



Centralizing Console and Log Management Across the zEnterprise

Mike Sine
IBM

February 7, 2013
Session Number 12461



Special Notices and Trademarks

Special Notices

This presentation reflects the IBM Advanced Technical Skills organizations' understanding of the technical topic. It was produced and reviewed by the members of the IBM Advanced Technical Skills organization. This document is presented "As-Is" and IBM does not assume responsibility for the statements expressed herein. It reflects the opinions of the IBM Advanced Technical Skills organization. These opinions are based on the author's experiences. If you have questions about the contents of this document, please contact the author at sine@us.ibm.com.

Trademarks

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

IBM, the IBM logo, Candle, DB2, developerWorks, iSeries, Passport Advantage, pSeries, Redbooks, Tivoli Enterprise Console, WebSphere, z/OS, xSeries, zSeries, System z, z/VM.

A full list of U.S. trademarks owned by IBM may be found at <http://www.ibm.com/legal/copytrade.shtml>.

NetView, Tivoli and TME are registered trademarks and TME Enterprise is a trademark of Tivoli Systems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, Internet Explorer, and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

Intel and Pentium are registered trademarks and MMX, Pentium II Xeon and Pentium III Xeon are trademarks of Intel Corporation in the United States and/or other countries.

Other company, product and service names may be trademarks or service marks of others.

Agenda

- **Introduction**
 - Centralized versus distributed management
 - A hybrid approach - combining the methodologies
 - Central area
 - Central collection
- **Where to start?**
 - Model z/OS mature practices
 - z/VM tools functionality (SCIF)
 - Console management
 - Syslog management
- **Enterprise event management**

Central vs Distributed Management

- **PROs of Central**
 - One place to look for messages
 - One system to maintain - simplifies maintenance, rules, alerts, etc
- **CONs of Central**
 - Shipping large number of messages across network
 - UDP reliability
- **PROs of Distributed**
 - Less Network traffic
- **CONs of Distributed**
 - Multiple systems to maintain
 - Multiple sources for support of business applications across the enterprise

A Hybrid Approach - Combining Methodologies

- The best of both worlds
 - May not be possible to completely centralize console and log management
 - Technically
 - Politically
 - Cost effectively
 - However, consolidating where appropriate/possible can realize some benefits

zEnterprise Makes Consolidated Management Easier

- Powerful z/VM hypervisor
 - Full OS with tools and applications
- Central area: Tightly integrated network(s) within zEnterprise
 - The reliability of log messages improves as the source generating the messages moves closer to the syslog server
- Central collection: Centralized operations and log storage

Agenda

- Introduction
 - Centralized versus distributed management
 - A hybrid approach - combining the methodologies
 - Central area
 - Central collection
- **Where to start?**
 - Model z/OS mature practices
 - z/VM tools functionality (SCIF)
 - Console management
 - Syslog management
- Enterprise event management

Where to Start

- z/OS has a mature management structure around the system console
 - NetView (or equivalent) enhances message attributes
 - Automated response to specific messages
 - Integration to enterprise level event monitoring
- z/VM
 - Someone needs to be watching the house (operations)
 - Focus often on distributed solutions for Linux on System z
 - z/VM and CMS guests often ignored
 - z/VM as a central base for Linux management often missed
- zBX
 - Introduces additional virtual and physical servers
 - Focus often on distributed solutions for these servers
 - Opportunity to include in Enterprise Management infrastructure
 - Geographical advantages
 - Architectural advantages

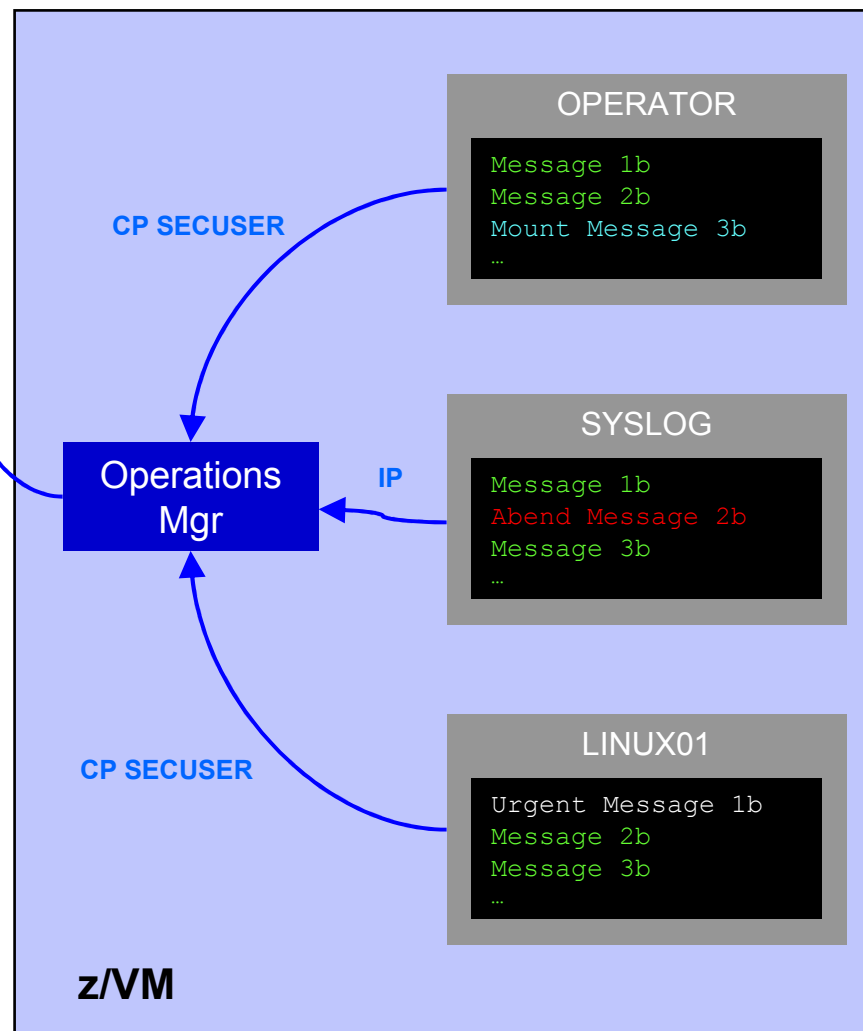
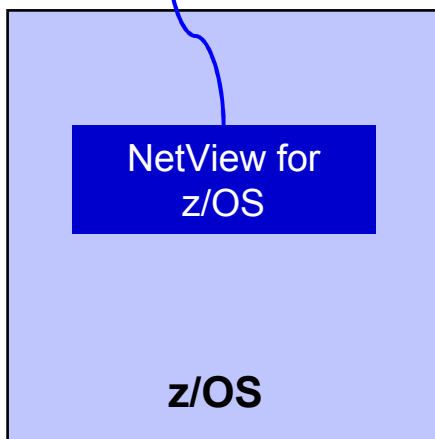
Where to Start

- Virtual server sprawl has increased distributed management structures in the traditionally centralized mainframe arena
- z/VM
 - Console management
- Linux on System z
 - Console management
 - Syslog management
 - Centralize Linux on System z with z/VM tools
- zBX
 - Centralize server logs on physical and virtual servers with z/VM tools
- Enterprise Management
 - Roll up appropriate console and log events to an enterprise alerting system

