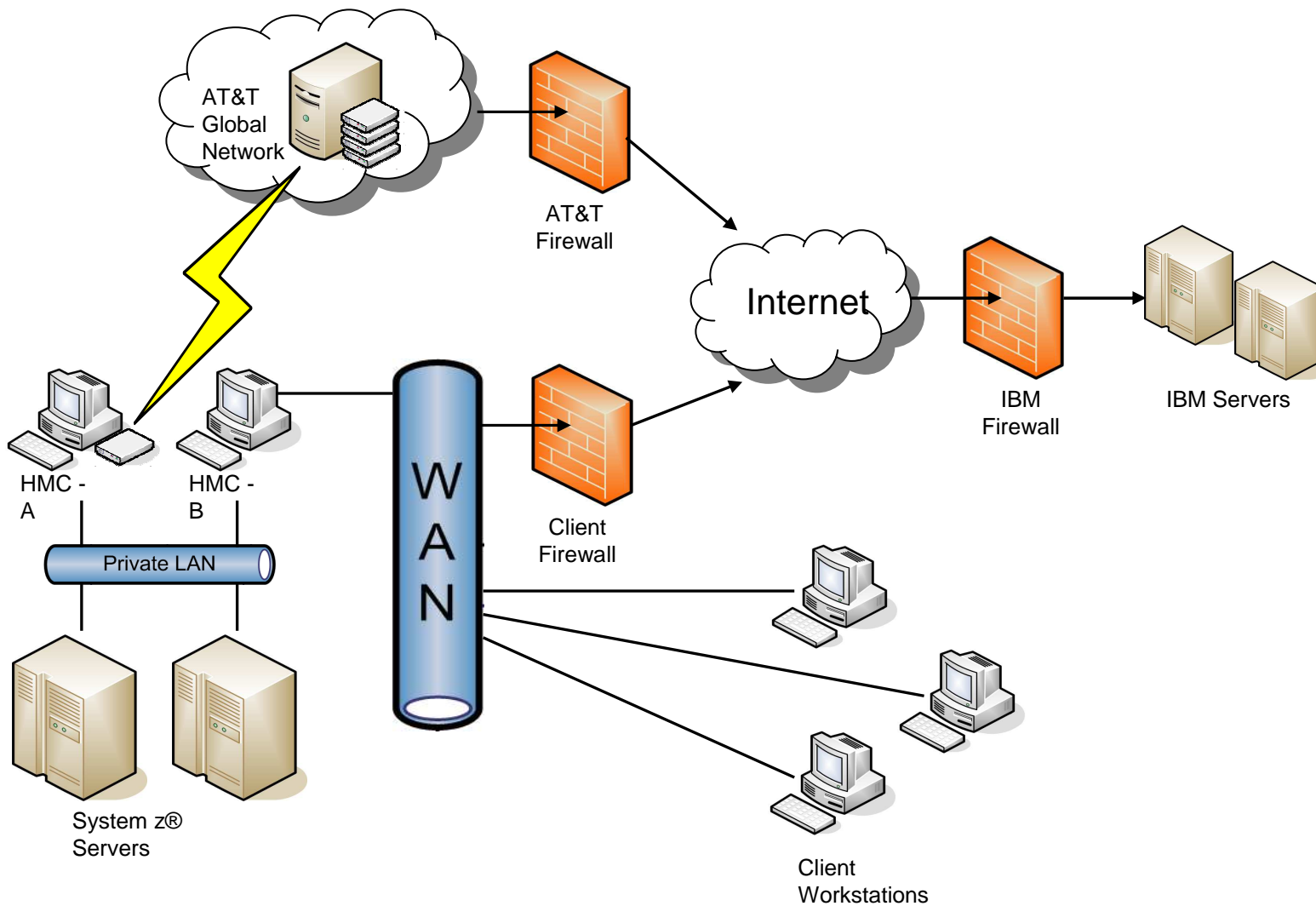
Best Practices

- Make sure the System z servers and other System z resources are physically located in a secure location, preferably an area that has physical access controlled and monitored, such as a raised floor.

- When possible install the HMC in the same type of physically secure environment as previously described for the System z resources.

- Connect the System z server and other resources only to a private, physically separate network; for example, connect all System z resources on a private raised floor network.

