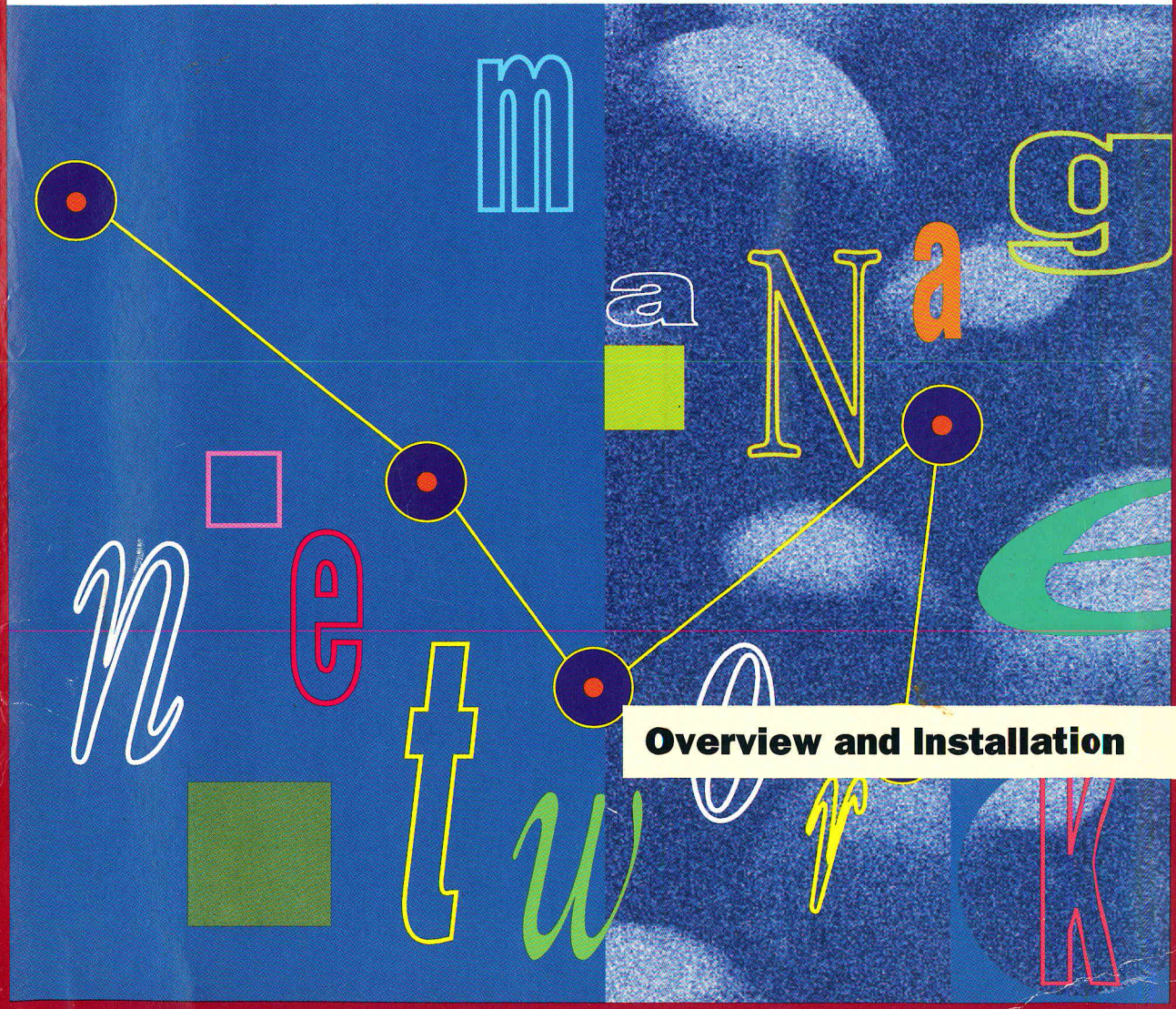
digital™

DIGITAL™ ServerWORKS™ Manager



ServerWORKS™ Manager

Overview and Installation

Part Number : ER-4QXAA-UA. F01

Digital Equipment Corporation

Contents

Preface

This document explains how to use DIGITAL's ServerWORKS Manager network management product to manage DIGITAL Prioris servers and AlphaServer systems. It also provides detailed procedures for installing, configuring, and using the ServerWORKS Manager components.

Audience

This guide is intended for the network administrator or server administrator.

Prerequisites

To use ServerWORKS Manager effectively, you should be familiar with the operational requirements for managing a network using the Simple Network Management Protocol (SNMP).

Terminology

The terms "Select" and "Choose" are used frequently in the procedures presented in this guide to perform operations. Both terms refer to specific mouse pointer or keyboard operations:

- Select—Move the mouse pointer to an item (icon, command, name, and so on) and single-click the mouse button, or use the specified set of keyboard keys.
- Choose—Move the mouse pointer to an item (icon, command, name, and so on) and double-click the operational mouse button, or use the specified set of keyboard keys.

Related Information

ServerWORKS Manager Documentation

In addition to this user's guide, ServerWORKS Manager includes extensive online help and other online-readable information.

See Chapter 5 for references to additional sources of information.

ServerWORKS Manager Order Information

For information about upgrading ServerWORKS Manager or other DIGITAL software products, contact your DIGITAL Sales Representative or Channel Partner.

Keyboard Conventions

To Do This:	Press These Keys:
Scroll one window up or down	PAGE UP or PAGE DOWN
Go to the beginning of the list	CTRL+HOME
Go to the end of the list	CTRL+END
Move focus left or right	LEFT or RIGHT ARROW
Move focus one line up or down	UP or DOWN ARROW
Move to next window	CTRL + TAB
Move to previous window	CTRL+SHIFT+TAB
Go to the next field	DOWN ARROW or TAB
Go to the previous field	UP ARROW or SHIFT+TAB
Go to the next group	CTRL+DOWN ARROW
Go to the previous group	CTRL+UP ARROW
Move the focus up or down without affecting the state of the previous line (to add or remove lines from a selected set)	SHIFT+UP ARROW or SHIFT+DOWN ARROW
Toggle the state of the focus item	SPACEBAR
Display Help	F1
Display Help (from a console window)	CTRL+ALT+F1

Introduction 1

What is ServerWORKS Manager?

ServerWORKS Manager lets network and server administrators monitor and manage:

- DIGITAL Prioris servers, AlphaServer systems, AlphaStation systems, and desktop and mobile PCs
- Other network components, such as bridges, routers, hubs, printers, and so forth

Its easy-to-use Windows-based interface makes performing many common server and network management tasks much easier.

From a single management console, you have access to your entire network through the ServerWORKS Manager's client/server architecture. ServerWORKS Manager uses the Simple Network Management Protocol (SNMP) for its primary communication with servers running a wide range of operating systems and the Desktop Management Interface (DMI) for its primary communications with desktop and mobile systems. Both these industry-standard protocols are used to monitor the network and its components for early signs of problems, thus avoiding expensive down time.

Why Install ServerWORKS Manager?

In your business environment, ServerWORKS Manager helps you handle a wide variety of situations and tasks:

- **Looking at your network configuration** —Before you can manage your network and its components efficiently, you need to know the elements that make up your network. ServerWORKS Manager provides the ability to discover your network, display the information in a hierarchy (tree view) or a topological map, and query individual components. You can customize these views or create new ones to organize the view of your network to reflect your corporate structure or job responsibilities.
- **Monitoring usage**—ServerWORKS Manager can provide baseline information on parameters such as network adapter statistics, disk storage, and CPU use. It lets you set alarms to notify you when the value of a parameter exceeds a threshold that you define, allowing you to make adjustments before minor problems grow into critical problems. By monitoring network traffic, disk storage use, CPU use, and more, you can determine how to better balance the system load and place resources where they are needed most.
- **Managing assets**—As a member of the IS team, you need to manage the asset inventory. You need to know not only what systems are on your network, but how they are configured and whether components such as memory and hard disks are adequate for present use and future software upgrades.

- **Proactive and reactive fault management**—As a server or network administrator, you need to identify and address system and network problems as soon as possible. You would prefer to solve problems before they cause costly down time to your users. When any server goes down or users cannot gain access to the network, you need to identify and fix the problem. ServerWORKS Manager's monitoring capabilities let you keep track of environmental factors such as temperature and voltage. The alarm capabilities provide the information you need to react to problems and proactively prevent conditions from reaching the problem stage.

The following subsections show how you might use ServerWORKS Manager to solve some typical problems that arise in network management.

Looking at the Network: IP Discovery and More

The network at Desktop, Inc. has grown enormously. Various groups are equipped with their own collection of workgroup servers and many individuals have several PCs and even their own hubs and routers.

Sophia works for the network administration organization, which manages the overall network and plans for future growth. Sophia uses ServerWORKS Manager's IP Discovery tool to build a topological map of the network. She chooses to map only the hubs and routers so she can get a better picture of the pieces of the network she controls. Figure 1-1 shows a portion of this map.

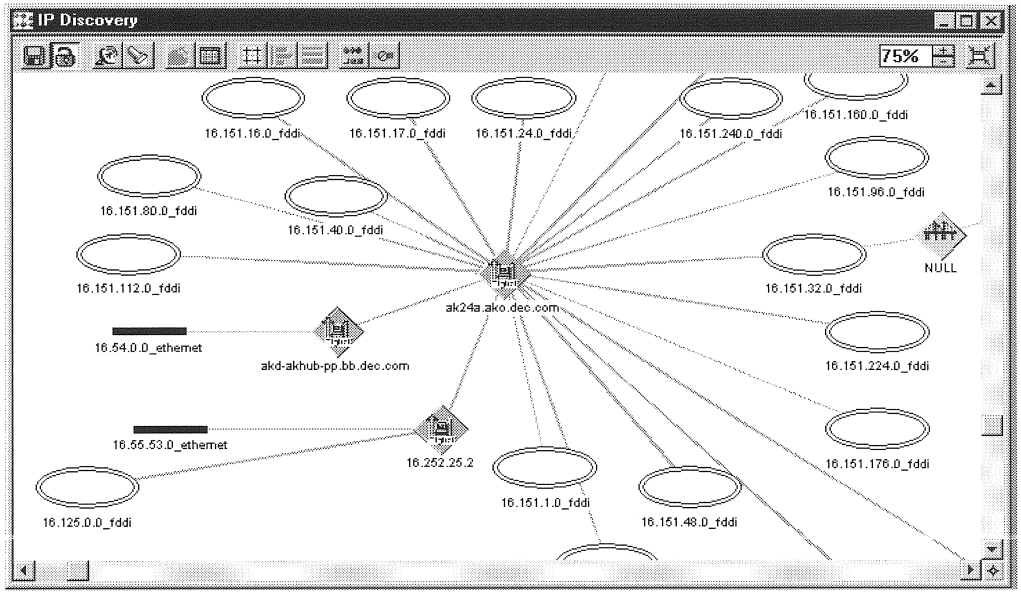


Figure 1-1: IP Discovery Map

Monitoring Performance: CPU Utilization

General Mercantile runs several CPU-intensive applications on a variety of servers. Balancing the CPU load is an important part of Rebecca's responsibilities. She uses ServerWORKS Manager to set an alarm if CPU utilization exceeds 80%. When CPU utilization reaches this point, she may decide to balance the CPU loads by switching applications from one server to another server. Rebecca sets the alarm so that once it is triggered, it will not be re-enabled until CPU use drops to 60%.

