



MANAGEMENT  
SOLUTION FOR  
9<sup>TH</sup>-GENERATION  
POWEREDGE SERVERS  
RUNNING NETWARE 6.5

---

REFERENCE ARCHITECTURE,  
STEP-BY-STEP IMPLEMENTATION,  
SUPPORT

CUSTOM SOLUTIONS ENGINEERING

V 1.0

# MANAGEMENT SOLUTION FOR 9<sup>TH</sup>- GENERATION POWEREDGE SERVERS RUNNING NETWARE 6.5

---

## INTRODUCTION

---

This document outlines:

- The reference architecture
- Step-by-step instructions on how to implement the architecture
- The support model for this configuration

The main goal of this architecture is to provide a method for the instrumented PowerEdge server and its internal storage to send SNMP alerts. The architecture separates the server from the storage and details instructions specific to each of the two subsystems. Although the information presented herein is not 9<sup>th</sup>-generation PowerEdge servers-specific, the architecture has been tested only on 9<sup>th</sup>-generation servers, thus it is supported only on these platforms.

The server hardware subsystem comprises all hardware components located in the PowerEdge server chassis with the exception of the SAS RAID controllers and the SAS hard drives. The storage subsystem comprises the internal SAS RAID controllers and drives.

The server hardware subsystem is being monitored by the Baseboard Management Controller (BMC) and/or the Dell Remote Access Card (DRAC). The BMC is a standard component for 9<sup>th</sup>-generation servers. The DRAC implementation for 9<sup>th</sup>-generation servers is named DRAC5 and it is an optional component. The customer can choose between BMC and DRAC5 depending on existing management infrastructure, previous experience on using one versus the other, etc. It is highly recommended to use only one of the two, not both, because of potentially confusing alert information.

For the storage subsystem, this architecture introduces two off-the-shelf SAS RAID controllers, the 4800SAS and 4805SAS. The controllers are almost identical with the exception of the PCI interface. The 4800SAS controller has a PCI-X interface. The 4805SAS controller has a PCIe interface. Both controllers are supported by the same software stack for NetWare – driver, management utility, CLI, etc.

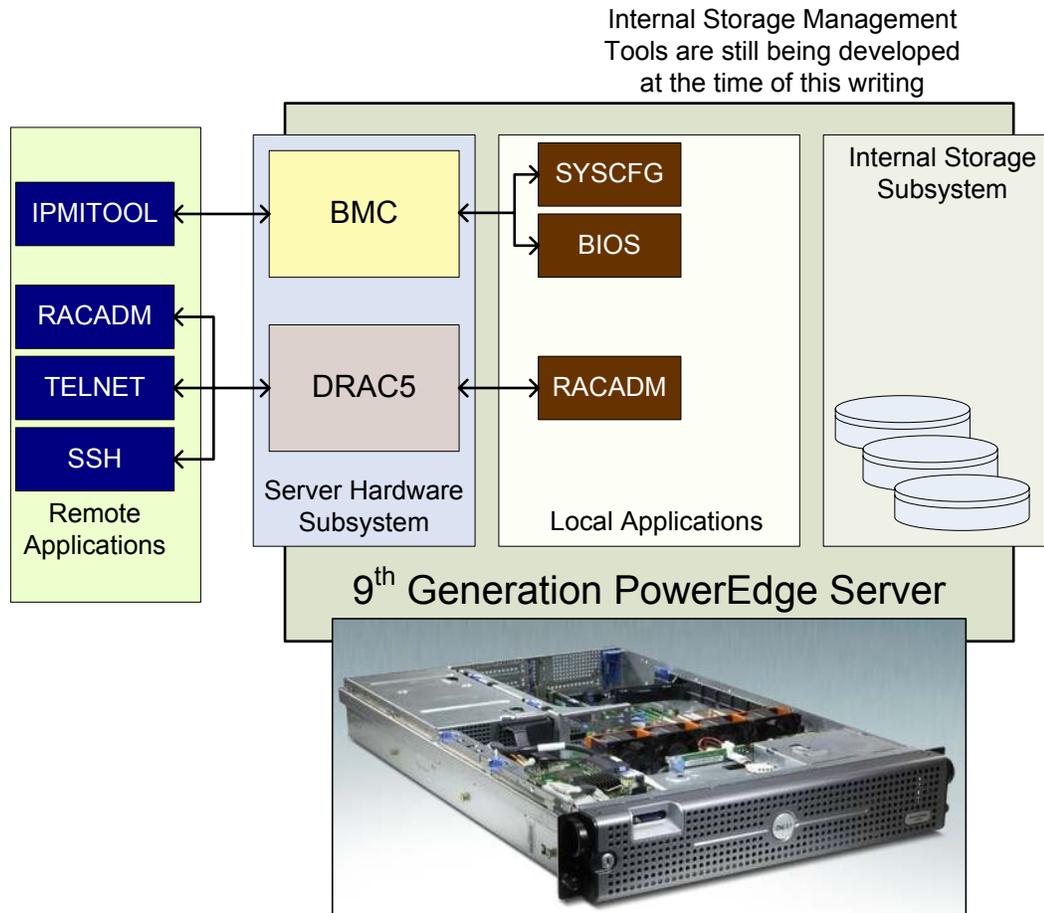
The architecture has no dependency on Dell OpenManage Server Administrator (OMSA) systems management software stack. Thus, there will be no OMSA running on the 9<sup>th</sup>-generation PowerEdge server running NetWare 6.5.

---

## REFERENCE ARCHITECTURE

---

As described in the introduction, the proposed architecture looks at the system as a sum of two separate entities: the server hardware (CPU, memory, PCI bus, power supplies, etc.) subsystem and the internal storage (hard drives and associated controllers) subsystem. The two entities are managed with different utilities, interface, software, etc.



The figure above highlights all the components (hardware and software) that are required to make this architecture work.

The server hardware subsystem is composed of all hardware components that are located inside the PowerEdge chassis with the exception of internal drives and SAS controller. The internal storage subsystem is composed of internal SAS controller and the attached internal hard disks.

The components that do the SNMP alerting need to be configured for the task. The applications used to configure the server subsystems are different from applications for storage subsystem.

For the server hardware subsystem, the Baseboard Management Controller (BMC) can be configured locally during BIOS POST (power-on system test) or with the DOS version of SYSCFG, a utility that is part of the Dell Deployment Toolkit (DTK). The BMC can be configured remotely using IPMITOOL, an open-source utility.

The Dell Remote Access Controller (DRAC) can be configured using RACADM. Locally, the DOS version of RACADM can be used. Remotely, the same configuration changes can be made using the remote connect capabilities of RACADM or executing the same RACADM comments in a Telnet or SSH shell session.

There is no need for any software running on the instrumented host once the BMC or the DRAC have been configured for monitoring and alerting. See next section for configuring either of the two.

The internal storage subsystem requires a Command Line Interface Tool.. This tool was still under development at the time of this writing. Please contact your account team for information on the availability of storage management tools.

---

## BMC-BASED SNMP ALERTING

---

The BMC alerts are very comparable to Dell OpenManage events, events are listed at the end of this documentation. One might want to forward the BMC events on to Dell ITA which is already built to receive the BMC events.