Consolidating Console and Log Management

IBM Tivoli Netcool\OMNibus

Node	Alert Group	Summary	Last Occurrence(+)	Count	Type	Expire Time
mwvtp	TEST	Test_Message	07/10/2008 02:45:57 PM	4	Problem	Not Set
hasd125	TESTEH	test_message_from_wif_2	08/19/2008 03:30:51 PM	2	Problem	Not Set
USIDHWZ\HSLV2	TESTMVS_SOURCE390		09/05/2008 09:38:25 AM	1	Problem	Not Set
OPMGRCT	WARN_EVENT	Fatal error on guest	04/24/2009 11:25:56 AM	2	Problem	Not Set
haske313LZ	ITM_Linux_CPU	Linux_High_CPU_Overload(title_CPU=10.	02/10/2010 07:39:46 PM	1	ITM Problem	Not Set
haske332	JJELD	A JJELD process running on haske332 ha	02/14/2010 11:55:10 PM	1	Problem	Not Set
9.85.208.193	Generic	Egg Neighbour Loss	02/15/2010 09:00:59 PM	3	Type Not Set	Not Set
Primary:HASLE337	ITM_NT_Monitored_Log	NT_Log_Space_Low(%_Usage=>95) ON	02/16/2010 12:12:47 PM	1	ITM Problem	Not Set
Primary:HASLE337	ITM_NT_Monitored_Log	NT_Log_Space_Low(%_Usage=>95) ON	02/16/2010 12:12:47 PM	1	ITM Problem	Not Set
9.82.24.129	Generic	Cold Start	03/03/2010 02:25:12 PM	1	Type Not Set	Not Set
haske332	MiscMissed	Disconnecting a@09522621 @09522621.1.	03/03/2010 04:54:00 PM	1	Problem	Not Set
haske332	Disc Event List	A e @09522621 @09522621.0 process e	03/06/2010 08:09:44 AM	1	Problem	Not Set
OPMGRCT	CPSEC	agent_is_aborting	03/08/2010 12:55:48 PM	26	Problem	Not Set
WSCPLEX:MVS:SV	ITM_Sysplex_DASD_Gr	KMS_No_Sysplex_DASD_Filter_Warn(Vol	03/09/2010 03:42:32 PM	2	ITM Problem	Not Set
Primary:HASLE337	ITM_NT_Logical_Disk	NT_Logical_Disk_Space_Warning(%_Fre	03/09/2010 04:28:37 PM	3	ITM Problem	Not Set
Primary:HASLE327	ITM_NT_Monitored_Log	NT_Log_Space_Low(%_Usage=>95) ON	03/11/2010 03:27:47 PM	1	ITM Problem	Not Set
HAVSVBL:MVS:SV	ITM_Sysplex_DASD_Gr	KMS_No_Sysplex_DASD_Filter_Warn(Vol	03/11/2010 03:30:17 PM	1	ITM Problem	Not Set
haske313PW	ITM_Disk_Utilization_LT	Warning threshold for disk utilization on	03/11/2010 11:24:46 PM	1	ITM Problem	Not Set
haske332	Generic	mttrapd probe on haske332: Heartbeat Me	03/12/2010 12:37:53 PM	2312	Type Not Set	Not Set
9.82.24.129	Generic	Authentication	03/12/2010 12:38:23 PM	1632	Type Not Set	Not Set
9.82.24.129	ZVM_SHMP	This user is abounding during demo. Send	03/12/2010 12:46:23 PM	9	Problem	Not Set



Where to Start: z/VM

- Console management for z/VM and Linux guests
 - PROP
 - Included in z/VM
 - Basic function to take actions based on z/VM console messages
 - IBM Operations Manager for z/VM
 - Provides z/OS style console management practices
 - *Higher level of functionality and flexibility over PROP*
 - *Console viewing and customizing*
 - *Take actions, including sending events to enterprise alerting system*
 - Other vendor solutions ...
- Syslog management for Linux on System z and zBX
 - IBM Operations Manager for z/VM
 - Consolidated log management and take action functions
 - Combined or separate views of each syslog
 - Take actions, including sending events to enterprise alerting system
 - Other vendor solutions ...

z/VM Tooling

- z/VM SCIF (Single Console Image Facility)
 - User logged on to a single virtual machine
 - Can control one or more disconnected virtual machines
 - Secondary user - controlling virtual machine
 - Primary user - disconnected virtual machine being controlled
- Example application using SCIF
 - Operations Manager for z/VM
 - Receiving console messages from primary user
 - Sending commands to primary user

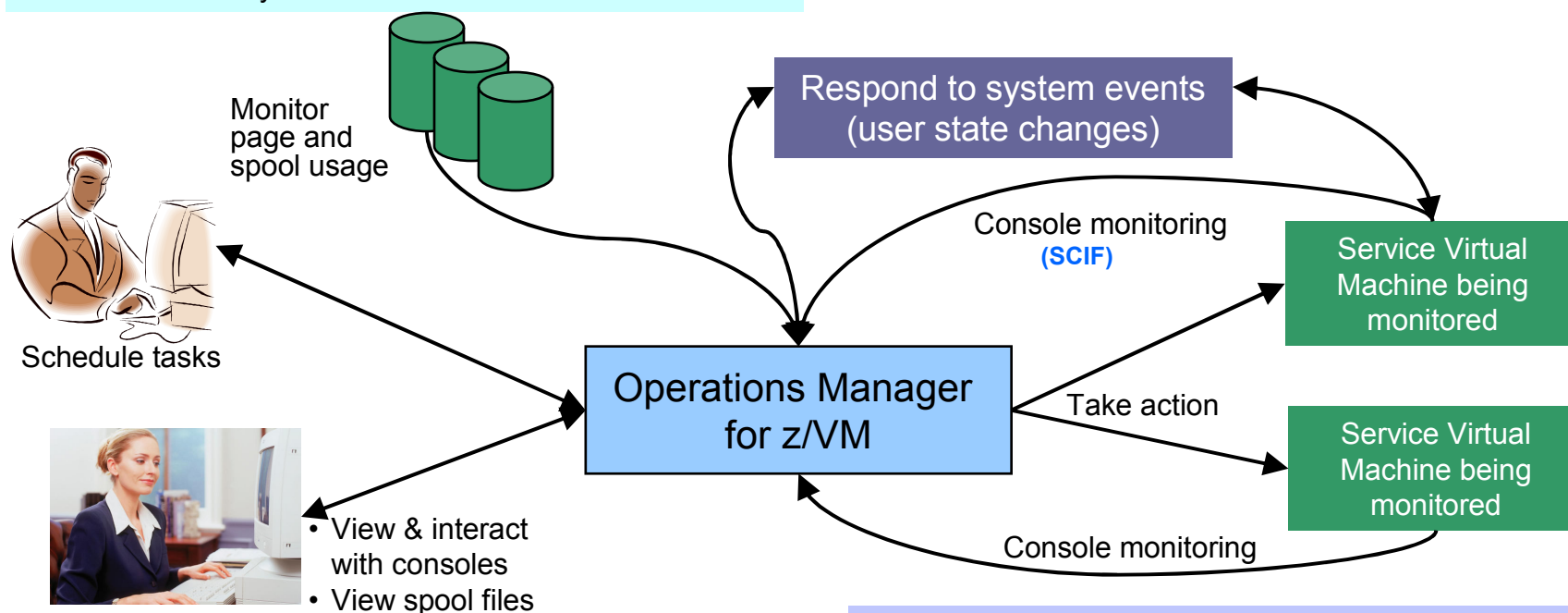
Operations Manager for z/VM

Increase productivity

- Authorized users to view and interact with monitored virtual machines without logging onto them
- Multiple users view/interact with a virtual machine simultaneously

Improve system availability

- Monitor virtual machines and processes
- Take automated actions based on console messages
- Reduce problems due to operator error



Automation

- Routine activities done more effectively with minimal operations staff
- Schedule tasks to occur on a regular basis

Integration

- Fulfill take action requests from performance monitoring products (e.g. OMEGAMON XE on z/VM and Linux)
- Send alerts to email, central event management systems (e.g. Netcool\OMNIBus), etc.