Rebecca also creates monthly snapshot reports and graphs of the CPU utilization for each of the servers when the applications are running. She provides her management with these reports. Last year, the IT organization used these reports to persuade General Mercantile management to add 10 AlphaServer systems and 25 Prioris servers to the network.

Monitoring the Network: Locating Network Interface Problems

At AKO Chemical, the IT group is having performance problems with a particular host Ethernet adapter. The host can handle 10,000 packets per second, but anything more could be a problem.

Andy uses ServerWORKS Manager to set an alarm to notify him when the number of packets the host is handling reaches this critical level. Since Andy normally works at his desk, he chooses to be notified of the alarm through electronic mail. ServerWORKS Manager sends the alarm whenever the network Interface Inbound Packets reach or exceed 10,000 packets.

To further isolate the problem, Andy sets an alarm on the Inbound Errors to understand if the slowdown on the host is caused by errors and hence re-transmissions by the higher layer protocol. He also sets an alarm on Inbound Packet Discards to determine if the slowdown is caused by the Inbound Packet not being delivered to a higher layer protocol because of buffer limitations or other transmission errors.

Because only a single protocol is being run at AKO Chemical, the company has a homogeneous environment. Andy can take advantage of this homogeneity and set an alarm on Network Interface Unknown Protocol to isolate random traffic produced by a device on the network.

Andy discovers that incoming bad packets are causing the problem. He uses the source address of the packets to track down and replace the device that is producing the bad packets.

Managing Windows NT Resources: Server Administration from a Single Console

Two companies merged to form Freeform Engineering. The new company still uses two different networks, and Diego has to manage both of them. He does this from a single console by installing ServerWORKS Manager on a Windows NT system.

One fourth of Diego's users are on DIGITAL Prioris servers running Novell NetWare. Using the NetWare tools from within ServerWORKS Manager, he sets up new clients, manages the print queues, and performs other network management tasks.

The remainder of the company uses DIGITAL AlphaServer systems and Prioris servers running Windows NT. Because Diego installed ServerWORKS Manager on a Windows NT system, he can use ServerWORKS Manager's NT Server Management from the same management console to set up print queues and create domain or server user accounts.

Managing the Desktop: Checking Clients for Software Upgrade

Quick Electronics plans to upgrade all of its desktops to a new version of the operating system, which requires at least 1 GB of hard disk storage and 16 MB of memory. Laura uses ClientWORKS MIF Browser in combination with Microsoft System Management Server (SMS) to check all the desktop systems she manages. Although she is responsible for 500 such systems, she is able to obtain this information in only a few hours. She learns that 10 percent of the systems need additional memory and 15 percent need hard disk upgrades before the new operating system can be installed.

Managing Storage: Setting Alarms on File Utilization

Disk storage is a problem at the Sometime Electric Company. Users frequently exceed the disk storage capacity and suddenly find themselves unable to access the server. John, the server administrator at Sometime Electric, uses ServerWORKS Manager to set an alarm when file system utilization reaches 95%. Because he is not always at his desk, John also uses ServerWORKS Manager's paging feature. When file system utilization reaches 95%, John is automatically notified and he can run his cleanup procedure to reclaim disk space.

John sets the threshold of the alarm at 95% with an automatic re-enable at 80%. Thus, once the alarm is triggered, it is disabled until it reaches the re-enable setting. In this way, John triggers only one alarm when the danger level is reached and provides for automatically re-enabling when the cleanup process is complete.

ServerWORKS Manager Features

Discovering Your Network

When you start ServerWORKS Manager for the first time, you see the ServerWORKS Explorer. When you expand the Explorer's root object, the Explorer displays the root objects that make up your network. If you have Novell NetWare networks or Microsoft networks, they will appear here automatically, and they will be discovered automatically when you open the object.

Information about server objects (DIGITAL hosts) and SNMP objects must be placed into the database before it can be viewed. Information can be inserted into the database manually, or you can use the IP Discovery Wizard to automatically search and locate all objects on your network or on some segment of the network. The IP Discovery Wizard searches the network for TCP/IP and SNMP objects and builds a database of information from that network.

IP Discovery can be configured to search only the local network or to find devices in locations other than your local network. It can locate all object types or filter the information to include only specified types, such as hubs, concentrators, or routers.

After the discovery is complete, the information is written to a database and displayed graphically in a map view. The Wizard also creates a report that you can view in Notepad, print, or save to a file. This report includes information about potential address and configuration problems that exist on your network.

You can run the IP Discovery Wizard whenever you need to add new information. After discovery is completed, the database is updated and the new information is displayed in the IP Discovery map or in another custom map.

Looking at Your Network

Once IP Discovery has run, you can use ServerWORKS Manager to monitor the discovered objects.

Map View: IP Discovery

The map view displays a graphical representation of your network's layout. The Map Viewer uses the ServerWORKS database to build the map, also called the logical topology, and automatically positions objects. When this map is complete, you can reposition the objects manually and save the changes so they will be preserved in any subsequent discovery that writes to the map view. Multiple discoveries can be run and the objects saved in the same map, or in different map views.

Hierarchical View: The ServerWORKS Explorer

The ServerWORKS Explorer is your main entry point into ServerWORKS Manager. The ServerWORKS Explorer opens with a tree view that consists of root objects for each of the object types in your network. From the hierarchical view, you display your Windows NT and Novell NetWare networks, if they exist. You can display DIGITAL servers and SNMP objects found during the discovery process in either map view or hierarchical view. SNMP objects are displayed with color to represent status and alarm bells to indicate unacknowledged alarms.

Customized Views

You can create your own map and hierarchical viewers to reflect your environment and needs. For example, you might want:

- A separate map viewer for each segment of your network
- A separate map viewer for each logical component of your network, such as Floor 1, Floor 2, Floor 3 or Manufacturing, Engineering, Personnel, Sales
- A customized hierarchical viewer that includes only the Windows NT servers and workstations that are in your building
- A map that includes only the hubs, routers, and bridges that make up your network

Monitoring Your Network

ServerWORKS Manager provides a variety of tools to help you monitor and manage your network and the systems in it, including three network browsers: the System Browser, the MIB Browser, and the MIF Browser. The MIF Browser is described in the section titled ClientWORKS Integration in this chapter.

The System Browser for DIGITAL Hosts

The System Browser displays and monitors information about the DIGITAL hosts on your network. With the System Browser, you can monitor information about the CPU, the storage, the network interfaces, and the environmental sensors. The exact information available varies according to the equipment, software, and sensors installed on the device you are monitoring.

In addition to viewing a static snapshot of the device, you can create a dynamic graph to monitor certain data over time. Data you can look at this way includes CPU load, file system utilization, network statistics, and readings from the thermal and voltage sensors.

Refer to the online help or the tutorial for more information about the System Browser and graphs.

The MIB Browser for SNMP Objects

ServerWORKS Manager provides the MIB Browser, which gives you the following capabilities for SNMP devices:

- Query SNMP agents to retrieve Management Information Base (MIB) variables, such as the system name, system ID, and up time for a router, hub, or bridge.
- View and set MIB variables

ServerWORKS Manager also provides tools to let you create, view, and modify MIB groups, associate a MIB grouping with an object, compile standard MIB definition files, and enroll new MIB groups into the ServerWORKS database.

Checking Network Status

ServerWORKS Manager uses color in both map and hierarchical viewers to indicate each object's operational status: whether it is up, not responding, or down. By default, the color green indicates that the object is operational, while red shows that the object has gone down. Magenta means that the system is not responding and should be looked at. You have the option of changing these colors.

Setting Alarms

While checking the status of network objects is useful, it does not notify you of potential problems. ServerWORKS Manager's alarming and notification feature lets you set alarms to warn you of specific events that are important in your environment and specify how you want to be notified.

You can set four types of alarms:

- System (interface) status alarms that report when system or interface changes status (for example, a workstation goes down)
- SNMP trap alarms that are triggered when a particular SNMP trap is generated.
- Component status alarms that report the operational status of a DIGITAL host's components (for example, a fan fails)
- Component threshold alarms that are triggered when some characteristic of a DIGITAL host meets a specified condition (for example, the temperature reaches some upper limit).
- When an alarm is triggered, the Alarm Counters on the management console's status bar are updated. After an alarm is triggered, it is disabled. You can define a value at which the alarm will automatically be re-enabled. Rebecca at General Mercantile uses this threshold and re-enable feature to set an alarm that is triggered when CPU load reaches 80% and re-enabled when CPU load drops to 60%.

In addition to displaying alarm information on the management console's screen, you can request that the alarm be sent to an electronic mail address or to a pager number. You can also automatically trigger an action that you define. You can display a help file that tells the system manager what the alarm means and what should be done about it. You can even take action to correct the problem. For example, John at Sometime Electric might want to execute a script that would delete all the files from the /TEMP directory of the server that triggered the alarm.

Refer to the online help or to the tutorial for more information on setting alarms, re-enabling thresholds, and receiving notification.

Viewing Alarms

ServerWORKS Manager displays alarms in two ways:

- Alarm bells displayed next to the name of an object in any viewer indicate a device that triggered an alarm.
- The Alarm Counter buttons, located on the status bar at the bottom of the ServerWORKS Manager window, show both the status of your network objects and the number of unacknowledged alarms of high, medium, or low severity.

To view more detail about a category of alarms, click the Alarm Counter button. The Alarm Viewer opens and displays all active alarms.

Managing Microsoft Windows NT Domains

If you have a Microsoft Windows NT network as part of your networking environment, you can use ServerWORKS Manager NT Server Management to manage it. NT Server Management allows you to administer your Microsoft network from the single interface of the ServerWORKS Manager rather than from the multiple windows and multiple utilities required by Windows NT.

ServerWORKS Manager automatically discovers your NT domains and lets you display the contents and properties of objects in the Explorer or as part of a custom collection or view. You can drag and drop objects such as users from one domain to another or to a server and otherwise take advantage of the single consistent interface. You can perform group operations easily. For instance, you could select several groups and modify their privileges.

You must install ServerWORKS Manager on a console that is running Windows NT V3.51 or greater to use NT Server Management. You must also have the appropriate privileges for the particular task you want to perform, since ServerWORKS Manager security is based on Windows NT security.

Refer to the ServerWORKS Manager NT Server Management on-line help for more information.

Managing Novell NetWare Servers

If you have Novell NetWare file servers on your network, you can list those servers in the ServerWORKS Explorer and perform management tasks by accessing the NetWare utilities on those servers. When you select a NetWare server, icons for the following NetWare utilities are displayed on the ServerWORKS Manager toolbar: Filer, Pconsole, Printcon, Rconsole, Syscon, Userdef, and NWAdmin. To start a utility, click on the button.