There are two major functions one wants to configure on the BMC chip; first configure the BMC via the BIOS and via a BMC config menu at startup. At this point one can point the 70 possible events to trap to an event reception console (likely ITA). The second task is to configure the BMC management utility to communicate with the BMC; this will need to be loaded on a remote Windows or Linux based server.

All pertinent documentation for this process is on the Dell product documentation CD but the important steps are listed here.

### CONFIGURING BMC IN BIOS

1. Turn on and restart your system.
2. Press <F2> immediately after you see the following message:

<F2> = Setup

The **System Setup** screen appears.

 **NOTE:** If your operating system begins to load before you press <F2>, allow the system to finish booting, and then restart your system and try again.

3. Use the up- and down- arrow keys to navigate to the Serial Communication field and press <Enter>.
4. Use the spacebar to select the appropriate serial communication option.
5. Select the appropriate option for Console Redirection. The following options are available:

**On without Console Redirection:** COM1 and COM2 are enabled and available for use by the operating system or applications. Console redirection is disabled. This is the default option.

**On with Console Redirection via COM1:** COM1 and COM2 are enabled and available for use by the operating system and applications. BIOS Console redirection is through COM1.

**On with Console Redirection via COM2:** COM1 and COM2 are enabled and available for use by the operating system or applications. BIOS Console redirection is through COM2.

Off: COM1 and COM2 are both disabled and not available for use by the operating system or applications. BIOS Console redirection is disabled.

 **NOTE:** Select **On with Console Redirection via COM2** to use Console Redirection with SOL.

6. Press <Enter> to select and return to the previous screen.
7. Use the up- and down- arrow keys to navigate to the External Serial Communication field and press <Enter>.
8. Use the spacebar to select the appropriate external serial communication option.

The available options are COM1, COM2, and Remote Access. The default option is COM1.

 **NOTE:** Select **Remote Access** to access the BMC through the serial cable connection. This option can be set to any value for using SOL and accessing the BMC over LAN.

9. Press <Enter> to select and return to the previous screen.
10. If required, use the spacebar to navigate to and change the settings for Redirection after Boot.
11. Use the up- and down- arrow keys to navigate to the Failsafe Baud Rate option and then use the space bar to set the console failsafe baud rate, if applicable.
12. Use the up- and down- arrow keys navigate to the Remote Terminal Type option and then use the space bar to select either VT 100/VT 200 or ANSI, if applicable.
13. Press <Enter> to return to the **System Setup** screen.
14. Press <Esc> to exit the System Setup program. The **Exit** screen displays the following options:
  - Save Changes and Exit
  - Discard Changes and Exit
  - Return to Setup

 **NOTE:** For most options, any changes that you make are recorded but do not take effect until you restart the system.

## BASEBOARD MANAGEMENT CONTROLLER CONFIGURATION

You can perform basic BMC configuration using the Remote Access Configuration Utility during system startup. See figure 1-1 below for initial screen.

## ENTERING THE REMOTE ACCESS CONFIGURATION UTILITY

1. Turn on or restart your system.
2. Press <Ctrl-E> when prompted after POST.

If your operating system begins to load before you press <Ctrl-E>, allow the system to finish booting, and then restart your system and try again.

## REMOTE ACCESS CONFIGURATION UTILITY OPTIONS

**Figure 1-1. Remote Access Configuration Utility**

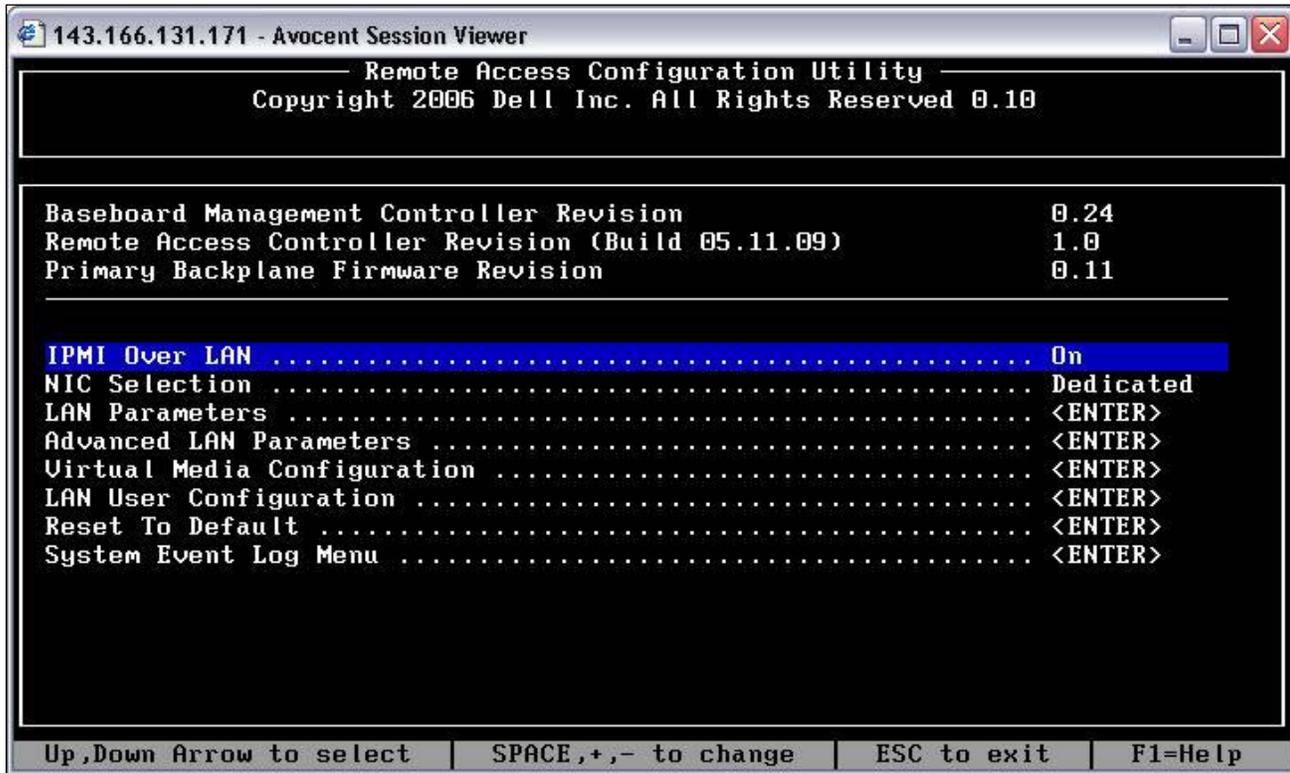


Table 1-1 lists the Remote Access Configuration Utility options and shows how to configure the BMC on a managed system.