Monitor Service Machine Consoles

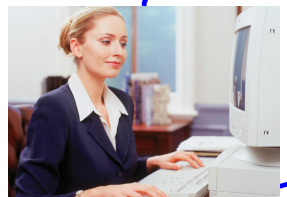
Test Data

OPERATOR

LINUX

TCPIP

syslog data



Operations Manager

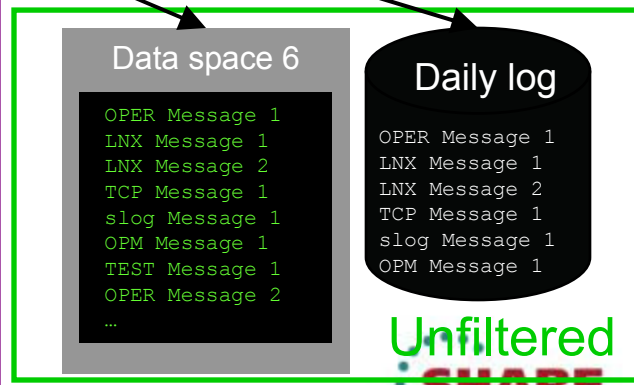
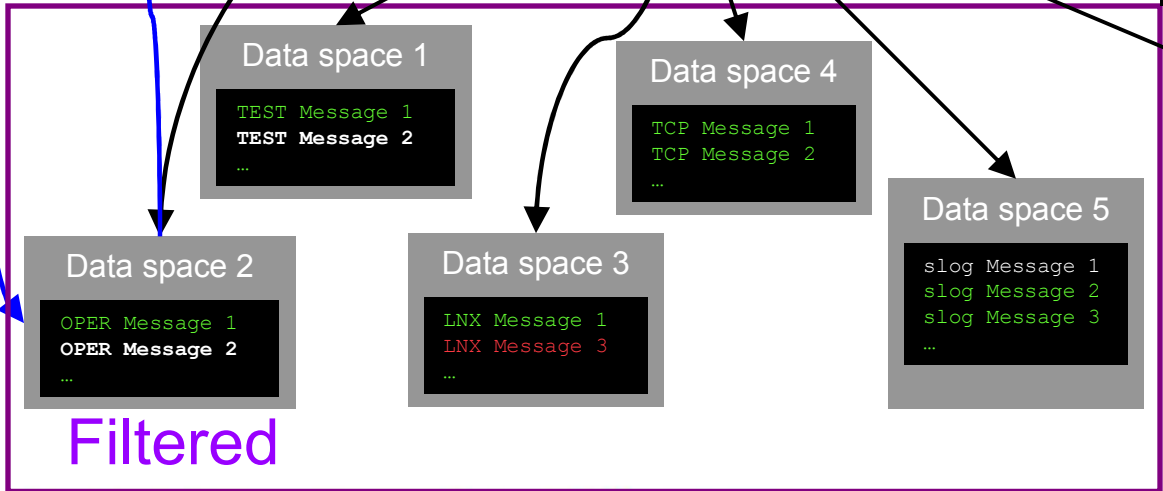
```
TEST Message 1
TEST Message 2
TEST Message 3
...
```

```
OPER Message 1
OPER Message 2
OPER Message 3
...
```

```
LNX Message 1
LNX Message 2
LNX Message 3
...
```

```
TCP Message 1
TCP Message 2
TCP Message 3
...
```

```
slog Message 1
slog Message 2
slog Message 3
...
```



Features and Functions

- Monitor service machine consoles
- Monitor page space and spool usage
- Monitor system events
- Schedule events/actions
- Take actions automatically based on monitoring results
- View and interact with monitored consoles from authorized user IDs
- Find and view spool files
- Dynamic configuration
- Separation of access control

Monitor Service Machines

- Define rules to
 - Scan console messages for text matching
 - Includes column, wildcard, and exclusion support
 - Optionally restrict to specific user ID(s)
 - Take actions based on matches
 - Change color, highlight, hold, or suppress a console message
 - CP or CMS commands
 - REXX EXECs
- Multiple rules can apply to one message
 - Rules processed in order of definition in the configuration file
 - FINAL option available to indicate no additional rules should be evaluated
- Take multiple actions based on one message
 - Chain actions together
- Rules apply to consoles received by local Operations Manager server

View and Interact with Consoles

- Authorized users can view live consoles of monitored service machines and guests
 - Multiple users can view the same console simultaneously
 - No need to logon to the service machine to see its console
 - Test data treated as a “console”
 - Views can be defined to look at a group of consoles in one view
- Full screen mode
 - Scroll up and down to view and search historical data
 - Auto scroll (on or off) as new output is displayed on the console
 - From command line, issue commands back to the monitored console
- Amount of data that is visible depends on specified or default data space size
- Rules/actions may modify the view
 - Suppress messages from the console
 - Hold or highlight messages with color, blinking, etc.
- Authorized users can view the log file
 - Can also request a copy of the log file from today or a previous day

View Syslog Messages - Automation

- Authorized users can view syslog messages as if they were live consoles of monitored service machines
 - Multiple users can view the same syslog “console” simultaneously
 - Views can be defined to look at a group of syslog “consoles” in one view
- Full screen mode
 - Scroll up and down to view and search historical data
 - Auto scroll (on or off) as new output is added to the syslog (and displayed on the “console”)
- Amount of data that is visible depends on specified or default data space size
- Rules/actions may modify the view
 - Suppress messages from the console view of syslog
 - Hold or highlight messages with color, blinking, etc.
- Included in the Operations Manager log file

Agenda

- Introduction
 - Centralized versus distributed management
 - A hybrid approach - combining the methodologies
 - Central area
 - Central collection
- Where to start?
 - Model z/OS mature practices
 - z/VM tools functionality (SCIF)
 - Console management
 - **Syslog management**
- Enterprise event management

Console Management

- Most z/OS customers provide a centralized management console in their operations center:
 - Often enhanced using IBM Tivoli NetView for z/OS
 - Highlight messages
 - Automate actions associated with known messages
 - Suppress messages
- Highlighted and held messages designed to grab the operator's attention.
- Most operations staff is accustomed to this type of message monitoring and quickly adapts to the look and feel.

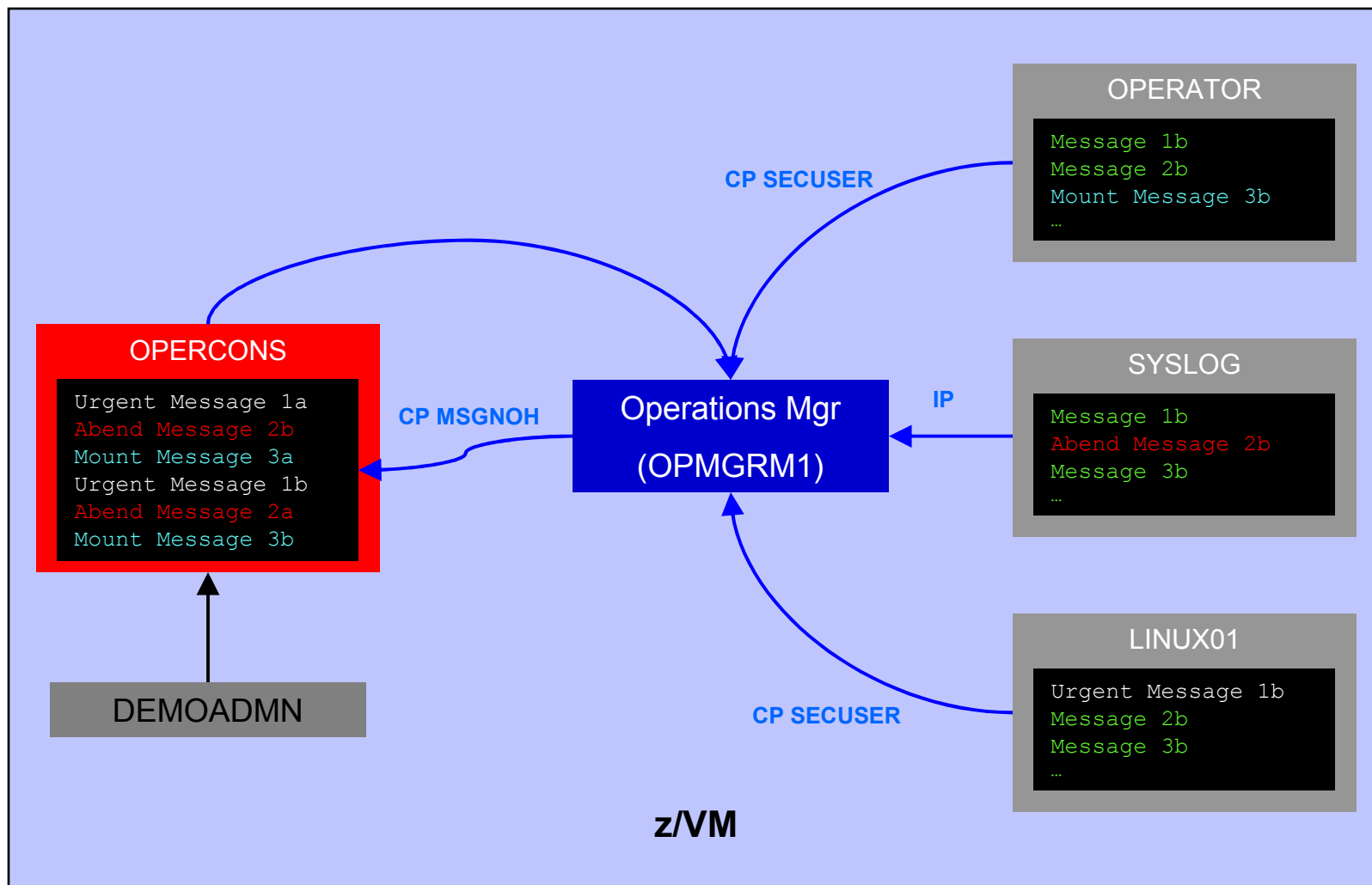
Console Management

- z/VM OPERATOR user ID similar to a systems console
 - May not be appropriate to suppress messages on OPERATOR
 - Not all important messages go to OPERATOR by default
 - Often don't want operations staff to access OPERATOR
 - High level authority
 - Reserved for sysprogs
- Prefer to create a custom console for the operations staff
 - Appropriate authorization
 - Message attributes
 - Automation
 - Mimic z/OS systems console
- Introduce z/VM to the operations staff

