

Managing VMware ESX Server using IBM Director

Version 2.5

December 22, 2005

**Jason Brunson
Wayne Wigley
Craig Elliott**

Revision History

v1.0 (October 25, 2004)	Initial Version
v2.0 (May 02, 2005)	Second Version Includes managing VMware ESX Server as a SNMP Device, as an IBM Director Agent, and using Virtual Machine Manager
v2.01 (May 10, 2005)	Includes slight modification of disclaimer
v2.5 (December 22, 2005)	Updated for IBM Director v5.10 and VMM 2.01

Notices:

This paper is intended to provide information regarding IBM Director. It discusses findings based on configurations that were created and tested under laboratory conditions. These findings may not be realized in all customer environments, and implementation in such environments may require additional steps, configurations, and performance analysis. The information herein is provided "AS IS" with no warranties, express or implied. This information does not constitute a specification or form part of the warranty for any IBM or non-IBM products.

Information in this document was developed in conjunction with the use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

The information contained in this document has not been submitted to any formal IBM test and is distributed as is. The use of this information or the implementation of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

IBM may not officially support techniques mentioned in this document. For questions regarding officially supported techniques, please refer to the product documentation and announcement letters.

This document makes references to 3rd party applications or utilities. It is the customer responsibility to obtain licenses of these utilities prior to their usage.

Table of Contents

Table of Contents	3
Overview	4
VMware ESX Server as a SNMP Device	5
Enable the VMware ESX Server SNMP Agent	5
Configure the IBM Director Server	6
Compiling the VMware ESX Server MIBs.....	7
Discover and Manage SNMP Devices.....	8
SNMP Traps From VirtualCenter	14
Configuring VirtualCenter to Send SNMP Traps	14
Processing VirtualCenter Traps in IBM Director.....	15
Running the IBM Director Agent on VMware.....	17
Installing the Agent.....	17
Level 0 Agent.....	17
Level 1 Agent.....	17
Level 2 Agent.....	17
Adding the Agent to IBM Director Server	18
Discovery Preferences – Level 0 Agents.....	18
Discovery Preferences – Level 1 Agents.....	19
Discovery Preferences – Level 2 Agents.....	20
Requesting Access to an Agent.....	21
Managing the Agent	23
Level 0 Management Tasks.....	23
Level 1 Management Tasks.....	24
Level 2 Management Tasks.....	24
Managing VMware ESX Server with Virtual Machine Manager.....	31
Appendix	31
Inventory Data	31
Event Data Substitution	31
References	31
Trademarks	31

Overview

VMware ESX Server is virtual infrastructure software for partitioning, consolidating and managing systems in mission-critical environments. VMware ESX Server transforms physical systems into a pool of logical computing resources. Operating systems and applications are isolated in multiple virtual machines that reside on a single physical server. System resources are dynamically allocated to virtual machines based on need and administrator set guarantees, providing mainframe-class capacity utilization and control of server resources.

VMware ESX Server uses a unique bare-metal architecture that inserts a small and highly robust virtualization layer between the x86 server hardware and the virtual machines. This approach gives VMware ESX Server complete control over the server resources allocated to each virtual machine and it avoids the performance overhead, availability concerns and costs of server virtualization architectures built on a host operating system.

VMware ESX Server simplifies server infrastructure by partitioning and isolating server resources in secure and portable virtual machines. VMware ESX Server runs directly on the system hardware to provide a secure, uniform platform for deploying, managing, and remotely controlling multiple virtual machines.

With this new infrastructure comes new management demands. The combination of the integrated service processor in the xSeries server, IBM Director Agent, and Virtual Machine Manager, working in conjunction with VirtualCenter and VMotion, provides a comprehensive systems management solution that addresses these management requirements.

This document will focus on using IBM Director v5.10, Virtual Machine Manager v2.01, and various other IBM Director Extensions to manage VMware ESX Server v2.51.

VMware ESX Server as a SNMP Device

VMware ESX Server ships with a SNMP agent that is disabled by default. This agent can be enabled, allowing VMware ESX Server to be discovered by IBM Director and managed as a SNMP device. Managing VMware ESX Server using SNMP requires no additional software to be installed on the Console O/S.

The SNMP implementation is set to Read-Only, only providing configuration and fault information. The variables available in the VMware ESX Server MIB are detailed in the *ESX Server Administration Guide* available for download from http://www.vmware.com/pdf/esx25_admin.pdf.

Enable the VMware ESX Server SNMP Agent

The SNMP agent must first be enabled on the VMware ESX Server. To do this, in the MUI (browser interface), log in as `root` and select the Options tab. This will display the VMware ESX Server Options as shown in Figure 1 – VMware Options on page 5.

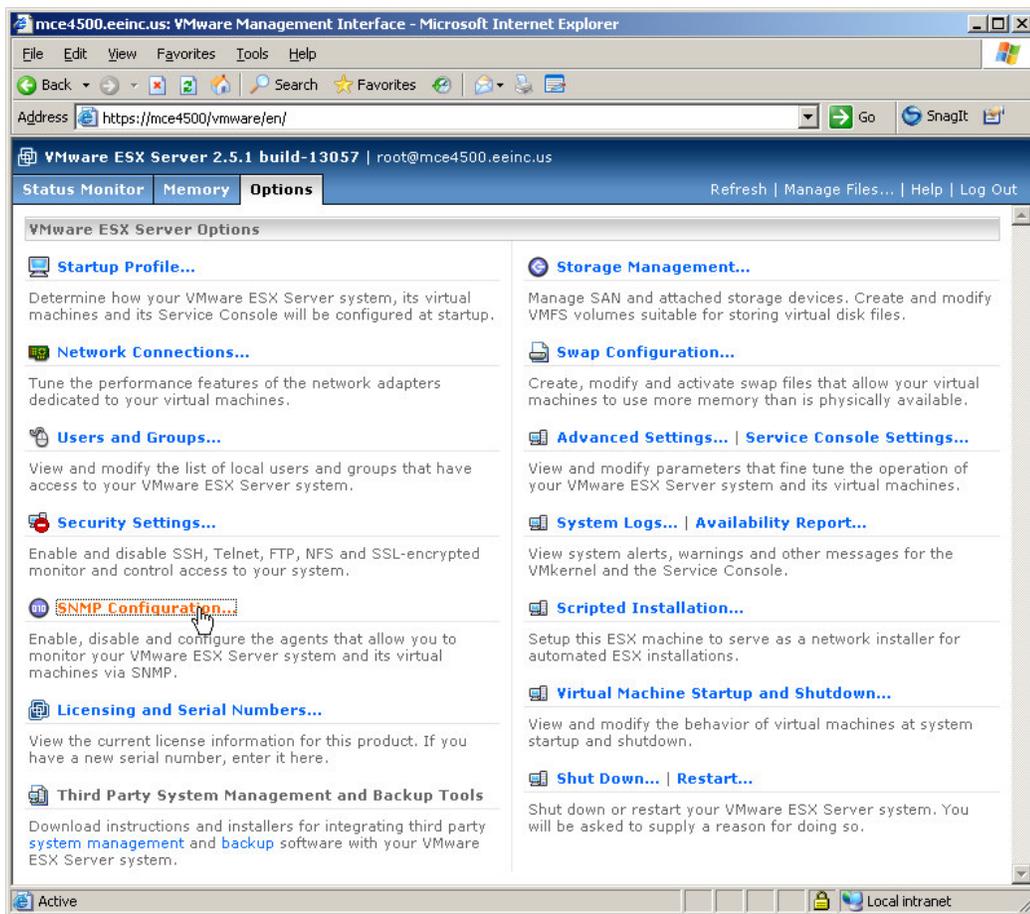


Figure 1 – VMware Options

From the Options tab, select SNMP Configuration. This will display the Current SNMP Status and Configuration, as shown in Figure 2 – SNMP Configuration on page 6.

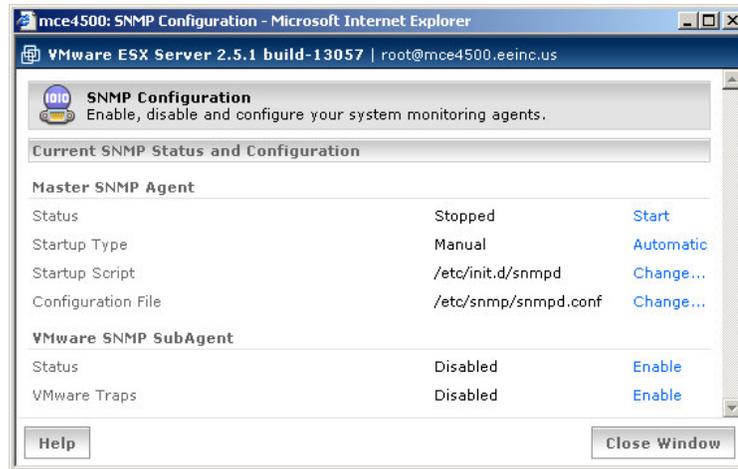


Figure 2 – SNMP Configuration

Under Master SNMP Agent, set the Startup Type to *Automatic*. Under VMware SNMP SubAgent, set the Status to *Enable*. Also set VMware Traps to *Enable*.

Next, edit the SNMP Configuration File `/etc/snmp/snmpd.conf`. Change the line `syscontact` and `syslocation` to reflect the appropriate values. Change the `rocommunity` and `trapcommunity` to match the SNMP community names being used by IBM Director. Finally, change the `trapsink` line to the hostname or IP address of the IBM Director Server. Refer to Figure 3 – `snmpd.conf` on page 6 for an example.

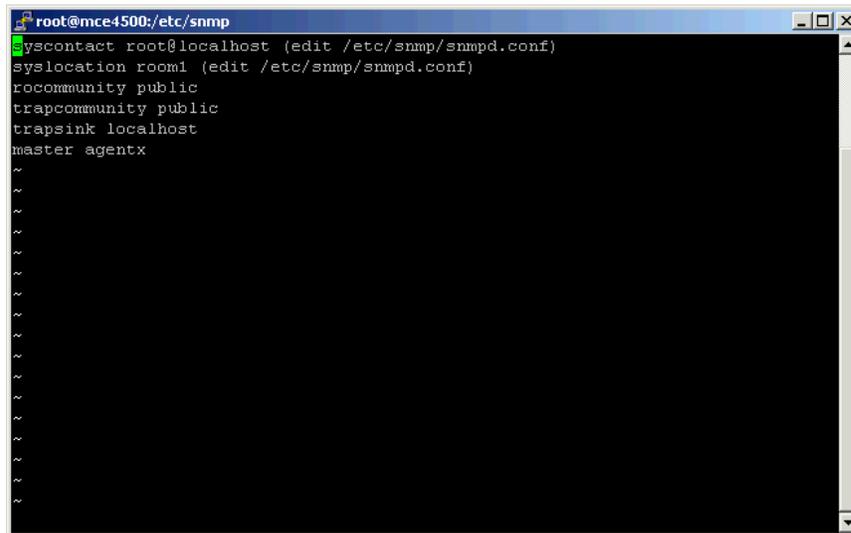


Figure 3 – `snmpd.conf`

Finally, return to the MUI interface and set the Status to *Start*. The SNMP agent is now enabled and configured to forward traps to the IBM Director server.

Configure the IBM Director Server

IBM Director needs to be configured to browse the SNMP MIBs, interpret the SNMP Traps, and to discover the VMware ESX Server as a SNMP device. These tasks are defined in the following sections.

Compiling the VMware ESX Server MIBs

The first step is to compile the VMware ESX Server MIBs into IBM Director. Copy the MIBs to the IBM Director Server. The VMware ESX Server MIBs are found in `/usr/lib/vmware/snmp/mibs`. A Secure Copy client such as PuTTY's `PSCP.EXE` can be used for this.

Next, compile the MIBs using IBM Director's Compile MIB tool. To launch the tool, in the IBM Director Console, select the **Tasks** menu item, then select **SNMP Browser** → **Manage MIBs...** Alternately, you can show the **Tasks** pane of the console, right-click on **SNMP Browser**, and select **Manage MIBs...** Refer to Figure 4 – Compile a New MIB on page 7 for an example.

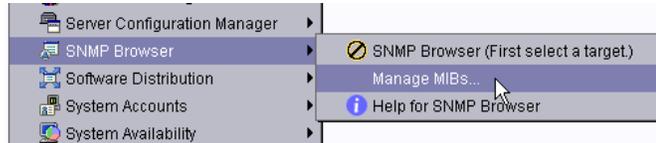


Figure 4 – Compile a New MIB

Browse to the directory where the VMware ESX Server MIBs reside, and select the MIB to compile. Refer to Figure 5 – Select MIB to Compile on page 7 for an example.

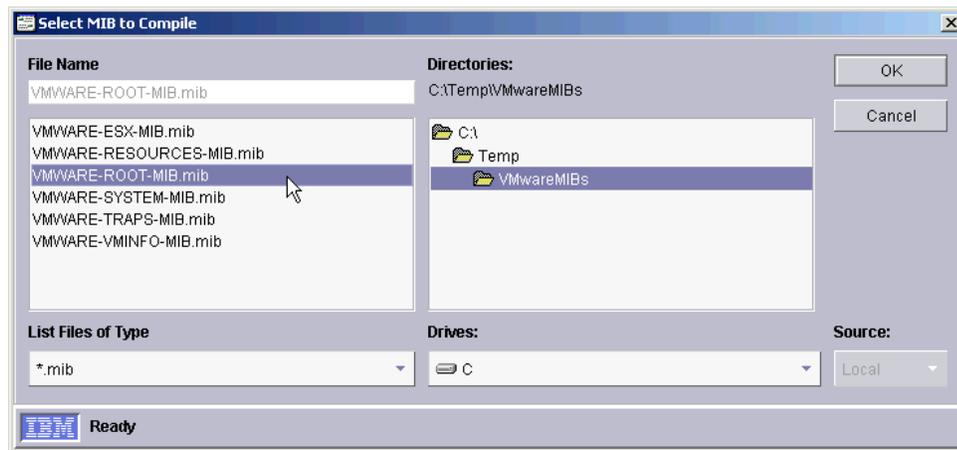


Figure 5 – Select MIB to Compile

Note that `VMWARE-ROOT-MIB.mib` must be compiled first, because the other MIBs reference it. Refer to Figure 6 – Compile MIB on page 7 for an example of a successful completion message.