Option	Description
IPMI Over LAN	Enables or disables the out-of-band LAN channel access to the shared network controller.
NIC Selection <b>NOTE:</b> This option is available only on Dell PowerEdge x9xx systems.	Displays the configuration option. <ul style="list-style-type: none"> <li>• Shared               <p>Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating system is configured for NIC teaming.</p> <p>The remote access device receives data through NIC 1 and NIC 2, but transmits data only through NIC 1.</p> <p><b>NOTE:</b> If NIC 1 fails, the remote access device will not be accessible.</p> <p><b>NOTE:</b> The NIC 2 is not available on the PowerEdge 1900 system.</p> </li> <li>• Failover               <p>Select this option to share the network interface with the host operating system. The remote access device network interface is fully functional when the host operating system is configured for NIC teaming.</p> </li> </ul>

	<p>The remote access device receives data through NIC 1 and NIC 2, but transmits data only through NIC 1. If NIC 1 fails, the remote access device fails over to NIC 2 for all data transmission.</p> <p>The remote access device continues to use NIC 2 for data transmission. If NIC 2 fails, the remote access device fails over all data transmission back to NIC 1.</p> <p><b>NOTE:</b> This option cannot be selected on the PowerEdge 1900 system.</p> <ul style="list-style-type: none"> <li>• Dedicated</li> </ul> <p>Select this option to enable the remote access device to utilize the dedicated network interface available on the Remote Access Controller (RAC). This interface is not shared with the host operating system and routes the management traffic to a separate physical network, enabling it to be separated from the application traffic.</p> <p><b>NOTE:</b> This option is available only if a DRAC card is installed in the system.</p>
Encryption Key	<p>Is used to encrypt the IPMI sessions.</p> <p><b>NOTE:</b> This option is available only on PowerEdge x9xx systems.</p> <p><b>NOTE:</b> The encryption key must be a hexadecimal number with a maximum length of 20 bytes, for example, 01FA3BA6C812855DA0.</p>
Static IP vs. DHCP Source	<p>Displays whether the network controller will be assigned a static IP address or a DHCP address.</p>
BMC IP Address	<p>The static IP address of the BMC. This field is limited to a maximum value of 255.255.255.255.</p> <p><b>NOTE:</b> IP address 169.254.0.2 is returned when the BMC is unable to contact the DHCP server.</p> <p><b>NOTE:</b> Two rules apply to the IP address when it is being entered:</p> <ul style="list-style-type: none"> <li>• It cannot be 127.xxx.xxx.xxx.</li> <li>• 1st octet must be between 001-223.</li> </ul>
MAC Address	<p>Displays the network controller's BMC MAC address.</p>
Subnet Mask	<p>The subnet mask for the static IP address.</p>
Default Gateway	<p>The IP gateway for the static IP address.</p>
VLAN Enable	<p>Enables or disables the virtual LAN ID.</p>
VLAN ID	<p>A valid value for the virtual LAN ID must be a number from 1 to 4094.</p> <p><b>NOTE:</b> If you enter a value outside the specified range, an error message displays when changes are applied.</p>

VLAN	Specifies the priority of the VLAN. The valid values range from 0-7.
Alerting	Enables or disables BMC alerting.
Alert IP Address	Displays the address of the first alert destination.
Alert Destinations	Enables or disables BMC alerting destinations.
Hostname	Specifies the managed system hostname used to correlate Platform Event Traps to the system on which they originate.
Advanced LAN Parameters <b>NOTE:</b> This option is available only on systems installed with a DRAC card.	Enables setting the LAN speed and configuring Domain Name (DN) and Servers options, such as setting the IP address for the DN servers, registering the RAC name, and setting the domain name from DHCP.
Virtual Media Configuration <b>NOTE:</b> This option is available only on systems installed with a DRAC card.	Enables setting the virtual media and virtual flash.
LAN User Configuration	Enables setting the user name, user password, user privilege, and enables user access for user ID=2.
Reset To Default	Clears the BMC settings and resets the BMC setting to the defaults.
System Event Log	Enables viewing and clearing the system event log.

 **NOTE:** If the first integrated network interface controller (NIC 1) is used in an Ether Channel team or link aggregation team, the BMC management traffic will not function on PowerEdge x8xx systems. The NIC teaming option is supported only on PowerEdge x9xx systems. For more information about network teaming, see the documentation for the network interface controller.

## INSTALLING BMC MANAGEMENT UTILITY ON SYSTEMS RUNNING SUPPORTED WINDOWS OPERATING SYSTEMS

Find the BMC management utility on the OpenManage Server Administrator CD.

To install the BMC Management Utility on a management station running the Windows operating system, perform the following steps:

1. Log in with administrator privileges to the system where you want to install the systems management software components.
2. Exit any open application programs and disable any virus-scanning software.
3. Insert the *Dell OpenManage™ Systems Management Consoles* CD into your system's CD drive.

If the CD does not automatically start the setup program, click the **Start** button, click **Run**, and then type `x:\windows\setup.exe` (where x is the drive letter of your CD drive).

The **Dell OpenManage Management Station Installation** screen appears.

4. Click **Install, Modify, Repair or Remove Management Station**.

The **Welcome to Install Wizard for Dell OpenManage Management Station** screen appears.

5. Click **Next**.

A software license agreement appears.

6. Select **I accept the terms in the license agreement**, if you agree.

The **Setup Type** screen appears.

7. Select **Custom Setup** and click **Next**.

The **Custom Setup** screen appears.

8. From the drop-down, which appears on the left side of BMC Console, select **this feature, and all sub features will be installed on the local hard drive**.

To accept the default directory path, click **Next**. Otherwise, click **Browse** and navigate to the directory where you want to install your software, and then click **Next**.

The **Ready to Install the Program** screen appears.

9. Ensure that all information is correct and click **Install**.

The **Installing Dell OpenManage Management Station** screen appears and displays the status of the installation.

10. When installation is complete, the **Install Wizard Completed** screen appears. Click **Finish**.

 **NOTE: Enable the virus scanning software after installation.**

See the *Dell OpenManage Version 5.0 User's Guide* for additional information about installing the BMC Management Utility on a management station.

By default, the installation program copies the files to the following directory:  
**C:\Program Files\Dell\SysMgt\bmc.**

The SOL Proxy service does not auto-start after installation. To start the SOL Proxy service after installation, you can reboot the system (SOL Proxy automatically starts on a reboot). To restart the SOL Proxy service on Windows systems, complete the following steps:

1. Right-click My Computer and click Manage. The Computer Management window is displayed.
2. Click Services and Applications and then click Services. Available services are displayed to the right.
3. Locate DSM\_BMU\_SOLProxy in the list of services and right-click to start the service.