Console Management

- Create a new user ID as the operations console
 - Standard z/VM CMS guest user ID: OPERCONS
 - Only has permissions appropriate for the operations staff
 - Privilege class G, in our example
- Operations Manager for z/VM rules defined
 - Look for critical messages to be forwarded to OPERCONS (filter stage)
 - Apply attributes to them on OPERCONS for viewing by operations staff (attribute stage)

Creating a Central Console on One z/VM System



Console Management: Filter Stage

- First stage of processing
 - Determine if the console message received is important for operations staff
 - If yes, create a rule in Operations Manager
 - Define an action associated with the rule
 - Forward/send message to OPERCONS
 - *Sent in its original or modified (reworded) form*

Console Management: Filter Stage

*

```
DEFRULE NAME(ABEND),+  
  MATCH(*abend*),+  
  EXUSER(OPERCONS),+  
  ACTION(MSG2OPER)
```



*

```
DEFACTN NAME(MSG2OPER),+  
  COMMAND(CP MSGNOH OPERCONS &U : &T),+  
  OUTPUT(LOG),+  
  ENV(LVM)
```

*

Console Management: Attribute Stage

- Second phase of processing
- Apply audio and/or visual attributes to messages
 - Only on operations console
 - Draw attention to the operations staff indicating the severity of the alert

```
DEFRULE NAME(ABENDHLT),+  
MATCH(*abend*),+  
USER(OPERCONS),+  
ACTION(HLTHOLD)
```

*

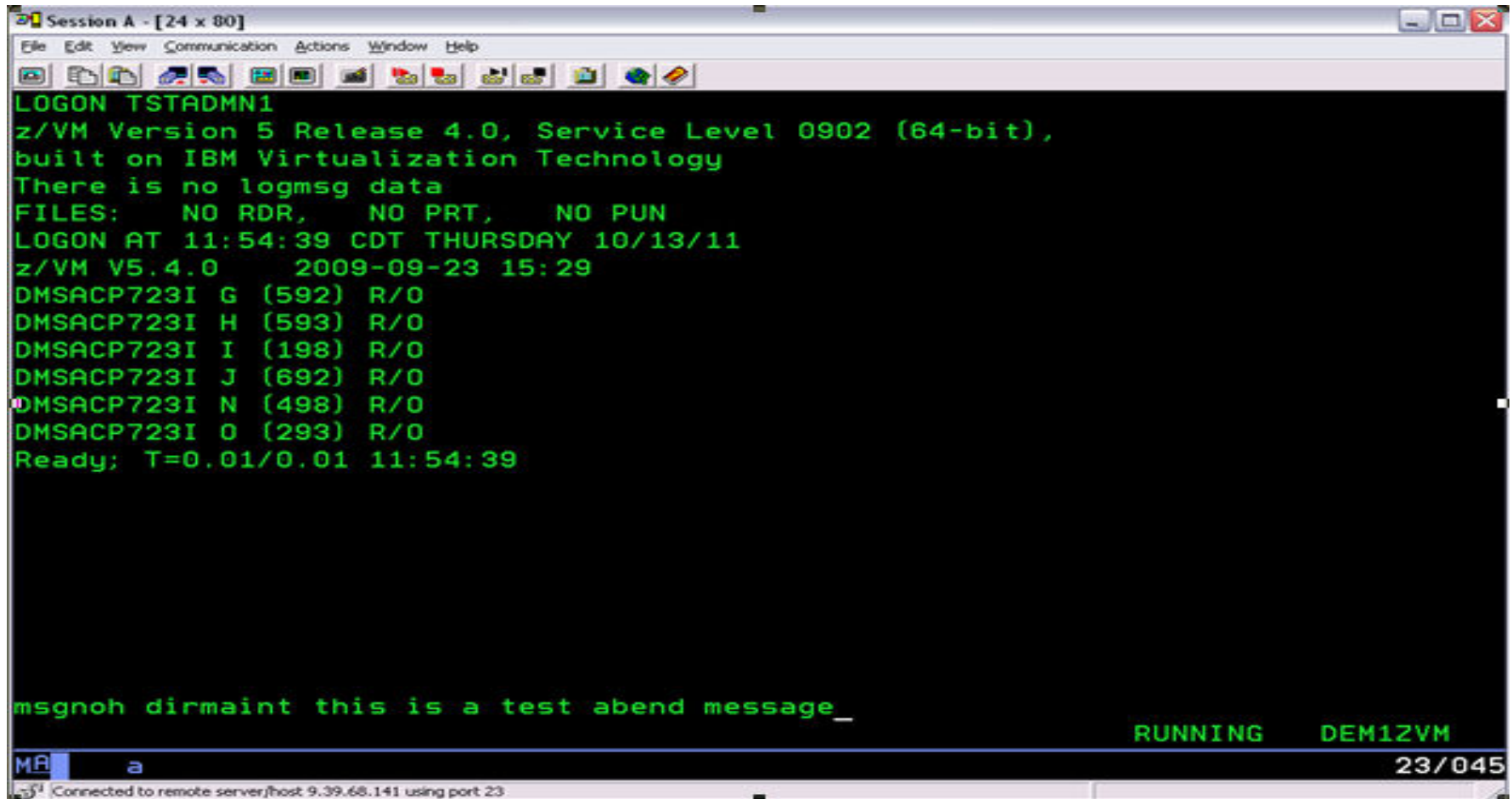
```
DEFACTN NAME(HLTHOLD),+  
INPUT(AHI,HLD)
```

*

Console Management: Attribute Stage

- Audio and visual attributes in Operations Manager:
 - AAL - Audible alarm
 - ABL - Blinking
 - AHI - High intensity / highlight
 - ARV - Reverse video
 - AUL - Underline
 - CBL - Blue
 - CCY - Cyan
 - CGR - Green
 - CPI - Pink
 - CRE - Red
 - CWH - White
 - CYE - Yellow
 - HLD - Holds the message when viewing the console until it is unheld

Console Management: An Example



```
Session A - [24 x 80]
File Edit View Communication Actions Window Help
LOGON TSTADMN1
z/VM Version 5 Release 4.0, Service Level 0902 (64-bit),
built on IBM Virtualization Technology
There is no logmsg data
FILES:  NO RDR,  NO PRT,  NO PUN
LOGON AT 11:54:39 CDT THURSDAY 10/13/11
z/VM V5.4.0      2009-09-23 15:29
DMSACP723I G (592) R/O
DMSACP723I H (593) R/O
DMSACP723I I (198) R/O
DMSACP723I J (692) R/O
DMSACP723I N (498) R/O
DMSACP723I O (293) R/O
Ready; T=0.01/0.01 11:54:39

msgnoh dirmaint this is a test abend message_

RUNNING  DEM12VM
MA a 23/045
Connected to remote server/host 9.39.68.141 using port 23
```

Console Management: An Example

```

Session A - [24 x 80]
File Edit View Communication Actions Window Help
10:16:53 OPERATOR : * MSG FROM TSTADMN1: TEST ABEND
10:18:37 OPERATOR : * MSG FROM TSTADMN1: REMOTE TEST ABEND
11:57:06 DIRMAINT : THIS IS A TEST ABEND MESSAGE
12:01:01 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:01:01
12:01:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.02 12:01:02
12:05:21 BKRCATLG : OUTPUT LINE 1 : CATALOG GRANULE D1
12:05:21 BKRCATLG : RETURN CODE: 0
12:06:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:06:02
12:11:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:11:02
12:16:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:16:02
12:21:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:21:02
12:26:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:26:02
12:31:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:31:02
12:36:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:36:02
12:41:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:41:02
12:46:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:46:02
12:51:02 DIRMAINT : DIRMAINT DEM12VM. - 2011/10/13; T=0.01/0.01 12:51:02
12:51:36 * -- Operations Manager VIEWCON session from TSTADMN1 entered the foll
12:51:36 altrcon
12:51:36 Unknown CP/CMS command
PF01= SCROLL PF02= VIEWPF PF03= END PF04= HELP PF05= HOLD PF06= FORMAT
PF07= UP PF08= DOWN PF09= CMS CO PF10= LEFT PF11= RIGHT PF12= RECALL

OPERCONS (Scroll) 11)
MA a 23/001
Connected to remote server/host 9.39.68.141 using port 23
  
```

Agenda

- Introduction
 - Centralized versus distributed management
 - A hybrid approach - combining the methodologies
 - Central area
 - Central collection
- Where to start?
 - Model z/OS mature practices
 - z/VM tools functionality (SCIF)
 - Console management
 - **Syslog management**
- Enterprise event management