- Connect the HMC to the previously described private System z resources network. If connectivity to the HMC is needed from other networks in the customer's enterprise, provide this connectivity by connecting the second HMC network adapter to the appropriate customer network. (Remember: the HMC never routes network traffic, so the private System z network is still secure and isolated.)

Best Practices (continued…)

- Make sure the automatic logon capability of the HMC is not enabled in order to prevent the HMC from being logged on while unattended.

- Unless required, make sure that remote access to the HMC is disabled. If remote access is required, make sure to only allow remote access for the specific userids that require this type of access.

- At a minimum, change the passwords for all the default HMC userids. A more secure approach is to remove all of the default userids and define a userid for each individual user of the HMC.

- Do not share HMC userids among multiple people.

- Define password rules that adhere to the guidelines for the customer enterprise and make sure each userid is configured to use this password rule. If no guidelines exist, then make sure each userid is configured to use the "Standard" password rule.

- Make sure each userid is only permitted access to the tasks and managed resources needed to perform their job responsibilities.

Best Practices (continued…)

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

- Unless required, make sure all automation interfaces of the HMC are disabled. If automation is required, then make sure to configure each of these interfaces in a secure manner (for example, do not use common authentication tokens or world-write types of access).

- 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.

SHARE Session 9026

End user operational control

- **Secure SSL based remote access (optional)**

- **Full complement of certificate management capabilities**

- **Complete user management suite**
  - ► **Full function user definition**
  - ► **Highly flexible password rule definition**
  - ► **Centralized authentication using LDAP**
  - ► **Full access controls for tasks and resource allowed for each user (i.e. User Roles)**

- **Automatic replication of configuration data**

Network

- Full function embedded firewall

- Completely closed by default; services opened as enabled

- SSL encrypted communications

- Secure outbound communications for problem reporting and patch retrieval

- **No** inbound communications

- Passes with flying colors IBM Research *"ethical hacking"* attacks

Security Logging

- Logging of all security related events

  - ► **User access and changes**

  - ► **Disruptive actions**

  - ► **Configuration changes**

  - ► **Change management activity**

  - ► **Remote support calls**

- Off load capabilities

SHARE Session 9026

HMC Security Summary

- **Standard PC based appliance used to manage System z® resources**

- **Default configuration provides for maximum security (i.e. remote access disabled, …)**

- **Full complement of application level security features (i.e. user and certificate management, …)**

- **Complete auditing capabilities**
  - ► **configuration changes,**
  - ► **user access,**
  - ► **disruptive actions, …**

- **Intended to be a network device**
  - ► **SSL encrypted communications**
  - ► **Full function firewall**

- **Allows for complete physical security**

HMC Security Paper Available On IBM Resource Link

- **Resource link url:** http://www.ibm.com/servers/resourcelink/

- **Sign into resource link with your registered id**

- **Select "Library" from the set of links on the left**

- **Select "z196"**

- **Select the "Technical Notes" by clicking on the tab'**

- **Select "System z Hardware Management Console Security"**

Additional Materials (Backup)

- **Other SHARE Sessions of Related Interest**

- **HMC Security**

- **Registering for IBM Resource Link Access**

- **Notable HMC/SE Publications**

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.**

Additional Materials (Backup)

- **Other SHARE Sessions of Related Interest**

- **HMC Security**

- **Registering for IBM Resource Link Access**

- **Notable HMC/SE Publications**

SHARE Session 9026

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 SC27-2606: zEnterprise System Hardware Management Console Operations Guide for Ensembles**

  - ► **IBM SC28-6895: Hardware Management Console Operations Guide (Version 2.11.0)**

  - ► **IBM SC28-6896: Support Element Operations Guide (Version 2.11.0)**

  - ► **IBM GC27-2607: zEnterprise System Ensemble Performance Management Guide**

  - ► **IBM GC27-2608: zEnterprise System Ensemble Planning and Configuring Guide**

  - ► **IBM SC27-2606: zEnterprise System Hardware Management Console Operations Guide for Ensembles**

  - ► **IBM GC27-2609: zEnterprise System Introduction to Ensembles**

- Available from IBM Resource Link: Library->z196->Technical Notes

  - ► **System z Hardware Management Console Security**

Trademarks

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

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

* 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.