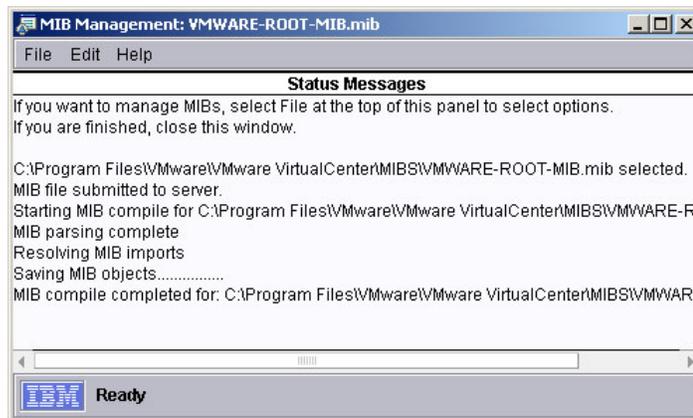


Figure 6 – Compile MIB

Repeat the process for the remaining MIBs. IBM Director is now able to correctly interpret SNMP traps from VMware ESX Server, as well as browse the VMware ESX Server MIBs.

Discover and Manage SNMP Devices

VMware ESX Server must be added to IBM Director as a SNMP Device. This can be done in one of four ways. First, ensure IBM Director can discover the VMWare ESX Server's SNMP agent by configuring the discovery preferences. The discovery preferences are accessed within the IBM Director Console by selecting Options → Discovery Preferences. In the Discovery Preferences window, select the SNMP Devices tab, and then enter the correct IP Address and Subnet Mask for the VMware ESX Server. Refer to Figure 7 – SNMP Discovery Preferences on page 8. Also, enter the correct SNMP Community Name as specified in Figure 3 – snmpd.conf on page 6. IBM Director should now discover VMware ESX Server as a SNMP device during its discovery process. To eliminate the need to perform a discovery, ensure the item `Auto-add unknown agents which contact server` is selected. The next time the VMware ESX Server SNMP agent is restarted, it will send a cold-start trap to IBM Director, and will automatically be registered.

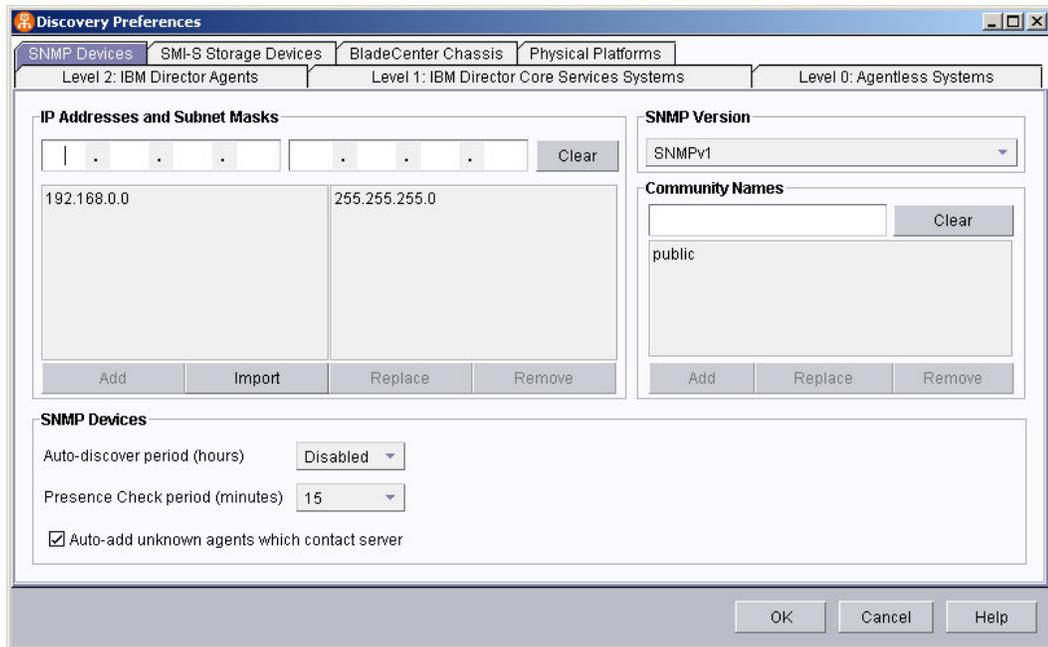


Figure 7 – SNMP Discovery Preferences

A third option to discovering the SNMP agent is to manually add it. Right-click in the center pane of the IBM Director Console and select New → SNMP Devices. In the Add SNMP Devices window, enter the IP Address and Community Name of the VMware ESX Server. Refer to Figure 8 – Add SNMP Device on page 9. The Community Name must match what was configured in Figure 3 – snmpd.conf on page 6.



Figure 8 – Add SNMP Device

Finally, the SNMP Device can be added to IBM Director using the Command Line Interface. To add the VMware ESX Server as a SNMP Device using the Command Line Interface, execute the command:

```
dircli mkmo type="SNMP Device" ip=IpAddress version=n community=name seed=yesno
```

where:

- IpAddress* is the IP Address of the VMware ESX Server
- n* is the SNMP Version
- name* is the SNMP Community Name
- yesno* is yes or no

To see a list of IBM Director Tasks that can be executed against VMware ESX Server, right-click on the VMware ESX Server SNMP object in the Director Console. Refer to Figure 9 – IBM Director SNMP Tasks on page 9.

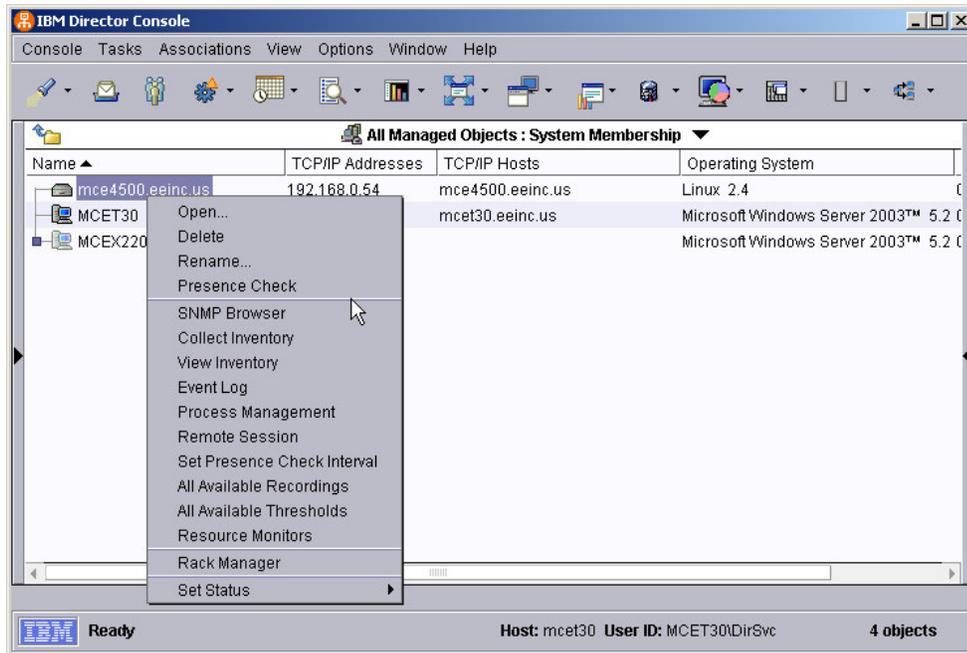


Figure 9 – IBM Director SNMP Tasks

Select the SNMP Browser Task on the VMware ESX Server to see the VMware ESX Server SNMP information. Expand the tree next to the machine_name → iso → org → dod → internet → private → enterprises → vmware to see the available VMware ESX Server information. Refer to Figure 10 – SNMP Browser on page 10.

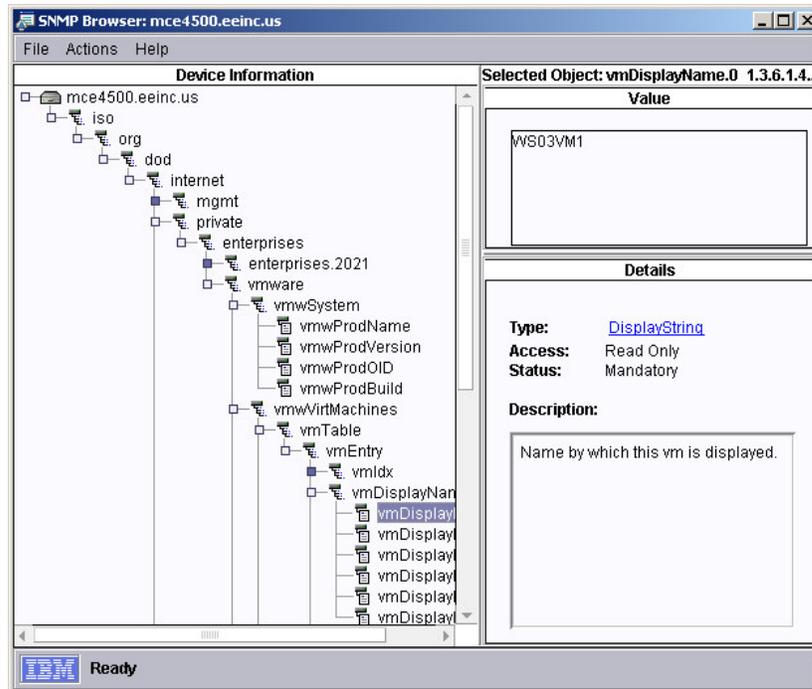


Figure 10 – SNMP Browser

The IBM Director Event Log Task will show the SNMP traps that have been received from VMware ESX Server. The VMware ESX Server traps are limited to the following:

- vmPoweredOn
- vmPoweredOff
- vmHBLost
- vmHBDetected
- vmSuspended

Refer to Figure 11 – Event Log on page 11.

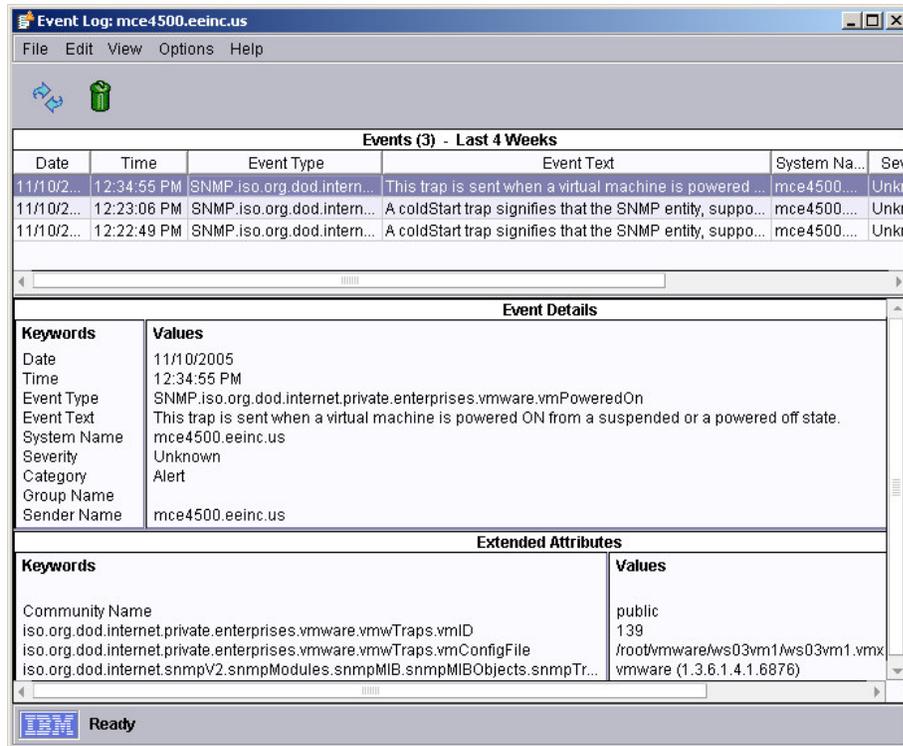


Figure 11 – Event Log

The Inventory Task of IBM Director collects system inventory information about the VMware ESX Server Console O/S from the VMware ESX Server SNMP agent. The information can be viewed using the Inventory Query Browser. Refer to Figure 12 – Inventory on page 11. For a list of inventory data returned, refer to Table 1 – Inventory Data on page 31. The actual data returned may differ based on Machine-Type and Model.

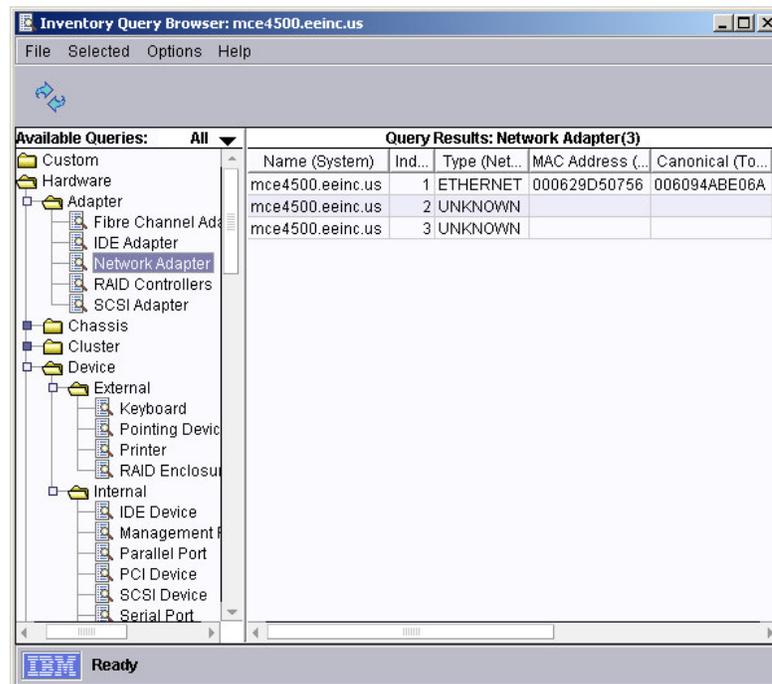


Figure 12 – Inventory

The inventory information can be used to create dynamic groups of systems. For example, to create a group of all VMware ESX Servers, use the Installed Packages criteria, and select VMware-esx. Refer to Figure 13 – Dynamic Group Creation on page 12.