Integration with Enterprise-Level Network Management Tools

Because ServerWORKS Manager uses the SNMP protocol, it can work with other enterprise network tools that use this protocol. ServerWORKS Manager can obtain information about all devices that follow the SNMP standard; likewise, DIGITAL MIBs can be compiled into another network management tool and DIGITAL hosts can then be browsed from that tool.

The DIGITAL Server Agent component of ServerWORKS Manager uses the operating system's native SNMP protocol stack and extendible SNMP agent. You can set up the DIGITAL server's SNMP agents to send traps to a network management system such as ServerWORKS Manager. Traps can be forwarded from ServerWORKS Manager to an enterprise manager, such as HP OpenView NT or Tivoli TME-10.

Refer to Chapter 4, Managing Servers Using SNMP-Based Enterprise Management Systems, for more information.

Integration of Companion and Other Applications

ServerWORKS Manager includes companion applications that are integrated into ServerWORKS Manager. These applications include:

- ***Global Array Manager (Mylex GAM)***—Mylex's client/server package used to monitor and manage the disk array subsystems attached to a Mylex RAID controller.
- ***StorageWORKS Command Console (SWCC)***—DIGITAL's client/server package used to monitor, manage, and troubleshoot large storage subsystems attached to a DIGITAL StorageWORKS RAID controller.
- ***Remote Server Manager (RSM)***—DIGITAL's package for out-of-band management of Prioris servers includes both hardware and software components, purchased separately. The software component can be purchased separately and is included on the ServerWORKS CD. The RSM software is installed on a Windows NT management console and is able to manage remote Prioris servers that contain RSM hardware. When the RSM software is installed on your ServerWORKS Manager console, it automatically integrates into ServerWORKS Manager. This integration means that all of the RSM functions can be performed from within ServerWORKS Manager. Because RSM uses a modem to connect from the management console to the remote server, RSM can still run even when the network is down.
- ***Remote Management Console (RMC)*** —DIGITAL's package used to monitor and manage AlphaServer systems that have either:
  - KCRCM option hardware installed (AlphaServer systems 2000, 2100, 2100A, 1000A, and 1000)
  - RMC functionality built into the system (AlphaServer 4100, 4000, and 800 System)

- When RMC software is installed onto the ServerWORKS Manager console, RMC automatically integrates into ServerWORKS Manager. This integration means that all RMC capabilities are available from within ServerWORKS Manager. For example, you can monitor the power supplies, temperature, and fans. You can also halt and power off an AlphaServer system. Because the connection from the management console to the remote AlphaServer system is through a modem, the RMC functionality can be used even when the network is down.

  Third-party applications—Integration of other third-party applications is explained in a document available from the web. The document is located in the DIGITAL Windows Enterprise Computing web site at the following address:
  `http://www.windows.digital.com/products/products.asp`

  Once at this Internet page, click on ServerWORKS under the heading "Software Solutions/Server Management Tools."

ClientWORKS Integration: MIF Browsing Using DMI

ClientWORKS, DIGITAL's implementation of the Desktop Management Interface (DMI) standard, allows you to retrieve information both locally and remotely.

DMI uses Management Interface Format (MIF) files to provide detailed information on the hardware and software components of desktop, server, and mobile computers. Each component, peripheral, or application that has an associated MIF file can be browsed by a DMI-enabled application, such as the ClientWORKS MIF browser. This information can be displayed to users and administrators alike.

Integration into Microsoft's SMS

The MIFmaker program, also installed as part of ClientWORKS, is used to create up-to-date snapshots of MIF information that can be used with asset management and software distribution tools like Microsoft SMS to allow you to manage hardware and software for your entire enterprise—for example, to determine how many of your servers have 64 MB of memory or more.

SMS obtains information for its database by reading a Windows system's MIF file. The MIF information is pushed to the SMS server when the desktop SMS script is executed, generally when the user logs in. The ClientWORKS MIFmaker component automatically generates MIF snapshot files at set intervals that you, the administrator, define. Your SMS administrator can use tools in SMS to control MIFmaker and collect the MIF snapshot files in its database.

Supported Platforms – SNMP Agents

The SNMP agents running on DIGITAL's Prioris servers and AlphaServer systems provide the communication channel to the management console. The SNMP protocol is used over an IP network. These agents provide real-time system and performance data along with information about alarms. The DMI agents provide configuration data on DIGITAL's servers, desktops, or mobile systems.

The following table indicates which operating system SNMP and DMI agents are provided with ServerWORKS Manager V3.0 (unless otherwise indicated).

Minimum OS Version Supported	Host Resource SNMP Agent	DIGITAL Prioris Server SNMP Agent	DIGITAL AlphaServer System SNMP Agent	DIGITAL DMI Agent
NetWare® V3.12 and V4.1 (Prioris servers)	✔	✔	N/A	N/A
Windows NT ® V3.51 and V4.0 workstation and server (for Prioris servers or AlphaServer systems)	✔	✔	✔	✔
SCO® UNIX Open Server V5.0	✔	✔	N/A	N/A
DIGITAL UNIX V3.2d-1 [1] and greater (for AlphaServer systems)	✔	N/A	Future	N/A
DIGITAL OpenVMS V6.2 [2] (AlphaServer systems only)	✔	N/A	Future	N/A
Windows 95 [3] (Prioris only)	✔	N/A	N/A	✔
OS2/Warp 3.0 [4] (Prioris only)	✔	N/A	N/A	N/A

[1] Shipped on ServerWORKS CD for V3.2d-1 agent; provided as part of the operating system for later versions

[2] Available with DIGITAL TCP/IP Services for OpenVMS Version 4.1 (also known as UCX)

[3] Provided with ClientWORKS on DIGITAL's desktop and mobile computers

[4] Provided as part of OS/2 operating system

Installation 2

Introduction

This chapter explains how to install ServerWORKS Manager, which is comprised of several installation kits. The installation is accomplished by using a navigation tool called AutoPlay. AutoPlay's role in the installation is to make the job of navigating through the various installation kits easier.

On systems running Windows 95 or Windows NT V4.0, simply insert the ServerWORKS Manager CD-ROM into the drive and AutoPlay is automatically initiated. On systems running Windows NT 3.51, execute **AutoPlay.exe**, found in the top level directory of the CD-ROM. For other operating systems, please follow the instructions in *install.txt*.

Note: *Shut down any other applications that are running before starting the installation process.*

AutoPlay displays options on its main screen. Depending on the option selected, the appropriate component is started. The main screen displayed by AutoPlay provides the following options:

- *View the **Welcome** screen*—Displays overview information
- ***Install** components*—Provides a second level screen containing the Installation Kits. Refer to the section "Installation Kits" in this chapter for more information.
- *View the **Tutorial***—Runs the on-line tutorial.
- *View the **Documentation***—Displays the on-line manuals and other documentation using the Adobe Acrobat reader located on the CD-ROM. Note that Adobe Acrobat does not have to be installed on your system in order to view the documentation from the CD-ROM.
- ***Finish***—offers to either start ServerWORKS Manager Console, if it was installed, or to exit. If ServerWORKS Manager Console was not installed, the only option is to exit.

AutoPlay senses the configuration of the system and uses this information to determine what should be offered as installable options on the platform that it is running on. If the option cannot be automatically installed on that system, information on how to install it is displayed.

Prerequisites

ServerWORKS Manager has minimum requirements for the management console hardware and software, the agent hardware and software, and the DIGITAL agents. These are listed in the following sections.

Note that management console refers to the system on which ServerWORKS Manager console is installed and from which the servers will be managed. This system may also be a server.

Management Console Hardware

Component	*Minimum Requirements*
Processor	Intel 486DX2 66 MHz
Storage Devices	1 GB hard drive CD-ROM drive 3.5-inch diskette drive
Network Interface Card	Network adapter with TCP/IP support installed
Monitor	SVGA 800 x 600 (1024x768 resolution recommended)
Memory	16 MB (32 MB recommended)

Management Console Software

Component	*Minimum Requirements*
Operating System	One of the following: • Windows NT V3.51 or V4.0 • Windows 95
Management Protocol	SNMP service [5] -- Install the SNMP provided with the operating system..
Transport and Network Protocols	TCP/IP - Install the TCP/IP provided with the operating system. TCP/IPX[6] - install the TCP/IPX provided with the operating system.

[5] ServerWORKS Manager requires SNMP service only if an agent is being installed.

[6] The IPX stack is only required if the NetWare OMM is needed. In addition, Novell's IPX stack must be used ; others may not work.

Agent Hardware

Component[7]	*Minimum Requirements*
Prioris servers	LX, MX, XL, HX and ZX
AlphaServer systems	300, 400, 800, 1000, 1000A, 2000, 2100, 2100A, 4000, 4100, 8200 (Not Windows NT), and 8400 (Not Windows NT)
Desktop computers [8]	Venturis FX, Venturis GL 6xxx, Venturis 486, Venturis 486 LP, Venturis Pentium, Venturis Pentium LP, Celebris XL 6xxx, Celebris GL 6xxx, and Celebris GL 5xxx.
Notebook computers [9]	HiNote, HiNote Ultra, HiNote Ultra II, and HiNote VP
Network Interface Card	Prioris Intel servers — TCP/IP adapter (Ethernet, Token Ring, or RAS)
	AlphaServer systems—All TCP/IP network adapters

[7] Note that ServerWORKS software is shipped only with Prioris servers and AlphaServer systems

[8] Desktop computers may not support either environmental parameters, RSM, or RMC.

[9] Notebook computers may not support either environmental parameters, RSM, or RMC.

Agent Software

Component		*Minimum Requirements*
Network Operating System	Prioris servers	Novell NetWare[10] V3.12 and V4.1
		SCO UNIX V5.0, V5.01, V5.02
		Windows NT V3.51, 4.0
		OS/2 3.0
	AlphaServer systems	Digital UNIX V3.2D-1 or greater
		OpenVMS 6.2
		Windows NT V3.51, V4.0 for AlphaServer systems (for agents only)
Network Protocol		SNMP TCP/IP IPX (on NetWare servers only)

[10] Also known as IntraWare.

DIGITAL Extension Agents

The ServerWORKS Manager CD-ROM includes SNMP agents for various server operating systems. The SNMP agents from the ServerWORKS Manager CD-ROM must be installed even if the operating system comes with SNMP agents.

The following is a list of operating systems Management SNMP Agents that are supported by ServerWORKS Manager. The (✓) indicates that the agent is resident on the ServerWORKS Manager CD-ROM while the (×) indicates that the agent is resident elsewhere.