**CONFIGURING BMC EVENTS USING SYSCFG:**

Syscfg is the part of Dell-DTK tool (That works in PRE-OS boot environment) With syscfg one can set the BMC alerts. Following are the BMC options to set the platform events using syscfg

syscfg --help pcp	Help on pcp command.
syscfg pcp	List the current settings for the platform event filters.
syscfg pcp <Sub-options>	<p>Sub-options:</p> <p>--filter</p> <p>Valid Arguments:</p> <p><b>Fanfail</b> The fan is running too slow or not at all</p> <p><b>volfail</b> The Voltage is too low for proper operation</p> <p><b>descretevoltfail</b> The Voltage is too low for proper operation</p> <p><b>tempwarn</b> Temperature is approaching excessively high or low limits</p> <p><b>tempfail</b> Temperature is either too high or too low for proper operation</p> <p><b>intrusion</b> The system chassis has been open</p> <p><b>redundegraded</b> Redundancy for the fans and/or power supply has been reduced</p> <p><b>redunlost</b> No redundancy remains for the system's fan and/or power supplies</p> <p><b>proccwarn</b> A process is running less than peak performance or speed</p> <p><b>Proccfail</b> A processor has failed</p> <p><b>powerwarn</b> The power supply, voltage regulator, module or DC-to-DC converter is pending a failure condition</p> <p><b>powerfail</b> The power supply, voltage regulator, module or DC-to-DC converter is pending has failed</p> <p><b>hardwarelogfail</b> Either an empty or full hardware log requires administrator attention</p> <p><b>autorecovery</b> The system is hung or is not responding and is taking an action configured by automatic system recovery</p> <p>--filteraction</p> <p>Valid Arguments powercycle reset powerdown none</p> <p>--hostname &lt;string&gt;</p> <p>--filteralert &lt;enable/disable&gt;</p> <p>--alertpolnum &lt;1,2,3,4&gt;</p> <p>--alertpolstatus &lt;enable/disable&gt;</p>

For Example:

```
syscfg pcp --filter=intrusion --filteraction=reset
```

Set the action server rest for a particular filter like chassis intrusion.

## CONFIGURING ALERTS USING IPMITOOL:

IPMITOOL event send predefined events to Management Controller

IPMITOOL EVENT <NUM>	Send generic test events 1: Temperature - Upper Critical - Going High 2: Voltage Threshold - Lower Critical - Going Low 3: Memory - Correctable ECC
IPMITOOL EVENT FILE <FILENAME>	Read and generate events from file  USE THE 'SEL SAVE' COMMAND TO GENERATE FROM SEL
Ipmitool event <sensorid> <state> [event_dir]	sensorid: Sensor ID to use for event data state:Sensor state, use 'list' to see possible states for sensor event_dir : assert, deassert [default=assert]

## EVENTS GENERATED BY BMC:

Trap ID	Description	Severity
262402	Generic Critical Fan Failure	Critical
262530	Generic Critical Fan Failure Cleared	Informational
131330	Under-Voltage Problem (Lower Critical - going low)	Critical
131458	Under-Voltage Problem Cleared	Informational
131841	Generic Critical Voltage Problem	Critical
131840	Generic Critical Voltage Problem Cleared	Informational
65792	Under-Temperature Warning (Lower non-critical, going low)	Warning
65920	Under-Temperature Warning Cleared	Informational
65794	Under-Temperature Problem (Lower Critical - going low)	Critical
65922	Under-Temperature Problem Cleared	Informational
65799	Over-Temperature warning (Upper non-critical, going high)	Minor
65927	Over-Temperature warning Cleared	Informational
65801	Over-Temperature Problem (Upper Critical - going high)	Critical
65929	Over-Temperature Problem Cleared	Informational

131328	Under-Voltage Warning (Lower Non Critical - going low)	Warning
131456	Under-Voltage Warning Cleared	Informational
131330	Under-Voltage Problem (Lower Critical - going low)	Critical
131458	Under-Voltage Problem Cleared	Informational
131335	Over-Voltage Warning (Upper Non Critical - going high)	Warning
131463	Over-Voltage Warning Cleared	Informational
131337	Over-Voltage Problem (Upper Critical - going high)	Critical
131465	Over-Voltage Problem Cleared	Informational
131841	Generic Critical Voltage Problem	Critical
131840	Generic Critical Voltage Problem Cleared	Informational
356096	Chassis Intrusion - Physical Security Violation	Critical
356224	Chassis Intrusion (Physical Security Violation) Event Cleared	Informational
262400	Generic Predictive Fan Failure (predictive failure asserted)	Minor
262528	Generic Predictive Fan Failure Cleared	Informational
262402	Generic Critical Fan Failure	Critical
262530	Generic Critical Fan Failure Cleared	Informational
264962	Fan redundancy has been degraded	Warning
264961	Fan Redundancy Lost	Critical
264960	Fan redundancy Has Returned to Normal	Informational
2715392	Battery Low (Predictive Failure)	Warning
2715520	Battery Low (Predictive Failure) Cleared	Informational
2715393	Battery Failure	Critical
2715521	Battery Failure Cleared	Informational

487169	CPU Thermal Trip (Over Temperature Shutdown)	Critical
487297	CPU Thermal Trip (Over Temperature Shutdown) Cleared	Informational
487168	CPU Internal Error	Critical
487296	CPU Internal Error Cleared	Informational
487173	CPU Configuration Error	Critical
487301	CPU Configuration Error Cleared	Informational
487175	CPU Presence (Processor Presence detected)	Informational
487303	CPU Not Present (Processor Not Present)	Critical
487170	CPU BIST (Built In Self Test) Failure	Critical
487298	CPU BIST (Built In Self Test) Failure Cleared	Informational
487176	CPU Disabled (Processor Disabled)	Critical
487304	CPU Enabled (Processor Enabled)	Informational
487178	CPU Throttle (Processor Speed Reduced)	Warning
487306	CPU Throttle Cleared (Normal Processor Speed)	Informational
527106	Power Supply Redundancy Degraded	Warning
527105	Power Supply Redundancy Lost	Critical
527104	Power Supply Redundancy Has Returned to Normal	Informational
552704	Power Supply Inserted	Informational
552832	Power Supply Removed	Warning
552705	Power Supply Failure	Critical
552833	Power Supply Failure Cleared	Informational
552706	Power Supply Warning	Warning
552834	Power Supply Warning Cleared	Informational
552707	Power Supply AC Lost	Critical

552835	Power Supply AC Restored	Informational
789249	Memory Redundancy Has Been Lost	Critical
789248	Memory redundancy Has Returned to Normal	Informational
1076994	System Event Log (SEL) Cleared	Informational
1076996	System Event Log (SEL) Full (Logging Disabled)	Critical
2322176	ASR (Automatic System Recovery) Timer Expired	Critical
2322177	ASR (Automatic System Recovery) Reset Occurred	Critical
2322178	ASR (Automatic System Recovery) Power Down Occurred	Critical
2322179	ASR (Automatic System Recovery) Power Cycle Occurred	Critical

SNMP is often used to monitor systems for fault conditions such as voltage failure or fan malfunction. Management applications such as ITA can monitor faults by polling the appropriate object identifiers (OIDs) with the get command and analyzing the returned data. However, this polling method has its challenges. Performed frequently, polling can consume significant amounts of network bandwidth. Performed infrequently, this method may not allow administrators to respond quickly enough to the fault condition.

SNMP agents, supported by the DRAC, can overcome such limitations by sending alerts or SNMP traps to designated recipients. The DRAC can notify administrators when a system fails or is going to fail. To receive DRAC SNMP traps at a management station running IT Assistant, the DRAC must be configured for the trap destination, trap community name, and so on.