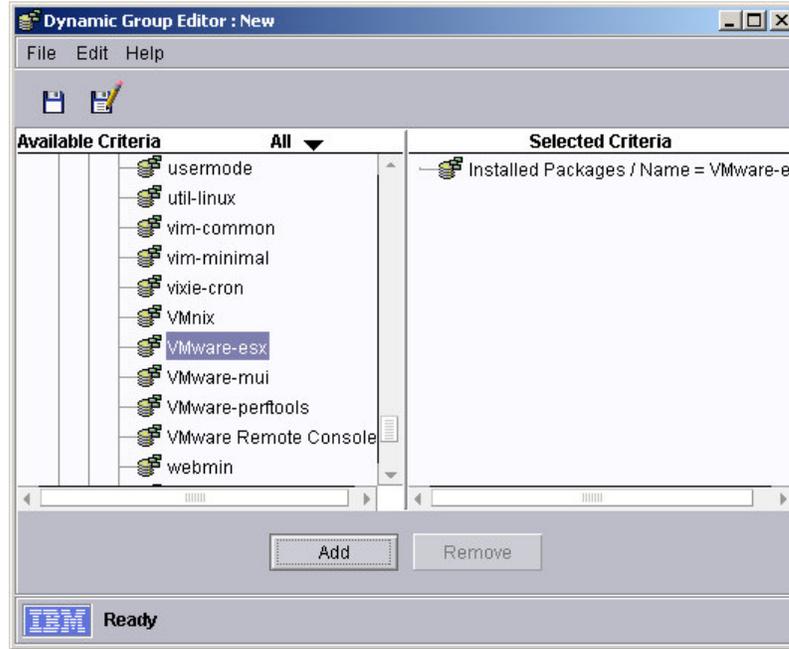


Figure 13 – Dynamic Group Creation

The Process Management Task lists the processes currently running on VMware ESX Server Console O/S. Unlike other Agent types, processes cannot be started or stopped on SNMP devices. Processes also cannot be monitored for running status. Refer to Figure 14 – Process Management on page 12.

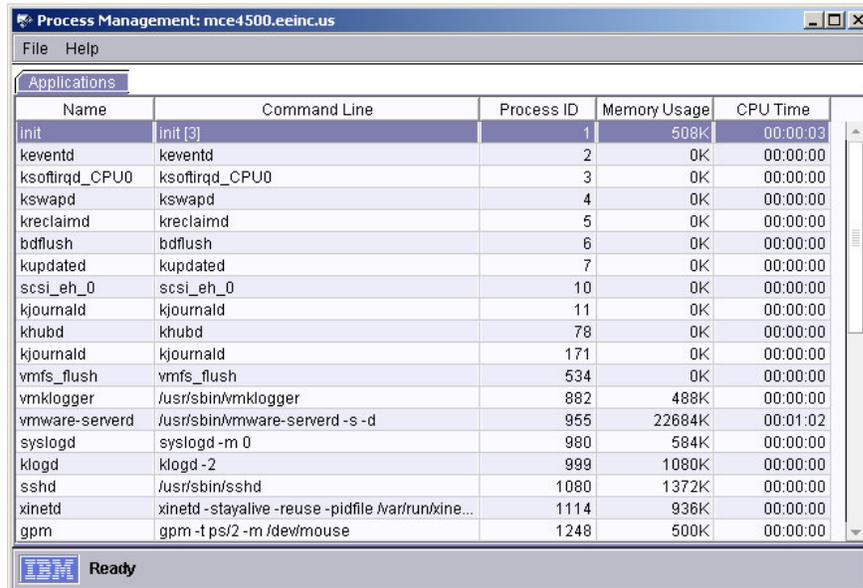


Figure 14 – Process Management

The Remote Session Task opens a SSH or TELNET session with the VMware ESX Server. It initially attempts SSH, and if SSH isn't available, reverts to TELNET. Once the session is established, you are prompted to log-in. Refer to Figure 15 – Remote Session on page 13.

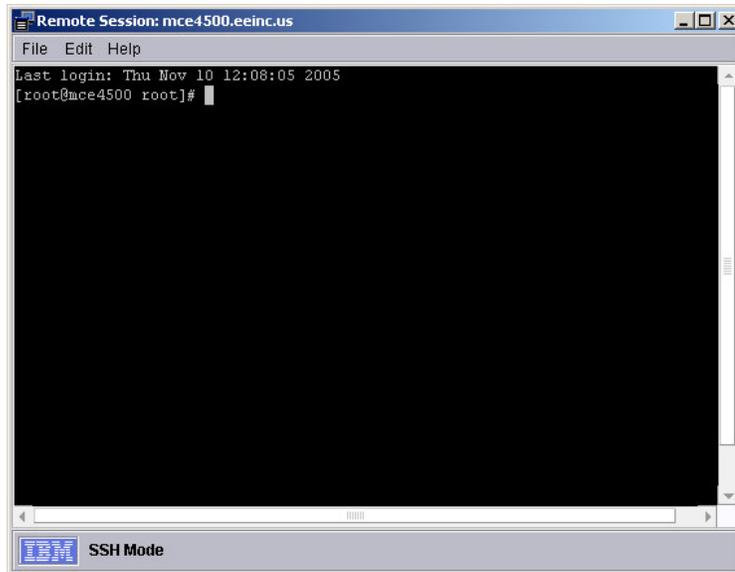


Figure 15 – Remote Session

The Resource Monitor Task enables the creation of user-defined thresholds to monitor SNMP MIB variables. These variables represent resources available to the VMware ESX Server Console O/S. If the threshold is exceeded, an Event will be sent to IBM Director. Since most MIB variables are arranged in tables, care should be taken to ensure the item selected is the desired item. For example, in Figure 16 – Resource Monitors on page 13, the root partition is referenced by the first entry in the `hrStorageTable`. This becomes even more critical when attempting to monitor software, using the `hrSWRunPerf` table, since the processes are indexed by process ID, and processes may not have the same process ID each time they are executed.

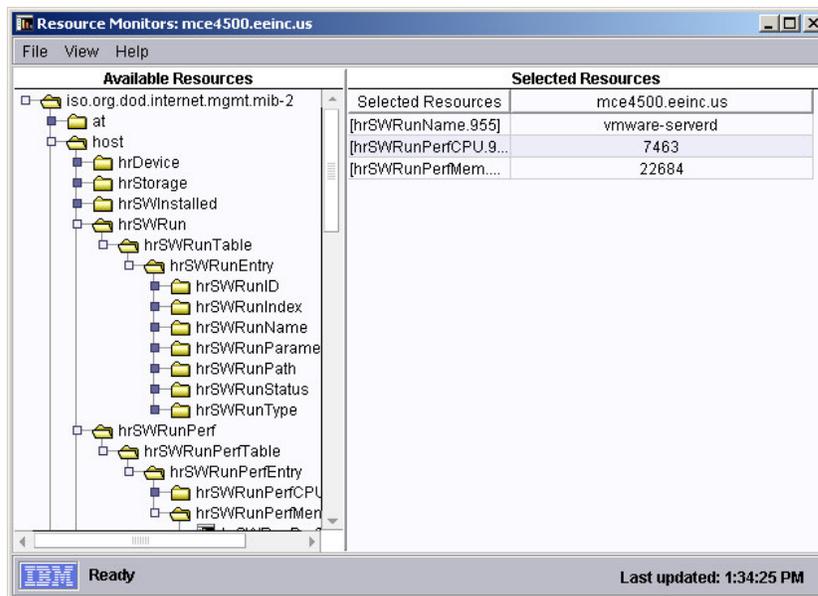


Figure 16 – Resource Monitors

An Event Action Plan is the mechanism used by IBM Director to specify the Action to take when a specific Event is received. Events are specified using an Event Filter. To select an Event from VMware ESX Server, deselect the Any check-box, and expand SNMP → iso → org → dod → internet → private → enterprises → vmware. Refer to Figure 17 – Event Filter on page 14.

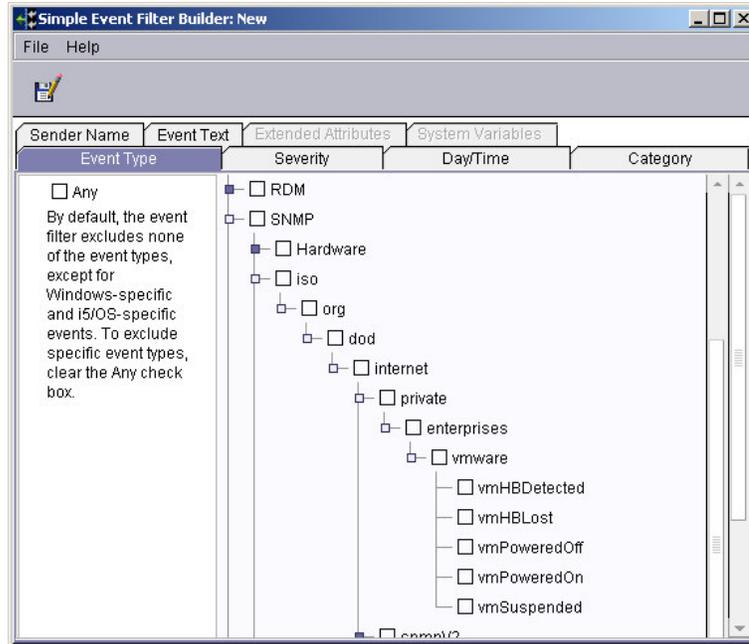


Figure 17 – Event Filter

To include the contents of a MIB variable in an Event Action message, specify `&"oid` where `oid` is the OID of the desired variable. For example, to include the name of the VMware Configuration File, use

`&"iso.org.dod.internet.private.enterprises.vmware.vmwTraps.vmConfigFile`.

Note that a `"` is specified prior to the OID, but not following it. Refer to Figure 18 – Event Action on page 14.

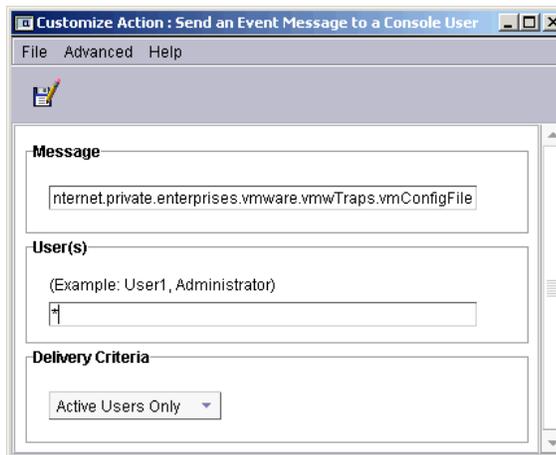


Figure 18 – Event Action

SNMP Traps From VirtualCenter

If you have Virtual Center in your environment, additional alerting is possible using VirtualCenter's Alarms. VirtualCenter can send SNMP Traps to IBM Director based on CPU Usage, Memory Usage, or Host Connection status.

Configuring VirtualCenter to Send SNMP Traps

The first step is to configure VirtualCenter to send SNMP traps. This is done from within the VirtualCenter Console. Select `File` → `VMware VirtualCenter Settings...` Within the VMware

VirtualCenter Settings window, select the Advanced tab. Change the value of `snmp.receiver.1.name` to the hostname or IP address of the IBM Director Server. Refer to Figure 19 – VirtualCenter Trap Destination on page 15.

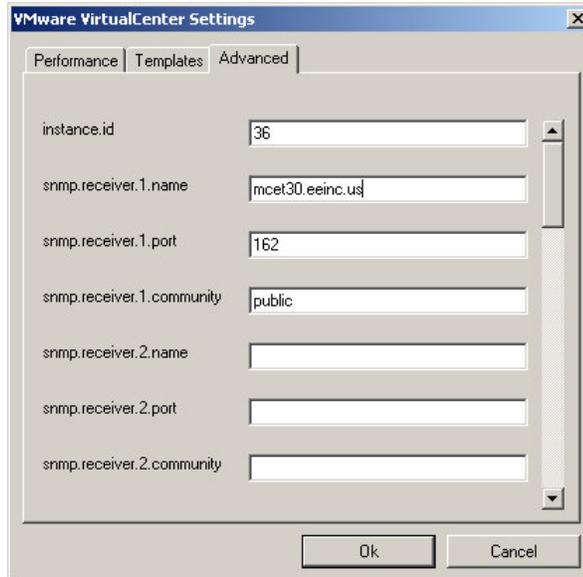


Figure 19 – VirtualCenter Trap Destination

Next, in the VirtualCenter Console, select the item Server Farms. Click on the Alarms tab to display the predefined alarms. To customize one of the predefined alarms, right-click on it and select properties. Within the Alarm Properties window, select the Actions tab. Change the action to Send a notification trap. Select all of the option check-boxes to be alerted for all changes. Repeat the process for each alarm you wish to modify. Refer to Figure 20 – VirtualCenter Alarms on page 15.

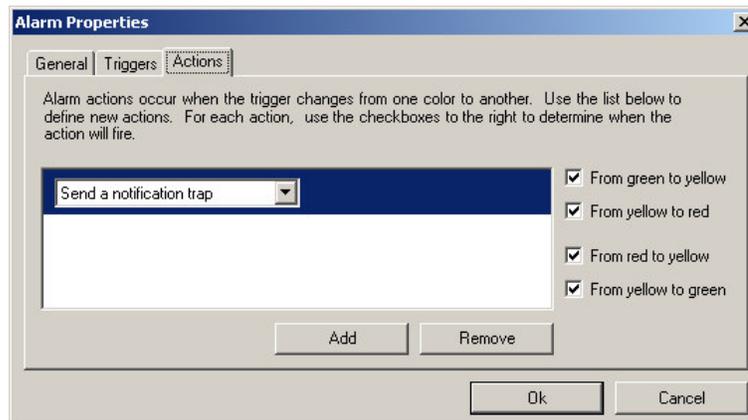


Figure 20 – VirtualCenter Alarms

Processing VirtualCenter Traps in IBM Director

Since VirtualCenter isn't running a SNMP Agent, the traps will be displayed within IBM Director with a blank System Name. This will not prevent IBM Director from processing them. However, any Event Action Plan that will process these events must be assigned to the All Managed Objects group.