Operating System	Supported on Prioris servers	Supported on AlphaServer systems
NetWare[11] 3.12 or 4.x	✓	
SCO UNIX 5.0 or greater	✓	
DIGITAL UNIX 3.2D-1 (see Note 3)		✓
Windows NT 3.51 or greater	✓	✓
IBM OS/2 Warp 3.0 (see Note 1)	×	
OpenVMS (see Note 2)		×

Note 1: *In the current implementation of ServerWORKS Manager, OS/2 DIGITAL Servers are discovered as "server" objects, and not as "server.Digital. "In order to manage OS/2 DIGITAL Servers, it is necessary to manually change the server by first selecting the server, then selecting "Properties" from the "Actions" pull down Menu. The server is displayed in the "Selected Objects" list box. From the "Properties" list box, select "General Information." (Interface Information is the*

[11] This is also known as IntraWare.

default selection.) In the "type list" box, search for "server.Digital" and select it. Select "OK" to exit the dialog box.

Note 2: *The OpenVMS SNMP agent for AlphaServer or AlphaStation systems is included in the DIGITAL TCP/IP Services for OpenVMS product V4.1 or greater (this is a component of the NAS Client/Server Package). The SNMP agent is installed when TCP/IP is installed. The package also contains installation instructions for TCP/IP.*

Note 3 *Agents for DIGITAL UNIX 3.2D and higher are supplied with the operating system. Refer to the instructions provided with the operating system to ensure the SNMP agent is enabled.*

RSM

If RSM software was installed on a Prioris server into its default directory "<windows drive>:\re_mgr", it is automatically integrated into ServerWORKS Manager Console when ServerWORKS Manager Console V3.x is installed. If RSM is installed at a later day or if it is not installed in the default directory, the RSM button may be selected from AutoPlay to manually integrate RSM into ServerWORKS Manager Console V3.

If RSM is successfully integrated into ServerWORKS Manager Console V3.x, the installation reports a successful integration on its summary screen.

RMC

RMC uses either TERMINAL.EXE on Windows NT V3.51 or HYPERTRM.EXE on Windows NT V4 and on Windows 95.

HYPERTRM.EXE is an installable option during the installation of Windows 95 or Windows NT 4.0. Therefore, it may need to be installed from the operating system kit ***BEFORE*** the ServerWORKS Manager Console installation is started.

ClientWORKS

ClientWORKS is a tool that provides DMI browsing. There are three ways that ClientWORKS may be installed on your system. These are:

- Factory-installed
- Installed during Windows NT agent installation
- Installed during ServerWORKS Manager Console installation

The version of ClientWORKS that is either installed by the NT agent or that is factory installed, provides both the remote and local browsing capability. The ClientWORKS installed by ServerWORKS Manager Console is configured for remote browsing only.

ClientWORKS installation by the NT agent requires that any existing ClientWORKS software be de-installed before starting the agent installation.

In most cases, the factory-installed ClientWORKS and the ClientWORKS installed as part of the agent installation may be used directly by the ServerWORKS Manager Console. If it is usable, the existing ClientWORKS is not replaced with the one that is part of the ServerWORKS Manager Console kit and as a result, ClientWORKS offers both the local and remote DMI browsing.

If the ClientWORKS is not usable by ServerWORKS Manager Console, the installation procedure either removes it or asks you to remove it (refer to the section “De-Installing ClientWORKS in this chapter). If the installation is successful in removing the ClientWORKS, it is replaced with the ClientWORKS that is part of the ServerWORKS Manager Console kit which supports remote browsing.

Startup Groups

Startup tasks may interact or interfere with the installation of ServerWORKS Manager components. To ensure this does not occur, remove all entries from your startup groups. The procedure for finding the groups is listed in the following.

For Windows NT 4.0

Select Start, Settings, and then the Task bar. Click on the page for "Start Menu Programs" and then the "Advanced" button. Use the "Tools" pull-down menu and select "Find". Select the "Files" and then enter "Startup" for the search criteria.

Open the startup groups and rename them for the duration of the installation.

For Windows NT 3.51

This requires privileges to the "common" and "all user" startup groups.

Select Start, Settings, and then the Task bar. Click on the page for "Start Menu Programs" and then the "Advanced" button. Use the "Expand programs looking for Startup". The startup group appears as the list is expanded.

Installation Kits

The ServerWORKS Manager CD-ROM contains the installation kits listed in the following table. AutoPlay lists all of the kits on the CD-ROM. After a kit has been selected, AutoPlay automatically determines the installation options on the kit, for this system, and presents them accordingly.

The installation should be done in the order suggested by AutoPlay. For example, install the agents first followed by ServerWORKS Manager Console.

Kits are:

- ServerWORKS Manager Agent Software
- ServerWORKS Manager Console Software
- Mylex Global Array Manager (GAM)
- StorageWORKS Command Console (SWCC)
- Remote Server Manager (RSM)

ServerWORKS Manager Agent Software

ServerWORKS Manager Agent software is installed on servers by placing the CD-ROM in the server drive and running AutoPlay.exe. On Windows 95 and Windows NT V4.0, placing the CD-ROM into the drive automatically starts the program.

AutoPlay checks the system it is running on and provides the appropriate SNMP agent options for that operating system.

If a problem occurs during the installation, refer to the install.txt or readme.txt files for information. These files are on the ServerWORKS Manager CD-ROM root directory.

Note: *All previous versions of ClientWORKS must be de-installed before installing the agent. The installation attempts to de-install ClientWORKS. If the attempt fails, ClientWORKS must be de-installed manually. The instructions for this are located in the section "De-Installing ClientWORKS" at the end of this chapter.*

ServerWORKS Manager Console Kit

At the beginning of the installation, ServerWORKS Manager Console Installation checks to see if a version of ServerWORKS Manager Console exists on the system. It does this by checking the WIN.INI file for a section called "[ManageWORKS user info]".

If the installation determines that a previous version of ServerWORKS Manager Console exists on the system, then the following options are presented:

- *Preserve the database*—selecting this option changes the existing database. If it is a V2.x format, the database is converted to V3. For additional information, refer to section "Database Conversion" in this chapter.
- *Remove previous version*—this deletes the old version of ServerWORKS Manager Console, including the companion database. If this option is not selected, the old version is left on the system, but is not directly accessible. If necessary, it is possible to restore the links between the database and ServerWORKS Manager Console (refer to "Restoring the Links to a previous version of ServerWORKS Manager Console" in this chapter).

Note: *During the installation, if the current version of ServerWORKS Manager Console is installed in the same directory as the previous version, the previous version is deleted first.*

Default Paths

If this is a new installation of ServerWORKS Manager Console, the default path is as follows:

<windows drive>:\program files\digital\swmgr

If a V2.x or later version of ServerWORKS Manager was installed on the system, the default path is as follows:

<drive of your current ServerWORKS Manager Console installation>:\program files\digital\swmgr

Database Conversion to ACCESS

ServerWORKS Manager Console V3.0 uses an Microsoft Access database to store information.

Version 2.x "Ini" files such as swextomm.ini are no longer used. All information is now stored in the database. If there is an existing V2.x database, it must be converted to be used with V3.0. This is done automatically by the installation procedure.

The following summarizes the process used by the installation procedure to preserve the existing database (assuming that ServerWORKS Manager Console is being installed into "<install drive>:\program files\digital\swmgr"):

1. The original database is copied to:

   <install drive>:\program files\digital\swmgr\database\old"

2. Assuming a V2.x database (in DB4 format), it is converted to an Microsoft Access format and placed in:

   "<install drive>:\program files\digital\swmgr\database"

   If the database is a ServerWORKS Manager V3.0 database, it is simply copied to:

   "\program files\digital\swmgr\database"

   In this case, conversion is not needed.

As part of an installation, ServerWORKS installs a pre-initialized V3 database in the location:

"<install drive>:\program files\digital\swmgr\database\empty"

If this is either a new installation or the previous database is not being preserved, the initial database (preloaded with MIB definitions and data) is also copied to:

"<install drive>:\program files\digital\swmgr\database"

Tutorial

The ServerWORKS Manager Tutorial is installed as part of the ServerWORKS Manager Console software. This tutorial contains basic information about ServerWORKS Manager. The complete tutorial has been designed so that it can be completed in 20 minutes. If you are a first-time user, DIGITAL recommends that you review the tutorial.

The tutorial may also run directly from the CD-ROM. Select the "Tutorial" button on the AutoPlay initial screen.

Documentation

During the ServerWORKS Manager Console installation, the readme.txt and install.txt files are copied to the root of the installation directory.

Remote Server Manager (RSM) Integration

Integration of a previously installed version of RSM (RSM sold separately) into ServerWORKS Manager Console is automatic (if it was installed into its default directory "<windows drive>:\re_mgr") when ServerWORKS Manager Console V3.x is installed. If RSM is installed at a later date or if it not installed in the default directory, the RSM button may be selected from AutoPlay to manually integrate RSM into ServerWORKS Manager Console V3.x.

Note: *At the end of the upgrade, the installation procedure confirms if the links between RSM and the ServerWORKS Manager Console V3.x software were successfully made. This information appears on the Summary screen when the installation is completed.*

RMC Integration

Refer to the RMC manual to install the hardware[12] and software. (KCRCM option hardware is sold separately.)

RMC is automatically configured to be used with ServerWORKS Manager Console. Integration into ServerWORKS Manager Console is automatic. It uses either the TERMINAL.EXE on Windows NT V3.51 or HYPERTRM.EXE on Windows NT V4 and on Windows 95.

---

[12] KCRCM is a hardware option for AlphaServer systems 2000, 2100, 2100A, 1000, and 1000A. AlphaServer systems 800, 4000, and 4100 have built-in RMC capability.

Note:	*At the end of the upgrade, the installation confirms that the links between RMC and ServerWORKS Manager Console were successfully made. This information appears on the Summary screen when the installation process is completed.*

StorageWORKS Command Console Integration

A previously installed version of StorageWORKS Command Console (SWCC) that was used with ServerWORKS Manager Console V2.x cannot be used with ServerWORKS Manager Console V3. SWCC must be re-installed using either the kit provided on the ServerWORKS Manager CD-ROM or with a more recent version.

Note:	*ServerWORKS Manager Console must be installed before SWCC.*

Mylex Global Array Manager Integration

A previously installed version of Mylex Global Array Manager (GAM) that was used with ServerWORKS Console V2.x cannot be used with ServerWORKS Manager Console V3. Mylex GAM must be re-installed using either the kit provided on the ServerWORKS Manager CD-ROM or a more recent version.

Note:	*ServerWORKS Manager Console must be installed before Mylex GAM.*

Installation Summary Screen

At the end of the installation process, an Installation Summary is displayed. The installation summary has three parts:

- *Database status*—reports whether an existing database is being used or whether a new one was created, and whether an existing V2.x database was converted from DB4 to Microsoft Access format.

- *ClientWORKS status*—reports whether a previous version of ClientWORKS is being used, or a new copy was installed, or whether the installation of ClientWORKS was started and then aborted.
- *Companion Application Integration*—reports whether a previously installed version of RSM or RMC has been successfully linked.

Confirm that everything that was selected for installation is described as "successfully completed" on this screen. If there are any discrepancies or problems, refer to the ReadMe.txt file.