The DRAC can also be configured to notify different trap destinations for different events by setting the proper SNMP trap filter. When the DRAC detects a new event, the DRAC inspects the event against each destination's trap filter and sends an SNMP trap to the appropriate destination. Configuring alerts DRAC alerts consist of e-mail alerts and SNMP traps. The e-mail alert contains the following information: message, event description, date, time, severity, system ID, model, asset tag, service tag, managed system host name, and Embedded Server Management (ESM) version. The SNMP trap provides specific information describing the cause and source of the event. This information includes sensor identification, entity or Intelligent Platform Management Bus (IPMB) slave address, sensor number, sensor ID string (if possible), current sensor reading, range, and threshold values.

### ADDING A USER WITH ALERT CAPABILITIES

To add a user who can receive e-mail notification, first locate the appropriate user index by entering `racadm getconfig -u username` command. Then, enter the following commands:

1. `racadm config -g cfgUserAdmin -o cfgUserAdminEmailEnable -i index 1`
2. `racadm config -g cfgUserAdmin -o cfgUserAdminEmailAddress -i userindex email_address`
3. `racadm config -g cfgUserAdmin -o cfgUserAdminEmailCustomMsg -i userindex Custom Message`
4. `racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr SMTP_Server_IP`

**NOTE:** For remote execution of RACADM, precede each subcommand with `-r <rac_ip> -u <username> -p <password>`, where `<rac_ip>` is DRAC's IP address, and `<username>/<password>` are proper DRAC credentials. For example, the syntax for the first config command above is:

```
racadm -r 192.168.0.120 -u root -p calvin config -g cfgUserAdmin -o cfgUserAdminEmailEnable -i index 1
```

### ENABLING SNMP TRAPS

Up to 16 SNMP trap entries can be stored in the DRAC MIB. To locate an available index to add a new SNMP trap, execute the following command for each index from 1 through 16 until an available index is located:

```
racadm getconfig -g cfgTraps -i trapindex
```

After an available index is located, enter the following command to enable an SNMP trap:

```
racadm config -g cfgTraps -o cfgTrapsEnable -i trapindex 1
```

```
racadm config -g cfgTraps -o cfgTrapsDestIpAddr -i trapindex IP_Address
```

```
racadm config -g cfgTraps -o cfgTrapsSnmpCommunity -i trapindex Community_Name
```

To create a test trap, enter the following command:

```
racadm testtrap -i trapindex
```

---

## STORAGE SUBSYSTEM FOR 9<sup>TH</sup>-GENERATION POWEREDGE SERVERS

---

Serial Attached SCSI (SAS) is the enterprise storage interface that takes SCSI into new dimensions of performance, flexibility and scalability. With SAS you can enjoy performance many times faster than traditional SCSI and mix and match SAS and Serial ATA (SATA) drives for cost and performance optimization.