To properly translate the traps, the appropriate MIBs must be loaded. The VirtualCenter MIBs can be found in the `\Program Files\VMware\VMware VirtualCenter\MIBS` directory on the VirtualCenter server. Copy them to the IBM Director Server and compile them using IBM

Director's MIB Management tool. Refer to Compiling the VMware ESX Server MIBs on page 7 for instructions on compiling MIBs in IBM Director.

To view the traps, double-click on the Event Log item in the Tasks pane of the IBM Director Console. Refer to Figure 21 – VirtualCenter Event on page 16.

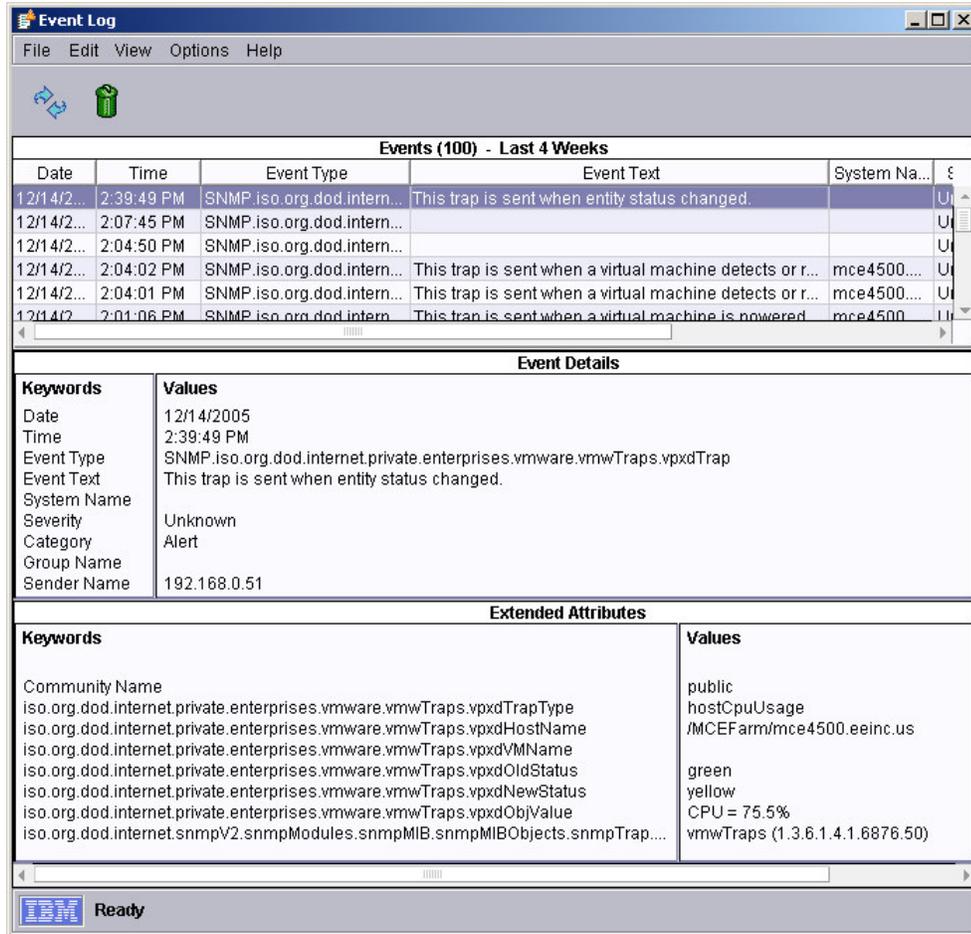


Figure 21 – VirtualCenter Event

Just as with the other SNMP traps, the data from the VirtualCenter traps can be passed to other applications using IBM Director's Event Data Substitution. For example, to pass the current value, use the following:

```
&"iso.org.dod.internet.private.enterprises.vmware.vmwTraps.vpxdObjValue
```

Running the IBM Director Agent on VMware

Additional management functionality can be gained by installing the IBM Director Agent in the VMware ESX Server Console O/S. This section of the document will assist with the installation of the IBM Director Agent, as well as provide information about the additional benefits of the IBM Director Agent. For a complete list of installation instructions, refer to the IBM Director *Installation and Configuration Guide* Version 5.10

(ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir510_docs_install.pdf). For a complete list of IBM Director functions, refer to the IBM Director *Systems Management Guide* Version 5.10 (ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir510_docs_sysmgt.pdf).

Installing the Agent

IBM Director Version 5.10 offers multiple Agent “levels”, with each (Level 0, Level 1, and Level 2) offering increasing functionality. The following sections will address managing VMware ESX Server running each level of Agent.

Level 0 Agent

The Level 0 Agent does not require any IBM Software. The IBM Director Server manages a Level 0 Agent using industry standard protocols. For VMware ESX Server, this uses SSH.

Level 1 Agent

The IBM Director Level 1 Agent (Core Services) can be installed in one of three ways: locally from the VMware ESX Console, remotely from a SSH session, or remotely by promoting a Level 0 Agent to a Level 1 Agent. Installation instructions are contained in Chapter 3 of the *IBM Director Installation and Configuration Guide* Version 5.10.

Once the Level 1 Agent has been successfully installed, it will be started automatically.

Note: The IBM Director Level 1 Agent (Core Services) is a small footprint agent designed for hardware management only. Unfortunately, it has minimal benefit in a VMware ESX environment. This is true for two reasons. First, the service processor drivers (neither IPMI-BMC nor the RSA-II) are not supported running in the VMware ESX Server Console O/S. Without these drivers, the Level 1 Agent cannot receive in-band hardware events. Second, the stand-alone ServeRAID Manager is also not supported running in the VMware ESX Server Console O/S. Without this agent, the Level 1 Agent cannot receive RAID events. Therefore, the only benefit of the Level 1 Agent is enhanced inventory information over that provided by the Level 0 Agent. This includes the ability to collect inventory information such as firmware versions, FRU numbers, and serialization information.

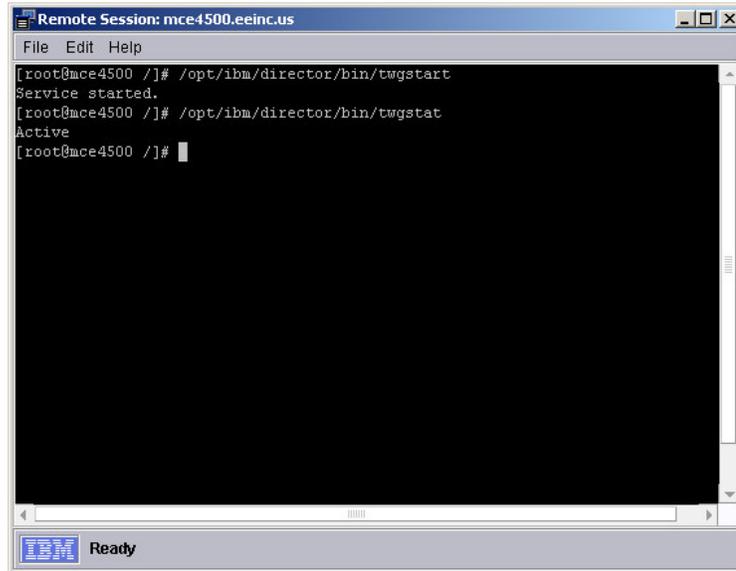
Level 2 Agent

The IBM Director Level 2 Agent can be installed in one of three ways: locally from the VMware ESX Server Console, remotely using a SSH session, or remotely by promoting a Level 0 Agent (or Level 1 Agent) to a Level 2 Agent. Installation instructions are contained in Chapter 3 of the *IBM Director Installation and Configuration Guide* Version 5.10.

Note: The IBM Director Level 2 Agent is a full-featured agent designed for hardware management as well as system management. Unfortunately, it has limited hardware management capabilities in a VMware ESX environment. This reason for the limitation is that the service processor drivers (neither IPMI-BMC nor the RSA-II) are not supported running in the VMware ESX Server Console O/S. Without these drivers, the Level 2 Agent cannot receive in-band hardware events. Unlike the Level 1 Agent, the integrated ServeRAID Manager is supported running in the VMware ESX Server Console O/S. This agent allows the Level 2 Agent to send RAID events. In addition to RAID management the Level 2 Agent collects enhanced inventory information similar to that provided by the Level 1 Agent. This includes information such as firmware versions, FRU numbers, and serialization information. The Level 2 Agent can

also be extended to include additional IBM Director Extensions such as Capacity Manager and System Availability. The functionality of these tools will be included in the sections that follow.

Once the IBM Director Level 2 Agent has been installed, it can be started using the script `/opt/ibm/director/bin/twgstart`. This script can be launched using a Remote Session with the Level 0 Agent. The O/S doesn't need to be restarted prior to starting the Level 2 Agent for the first time. To check the operational status of the Level 2 Agent, execute the script `/opt/ibm/director/bin/twgstat`. Refer to Figure 22 – Director Agent Commands on page 18 for an example of the output of these commands.



```
Remote Session: mce4500.eeinc.us
File Edit Help
[root@mce4500 /]# /opt/ibm/director/bin/twgstart
Service started.
[root@mce4500 /]# /opt/ibm/director/bin/twgstat
Active
[root@mce4500 /]#
```

Figure 22 – Director Agent Commands

Adding the Agent to IBM Director Server

Once the Agent has been installed and started, it is able to be discovered by the IBM Director Server. IBM Director Server has discovery preferences for each of the 3 Agent levels. The discovery preferences are accessed within the IBM Director Console by selecting Options → Discovery Preferences. Once the discovery preferences have been specified, you may initiate a system discovery by either right-clicking in the center pane of the IBM Director Console and selecting Discover, then selecting the desired Agent level, or selecting Discover → All Managed Objects. Please note that it may take a while for Level 0 or Level 1 Agents to be discovered.

Discovery Preferences – Level 0 Agents

In the Discovery Preferences window, select the Level 0: Agentless Systems tab. Select the Add button, and enter a Unicast Address (to discover a single device) or Unicast Range (to discover all Level 0 Agents on the specified subnet. Refer to Figure 25 – Level 2 Agent Discovery Preferences on page 19.

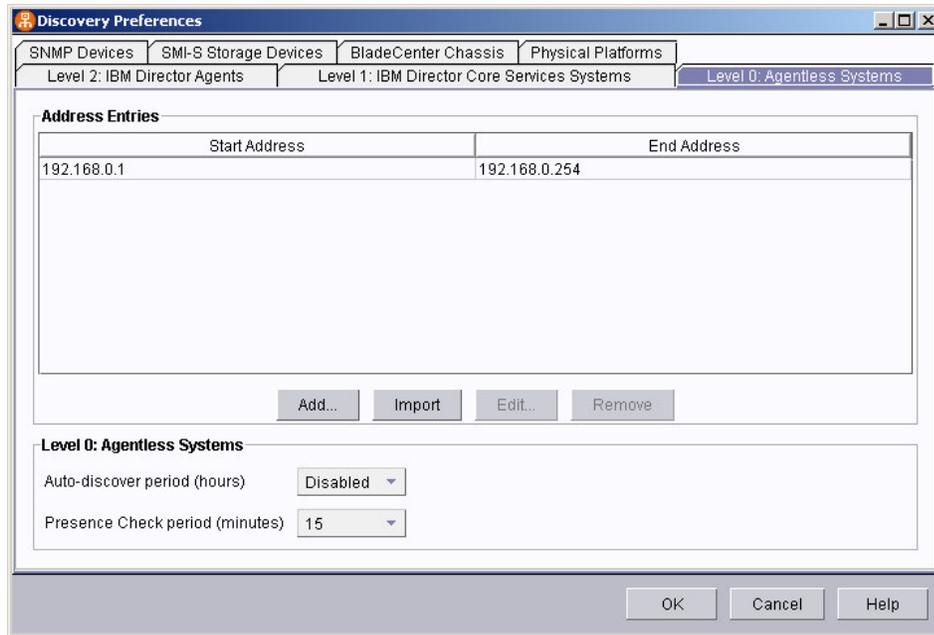


Figure 23 – Level 0 Agent Discovery Preferences

Discovery Preferences – Level 1 Agents

In the Discovery Preferences window, select the Level 1: IBM Director Core Services Systems tab. Select the appropriate Add button to add either a Predefined directory agent server or a SLP Scope. Refer to Figure 24 – Level 1 Agent Discovery Preferences on page 20.