Mylex Global Array Manager Kit

Mylex Global Array Manager (GAM) may also be installed using AutoPlay. AutoPlay senses what should be offered as an installable options on the system that it is running on, or if it cannot be automatically installed on that system, information on how to install it is displayed.

StorageWORKS Command Console Kit

StorageWORKS Command Console (SWCC) may also be installed using AutoPlay. AutoPlay senses what should be offered as an installable options on the system that it is running on, or if it cannot be automatically installed on that system, information on how to install it is displayed.

RSM Kit

The RSM button from AutoPlay is selected to integrate an existing RSM installation into the ServerWORKS Manager Console V3 in these conditions:

- RSM was not installed in the default directory
- RSM is installed after ServerWORKS Manager Console V3.0 is installed

Refer to the sections "RSM" and "Remote Server Manager (RSM) Integration" for information on automatic integration of RSM. Note that ServerWORKS Manager Console V3.x must already be installed on the system.

Restoring the Links to a Previous Version of ServerWORKS Manager

The ServerWORKS Manager Console software is linked to a database. If V2.x (or another V3.0) of ServerWORKS Manager Console is on the system, installing this version and keeping the old version on the system results in the link to the old version being replaced with the link to the new version. If the link needs to be restored to the old version, follow this procedure:

1. Find the ServerWORKS section in the WIN.INI file. This is labeled [ManageWORKS user info].
2. Find the following line within this section (this specifies the current location of ServerWORKS Manager):
   "INI file=<location of ServerWORKS Manager Console>\SWMGR.INI"
3. Change this line to the following format for a link to ServerWORKS Manager V2.x:
   "INI file=<drive letter and path of previous installation>\MWORKS.INI"

   Change this line to the following format for a link to ServerWORKS Manager V3.x:
   "INI file=<drive letter and path of previous installation>\SWMGR.INI"

Note: *During the installation, if the current version is installed in the same directory as the previous version, the previous version is deleted first.*

De-Installing ClientWORKS

The following procedure should be used to manually de-install ClientWORKS from the management console.

For Windows NT V3.51:

1. Log in as "administrator"
2. Type "net stop DMISL" from a command prompt to stop the XDMI and DMISL services. This also stops the DMI service layer and the remoting layer.
3. Type the following two commands from the directory where ClientWORKS is installed:
   DMISLSRV remove
   XDMISRV remove
4. Run the registry editor, regedt32.exe and find the entry
   "HKEY_LOCAL_MACHINE\
   SOFTWARE\
   DigitalEquipmentCorporation"
   Delete any entries here that contain the words
   - "ClientWORKS",
   - "AssetWORKS",
   - "LiveLINK".
5. Using File Manager, remove the ClientWORKS directory.
6. Remove the ClientWORKS Program Group and the Program items and reinstall.

For Windows 95 and Windows NT V4.0:

1. Run the registry editor regedit.exe. Find the entry:

   "HKEY_LOCAL_MACHINE\
   SOFTWARE\
   DigitalEquipmentCorporation"

   Delete any entries here that contain the words
   - "ClientWORKS",
   - "AssetWORKS",
   - "LiveLINK".

   Find the entry:

   "HKEY_LOCAL_MACHINE\
   SOFTWARE\
   MICROSOFT\
   Windows\
   CurrentVersion\
   RunServices"

   Delete any entries here that contain the words
   - "DMI Remoting Layer"

2. Restart Windows 95 or Windows NT 4.0, whichever is relevant.
3. Using File Manager, remove the ClientWORKS directory.
4. Remove the ClientWORKS Program Group and the Program items and reinstall.

ServerWORKS Manager Console Components

3

Introduction

ServerWORKS Manager Console is designed to manage Prioris servers, AlphaServer systems, desktop PCs, and mobile devices. It may also be used as an interface to perform administrative tasks for Microsoft NT or Novell NetWare[13] servers.

The contents of this section are as follows:

- ***Discovery***—collect information about the objects on the network
- ***Viewers***—display the objects that can be managed
- ***Browsers***—set or display specific parameters on objects
- ***Alarming and Actions***—set alarms for user-defined events and starts appropriate actions
- ***Monitoring and Status***—display color-coded information on the objects
- ***Reports***—generate specific information

---

[13] Novell NetWare is also known as IntraWare.

Each of these is briefly discussed in the following sections. For more information on any particular topic, refer to the Windows-based on-line help integrated into ServerWORKS Manager Console.

Discovery

Discovery is the process used to discover objects on the network. There are three methods used to discover objects on the network:

- NT Server Management Discovery
- Novell NetWare Discovery
- IP Discovery

The first two methods are done dynamically every time the object is expanded from ServerWORKS Explorer. For example, each time the NT Server Management (Microsoft Networks) object is expanded, a discovery is done.

The third method is IP Discovery. This is done in a separate process using the IP Discovery tool and is initiated by the user in order to minimize the amount of IP network traffic.

NT Server Management Discovery

NT Server Management Discovery lists the Microsoft Network objects (those running LAN Manager V3.0 Protocol). ServerWORKS Explorer displays the root object, which may be expanded to show the entire Microsoft Network. Objects found may include more objects than just NT servers (such as OS/2, Windows 95, and PATHWORKS servers). The systems that respond may not have the full functionality of Windows NT, and as a result may not have all its capabilities. Therefore, NT Server Management tools may be used to administer some tasks on that system, but not necessarily all.

NT Server Management Discovery information is not stored in the database, but is obtained each time that the NT Server Management object is expanded.

Novell NetWare Discovery

Novell NetWare discovery is similar to the NT Server Management discovery in that it is started by expanding the root NetWare object in the ServerWORKS Explorer. This results in dynamically finding the NetWare objects on the LAN. Note that NetWare V3.x and V4.x systems have different capabilities.

NetWare Discovery information is not stored in the database, but is obtained each time that the Novell NetWare object is expanded.

IP Discovery

The IP Discovery wizard finds TCP/IP and SNMP objects on the network and places information about these devices in the database. After discovery is complete, the IP Discovery tool uses the information in the database to create a default network map (IP Discovery Viewer).

In addition to finding devices on the network, discovery also assigns an **object type** to each device. A device is defined according to information that the discovery tool receives when it "discovers" the device. The object type defines what the device is, for example: a router, server, bridge, or hub.

Subsequent Discoveries

The Discovery process may be incremental—it may be run repeatedly on a viewer to update the information in the database and subsequently, the map. If more than one map exists, a specific map may be selected to be updated with the discovery results.

When an incremental discovery is done, the following occurs:

- New connections and nodes are added to the specified map(s).
- Configuration information for previously existing nodes is updated only if there is a change.
- Customized maps are preserved.

Adding Devices Manually

The IP discovery wizard does not have to be used to populate a viewer. IP devices may be manually added to the database and map and hierarchical viewers.

Viewers

Viewers are used to display objects and may also illustrate the relationship between these objects. ServerWORKS Manager Console provides two types of viewers:

- ***Hierarchical***—listing of the objects under the applicable root object
- ***Map***—topological representation of objects and the connections between objects

Map Viewers

Map viewers are graphical displays of the network topology at various levels. If the map is at its highest level, clicking on an object results in that object opening up and displaying the next level of detail. Once at the lowest level, an object such as a DIGITAL server or a router can be selected and then its operation monitored using either the pull-down menus or by double-clicking on the object to bring up its default browser.

Hierarchical Viewers

Hierarchical viewers display all local and network resources by using a tree structure. Different levels of the tree can be expanded or collapsed using the "+" and "-" tree controls. One hierarchical viewer is the ServerWORKS Explorer. This viewer is displayed when ServerWORKS Manager Console is initially started.

ServerWORKS Explorer

ServerWORKS Manager Console comes with a default hierarchical viewer known as the ServerWORKS Explorer. ServerWORKS Explorer is a viewer that displays all network resources and management tools.

ServerWORKS Explorer is read-only—it cannot be deleted. In addition, the order of its contents and the way that the objects are organized cannot be changed.

By default, there may be up to four root objects listed under the ServerWORKS Explorer. These are:

- Server Objects
- SNMP Objects

- NT Server Management—only listed if the management console is running Microsoft NT for Servers
- NetWare File Servers—only listed if the management console is running Novell NetWare

Objects may be listed under one or more root objects. For example, a DIGITAL Prioris server running Microsoft Windows NT would be an object in the tree structure under Server Objects, SNMP Objects, and NT Server Management. It is listed under all three categories because it fulfills the requirements of each of these categories. The specifications for the categories are described in the following sections.

Server Objects

The Server Objects category includes Prioris servers and AlphaServer systems with the following characteristics.

- Prioris server running NT (with DIGITAL's SNMP Extension Agents)
- Prioris server running Novell (with DIGITAL's SNMP Extension Agents)
- Prioris server running SCO UNIX (with DIGITAL's SNMP Extension Agents)
- Prioris server running OS/2[14] (with OS/2 SNMP agents installed; at a minimum, Host Resources Agent must be installed)
- AlphaServer system running NT (with DIGITAL Agents)
- AlphaServer system running DIGITAL UNIX
- AlphaServer system running OpenVMS

SNMP Objects

This category includes all devices running the SNMP protocol, such as:

- Bridges
- Routers
- Hubs

---

[14] Prioris servers with OS/2 are manually discovered

- Servers
- Desktop systems
- Token Ring networks
- Ethernet networks
- FDDI rings

Microsoft Windows NT Server Manager

This category includes all DIGITAL servers on a LAN running the Microsoft NT operating system. Most Microsoft NT Server administration tasks may be performed for systems in this category. The integration is such that ServerWORKS Manager Console menus and dialog boxes may be used to perform Microsoft NT Server Management tasks.

Note: *The NT Server Management tools are only available if the management console has Windows NT Workstation or Microsoft NT Server installed. If either one of these is not installed, the NT Server management object is not included in the ServerWORKS Explorer tree structure.*

Novell NetWare Server Manager

This category includes all DIGITAL servers on a LAN running the Novell NetWare operating system and which could be managed using the NetWare Management tools.

Note: *The NetWare Server Management tools are only available if the management console is running Windows NetWare Client from Novell. If it is not running, the NetWare Server management object is not included in the ServerWORKS Explorer tree structure.*

Customizing Viewers

ServerWORKS Explorer is the starting point for customizing viewers by using it as a source of objects to copy into other views.

Both hierarchical and map viewers may be customized to meet specific requirements. A customized view may be updated by running a discovery and selecting that view to be updated.

Several different viewers may be created to serve different purposes. For example, one view may contain all of the servers in the organization, while another may display files and applications on multiple servers, while a third may display the TCP/IP topology. Any type of information may be grouped in a view, regardless of its source or content.

Manually Placing Objects into Views

There are four ways to manually add objects into viewers:

- Using Insert from the Edit menu
- Using the map palette to insert objects into the map viewers
- Using the mouse to drag and drop objects from one viewer to another viewer
- Cutting, copying and pasting objects between views or within a view

In addition to putting objects into a view, viewers may also be customized by changing the format, layout, and colors assigned to certain objects. A background may also be specified for a topological map view.