---

## STORAGE SUBSYSTEM SNMP ALERTING

---

### SUBSYSTEM SNMP ALERTING

#### NETWARE SNMP — GET CONFIGURATION

Here is the configuration of SNMP on a NetWare box,

1. Load the inetcfg tool.
2. Select Manage Configuration.

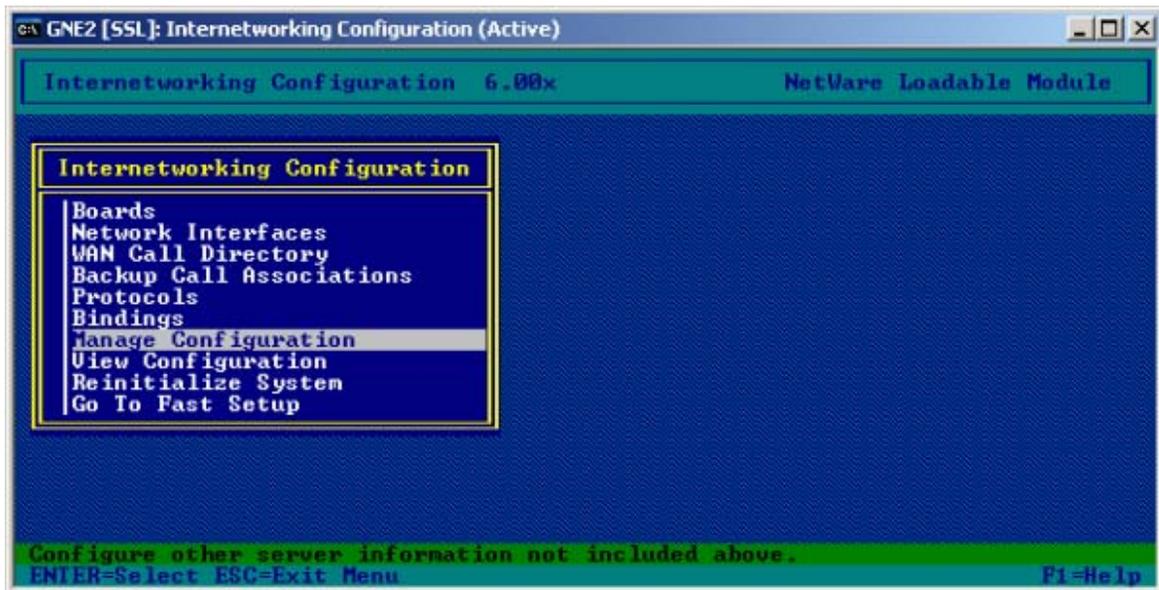


Figure 1 - Manage Configuration in inetcfg

3. Select Configure SNMP Parameters.

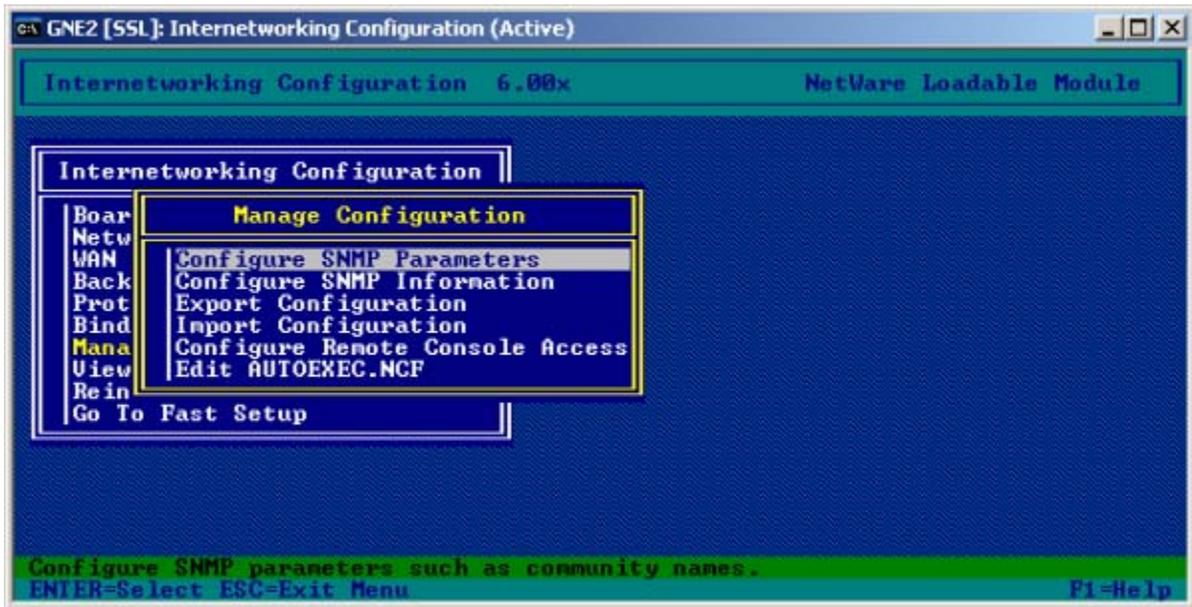


Figure 2 - Configure SNMP parameters

4. Set the parameter values.

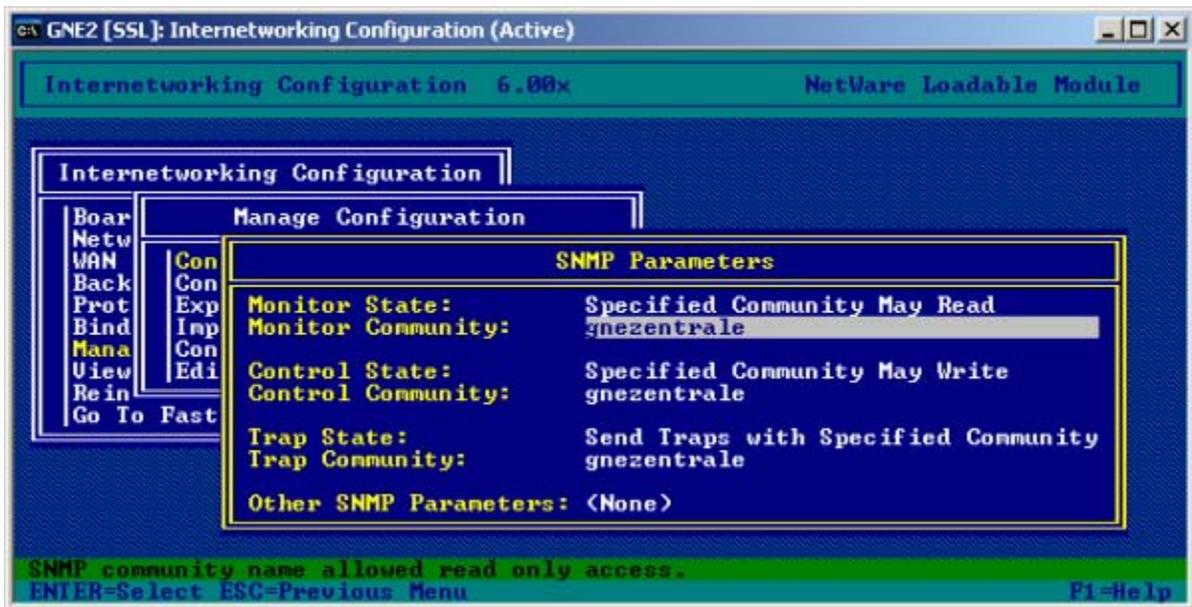


Figure 3 - SNMP parameter values

Here you can set the Community name. The default is 'public', but it can be changed for security reasons. Primarily, only the <Read> Community is needed. It also makes sense to set the Trap Community so that later on the SNMP receiving application can manage the NetWare Traps.

In the next step, configure the SNMP System Information, but that is not necessary.

**Note:** NetWare supports only SNMP v1, so no SNMP authentication is possible.

#### TESTING SNMP FROM LINUX SERVER TO NETWARE

Once you have configured SNMP, do a 'Reinitialize System' so your server can respond to SNMP Get calls.

```
snmpwalk -On -v 1 -c <yourcommunity>
```

The output will look something like this:

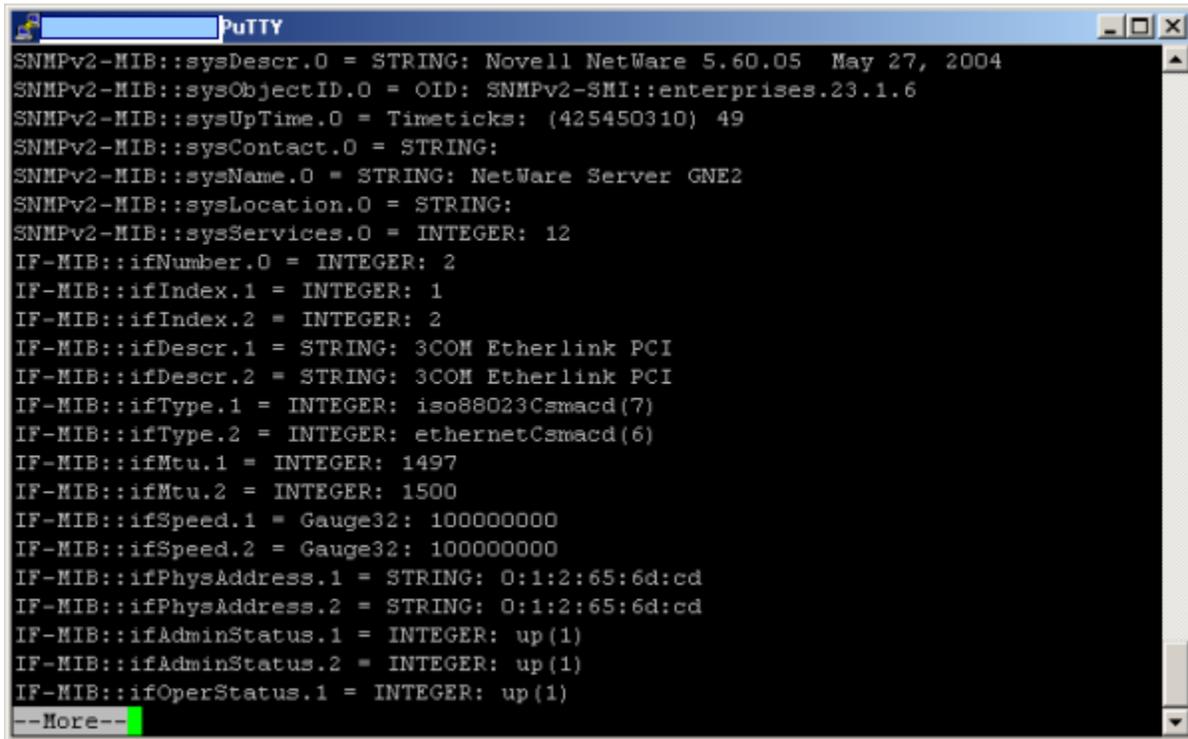


Figure 4 - Output from SNMP Get

If this was successful, you now need to add the OID you want to monitor. A few OIDs are shown below:

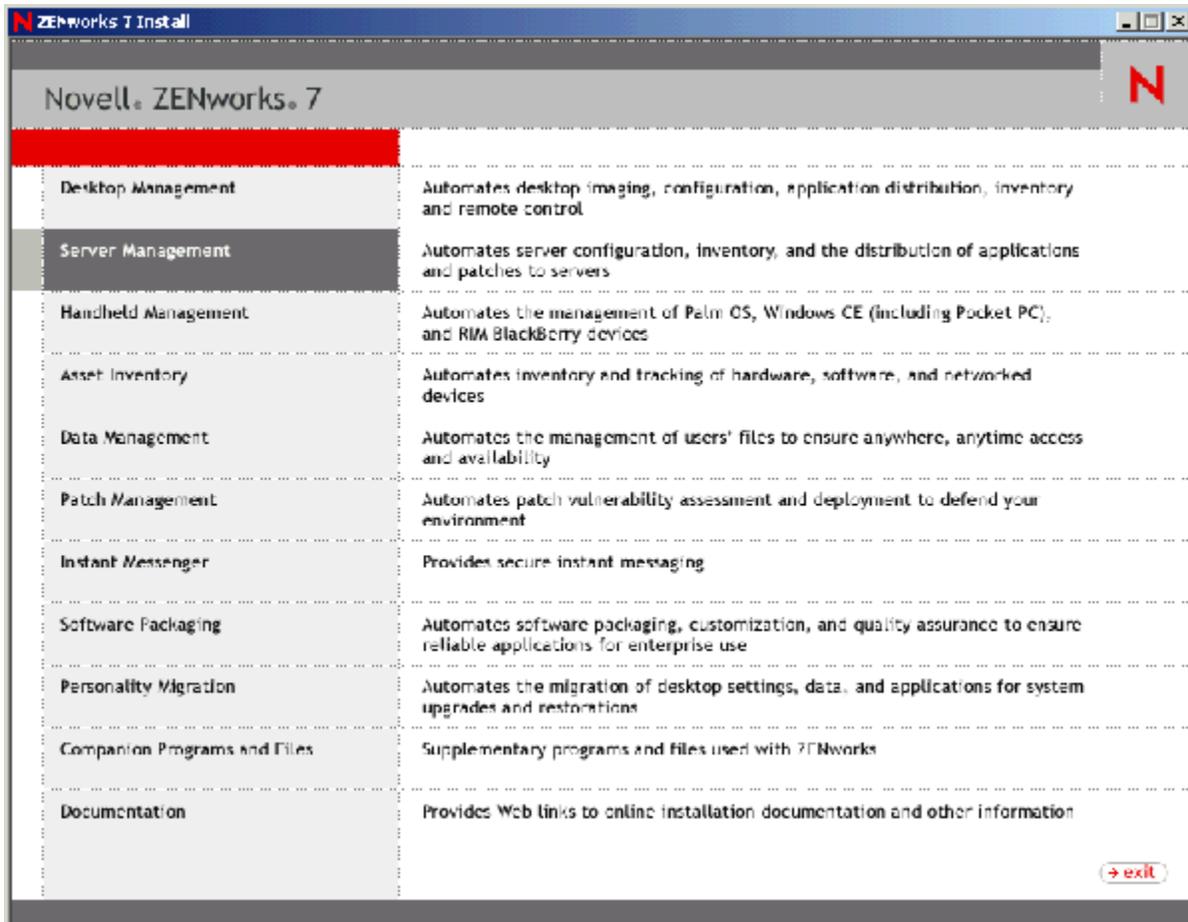
OID	Description
.1.3.6.1.2.1.25.2.3.1.5.1	DOS Memory
.1.3.6.1.2.1.25.2.3.1.5.2	Alloc Memory Pool
.1.3.6.1.2.1.25.2.3.1.5.3	Cache Buffers
.1.3.6.1.2.1.25.2.3.1.5.4	Cache Movable Memory
.1.3.6.1.2.1.25.2.3.1.5.5	Cache Non-Movable Memory
.1.3.6.1.2.1.25.2.3.1.5.6	Code And Data Memory
Note: The Settings above are 4K Blocks	
1.3.6.1.2.1.27.1.1.6.1 = String: 1	GW MTA Loaded
1.3.6.1.2.1.27.1.1.6.1 = String: 2	GW POA Loaded
'( .1.3.6.1.2.1.25.5.1.1.2.1146460160 = INTEGER: 1935 Kbytes Free ECB Count')	
.1.3.6.1.4.1.23.2.27.3.16.1.7.1	available processor threads
.1.3.6.1.4.1.23.2.70.1.8.0	Incoming Messages GW
.1.3.6.1.4.1.23.2.70.1.7.0	Outgoing Messages GW

If you do a 'snmpwalk' you can also see all the loaded modules on a NetWare Server.

## NETWARE CONFIGURATION

If your server is not NetWare 6.5/OES, you need to install the Trap files from the ZSM 7 Trial CD to your NetWare Server.

1. From the Welcome screen, choose Server Management.



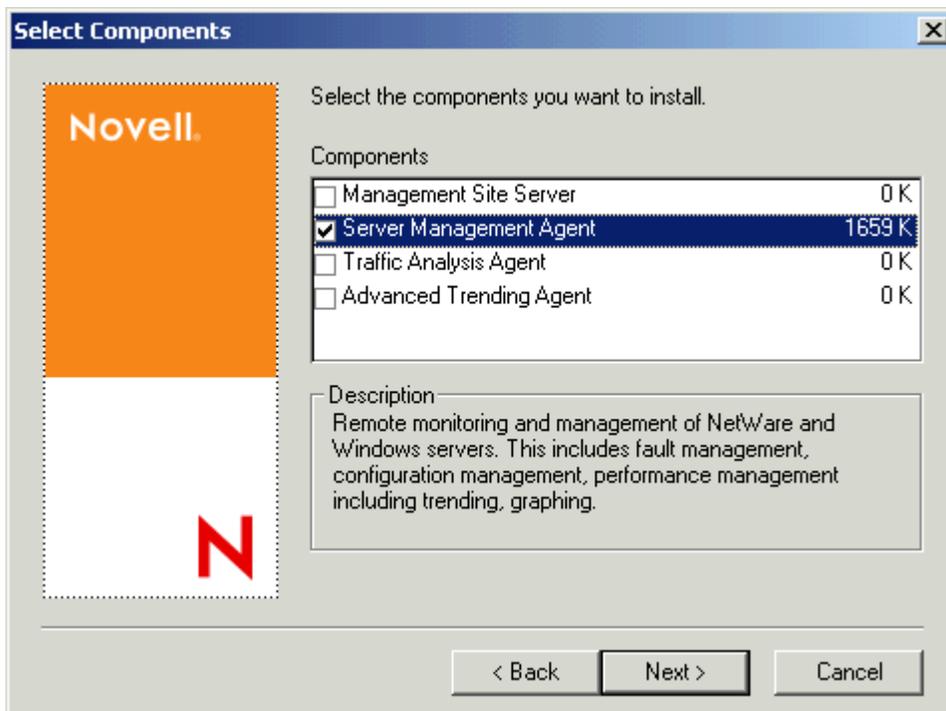
2. Choose Management and Monitoring Service.