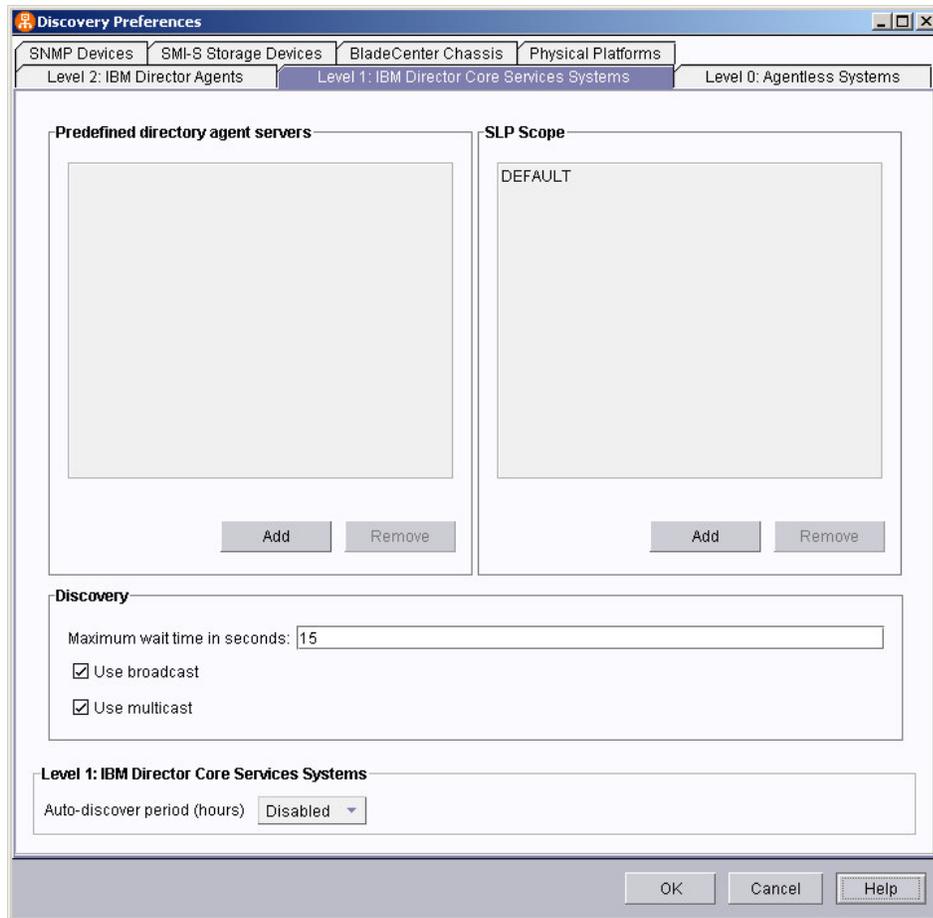


Figure 24 – Level 1 Agent Discovery Preferences

Discovery Preferences – Level 2 Agents

In the Discovery Preferences window, select the Level 2: IBM Director Agents tab, select the System Discovery (IP) radio button, then select the Add button to add a Broadcast, Relay, Unicast Address, or Unicast Range for the VMware ESX Server. Refer to Figure 25 – Level 2 Agent Discovery Preferences on page 21.

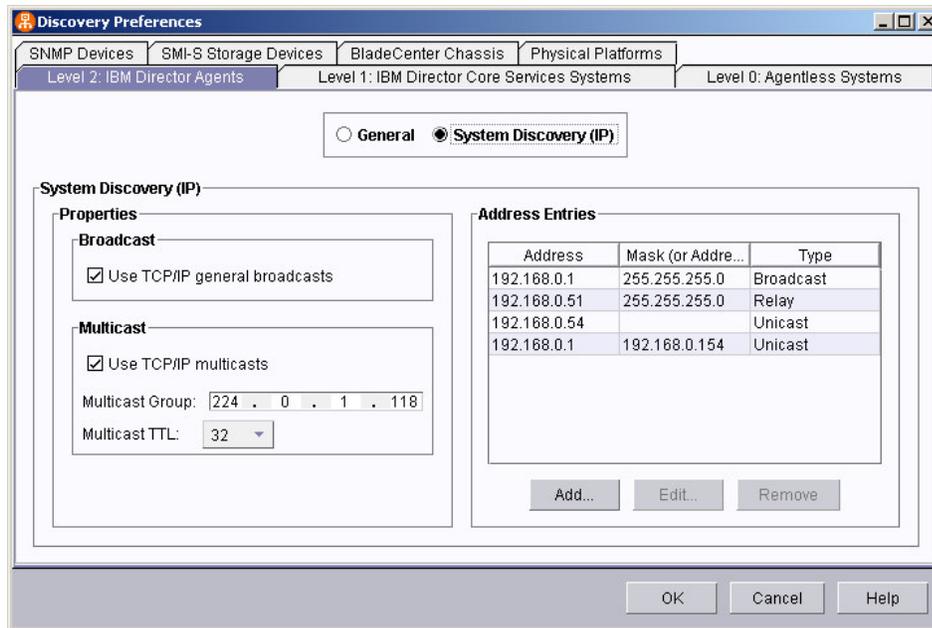


Figure 25 – Level 2 Agent Discovery Preferences

Alternately, you may manually add the Level 0, 1, or 2 Agents. To manually add the Agent, right-click in the center pane of the IBM Director Console and select New → Systems. In the Add Systems window, type the System Name and Network Address, and select the OK button. Refer to Figure 26 – Add System on page 21.

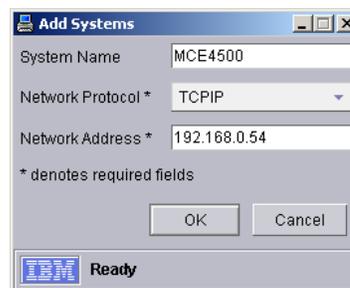


Figure 26 – Add System

Finally, you may add Agents to IBM Director using the Command Line Interface. To use the Command Line Interface to add the Agent, execute the command:

```
dircli mkmo type=Systems name=ComputerName ip=IpAddress
```

where:

ComputerName is the label for the object in the IBM Director Console
IpAddress is the IP Address of the VMware ESX Server to be added

Note: You must be logged in locally on the IBM Director Server system using a DirSuper ID in order to run the IBM Director Command Line Interface.

Requesting Access to an Agent

Once discovered, the Agent will be “locked” or “secured to itself”. Access to the Agent must be gained by right-clicking on the Agent icon and selecting Request Access. Refer to Figure 27 – Request Access on page 22.

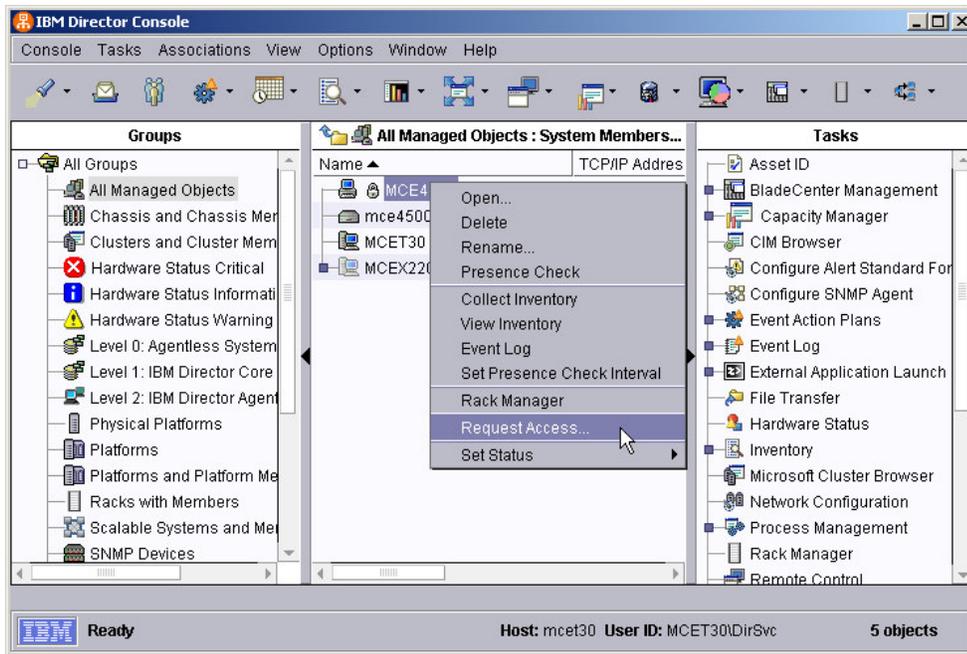


Figure 27 – Request Access

Selecting Request Access will open a dialog box requiring a User ID and Password to proceed. The User ID **must** be `root`. Refer to Figure 28 – User Credentials on page 22.



Figure 28 – User Credentials

Once valid log-on credentials are specified, the Request Access will display a success message. Refer to Figure 29 – Access Request Succeeded on page 22.



Figure 29 – Access Request Succeeded

When access is granted, the IBM Director Server will immediately initiate an Inventory collection against the IBM Director Agent. VMware ESX Server can now be managed as an IBM Director Agent.

You may also request access to the Agents using the Command Line Interface. To use the Command Line Interface to request access to the Agent, execute the command:

```
dircli accessmo -n ComputerName -t Type -u UserId -p Password
```

where:

ComputerName is the label for the object in the IBM Director Console

Type is the managed object type

(Run the command `dircli lsmo -i` for a list of object types)

UserId is the root user ID

Password is the password for the root user ID

Note: You must be logged in locally on the IBM Director Server system using a DirSuper ID in order to run the IBM Director Command Line Interface.

Managing the Agent

To see a list of IBM Director Tasks that can be executed against VMware ESX Server, right-click on the VMware ESX Server's object in the IBM Director Console. Refer to Figure 30 – IBM Director Agent Tasks on page 23. Note that the available tasks and their behavior may differ depending on the Agent level.

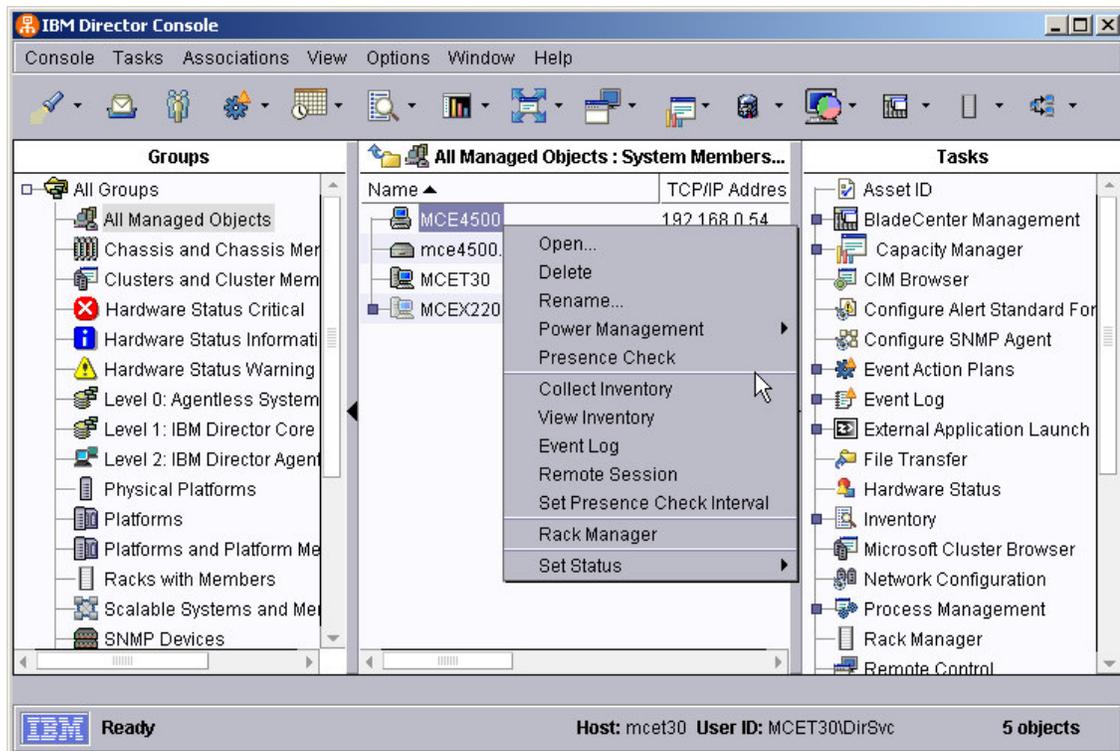


Figure 30 – IBM Director Agent Tasks

Level 0 Management Tasks

The Power Management task will enable you to restart the VMware ESX Server. This effectively executes the command `shutdown -r now` on the VMware ESX Server's Console O/S. It is up to the VMware ESX Server to cleanly shutdown any virtual machines prior to it restarting.

The Inventory Task of IBM Director collects system inventory information about the VMware ESX Server Console O/S. For a list of inventory data returned, refer to Table 1 – Inventory Data on page 31. The actual data returned may vary based on Machine-Type and Model. Note that more inventory information is available from a Level 0 Agent than is available from a SNMP Agent.

Just as when managing a VMware ESX Server as a SNMP device, the inventory collected from a Level 0 Agent can be used to create a dynamic group that contains all VMware ESX Servers. In

fact, the dynamic group example in Figure 13 – Dynamic Group Creation on page 12 will work the same for Level 0 Agents as it does for SNMP devices.

The IBM Director Event Log Task will show the events that have been received from VMware ESX Server. These events are typically limited to topology events for Level 0 Agents.

The Remote Session Task opens a SSH session with the VMware ESX Server. Unlike the Remote Session to a SNMP device, opening a Remote Session on a Level 0 Agent will not prompt you for logon credentials – it uses the persisted credentials entered when requesting access to the Level 0 Agent.

Level 1 Management Tasks

The Power Management task will enable you to restart the VMware ESX Server. This effectively executes the command `shutdown -r now` on the VMware ESX Server's Console O/S. It is up to the VMware ESX Server to cleanly shutdown any virtual machines prior to it restarting.

The Inventory Task of IBM Director collects system inventory information about the VMware ESX Server Console O/S. For a list of inventory data returned, refer to Table 1 – Inventory Data on page 31. The actual data returned may vary based on Machine-Type and Model. Note that more inventory information is available from a Level 1 Agent than is available from a Level 0 Agent.

Just as when managing a VMware ESX Server as a SNMP device or Level 0 Agent, the inventory collected from a Level 1 Agent can be used to create a dynamic group that contains all VMware ESX Servers. In fact, the dynamic group example in Figure 13 – Dynamic Group Creation on page 12 will work the same for Level 1 Agents as it does for SNMP devices or Level 0 Agents.

The IBM Director Event Log Task will show the events that have been received from VMware ESX Server. Since the Level 1 Agent is unable to receive in-band hardware or RAID events, these events are typically limited to topology events.

The Remote Session Task opens a SSH session with the VMware ESX Server. Similar to opening a Remote Session on a Level 0 Agent, opening a Remote Session on a Level 1 Agent will not prompt you for logon credentials – it uses the persisted credentials entered when requesting access to the Level 1 Agent.

The Hardware Status Task notifies you whenever a system or device has a hardware status change. However, since the Level 1 Agent is unable to receive in-band hardware or RAID events, it will typically be unable to display any hardware status information.