For more information on viewers and how to customize them, refer to the ServerWORKS Manager Console on-line help.

Browsers

ServerWORKS Manager Console provides three different browsers that may be used to query and set parameters on objects. These browsers are:

- System Browser
- MIB Browser
- MIF Browser

System Browser

The System Browser provides information on both static and dynamic parameters found in DIGITAL objects such as servers, desktop systems, and mobile devices. The System Browser uses information provided by DIGITAL's SNMP agents loaded on the server, desktop, or mobile system. The information supplied may be:

- Static information—details the system's configuration
  - — System firmware descriptions and revision levels

  - CPU and memory expansion board configurations
  - Power supply and fan configurations
  - Disks
  - Network Interface Cards (NICs)
  - Asset management information for Field Replaceable Units (FRUs)
- Dynamic information—details the current state of an object located on a server
  - CPU utilization
  - Disk utilization
  - Network statistics
  - Thermal and voltage readings and/or states
  - Fan and power supply states
  - Error status for the Error Correction Code (ECC) on the SIMMs
  - Reads and writes of the Operator Control Panel (OCP)

The System Browser also provides detailed reports and the ability to graph certain parameters such as CPU utilization, network statistics, and thermal and voltage readings. These graphs may be useful for fault management and performance management.

MIB Browser

The Management Information Base (MIB) Browser is used to query (**get**) and modify (**set**) MIB parameters on SNMP compliant objects on the network. After an SNMP object is specified, the MIB Browser lists all of the applicable MIB groups for that object type, as well as the MIB variables in each group. For example, suppose the object parvin.ako.dec.com is selected. The MIB Browser would then list all of the applicable MIB groups for that object type, as well as the MIB variables in each group

The MIB Browser provides the following capabilities:

- Perform SNMP **set** operations against one or more SNMP agents
- View the properties of any MIB variable (for example, the variable's data type or object identifier, access status, or a brief description of the variable)
- Access the MIB Profiler to modify or create MIB profiles (See "Additional Tools" in this chapter)

- Access the MIB Enroller to enroll new MIB groups into the ServerWORKS database or modify existing groups (See "Additional Tools" in this chapter)

For SNMP objects other than DIGITAL servers, the MIB Browser is the default management action. It is started from either the Map Viewer, the toolbar, or from the Tools Menu.

Some of the MIB variables are Read/Write, thereby allowing the variable to be "set" as well as read. For example, sysLocation is a Read/Write variable, which means that a new location can be entered for the system whenever the system is moved. The change is actually made in the MIB itself. A Read/Write variable may also be changed by other individuals using another network management system.

Note: ***Set*** *operations change the value of the parameter in the device and are usually only allowed for non-critical parameters. This is because SNMP Version 1.0 provides limited security capabilities and is therefore, unable to determine whether a set request is coming from an authorized user or system.*

MIF Browser

The Management Information Format (MIF) Browser is used in a similar fashion as the MIB Browser. It is used on desktop and mobile systems and may also be used on systems running Windows NT or Windows 95. With the DMI service layer running on the system to be browsed, you can see an inventory of various system software, hardware, settings and configurations. This information can be passed on to Microsoft System Management Server (SMS) through the MIF Maker program.

The MIF browser is available through an icon on the tool bar.

Alarming and Actions

This section covers the following alarm topics:

- Creating Actions
- Configuring alarms
- Viewing alarms
- Actions to take when an alarm occurs

Creating Actions

Actions are similar to scripts that define what is to be done when an alarm or event occurs. The actions are stored independently of the alarm settings and may be reused for different types of objects (such as servers or hubs) as well as for different types of alarms. Actions can be created before the actual alarm that may use it. This is done through the "Actions Directory Setup" component of the Alarm Configuration Tool.

Actions may take three forms:

- *Dial a paging device and supply a numeric message*
- *Send an email message*
- *Start an application*

Starting an application could consist of:

- Running a .wav file to notify individuals that are in the vicinity of the console
- Bring up a troubleshooting window to guide an administrator through an unfamiliar procedure
- Proactively fix the problem without operator intervention (for example if the system fills up with temporary files, the application could delete files in a temporary directory)

Configuring Alarms

The Alarm Configuration Tool is used to set alarms on DIGITAL Prioris servers, AlphaServer systems, desktop computers, and mobile systems. The same alarm can be configured simultaneously for more than one object as long as the feature being alarmed on is present in all the hosts.

Alarms can be set for status or threshold events.

- **Threshold alarms** are triggered when a preset value is reached. For example, an alarm may be set for File Utilization with the threshold set for 85%. Threshold alarms may be set for the following:
  - — CPU Utilization
  - — File System Utilization
  - — Disk storage used
  - — Voltage
  - — Temperature

  - Cooling, fans
  - Memory SIMM ECC status
  - Total Packets
  - Inbound Errors, errors while receiving data
  - Outbound Errors, errors occurring when transmitting data
  - Inbound Packets, number of packets received
  - Inbound Packet Discards, number of received packets that are discarded
  - Unknown Protocol Errors, packets received with unknown protocols
- **Status alarms** are set when a device fails, issues a warning, or comes back online. For example, fan sensors failing may result in a status alarm. The following are the categories for which status alarms can be set:
  - Processors
  - Disks
  - Fans Sensors
  - Voltage Sensors
  - Power Supply Sensors
  - Temperature Sensors
  - Memory Status
  - Cluster Group Status

The alarm configuration tool also provides SNMP Trap alarms for any SNMP device on the network. The alarms are set on traps occurring as the result of status changes.

Viewing Alarms

The Alarm Viewer (See Figure 3-5) is used to display the alarms that have occurred on objects. It allows:

- Viewing of unacknowledged alarms
- Acknowledging of alarms
- Searching for alarms based on specified criteria (filters)
- Displaying alarm criteria on alarms that have been set

Alarms at a Glance

The alarm counter buttons located on the status bar at the bottom of the ServerWORKS window display the number of unacknowledged alarms of high, medium, low, or informational severity:

To list all unacknowledged alarms of a particular severity, click the alarm counter button of the desired severity (High, Med, Low, or Info). The Alarm Viewer window appears, listing all unacknowledged alarms of that severity.

Additional SNMP Tools

There are additional SNMP tools which may be used. These are:

- ***Properties***—provides information about objects
- ***MIB Compiler***—adds new MIBs to ServerWORKS Manager Console
- ***MIB Profiler***—associates MIBs with an object type

Properties

ServerWORKS Manager Console's SNMP device tools provide the ability to view properties for any SNMP device (See Figure 3-7). The tool is available from the Action menu. It is also available when performing any of the other types of management functions such as NT Server or NetWare Server Management.

MIB Compiler

The MIB Compiler is used to load new MIB group and MIB variable definitions into the database.

The MIB compiler takes a MIB definition file in standard ASN.1 format, compiles the file and links the resulting MIB information into the database.

MIB Profiler

The MIB Profiler is used to associate MIBs with an object type. For example, a DIGITAL server object type has certain MIBs that have been defined to be associated with that object type.

If the MIBs associated with an object need to be modified, it is done using the MIB Profiler. The MIB profiler:

- Assigns MIB groups to an object type.
- Deletes (de-assigns) MIB groups from an object type.

The MIB Profiler saves the MIB group assignments in the database so they can be referenced by the MIB Browser. For example, after a particular SNMP object is selected, the MIB Browser obtains the object type and uses this information to display all the associated MIB groups from the database. Only the applicable MIB groups are listed in the MIB Groups field of the MIB Browser window. Then either a group or one or more variables from that group may be chosen to perform get and set operations against the specified object.

Monitoring and Status

A primary indication of a problem with an object is indicated by one of the following:

- a color change to its circle icon
- a color change to the map icon background
- a bell appearing next to the object.

The circle and icon background color are indications of the ICMP (Internet Control Message Protocol) status or SNMP polling, while the bell indicates alarms and traps.

Status Changes

Status changes in objects are indicated by color changes on the viewers. On a hierarchical viewer, the status is indicated by a circle to the left of the object while on a map viewer, status is indicated by the background color of the object icon. The meanings of the colors are as follows (note that these are the default colors):

- ***green***—is the result of either an ICMP or SNMP poll and indicates the device is up
- ***yellow***—is the result of a SNMP poll and indicates the device may be partially up or one interface may be down
- ***red***—is the result of a SNMP poll and indicates the device may be in the process of going down (may be intentional)
- ***magenta***—is the result of either an ICMP or SNMP poll and indicates the device is not responding

Status is detected by either polling or "pinging" an object. If the poll or the ping is successful, the status color is green. Otherwise, the status color of the object is magenta. The colors yellow and red are only seen in limited circumstances.

Alarms

The alarm bell is used to indicate alarms occurring on objects. On a hierarchical viewer, the bell is on the left side of the object while on a map viewer, the bell is in the upper right corner of the object icon.

The conditions that cause the bell to appear are either a trap or an alarm being triggered. The conditions for alarms are determined by what has been previously set using the Alarm Configuration Tool.

Reports

There are two types of reports available. These are:

- ***Discovery Report***—generated by IP Discovery and contains information about the objects discovered
- ***IP Address Report***—generated by the IP Address Report Utility and provides information on Media Access Control (MAC) addresses

Discovery Report

When a Discovery operation completes, a Discovery report is created that lists any newly discovered IP hosts, configuration changes, duplicate IP addresses, and misconfigured devices. All past reports are saved in the directory:

<installation Directory>\database\IPREPORT

The file name format is:

<month><date><hour><minutes>.txt

For example:

04071917.txt = (April 7th at 5:17pm)

IP Address Report Utility

The IP address report is created from the database after a discovery is completed. The information contained in the report is address, name, and MAC address of each discovered object. This is generally used to find conflicting IP address associated with their unique MAC addresses.

The IP Address Report Utility is located on the Tools pull down menu.

Background Tasks

The background tasks associated with ServerWORKS Manager Console are:

- ***Poller***—sends messages out at timed intervals to all objects with the intent of initiating a response from the object.
- ***Data Collector, Event Logger, and Event Dispatcher***—background processes that are associated with the ability to receive alarms and to perform further actions
- ***Ping Server***—performs user-initiated "polls" of one object

Poller

The Poller periodically requests status information (up, down, or no response) from specified network objects and their interfaces. The objects that may be polled are all interfaces belonging to network objects that have an SNMP agent or that support ICMP protocol (for example, routers and end nodes).

By default, the Poller is automatically started after IP discovery is done. Using the default settings, all objects that are listed in the database are polled at the same interval.

Polling may also be done on a user-defined group. A group may consist of a collection of objects that would be polled at the same intervals.

Status Changes

When the Poller detects a status change, it forwards the information to the management console.

When a hierarchical or map viewer receives the Poller status change information, it updates the status color in the viewers (icon background in the map viewer and the circle next to object in the hierarchical viewer). The meanings (default) of the colors are:

- ***Green***—up
- ***Red***—down
- ***Magenta***—no response

The colors may be customized.