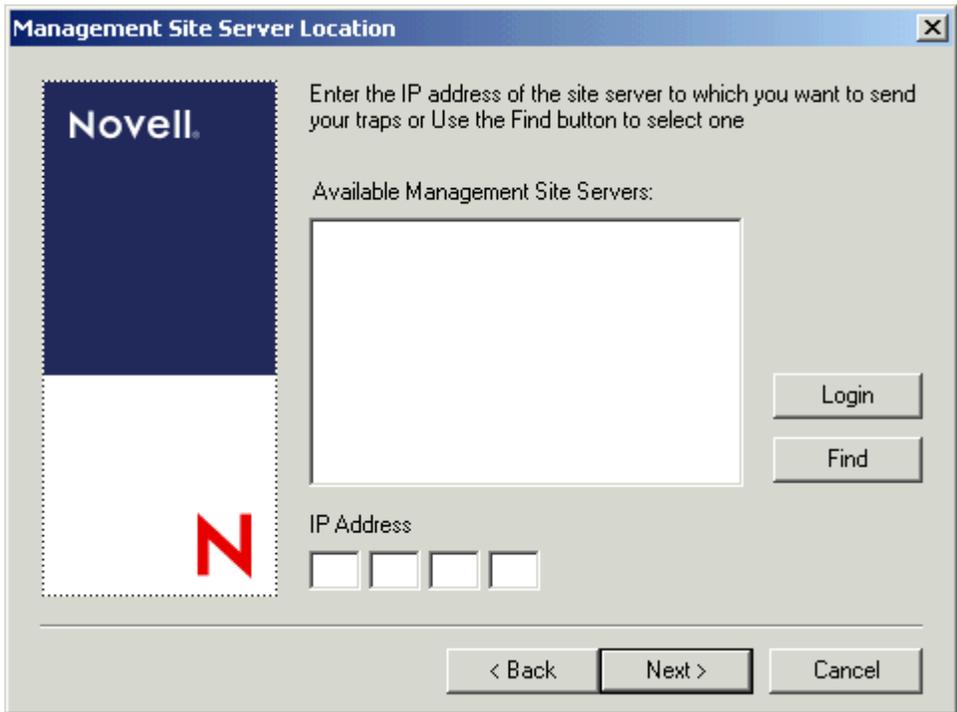
3. Choose Site Management Services and Agents.



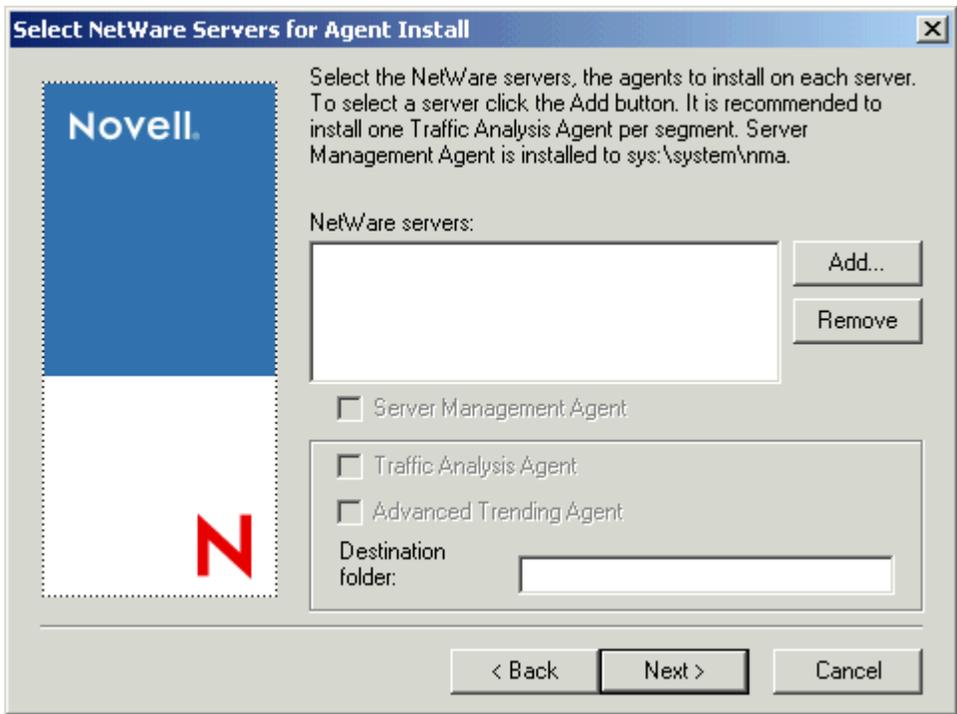
4. Install only the Server Management Agent - nothing else - and click Next.



5. Enter the IP address of your SNMP Trap Receiving Server in the dialog and click Next.



6. Add the Novell servers you need. Leave the Destination Folder default.



7. Leave the next screens blank. After installation on the NetWare servers all Files required by SNMPTrap are available. A reboot is not required.

8. The Trap Files need to be configured manually for the Information that should be send. The configuration files are found on X:\SYSTEM\NMA\ Below is an example for a Trap file Configuration.

```
HWTRAP.CFG (X:\SYSTEM\HMA) - GVIM
Datei Editieren Werkzeuge Syntax Puffer Ansicht Hilfe
[Icons]
Default interval = 10
Enable all

# Following traps are disabled to prevent the agent from sending too many
# traps. All these traps are of INFORMATIONAL, WARNING and MINOR severity.

Disable 36,40-43
Disable 51,54-56
Disable 74,86-98
Disable 91,107
Disable 115,125,126
Disable 142,143,148,149,164
Disable 183,185,186,188,189,198-198
Disable 202,203,209-211,216
Disable 223,224,227-229,232,236
Disable 241,242,250,251,252,253,255,256
Disable 261,262,265-269,274-280
Disable 281-286,288,289,294,295
Disable 301-308,311-314
Disable 319-327
Disable 344-350,352-360
Disable 362,363,365-370
Disable 371,377,378,385

#####
#
# In the following section, all trap numbers from NVALARM.MIB along with
```

**Important:** You should change the Trap Community for security purposes.

Once all the Trap-Config files are modified, the SYS:/etc/traptarg.cfg also needs to be modified with the IP address of the SNMP Trap Receiving server.

- 9. Enter the IP address below the Protocol UDP Entry, like this:  
192.168.1.1

```
TRAPTARG.CFG (X:\ETC) - GVIM
Datei Editieren Werkzeuge Syntax Puffer Ansicht Hilfe
[Icons]
#
#   The Protocol keyword, left justified, signifies the
#   start of a new protocol section.
#
#   Comments are preceeded by the hash mark, and proceed
#   to the end of the line
#
#####
Protocol IPX
# In this section you can put SNMP managers that want to receive
# traps from the local node over IPX. Managers can be identified
# by NetWare service name (a NetWare file server name, for example)
# or by IPX address. To specify by IPX address, use the following
# format:
#       IPX Network Number: MAC Address
#
# for example, c9990111:00001B555555

Protocol UDP
193.16.235.26
~
~
~
~
35,40 Ende
```

---

**SUPPORT**

---

Please contact <http://support.dell.com/support/index.aspx?c=US&l=en&s=DHS>

Or contact your account representative.