Level 2 Management Tasks

The Power Management task will enable you to restart the VMware ESX Server. This effectively executes the command `shutdown -r now` on the VMware ESX Server's Console O/S. It is up to the VMware ESX Server to cleanly shutdown any virtual machines prior to it restarting.

The Inventory Task of IBM Director collects system inventory information about the VMware ESX Server Console O/S. For a list of inventory data returned, refer to Table 1 – Inventory Data on page 31. The actual data returned may vary based on Machine-Type and Model. Note that more inventory information is available from a Level 2 Agent than is available from a Level 0 or Level 1 Agent.

Just as when managing a VMware ESX Server as a SNMP device, the inventory collected from a Level 2 Agent can be used to create a dynamic group that contains all VMware ESX Servers. In fact, the dynamic group example in Figure 13 – Dynamic Group Creation on page 12 will work the same for Level 2 Agents as it does for SNMP devices.

The Event Log Task will show all Events that have been sent from the IBM Director Agent. For a list of all possible Events the IBM Director Agent can send, please refer to the *IBM Director Events Reference Version 5.10* (ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir510_events_ref.pdf).

The Process Management Task lists the processes currently running on VMware ESX Server Console O/S, just as it did when managing VMware ESX Server as a SNMP device. However, unlike the limitations of managing a SNMP device, Process Management can start or stop processes on an IBM Director Level 2 Agent system. It can also monitor processes for running state – Start, Stop, or Fail.

Just as when managing VMware ESX Server as a SNMP device, the Remote Session Task opens a SSH or TELNET session with the VMware ESX Server when managed as an IBM Director Level 2 Agent.

The File Transfer Task allows the copying of files and / or directories between the IBM Director Console and VMware ESX Server or between the IBM Director Server and VMware ESX Server. The drag-and-drop interface provides a convenient method of copying the files, without requiring FTP, NFS, or Secure Copy to be enabled on VMware ESX Server. Refer to Figure 31 – File Transfer on page 25.

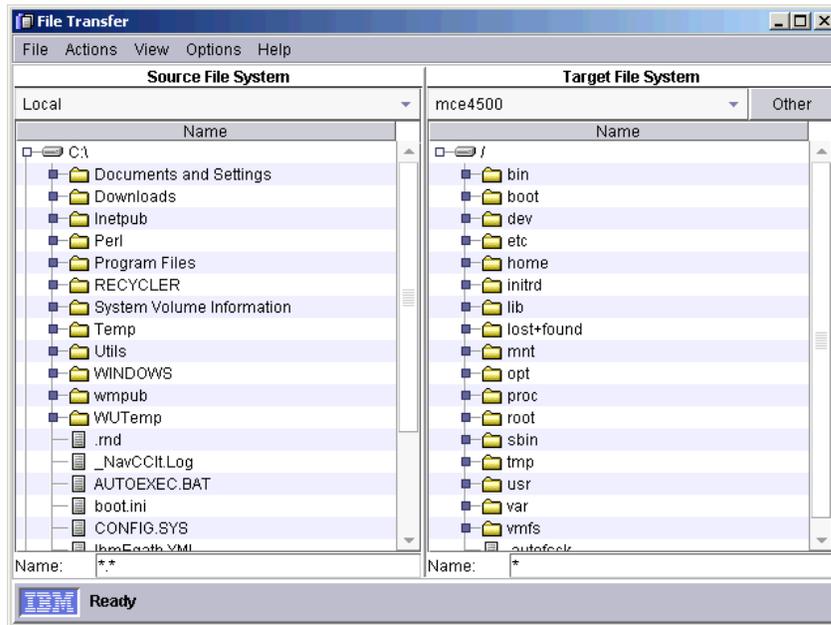


Figure 31 – File Transfer

The Resource Monitor Task enables the creation of user-defined thresholds to monitor key indicators of system performance. These Available Resources represent resources available to the VMware ESX Server Console O/S. Unlike monitoring a SNMP device, the IBM Director Level 2 Agent allows the monitoring of VMware ESX Server by selecting easy to understand labels rather than table entries. Refer to Figure 32 – Resource Monitors on page 26.

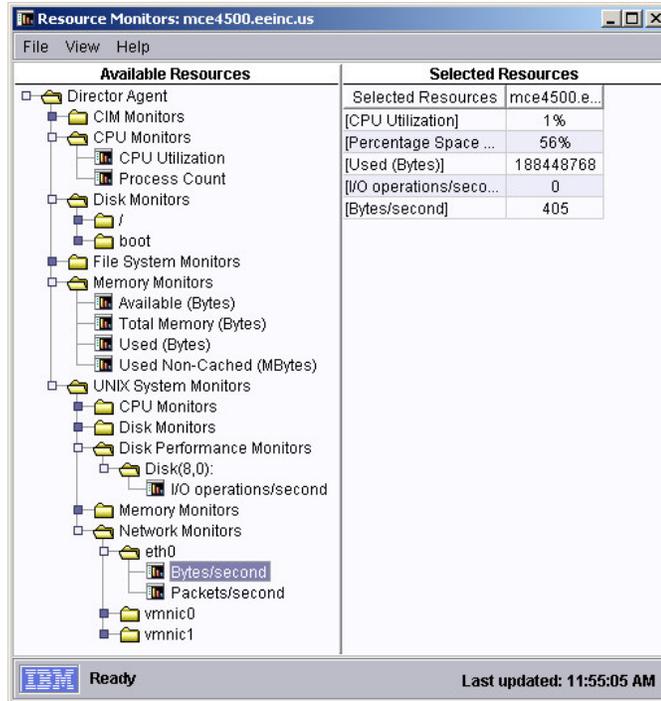


Figure 32 – Resource Monitors

IBM Director's Asset ID task allows you to view serialization information, as well as record personalization, lease, and warranty information for the server. This information is collected during an inventory collection and stored in the inventory database. Refer to Figure 33 – Asset ID on page 26.

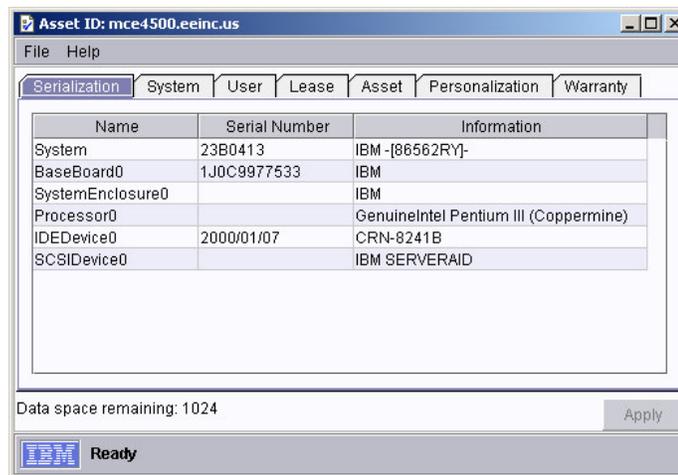


Figure 33 – Asset ID

The Configure SNMP Agent task is a convenient method of modifying the trap destination of the SNMP Agent configuration on VMware ESX Server. This is equivalent to editing the file `/etc/snmpd.conf` on VMware ESX Server. Refer to Figure 34 – Configure SNMP on page 27.



Figure 34 – Configure SNMP

For network changes, the Network Configuration task can be used to change the IP address of the Console O/S. You can also change the DNS settings as well as the hostname. Refer to Figure 35 – Network Configuration on page 27.

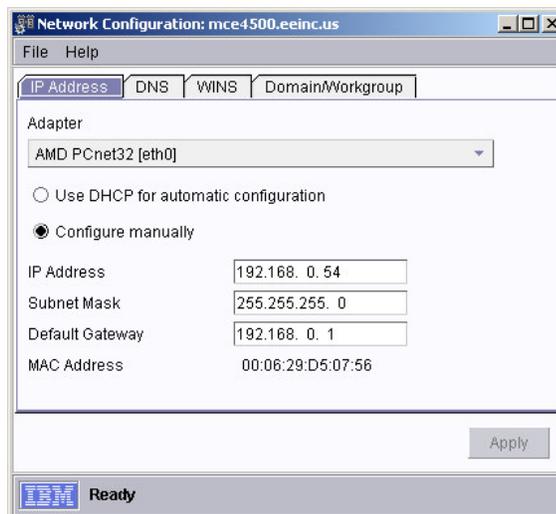


Figure 35 – Network Configuration

The System Accounts task allows you to perform user and group management for the Console O/S. This includes creating users, changing user settings, and modifying group membership. Refer to Figure 36 – System Accounts on page 28.

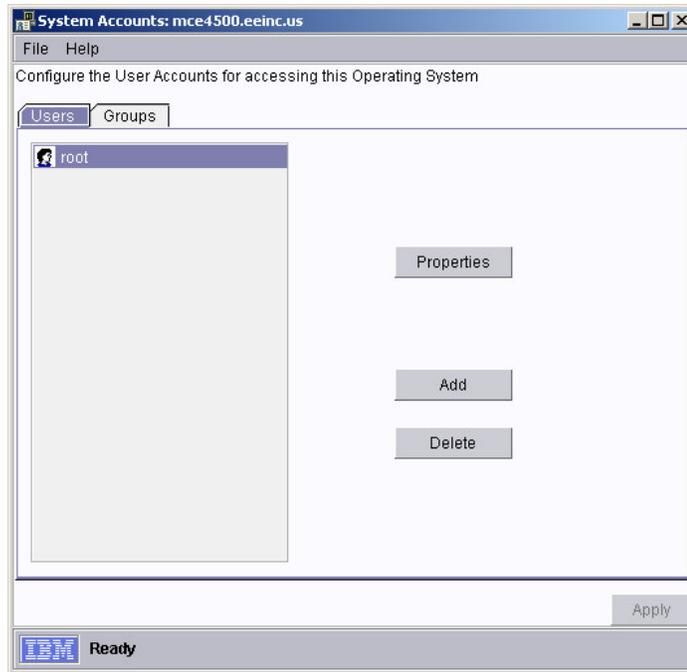


Figure 36 – System Accounts

The ServeRAID Manager task allows you to perform complete RAID management, including receiving events, creating/deleting arrays, and initialize/synchronize logical drives. Refer to Figure 37 – ServeRAID Manager on page 28.

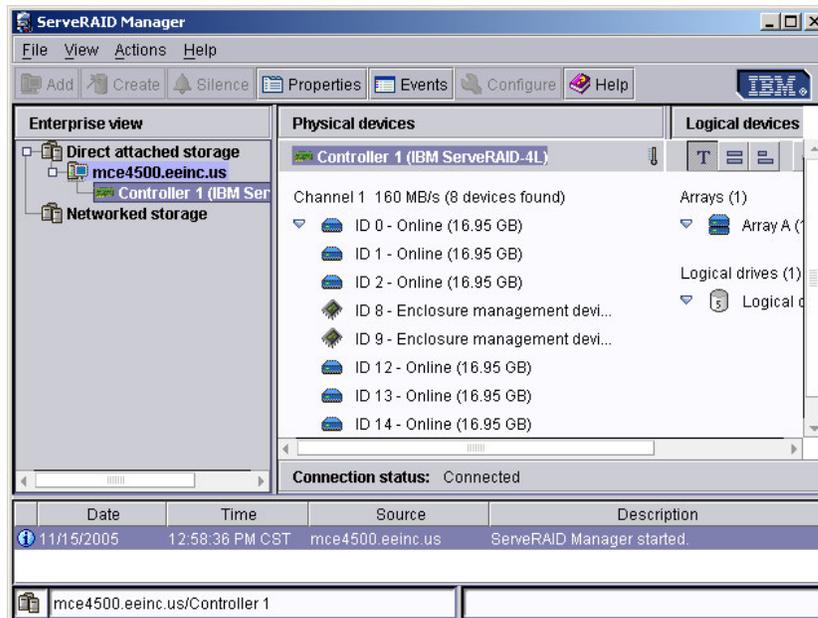


Figure 37 – ServeRAID Manager

The Capacity Manager Task, one of the IBM Director Extensions, enables capacity planning through trending, forecasting, and bottleneck identification. Performance data from the VMware ESX Server Console O/S is recorded on each VMware ESX Server. When a Capacity Manager report is executed, this data is gathered, analyzed, and displayed in a table and associated graphs. Refer to Figure 38 – Capacity Manager on page 29.

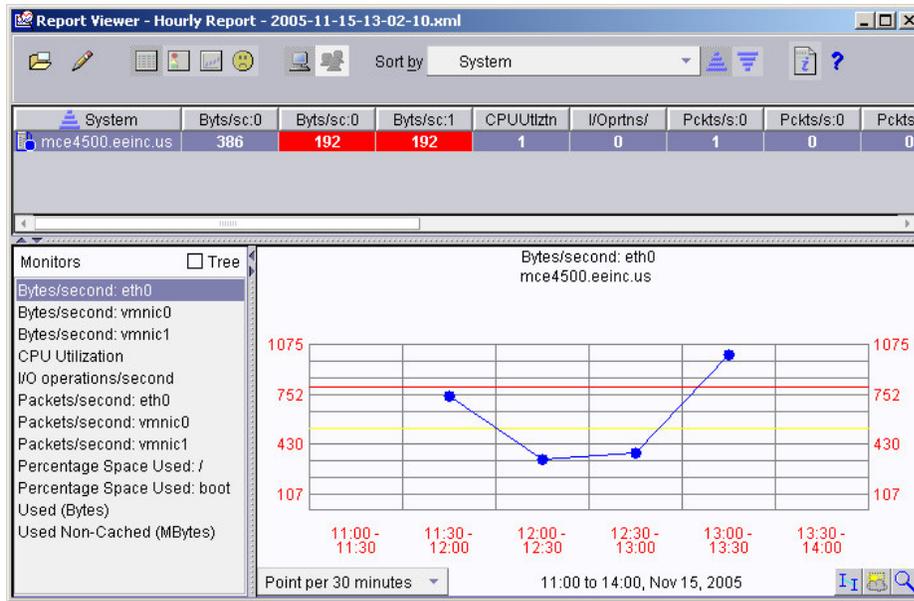


Figure 38 – Capacity Manager

The System Availability Task, another of the IBM Director extensions, tracks server up-time and downtime. Using VMware ESX Server Console O/S data from `/var/logs`, it produces an availability report, detailing all of the availability records and the system availability as a percentage. It also produces graphs to show uptime, downtime, and outages based on hour of the day and day of the week. Refer to Figure 39 – System Availability on page 29.