Syslog Management

- Why consider Syslog management?
 - Linux on System z
 - Centralize visibility into all guests
 - zBX: zEnterprise BladeCenter eXtension
 - Manage distributed servers as part of zEnterprise
 - Bring the applications closer to the data
 - Centralize visibility into all physical and virtual servers inside (and outside) the zEnterprise
 - Remote systems
 - Business or application level monitoring

Syslog Management

- Ability to collect data across the zEnterprise and beyond
- Central location for collection
 - Across platforms
 - Virtual and physical servers
- Collect and manage log data on all servers consistently
 - Based on console management on mainframe
- Contributes to a comprehensive management solution
 - Consistent with qualities of service and capabilities of the mainframe

Syslog Management

- Loghost
 - Alias defined to a system's /etc/hosts file
 - Specifies a central destination for syslog messages
- Can define Operations Manager for z/VM as the Loghost
 - Central host for syslogs across the zEnterprise and beyond
 - Treats syslog data like console data
 - View it live
 - Take actions based on messages
 - Add it to overall system log

Syslog Management: Example

- Three step process
 1. Configure Operations Manager to listen on TCP/IP port for syslog data
 2. In TCP/IP, authorize Operations Manager to listen on the port
 3. Configure each virtual or physical server to send syslog data to
 - *IP address of z/VM system*
 - *IP port where Operations Manager is listening*

Syslog Management: Configure Operations Manager

- Specify the DEFTCPA configuration statement in Operations Manager configuration file

```
DEFTCPA NAME(LXSYSLOG),+  
TCPUSER(TCPIP),+  
TCPAPPL(GOMRSYL),+  
TCPADDR(000.000.000.000),+  
TCPPOINT(00514),+  
PARAM(LXSYSLOG03330417UTF8)
```



Syslog Management: Authorize Operations Manager to TCP/IP



- Authorize Operations Manager to listen on the TCPIP port
 - Add the following line to PROFILE TCPIP
 - Usually on TCPMAINT 198 disk

```
514 UDP OPMGRM1 ; OPERATION MANAGER SYSLOG PORT
```

- Recycle TCPIP
 - Or dynamically activate the change without restarting the TCPIP server

```
netstat obey port 514 udp opmgrm1 noautolog
```

Syslog Management: Configure Source Server

- Several syslog daemons exist for Linux, Unix, and Windows
 - syslogd
 - Original Syslog Daemon
 - syslog-ng
 - Content-based filtering
 - Rich filtering capabilities
 - Flexible configuration options (ex: port flexibility)
 - Adds TCP for transport
 - rsyslog
 - Features of syslog-ng...plus
 - On-demand disk buffering
 - Reliable transport over TCP, SSL, TLS and RELP
 - Writing to databases
 - Email alerting

Syslog Management: Source Server Tasks

- Linux syslogd configuration

- Update /etc/hosts

```
9.39.68.141    dem1zvm.demopkg.ibm.com    dem1zvm
loghost
```

- Configure /etc/syslog.conf

```
*.*                @loghost
*.debug           @loghost
```

- Restart syslogd

```
/etc/init.d/syslog restart
```

Syslog Management: Source Server Tasks

- AIX syslogd configuration
 - Update /etc/hosts

```
9.39.68.141      dem1zvm.demopkg.ibm.com  dem1zvm
loghost
```
- Configure /etc/syslog.conf

```
*.*                @loghost
*.debug            @loghost
```
- Restart syslogd

```
refresh -s syslogd
```

Syslog Management: Source Server Tasks

- Linux syslog-ng configuration
 - Configure `/etc/syslog-ng/syslog-ng.conf`
 - `destination <destname> { destdriver params; destdriver params; ... ; };`
`destination loghost { udp("9.39.68.141" port(515));};`
 - `log { source S1; source S2; ... filter F1; filter F2; ... destination D1; destination D2; ... };`
`log { source(src); filter(f_messages); destination(loghost); };`
- Restart syslog-ng
`/etc/init.d/syslog restart`

Syslog Management: Linux tasks

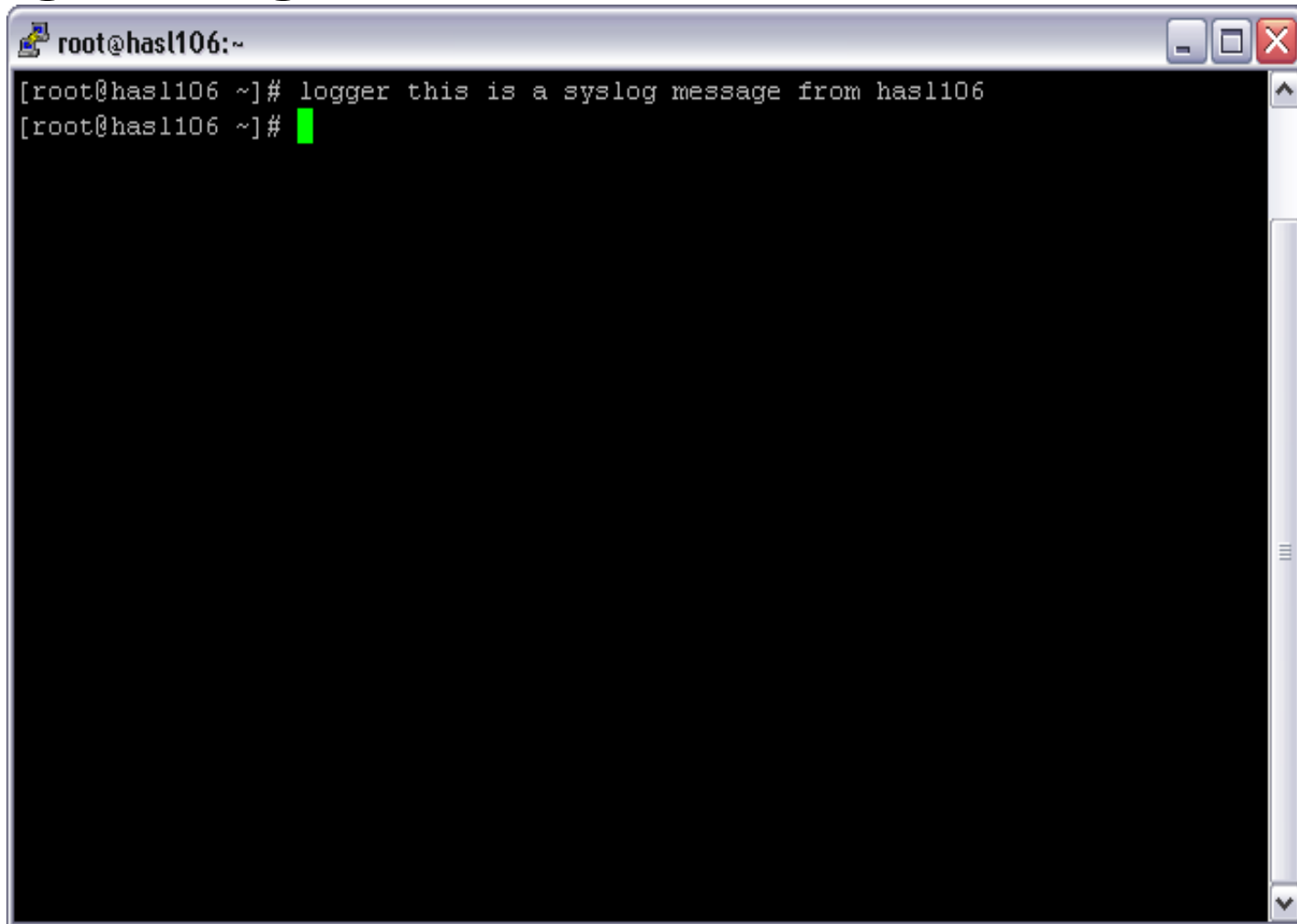
- Linux rsyslog configuration
 - Configure /etc/rsyslog.conf
 - Name/ip:port (port optional)
 - @ = UDP protocol, @@ = TCP protocol
 - *.* @9.39.68.141:514
 - *.* @@9.39.68.141:516
- Restart syslogd
 - /etc/init.d/service rsyslog restart

Syslog Management: Testing

- Simple and quick test: Linux “logger” command
 - Makes entries in the syslog
 - Shell command interface to the syslog(3) system log module
 - `logger [-isd] [-f file] [-p pri] [-t tag] [-u socket] [message ...]`