The Poller may also be configured to send SNMP trap information to an enterprise-level network management system. Refer to Chapter 4 for more information.

Data Collector, Event Logger, and Event Dispatcher

Both the Event Dispatcher and Event Logger must be running to receive alarms, notification of alarms, or to automatically run a script when an alarm threshold is reached. In addition, the ServerWORKS Manager Console Data Collector must also be running to receive alarms.

If these three utilities are not placed in the Windows NT or Windows 95 Startup Group, the Event Dispatcher and Event Logger are automatically initiated when ServerWORKS Manager Console is started.

Ping Server

ServerWORKS Manager Console has the capability to "ping" devices on the network.

Database and Associated files

ServerWORKS Manager Console Database

The database is composed of a set of files that are stored on the management console. Information gathered from IP Discovery, Polling, Alarm Configuration, Alarm Viewer, and other utilities are written to the database. If an alarm is added on a server or the MIB Enroller is used to add a MIB, these additions are only reflected in the database on the management console. They do not alter any of the information on the device.

Some changes are not only written to the database, but may affect systems on the network. For example, if NetWare Server Management or NT Server Management tools are being used, the information is not written to a database but directly affects the servers being managed.

ServerWORKS Database Files

The ServerWORKS database consists of the following files located in the \database directory:

- ***pcmgr.mdb file***—contains SNMP information about the devices on your network
- ***snmpomm.ini, dat***—contains the configuration of SNMP components and database validation entries
- ***swmgr.ini***—contains the configuration settings for the ServerWORKS Manager applications
- ***class.pod, .idx***—contains display information about viewers and objects
- ***contain.pod, .idx***—contains display information about viewers and objects
- ***object.pod, .idx***—contains display information about viewers and objects

In addition, the directories under <ServerWORKS-Installation-Directory>\database have the following purpose:

- ***empty***—files that represent the initial state of the ServerWORKS database
- ***ipreport***—contains the IP discovery reports
- ***bitmaps***—contains the bitmaps
- ***mail***—temporary storage for actions which use mail
- ***pager***—temporary storage for actions which use paging
- ***backgrounds***—contains ".bmp" files for map viewer backgrounds

Managing Servers Using SNMP-Based Enterprise Management Systems 4

This chapter explains how to use SNMP (Simple Network Management Protocol) and SNMP management tools with ServerWORKS Manager.

About SNMP

ServerWORKS Manager uses the SNMP protocol for its primary communication with servers running a variety of operating systems. ServerWORKS Manager implements SNMP-based MIBs and an SNMP agent extension component to provide the necessary framework for SNMP network management. It allows:

- Remote control of systems through SNMP Set and Get operations
- Setting of SNMP agent traps and alarms for the objects being managed
- Polling of SNMP variables to create console-based threshold alarms. Alarms generated by polling are set on host resource MIB variables; they do not define any SNMP traps.

SNMP System Components

SNMP stores its data in one or many *Management Information Bases* (MIBs) that describe the manageable objects on that host. In addition to system-supplied MIBs, vendors can define additional MIBs that allow vendor-developed devices to be monitored and manged by SNMP management consoles.

A MIB includes the following information about every object it describes:

- An object identifier that uniquely identifies the managed object on the network
- A definition of the data type used to define the object

- A textual description of the object
- An index method used for objects that are of a complex data type
- The read or write access that is allowed on the object

A *manager* is a program that requests data from other computers on the network. An *SNMP management console* is any computer running SNMP management software. When an administrator at the management console requests information about a managed object, the SNMP management program requests information about the object using its object identifier.

The *agent* is the program that receives management requests and processes them by accessing information from the MIBs on the computer. The agent then sends the requested information back to the SNMP management program that initiated the request.

The agent performs four operations:

- **Get** and **Get Next** retrieve information about the managed object and return it to the management console.
- **Set** changes the value of a managed object variable. Only variables whose object definitions allow read/write access can be set.
- **Trap** sends messages to the SNMP management console when a change or error occurs in a managed object. The trap is the only operation initiated by the agent without a specific request from a management program.

An *extension agent* is software that extends the functionality of the system agent. When the agent receives a request for information about one of the objects handled by an extension agent, it passes the request to the extension agent for processing. The extension agent returns the information to the SNMP agent, which returns it to the management console that requested the information, as shown in Figure 4-1.

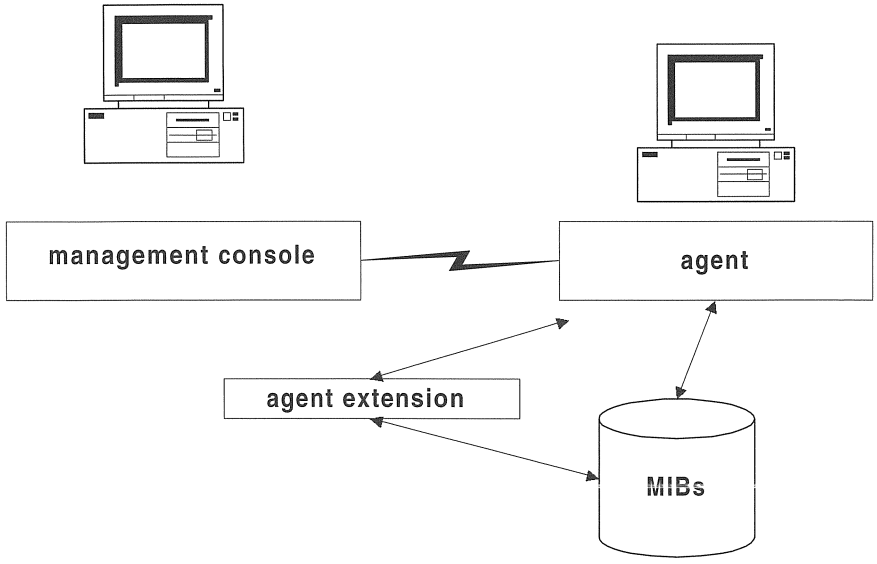


Figure 4-1: Extension Agents in SNMP

The DIGITAL SNMP Agent Extension

Most operating systems provide SNMP agent subsystems that allow you to construct extension modules for specific hardware and software. Server WORKS Manager supports all systems that provide an extendible SNMP subsystem. DIGITAL's Server Agent uses the operating system's native SNMP protocol stack and distribution mechanisms to return information about DIGITAL hardware and software and to export traps to other systems.

An SNMP agent can be configured to send its traps directly to any SNMP management console, including ServerWORKS Manager Console or to enterprise management systems, such as HP OpenView or Tivoli TME10, that use SNMP as their trap and alarming mechanism.

How ServerWORKS Manager Console Uses SNMP

ServerWORKS Manager Console functions as a management console without the SNMP service. Because it uses its own SNMP stack for decoding SNMP traps, it does not require that SNMP be installed on the console machine. However, systems that are to be viewed by the management console *must* have SNMP agents installed and configured. If the management console will be used to view the system on which it is installed, then SNMP must be installed and configured on the management console as well.

ServerWORKS Manager Console relies on the operating system SNMP components to provide the IP port number of the SNMP trap (usually 162). This entry can be found in the services file. On a Windows NT system, this file is usually found at c:\winnt\system32\drivers\etc\services. On a UNIX system, this file is found at \etc\services.

ServerWORKS Manager will attempt to use the trap port if it is not already in use. The ServerWORKS Manager Event Dispatcher receives traps from the SNMP trap port, so in order to run an enterprise manager on the same system as ServerWORKS Manager, you must close the Event Dispatcher process.

Note: *Some Windows 95 and Windows NT systems may have the snmp-trap entry removed. Make sure the following line is in the services file:*
snmp-trap 162/udp snmp

Configuring SNMP for Trap Forwarding

SNMP is a connectionless protocol. If the agent system and the management console system do not agree on the trap port number and other details about the exchange, no messages will pass between the two systems. No error will be detected and no exception message will be generated.

A system running Windows operating systems does not have the SNMP service installed by default. You must add the SNMP service explicitly from the control panel, then configure the SNMP agent with the correct security and access. You need to do this for both the management console and the system that will be generating the traps.

You find the SNMP setup in the control panel, under the network applet. You need to configure both the SNMP security and the traps (called "Traps" in the Windows NT V4.0/Windows 95 property page and "Service Configuration" in the NT V3.51 dialog box).

The screens differ in the two versions, but both require the same information:

- The community name or names you will be using
- The network name or the IP address of each SNMP management console that will be the destination for trap messages generated within a specific community

The following sections explain these items in more detail.

Configuring SNMP Security

The SNMP security service uses *community names* to authenticate messages. All SNMP messages must contain a community name. The SNMP agent that receives the message checks the community name against the list of names with which the SNMP service is configured. If the message contains a known community name, the message is processed. If no known community name matches the one in the message, the message is rejected. The "Send Authentication Trap" check box in the setup window determines whether the SNMP service sends a trap message to the requesting server when such an authentication failure occurs.

The default community name when the SNMP service is installed on a Windows NT-based computer is "public". You can add or remove community names as necessary. Note that if you remove all community names, including the default name, the SNMP service on that computer will authenticate and process SNMP messages containing any community name.

There is no relation between community names and domain or workgroup names. Community names function as a shared password for groups of hosts and should be selected and changed as you would any other password.

Only agents and managers that are configured with the same community name can communicate with each other. If the agent console does not recognize the community name contained in the SNMP messages from the management console, it will not accept any messages from the management console. Likewise, if the management console is not configured to recognize the community name the agent's system is using, it will not receive traps from the agent.

Configuring SNMP Traps

The SNMP agent generates trap messages, which are sent to an SNMP management console called the *trap destination.* If you want a system to forward SNMP traps to a management console, you must make sure both systems are properly configured:

- The management console must accept traps from the agent system, using the same community name as the agent system.
- The agent system must specify the management console system as a trap destination, using a community name the management console system recognizes.

When an agent trap condition occurs on the sending system, the agent sends the appropriate SNMP trap message to the management console system. If you do not configure both systems properly, no traps are passed.

Traps typically notify the management console about events such as a service starting or stopping, the existence of a serious error condition, or other event that is important to the agent. The SNMP agent or extension agent and its associated MIB defines what conditions cause a trap message to be generated, but the user controls where the message is sent.

You can identify the trap destination by name or by IP address. The trap destination must be a host that is running an SNMP manager program, such as ServerWORKS Manager or an enterprise manager.

Trap Forwarding

The management console that receives traps can in turn *forward* those traps to other systems. This allows workgroup-level managers to run ServerWORKS Manager, while enterprise-level managers run manager programs such as HP OpenView or Tivoli TME10. Forwarded traps are redirected by the ServerWORKS Manager Event Dispatcher and Event Logger, not by the agent.

To forward traps in ServerWORKS Manager, define the forwarding destinations in the file TRAPFWD.INI. You can find this file in the directory where you installed ServerWORKS Manager.