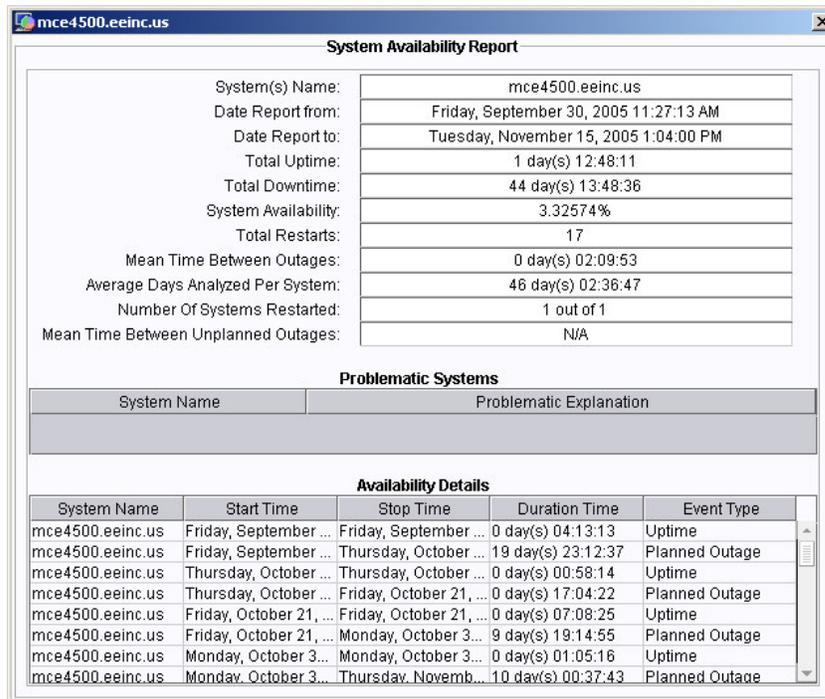


Figure 39 – System Availability

Event Action Plans can be created for IBM Director Agents similar to those created for SNMP devices. Rather than drilling-down thru the SNMP tree, the Events from the IBM Director Agent are dynamically published in the Director → Director Agent tree. This tree will be empty until a threshold has been configured, or an Event has been received from an IBM Director Agent.

Event details can also be included in Event Action messages. However, rather than using the OID, IBM Director Agent Events support variables available through Event Data Substitution. Refer to Table 2 — Event Data Substitution on page 31.

The Update Assistant Task provides an easy mechanism to update system software (i.e. BIOS, Diagnostics, Hard Drive Firmware) on a VMware ESX Server. These updates are imported from the UpdateXpress CD, and appear as Software Distribution subtasks. To apply the update, simply drag it to the VMware ESX Server. Refer to Figure 40 – Update Assistant on page 30. UpdateXpress is available for download from the IBM web site at <http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-53046>.

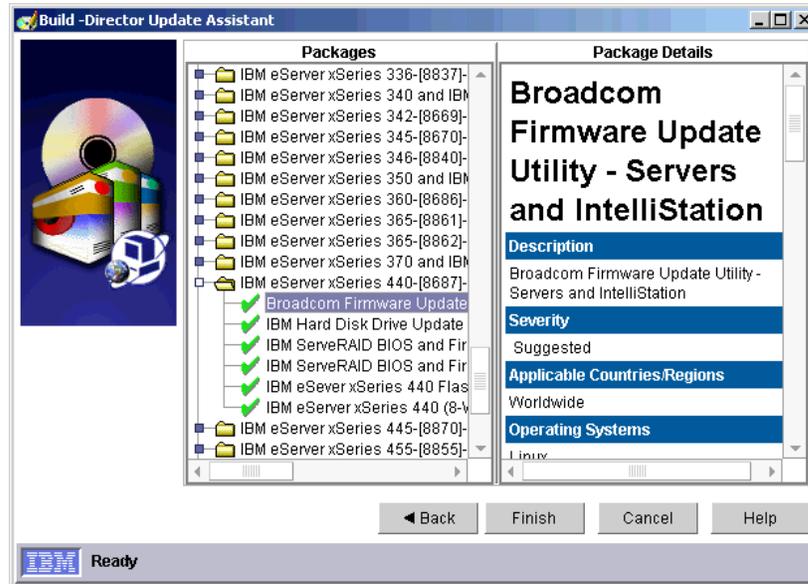


Figure 40 – Update Assistant

Managing VMware ESX Server with Virtual Machine Manager

IBM Virtual Machine Manager (VMM) is an extension to IBM Director that allows you to manage both physical and virtual machines from a single console. Virtual Machine Manager can manage VMware GSX Server, VMware ESX Server and Microsoft® Virtual Server environments using IBM Director. Virtual Machine Manager also integrates VMware VirtualCenter and IBM Director for advanced virtual machine management.

Virtual Machine Manager is comprised of several components – VMM Server, VMM Console, and VMM Agent. The VMM Server is installed on a system running the IBM Director Server. The VMM Console is installed on any IBM Director Console systems. If VirtualCenter is not being used, the IBM Director Agent and the VMM Agent are installed each ESX Server. If VirtualCenter is being used, the IBM Director Agent and the VMM Agent are installed on your VirtualCenter server, and the IBM Director Agent is installed on each ESX Server. Refer to Figure 41 – VMM Environment on page 31 for an example of the possible VMM deployment options.

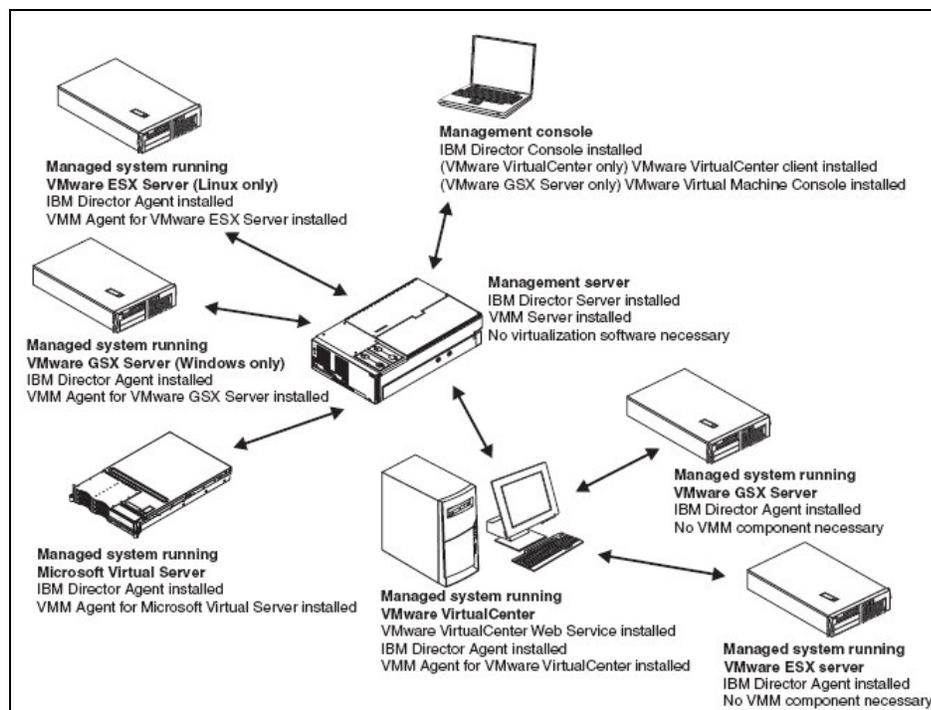


Figure 41 – VMM Environment

The following management tasks are provided by Virtual Machine management. The available management tasks differ depending on whether VirtualCenter is deployed or not.

Discovery

IBM Director can now discover systems running VMware and classify them as a VMM objects, displaying an additional icon to signify this classification. This icon will change depending on the object state. Additionally, IBM Director will discover all virtual machines on the VMware ESX Servers, also displaying the additional icon to signify the classification. Like the VMware ESX Server, this icon will also change depending on the state of the virtual machine. Virtual Machine Manager shows relationships between physical and virtual objects using the VMM Systems Membership association within the IBM Director Console. For example:

- VirtualCenter management server ¹

¹ With VirtualCenter

- Farm - grouping of Physical Hosts ¹
 - Physical Host ²
 - Virtual Machine ²
 - Operating System/Agent ²

Refer to Figure 42 – VMM Agent Discovery on page 31 for an example of the hierarchical view.

Name (arranged by Status) ▲	TCP/IP Addresses	TCP/IP Hosts
MCET30	192.168.0.51	mcet30.eeinc.us
MCEFarm		
mce4500.eeinc.us	192.168.0.54	mce4500.eeinc.us
RHEL40VM1	{ '192.168.0.116' }	
RHEL40VM2	{ '192.168.0.112' }	
rhel30vm2.eei...	192.168.0.112	
SLES9VM1	{ '192.168.0.103' }	
SLES9VM2		
WS03VM1		
WS03VM2	{ '192.168.0.115' }	
WS03VM2	192.168.0.115	WS03VM2
mce220.eeinc.us	192.168.0.52	mce220.eeinc.us
WS03VM3		
WS03VM3	192.168.0.108	WS03VM3

Figure 42 – VMM Agent Discovery

When discovering the VirtualCenter host running the IBM Director Agent and VMM Agent, credentials must be specified to allow IBM Director to access VirtualCenter. This is accomplished by right-clicking on the VirtualCenter host, and selecting Coordinator Management → Enter Credentials. The credentials specified are a User ID, Password, and Port used to access the VMware VirtualCenter Web Service. Refer to Figure 43 – VMM Credentials on page 31.

Enter Credentials

User ID

Password

Port

Figure 43 – VMM Credentials

Power Management

Virtual Machine Manager enhances the ability of the Power Management task, enabling you to perform power control of virtual machines. This includes:

- Power On
- Shutdown and Power Off
- Restart Now

¹ With VirtualCenter

² With or Without VirtualCenter

- Power Off Now
- Suspend
- Resume

Power Management tasks can be scheduled using the Job Scheduler to run at a specific time against any virtual machine. Note that the Shutdown and Power Off task requires a supported Operating System HAL/kernel.

Coordinator Management

These are tasks launched against the system running VirtualCenter, the IBM Director Agent, and the VMM Agent.

- Revoke Credentials
- Create VMM Farm
- Discover VMM Farms
- VMM Object Attributes

VMM Farm Management

These are tasks launched against the VMware Farms.

- Add Host to a VMM Farm
- Delete From Coordinator
- VMM Object Attributes

Host Management

These are tasks launched against the VMware hosts.

- Remove Host From VMM Farm ¹
- Discover Virtual Machines ²
- Create Virtual Machine ²
- Register Virtual Machine ³
- Create Migrate All Task ¹
- Power On All Stopped Virtual Machines ²
- Force Power Off All Running Virtual Machines ²
- Suspend All Running Virtual Machines ²
- Resume All Running Virtual Machines ²
- VMM Object Attributes ²

Virtual Machine Management

These are tasks launched against the virtual machines.

- Delete From Disk ²
- Create Single Migrate Task ¹
- Unregister From Host ³
- VMM Object Attributes ²
- Set Resources ²

¹ With VirtualCenter

² With or without VirtualCenter

³ Without VirtualCenter

Additional management tasks are available from the Tasks pane of the IBM Director Console. This includes the following:

Virtual Machine Manager Tasks

- Create VMM Farm ¹
- Help
- Migrate All Virtual Machine Tasks ¹
This task can be customized, allowing you to specify which host to migrate from and which host to migrate to. Additionally, you can specify to migrate to the host with the lowest CPU utilization. Refer to Figure 44 – Migrate All Virtual Machine Tasks on page 31.
- Migrate Single Virtual Machine Tasks ¹
This task can be customized, allowing you to specify which host to migrate a specific virtual machine to.
- Start Vendor Software ¹

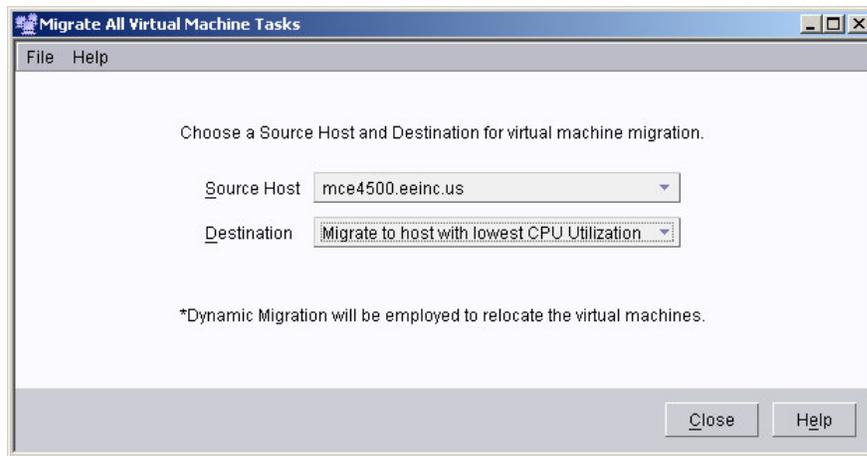


Figure 44 – Migrate All Virtual Machine Tasks

Event Processing

Events from Virtual Machine Manager are published to the Event Action Plan Filter Builder. These events can be used as part of an Event Action Plan, to provide notification or initiate management of VMware ESX Servers or Virtual Machines. The following events are published automatically:

- Agent Extension
 - Status Change
The VMM Agent is not running, it is not communicating with VirtualCenter, or it requires credentials to communicate with VirtualCenter
- Host
 - Started
 - Stopped
- Virtual Machine
 - Attribute Changed
 - Created
 - Deleted
 - Migration
 - Completed

¹ With VirtualCenter

- Started
- State
 - Pending
 - Powered Off
 - Powered On
 - Reset
 - Resumed
 - Suspended
- Task Failed
- VMM Farm
 - Created
 - Deleted
 - Host Added
 - Host Removed
 - Renamed

Refer to Figure 45 – Published Events on page 31 for an example.