`logger this is a syslog message from has106`

Syslog Management: Test Scenario

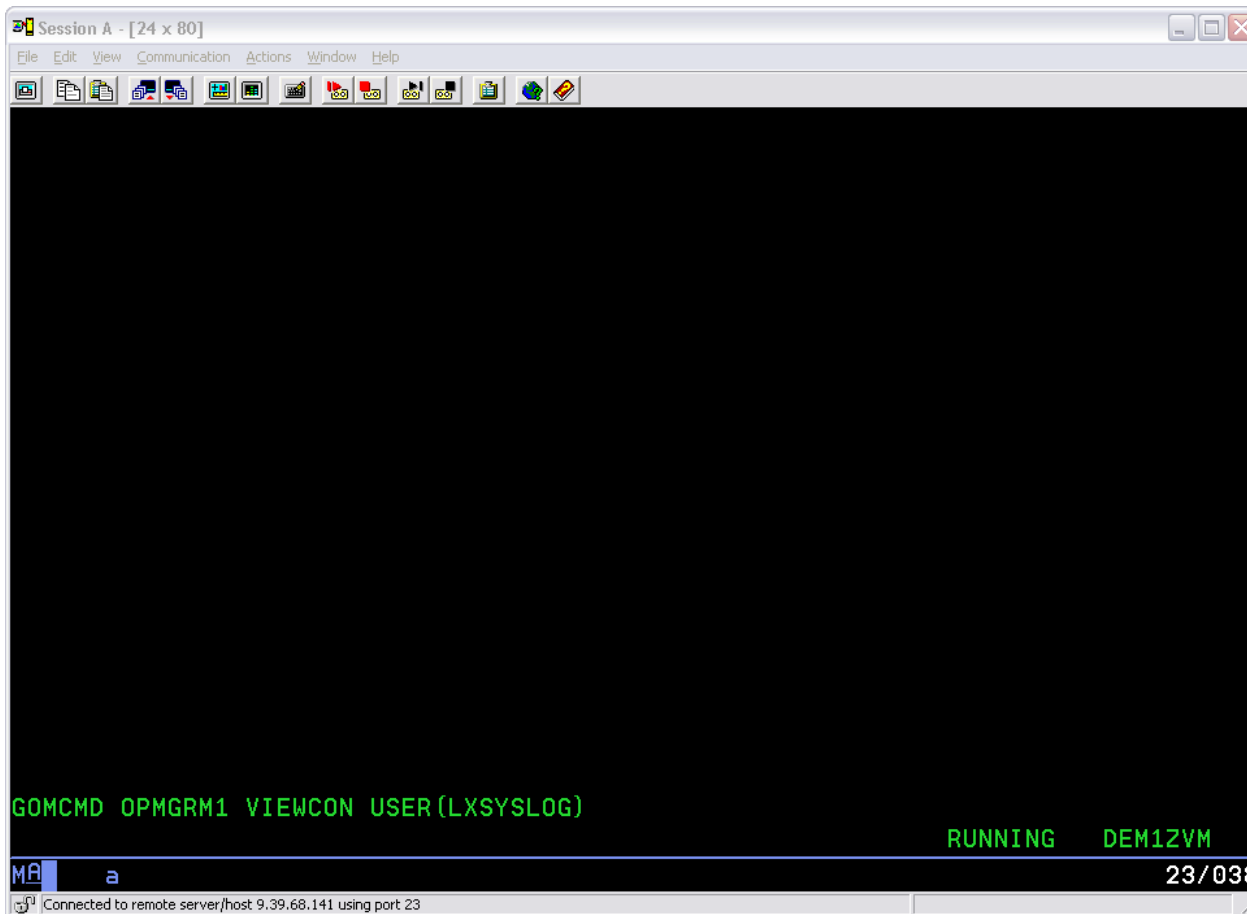


```
root@hasl106:~  
[root@hasl106 ~]# logger this is a syslog message from hasl106  
[root@hasl106 ~]#
```

Syslog Management: Test Scenario

- View the syslog from Operations Manager

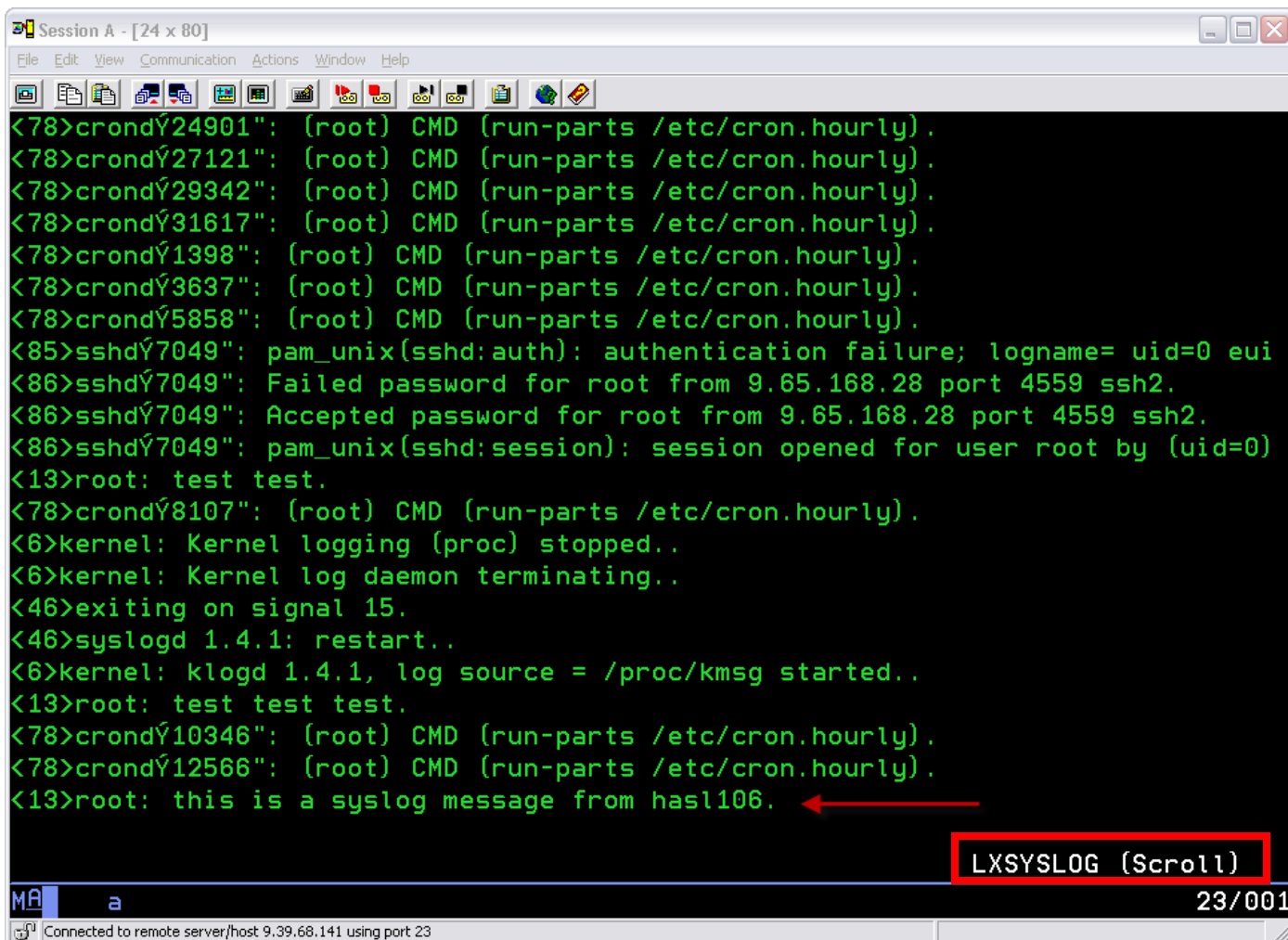
`gomcmd opmgrm1 viewcon user(lxsyslog)`



```
Session A - [24 x 80]
File Edit View Communication Actions Window Help
GOMCMD OPMGRM1 VIEWCON USER(LXSYSLOG)
RUNNING DEM1ZVM
23/038
Connected to remote server/host 9.39.68.141 using port 23
```

```
DEFTCPA NAME(LXSYSLOG),+
TCPUSER(TCPIP),+
TCPAPPL(GOMRSYL),+
TCPADDR(000.000.000.000),+
TCPPOINT(00514),+
PARM(LXSYSLOG03330417UTF8)
```