Trap forwarding takes place only when the Event Dispatcher and Event Logger are running. This implies that no other application has opened trap port 162. By default, no forwarding takes place. Only agent-based traps are forwarded, not Data Collector events. For example, ServerWORKS Manager would forward an alarm from a temperature sensor, but would not forward an alarm set on the CPU utilization value, which is generated internally by ServerWORKS Manager.

The following example shows a TRAPFWD.INI file that forwards traps to four different destinations. Note that the count is zero based. The semicolon (;) character is used as a comment delimiter.

```
; This file is used to tell the Event Dispatcher to
; forward all of the traps it receives to other
; management stations.  An example follows:
;

 [Trap Forward Addrs]
 agent count=4
 agent_0=16.20.204.163
 port_0=162

 agent_1=16.20.204.155
 port_1=162

 agent_2=16.20.204.90
```

```
 agent_3=16.20.204.163
 port_3=167

;
; Note:
;  DO NOT specify the Event Dispatcher node itself.
```

Specify the address and port for each destination. If a port number is not specified, as in the entry for agent_2 in the example, then port 162 is assumed. This is useful with systems which have multiple SNMP trap listeners on them.

All traps will be forwarded to each destination you define. ServerWORKS Manager allows up to four forwarding destination addresses. Set the agent count to the number of destinations you specify. In the example, the agent count of 4 tells the system to expect four agent entries. To forward all traps to a single management console and tell the system to send these traps to the IP address 16.20.204.163 using the TCP/IP port number 162, you would use an entry like this:

```
Trap Forward Addrs]
agent count=1
agent_0=16.20.204.163
port_0=162
```

Receiving ServerWORKS Traps in Enterprise-Level Managers

By default, traps forwarded from ServerWORKS Manager to an enterprise-level manager will be displayed as an unknown trap. To allow an enterprise manager such as HP OpenView or Tivoli TME-10 to display information about DIGITAL servers, you need to follow these basic steps:

- Enroll DIGITAL MIBs in the enterprise system
- Create the appropriate device class (object types and subtypes)
- Customize the alarm view, if you wish

The specific steps will vary depending on which enterprise-level manager you use. This section uses examples taken from Tivoli TME-10 NetView to illustrate the process.

You can launch ServerWORKS applications from both HP OpenView's NetServer Assistant and from Tivoli TME-10.

Enrolling DIGITAL MIBs in a Non-DIGITAL System

Most network managers allow you to compile a new MIB. After compiling a MIB, the same information displayed in the MIB Browser can be displayed using another workgroup manager's or enterprise manager's browser.

If you choose to enroll the DIGITAL-specific MIBs, you allow the user to get and set MIB variables from the systems on which the DIGITAL SNMP extended agents are running. A number of DIGITAL MIBs are found in the ServerWORKS Manager directory. You can integrate any or all of following MIBs into your SNMP management system:

MIB Name	Description
NTCMGT.MIB	DIGITAL NT Cluster MIB
RFC1514.MIB	Host Resource MIB
SVRMGT.MIB	DIGITAL Server Management MIB
SVRSYS.MIB	DIGITAL System MIB
MLXGAM.MIB	Mylex Global Array Manager MIB

To add a DIGITAL MIB to Tivoli TME-10 NetView on the target system, select MIB from the tools menu. Select Load. The MIB Loader opens. Select the MIBs you want to load.. If you choose the Server System MIB, you need to include RFC1213 (MIB II) as well because the Server System MIB references variables in RFC1213.

Launching ServerWORKS System Browser from an Enterprise-Level Manager

Another area of integration is application launch. Most enterprise managers, such as HP OpenView and Tivoli TME-10, allow you to add user-defined applications.

When you install ServerWORKS Manager on a system where Tivoli TME 10 NetView for Windows NT is installed, the ServerWORKS Manager installation automatically installs into TME-10 and registers the ServerWORKS Manager System Browser so it can be used with DIGITAL servers. When you select a DIGITAL host in the NetView IPMap, the System Browser entry in the TME-10 Tools pull-down menu is activated, as show in Figure 4-2.

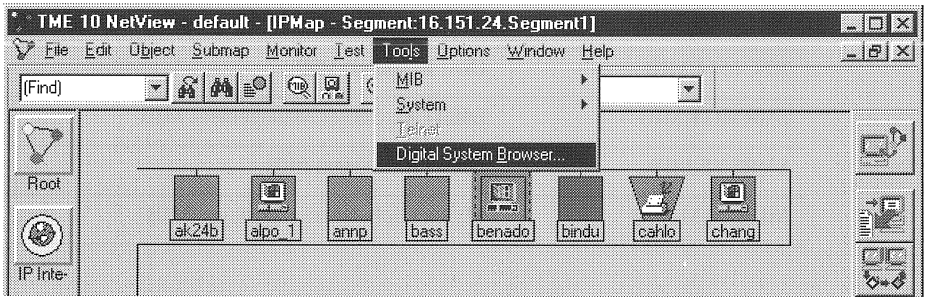


Figure 4-2: Launching the System Browser from TME10

Reference Information 5

Introduction

This chapter provides additional sources of information on topics covered in the manual.

Topic	Additional Source of Information
DIGITAL UNIX	Network Administration and Network Programmer's Guide
Discovering objects on your network	On-line help, Chapter 3 of this manual.
KCRCM	KCRCM AlphaServer Remote Console Module Installation and User's Guide (EK-KCRCM-IN) included with the KCRCM product
Monitoring Systems	The Simple Book - An Introduction to Internet Management by Marshall T. Rose, published by Prentice Hall 1991, second edition 1994 SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards by William Stallings, published by Addison Wesley 1993

Topic	Additional Source of Information
Monitoring Systems (continued)	Internetworking with TCP/IP, Volume 2, Design, Implementation, and Internals by Douglas E. Comer and David L. Stevens published by Prentice Hall 1991
	Internetworking with TCP/IP, Volume 1, Principles, Protocols, and Architecture by Douglas E. Comer published by Prentice Hall 1991, Second Edition
Mylex GAM	Mylex Global Array Manager 2 Installation and User's Guide (ER-MYL02-IA) found on the ServerWORKS Manager CD-ROM in the documentation section
Novell NetWare	Novell's Guide to Multiprotocol Internetworking, by Laura A. Chappell and Roger L. Spicer published by the Novell Press
	NetWare, The Professional Reference, Third Edition, published by News Rider Publishing 1994
OpenVMS	TCP/IP Networking on OpenVMS Systems and OpenVMS System Manager's Manual
RSM	RSM Installation Guide (ER-PCDSC-IA) and RSM Station Software User's Guide (ER-PCDSM-UA) included with the RSM product
SCO UNIX	SCO OpenServer Handbook, How to install, configure, and start using an SCO OpenServer system, published by The Santa Cruz Operation 1995

Topic	Additional Source of Information
Sending SNMP Traps	On-line help, Chapter 4 of this manual
	The Simple Book - An Introduction to Internet Management by Marshall T. Rose, published by Prentice Hall 1991, second edition 1994
	SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards by William Stallings, published by Addison Wesley 1993
Setting and Receiving Alarms	On-line help, Chapter 3 of this manual
SNMP	The Simple Book - An Introduction to Internet Management by Marshall T. Rose, published by Prentice Hall 1991, second edition 1994
	SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards by William Stallings, published by Addison Wesley 1993
	Internetworking with TCP/IP Volume 2 Design, Implementation, and Internals by Douglas E. Comer and David L. Stevens published by Prentice Hall 1991
SWCC	StorageWORKS Command Console Installation Guide (AA-R0HJB-TE) found on the ServerWORKS Manager CD-ROM in the documentation section

Topic	Additional Source of Information
Windows 95	Microsoft Windows 95 Resource Kit published by Microsoft Press 1995
Windows 95 SNMP	Microsoft Windows 95 Resource Kit published by Microsoft Press 1995
Windows NT	Windows NT Networking Guide - Windows NT Resource Kit by and published by Microsoft Press
Windows NT SNMP Service	Windows NT Networking Guide - Windows NT Resource Kit published by Microsoft Press

The following web sites may also provide additional information on ServerWORKS:

http://www.digital.com/info/alphaserver/sworks.html

Glossary

Term	Definition
Alarm	An SNMP trap generated by an agent or an event and triggered by the results of polling an agent.
Allocation Units	The size in bytes for a particular storage device. For example, the allocation units for a disk are typically 512, 1024, or 2048 bytes and are sometimes referred to as 'block size'
CPU Utilization	Average percentage of time that this processor was not idle.
Data Collector	Process that runs on the management console and polls objects for SNMP data. The collector analyzes the data and either generates alarms or passes the data on to registered applications such as the System Browser.
DMI	Desktop Management Interface
FAT	File Allocation Table (listed on the System Browser File System property page)
File System Utilization	The percentage of the file system being used (local file systems).

Term	Definition
IP	Internet Protocol (see also TCP/IP)
IP Address	An address of an object on a network. The standard address is composed of four numbers each of which is less than 255.
Management Information Base (MIB)	Data Specification for passing information using the SNMP protocol
MIF	Management Information File - This is a database file that defines a given host's configuration, hardware inventory, storage devices, processors, and memory.
Mount Point	The top level name for a mounted file system
MTU	Maximum Transmission Unit
Network Interface	Communication between the management console machine and the network. Usually completed through Network Interface cards
Network Interface Inbound Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Network Interface Inbound Packet Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space
Network Interface Inbound Packets	The number of packets delivered to a higher-layer protocol.

Term	Definition
Network Interface Outbound Errors	The number of outbound packets that could not be transmitted because of errors
Network Interface Unknown Protocol Errors	The number of packets received through the interface which were discarded because of an unknown or unsupported protocol
NOS	Network Operating System. The operating system and protocol used to communicate between objects on a network.
NTFS	NT File system. File system used on NT.
Polling Interval	The time between polling queries of a device.
Re-Enable Value	Value that can be set in the Threshold screen to automatically enable an alarm that has previously triggered
SNMP	Simple Network Management Protocol - The application protocol offering network management service in the Internet
SNMP Trap	An asynchronous event generated by the agent and sent to the SNMP manager.
Status Alarm	Alarm set on server processors or disks to indicate the status of the device (options are running, non-functional, and warning)
System Name	The name of the object on the IP network as returned by the Naming server or found in the Hosts file on the management console machine.
System Up Time	The time the system has been up since it was booted.

Term	Definition
TCP/IP	Transmission Control Protocol/Internet Protocol. A widely used set of software communications protocols. TCP delivers data over a connection between applications on different computer on a network: IP controls how packets (units of data) are transferred between computers on a network.
Threshold Alarm	Alarm triggered when a value entered on the Threshold Alarm screen meets a specified condition
Threshold Value	Value at which an alarm is triggered (e.g., 10000 packets per second)

Index

—L—

—M—

—N—

—O—

—P—

—R—

—S—

—T—

—V—

—W—

digital™

ER-4QXAA-UA. F01

Printed in Ireland