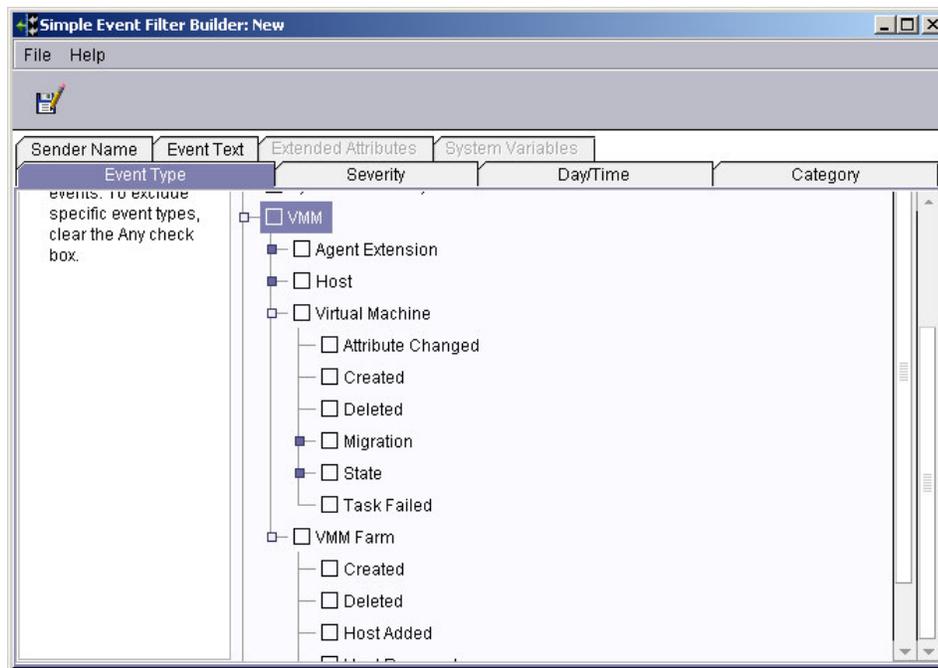


Figure 45 – Published Events

Virtual Machine Manager also adds new Actions to the Event Action Plan Builder. These Actions can be used as part of an Event Action Plan to automate management tasks in response to an Event. This includes the following Actions:

- Add a Host to a VMM Farm
- Add a Host to Virtual Center
- Manage a Host
 - Start (VirtualCenter only)
 - Stop (VirtualCenter only)
 - Power off all virtual machines
 - Power on all virtual machines
 - Resume all virtual machines
 - Suspend all virtual machines
- Manage a Virtual Machine

- Power on
- Shutdown and power off
- Power off now
- Suspend
- Resume
- Restart now
- Remove a Host from a Farm

Refer to Figure 46 – Event Actions on page 31 for an example.

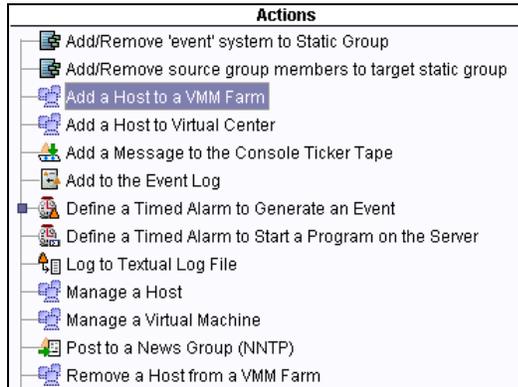


Figure 46 – Event Actions

Additional actions are available by using the action Start a Task on the “event” System to launch a migration task created from Host or Virtual Machine Management. Refer to Figure 47 – Start A Task Action on page 31.

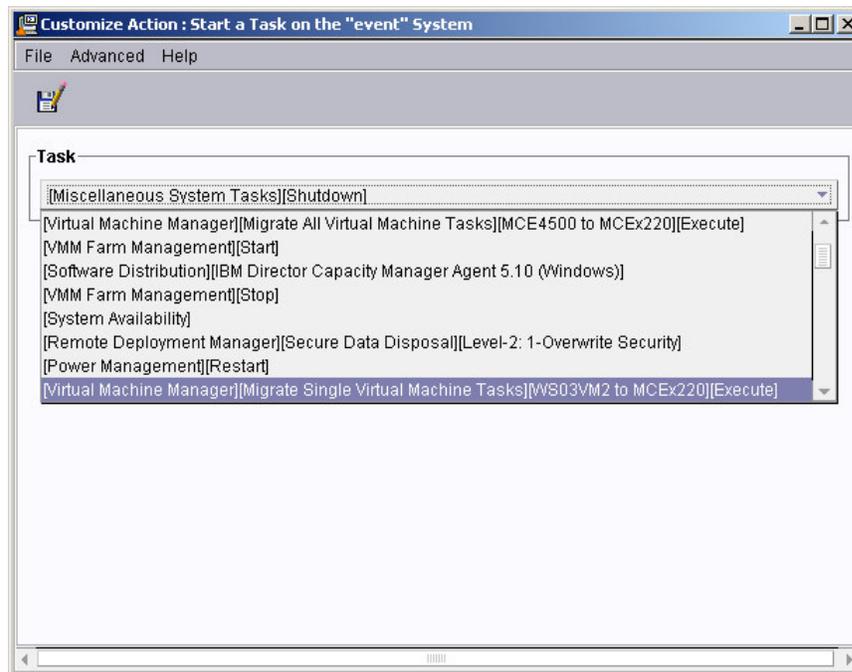


Figure 47 – Start A Task Action

Scheduled Tasks

Virtual Machine Manager Tasks can be executed on a reoccurring basis using the Scheduler. This includes the following:

- Coordinator Management
 - Discover VMM Farms
 - Revoke Credentials
- Host Management
 - Discover Virtual Machines
 - Force Power Off All Running Virtual Machines
 - Power On All Stopped Virtual Machines
 - Remove Host From VMM Farm
 - Resume All Suspended Virtual Machines
 - Start
 - Stop
 - Suspend All Running Virtual Machines
- Virtual Machine Management
 - Delete From Disk
- Virtual Machine Manager
 - Migrate All Virtual Machine Tasks
 - Migrate Single Virtual Machine Tasks
- VMM Farm Management
 - Delete From Coordinator
 - Start
 - Stop

Refer to Figure 48 – Virtual Machine Manager Jobs on page 31 for an example.

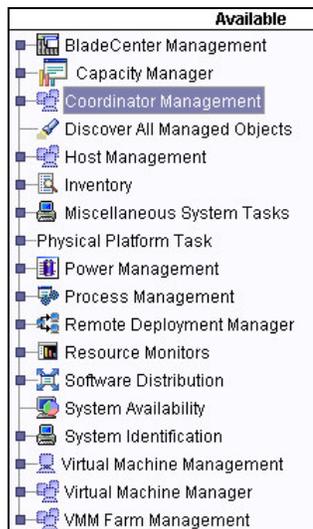


Figure 48 – Virtual Machine Manager Jobs

For more information on Virtual Machine Manager, refer to http://www-03.ibm.com/servers/eserver/xseries/systems_management/ibm_director/extensions/vmm.html.

Appendix

Inventory Data

Inventory Data	SNMP Agent	IBM Director Agent Level 0	IBM Director Agent Level 1	IBM Director Agent Level 2
Hardware				
Adapter				
Fibre Channel Adapter				
IDE Adapter				
Network Adapter	X	X	X	X
RAID Controllers				X
SCSI Adapter				
Chassis				
BladeCenter Chassis VPD				
Chassis Members				
Chassis Membership				
Device				
External				
- Keyboard				
- Pointing Device				
- Printer				
- RAID Enclosure				X
Internal				
- IDE Device				
- Management Processor				
- Parallel Port				
- PCI Device			X	X
- SCSI Device				
- Serial Port				
- System Slots				
Memory				
Cache			X	X
Installed Memory	X	X	X	X
Logical Memory				
Memory Modules		X	X	X
Network				
IP Address	X	X	X	X
IPX Address				
Management Processor Network Settings				
Network Adapter	X	X	X	X
Operating System Specific				
Geographic			X	X
LAN Network ID				
Lease			X	X
Operating System	X	X	X	X
Regional			X	X
Settings				
Alert On LAN Settings				
Alert Standard Format Settings				
ASP				

Inventory Data	SNMP Agent	IBM Director Agent Level 0	IBM Director Agent Level 1	IBM Director Agent Level 2
AssetID			X	X
Basic System Information	X	X	X	X
CIM			X	X
Device Drivers				
Director Agent			X	X
Director Systems		X	X	X
Firmware			X	X
FRU Service Numbers			X	X
IP Address	X	X	X	X
IPX Address	X			
iSeries Hardware				
Personalized Data				X
Port Connectors			X	X
Serial Number			X	X
System	X	X	X	X
System Location				X
System Resource				
System User				X
Unix Specific	X		X	X
User Details				X
Video				
Warranty			X	X
SMBIOS				
Baseboard		X	X	X
Component ID		X	X	X
On Board Device		X	X	X
Physical Enclosure		X	X	X
Processor	X	X	X	X
System BIOS		X	X	X
System Board Configuration		X	X	X
SNMP				
SNMP Agent	X			
SNMP Agent Configuration			X	X
SNMP Trap Destinations	X			
SNMP Users				
Storage				
Disk		X	X	X
Logical Drive		X	X	X
Partition		X	X	X
RAID Disk Drives				X
RAID Logical Drives				X
SMI-S Storage Device				
Software				
Device Drivers				
Installed Packages	X	X	X	X
Installed Patches				
Software				

Table 1 – Inventory Data

Event Data Substitution

Some event actions allow the inclusion of event-specific information as part of the text message. Including event information is referred to as event data substitution. Refer to the help associated with a specific event action template for information on where event data substitution can be used.

The text of an event message is divided into keywords. When used in a message, a keyword must be preceded by the ampersand symbol (&). The keywords are:

&date	Specifies the date the event occurred.
&time	Specifies the time the event occurred.
&text	Specifies the event text, if supplied by the event.
&type	Specifies the event type criteria used to trigger the event.
&severity	Specifies the severity level of the event.
&system	Specifies the name of the system for which the event was generated.
&sender	Specifies the name of the system from which the event was sent. This keyword returns null if unavailable.
&group	Specifies the group to which the target system belongs and is being monitored. This keyword returns null if unavailable.
&category	Specifies the category of the event.
&pgmtype	Specifies a dotted representation of the event type using internal type strings.
×tamp	Specifies the coordinated time of the event (milliseconds since 1/1 /1 970 12:00 AM GMT).
&rawsev	Specifies the non-localized string of event severity (FATAL, CRITICAL, MINOR, WARNING, HARMLESS, UNKNOWN).
&rawcat	Specifies the non-localized string of event category (ALERT, RESOLVE).
&corr	Specifies the correlator string of the event. Related events, such as those from the same monitor threshold activation, will match this.
&snduid	Specifies the unique ID of the event sender.
&sys uid	Specifies the unique ID of the system associated with the event.
&prop:filename#proprname	Specifies the value of the property string proprname from property file filename (relative to \tivoliWg\classes).
&sysvar:varname	Specifies the event system variable varname. This keyword returns null if a value is unavailable.
&slotid:slot-id	Specifies the value of the event detail slot with the non-localized ID slot Id.
&md5hash	Specifies the MD5 hash code (CRC) of the event data (good event specific unique ID).
&hashtxt	Specifies a full replacement for the field with an MD5 hashcode (32-character hexcode) of the event text.
&hashtxt16	Specifies a full replacement for the field with a

	short MD5 hashcode (16-character hexcode) of the event text.
&otherstring	Specifies the value of the detail slot with the localized label that matches otherstring. This ke.word returns OTHERSTRING if unavailable.

Table 2 — Event Data Substitution

Note: When you specify an event data substitution keyword containing more than one word, substitute the underscore character (“_”) for each space between words. For example, to use the keyword “User Login” you must enter “User_Logon” in the text of the event message. A sample entry containing this keyword might be: “User &User_Logon just logged on to the system.”

Example of message text with event data substitutions:

Please respond to the event generated for &system, which occurred &date. The text of the event was &text with a severity of &severity.

References

VMware ESX Server Installation Guide

http://www.vmware.com/pdf/esx25_install.pdf

VMware ESX Server Administration Guide

http://www.vmware.com/pdf/esx25_admin.pdf

VMware VirtualCenter User's Manual

http://www.vmware.com/pdf/vc_users12.pdf

IBM Director Installation and Configuration Guide Version 5.10

ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir510_docs_install.pdf

IBM Director Systems Management Guide Version 5.10

ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir510_docs_sysmgt.pdf

IBM Director Version 5.10 Hardware and Software Compatibility

ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir510_compatibility.pdf

IBM Director Release Notes Version 5.10

ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir5.10_docs_relnotes.pdf

IBM Director Events Reference Version 5.10

ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir510_events_ref.pdf

IBM Director Version 5.10 Information Center

http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp?topic=/dirinfo/fqm0_main.html

IBM UpdateXpress

http://www-1.ibm.com/servers/eserver/xseries/systems_management/sys_migration/xpress.html

IBM Server Plus Pack

http://www-1.ibm.com/servers/eserver/xseries/systems_management/director_spp.html

IBM Virtual Machine Manager

http://www-03.ibm.com/servers/eserver/xseries/systems_management/ibm_director/extensions/vmm.html

IBM eServer FORUMS

http://www-128.ibm.com/developerworks/forums/dw_esforums.jsp

Trademarks

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

Active PCI	Intellistation	ServerProven
AIX	iSeries	SurePOS
Asset ID	Netfinity	ThinkCentre
BladeCenter	NetView	ThinkPad
DB2	NetVista	Tivoli
DB2 Universal Database	OS/400	Tivoli Enterprise
e-business logo	PowerPC	Tivoli Enterprise Console
@server	Predictive Failure Analysis	Total Storage
IBM	pSeries	Wake on LAN
IBM i5/OS	RedBooks	xSeries
IBM Virtualization Engine	ServeRAID	

Intel and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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.

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