Syslog Management: Test Scenario



```
Session A - [24 x 80]
File Edit View Communication Actions Window Help
<78>crondY24901": (root) CMD (run-parts /etc/cron.hourly).
<78>crondY27121": (root) CMD (run-parts /etc/cron.hourly).
<78>crondY29342": (root) CMD (run-parts /etc/cron.hourly).
<78>crondY31617": (root) CMD (run-parts /etc/cron.hourly).
<78>crondY1398": (root) CMD (run-parts /etc/cron.hourly).
<78>crondY3637": (root) CMD (run-parts /etc/cron.hourly).
<78>crondY5858": (root) CMD (run-parts /etc/cron.hourly).
<85>sshdY7049": pam_unix(sshd:auth): authentication failure; logname= uid=0 eui
<86>sshdY7049": Failed password for root from 9.65.168.28 port 4559 ssh2.
<86>sshdY7049": Accepted password for root from 9.65.168.28 port 4559 ssh2.
<86>sshdY7049": pam_unix(sshd:session): session opened for user root by (uid=0)
<13>root: test test.
<78>crondY8107": (root) CMD (run-parts /etc/cron.hourly).
<6>kernel: Kernel logging (proc) stopped..
<6>kernel: Kernel log daemon terminating..
<46>exiting on signal 15.
<46>syslogd 1.4.1: restart..
<6>kernel: klogd 1.4.1, log source = /proc/kmsg started..
<13>root: test test test.
<78>crondY10346": (root) CMD (run-parts /etc/cron.hourly).
<78>crondY12566": (root) CMD (run-parts /etc/cron.hourly).
<13>root: this is a syslog message from hasl106.
LXSYSLOG (Scroll)
MA a 23/001
Connected to remote server/host 9.39.68.141 using port 23
```

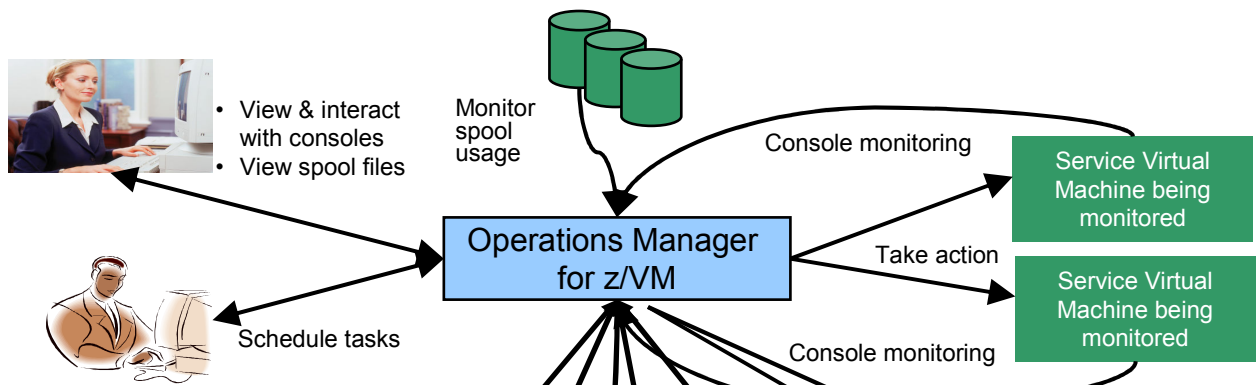
Logging Best Practices

- Source: www.syslog.org
- ✓ Forward syslog messages from clients to a secure syslog server
- ✓ Group “like sources” into the same log file (i.e. mail server, MTA, spamassassin and A/V scanner all consolidated to one file)
- ✓ Use an automated tool to establish a baseline of your logs and escalate exceptions as appropriate
- ✓ Review your records retention policy, if applicable, and determine if anything kept in logs falls under that policy. If so, establish retention periods based on the records policy. Legal requirements for keeping logs vary by jurisdiction and application
 - The “sweet spot” for log retention appears to be one year. Shorter than 1 year, and it is likely that key data would be unavailable in the wake of a long running attack, and longer than one year is most likely wasting disk space
- ✓ Include logs and log archives in a standard backup process for disaster recovery
- ✓ Change read/write permissions on logs files so they are not accessible to unprivileged user accounts

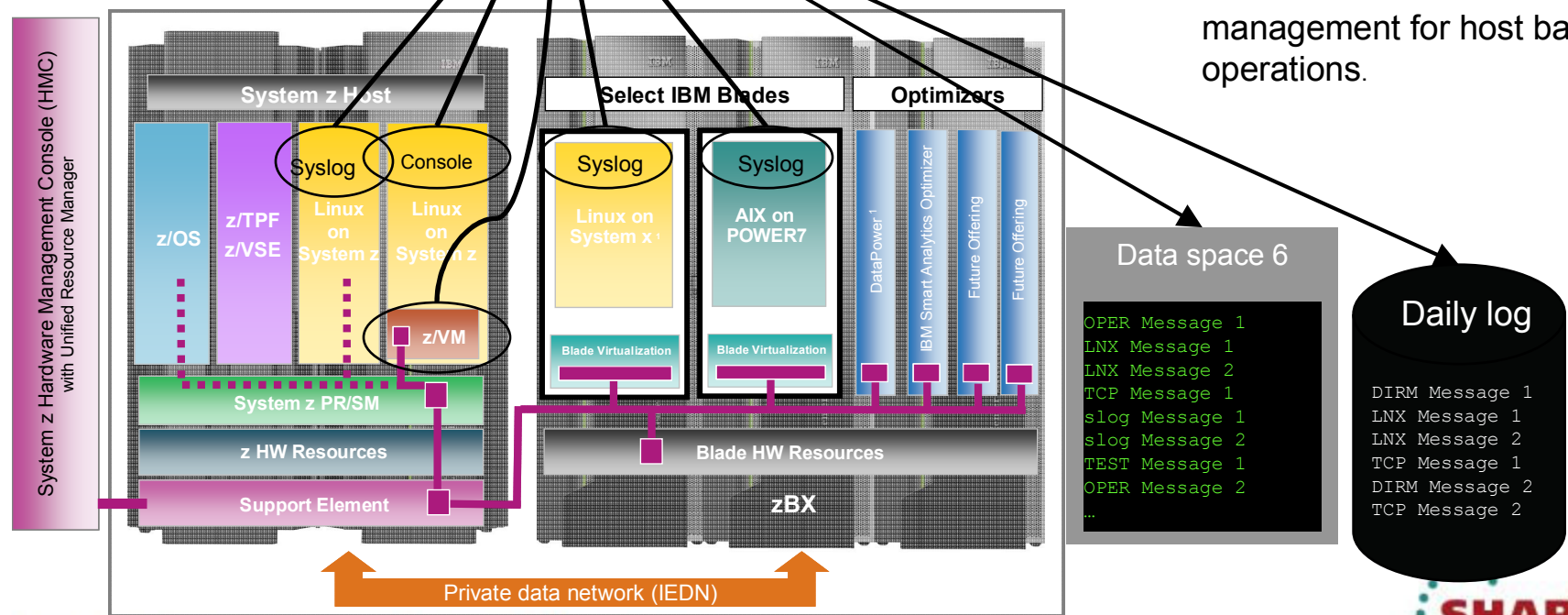
Logging Best Practices

- Syslog is a simple protocol
 - Easy to wrap security around it
- Goal: remove as many opportunities for the central syslog server to be compromised as practical
- Four aspects to hardening a syslog server
 1. The operating system
 2. The network
 3. The application
 4. The users and administrators
- Centralizing with a z/VM application on zEnterprise uniquely addresses these security recommendations of syslog.org

Enterprise level console/syslog management:



- Centralized console/syslog management.
- Message log console for operations and automation.
- Similar to z/OS console management for host based operations.



Note: All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Agenda

- Introduction
 - Centralized versus distributed management
 - A hybrid approach - combining the methodologies
 - Central area
 - Central collection
- Where to start?
 - Model z/OS mature practices
 - z/VM tools functionality (SCIF)
 - Console management
 - Syslog management
- Enterprise event management

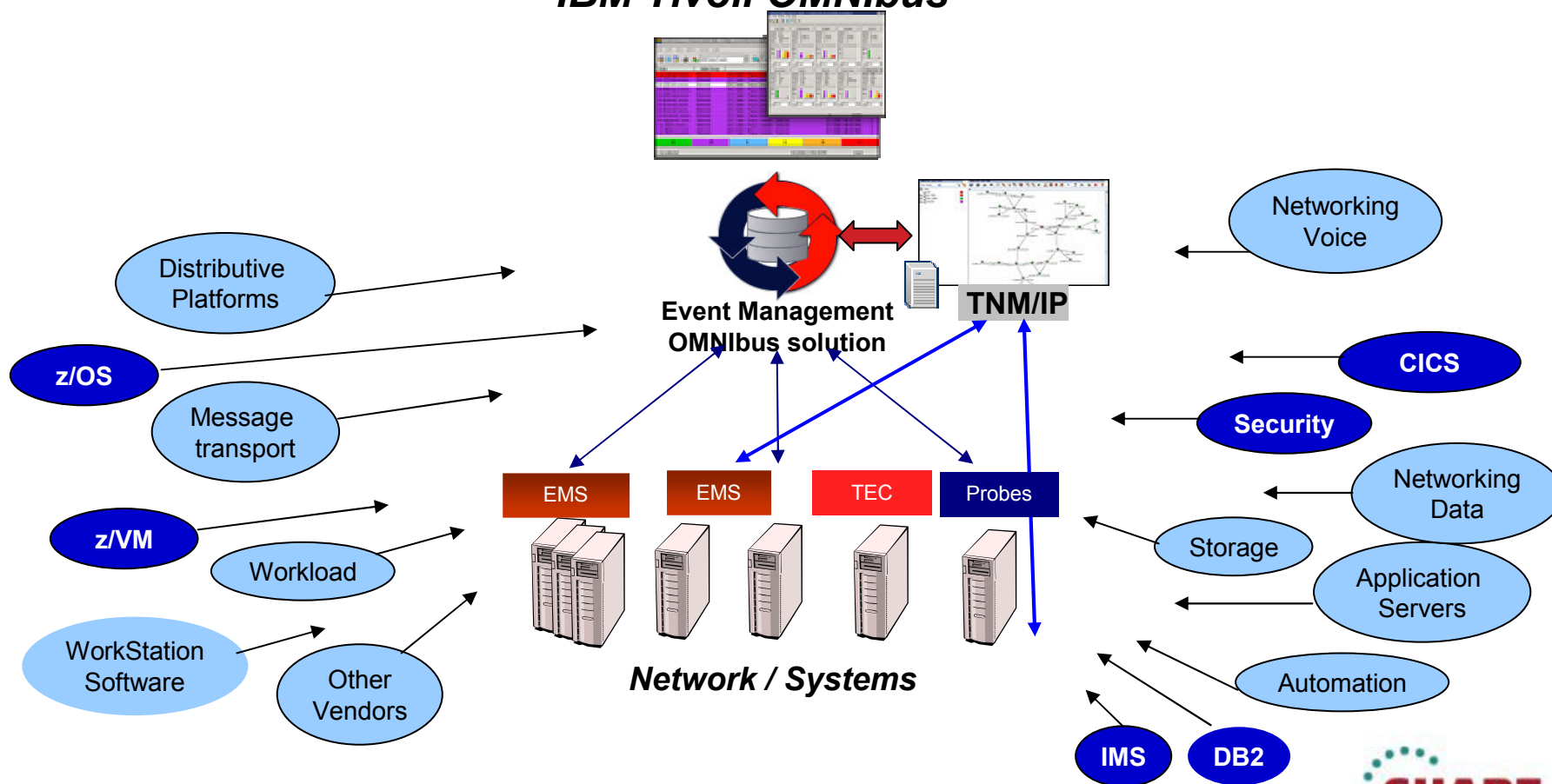
Enterprise Event Management

- z/OS tools today integrate with most enterprise management solutions
- z/VM tools collecting z/VM, Linux, and syslog data can also interface with enterprise management solutions
- Staging collection at the console and syslog management level
 - Allows pre-filtering - only forward appropriate events
 - Maintain and execute rules in one place

Tivoli z/OS Management

Integrated for end to end solutions

A Platform for Centralization of Events
IBM Tivoli OMNIbus



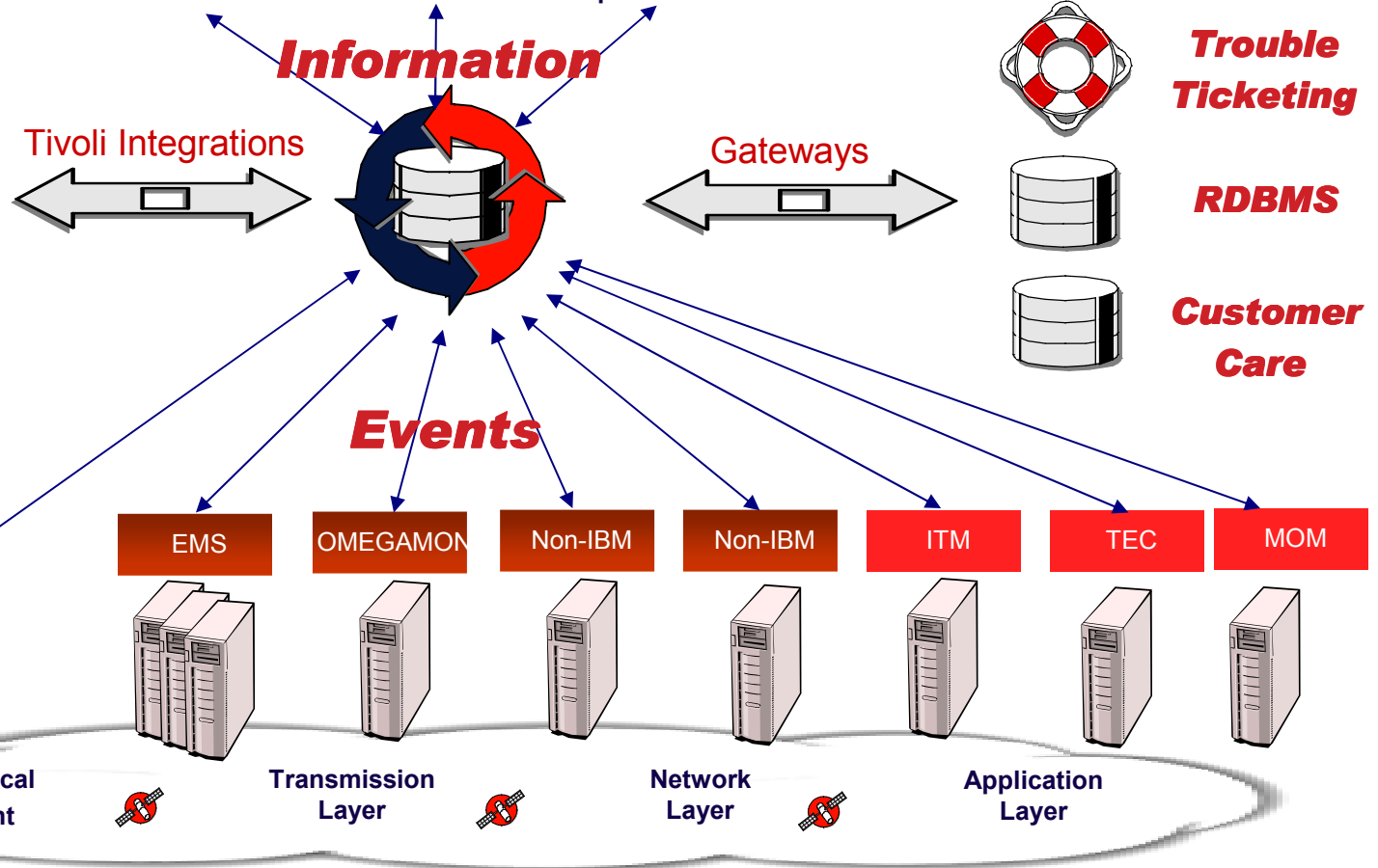
Tivoli Netcool/OMNibus : Event Management



Combined Web Views Business Views Operator Views

Tivoli

- ITNM
- Netcool/Impact
- Business Service Manager
- *ITM*
- *Event Pump for z/OS*
- *OMEGAMON XE*
- *NetView for z/OS*
- *Operations Manager for z/VM*



Summary

- z/OS console and event management is a mature process in most data centers
- z/VM tools can be used to bring z/VM and Linux consoles into the mature management process of the data center
- Centralizing Linux guest and remote syslog management with z/VM tools allows syslog data to
 - Be included in the mature processes of the datacenter
 - Meet syslog best practice standards
- z/OS and z/VM tooling integrates well with enterprise event management roll-up

Resources

- Creating an Event Console with Automation for z/VM and Linux
 - <http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102015>
- Routing Linux and UNIX SYSLOG data to IBM Operations Manager for z/VM
 - <http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101379>
- Integrating IBM Operations Manager for z/VM with IBM Tivoli Netcool/OMNibus
 - <http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101492>
- Automatically Logging on a User at Linux System Boot time for Console Management
 - <http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101634>



E
101

धन्यवाद

Hindi

多謝

Traditional Chinese

감사합니다

Korean

Спасибо

Russian

Gracias

Spanish

شكراً

Arabic

Thank You

English

Obrigado

Brazilian Portuguese

Grazie

Italian

Danke

German

多谢

Simplified Chinese

Merci

French

நன்றி

Tamil

ありがとうございました

Japanese

ขอบพระคุณ

Thai