

ServerWORKS™ Manager de DIGITAL

Manual de instalación y del usuario

Referencia: ER-4QXAA-UA. H01

Digital Equipment Corporation

Julio de 1998

La información contenida en este documento está sujeta a cambios sin previo aviso y no constituye compromiso alguno por parte de Digital Equipment Corporation. Digital Equipment Corporation declina toda responsabilidad por cualesquiera errores que pudieran aparecer en este documento.

La utilización o copia del software descrito en este documento se autoriza únicamente según los términos de una licencia válida concedida por Digital. No se asume responsabilidad alguna por el uso o la fiabilidad del software o los equipos que no sean suministrados por Digital Equipment Corporation o sus compañías filiales.

Copyright 1995, 1996, 1997, 1998 Digital Equipment Corporation. Reservados todos los derechos.

Las siguientes son marcas registradas de Digital Equipment Corporation: DIGITAL, el logotipo de DIGITAL, OpenVMS, ClientWORKS, ServerWORKS Manager, StorageWorks, SWCC, RSM, AlphaServer y AlphaGeneration.

Las siguientes son marcas registradas de otros proveedores:

APC es una marca comercial registrada de American Power Conversion, Inc.

Insight Manager es una marca registrada de Compaq, Inc.

Lexmark es una marca registrada de Lexmark, Inc.

Hewlett-Packard es una marca comercial registrada de Hewlett-Packard Company.

IBM es una marca comercial registrada y NetView es una marca registrada de International Business Machines Corporation.

Microsoft, MS-DOS, Windows 95 y Windows NT son marcas registradas de Microsoft Corporation.

Mylex es una marca comercial registrada y Global Array Manager es una marca registrada de Mylex Corporation.

NetBIOS es una marca comercial registrada de Micro Computer Systems, Inc.

Novell y NetWare son marcas comerciales registradas de Novell, Inc.

OnliNet es una marca comercial registrada de Exide Electronics, Inc.

PATROL es una marca comercial registrada de BMC Software, Inc.

SCO UNIX es una marca comercial registrada cuya licencia se obtiene exclusivamente a través de Santa Cruz Operation, Inc.

TME 10 es propiedad de Tivoli Corporation e International Business Machines Corporation.

Unicenter es una marca comercial registrada de Computer Associates International, Inc.

UNIX es una marca comercial registrada en los Estados Unidos y demás países con licencia exclusiva a través de X/Open Company Ltd.

Tabla de materias

1 Introducción

Los objetos que descubre ServerWORKS.....	1-2
Integración con herramientas de administración a nivel de empresa.....	1-3
Minimal Health	1-4
Supervisión inteligente.....	1-4
Uso detallado de componentes.....	1-4
Opciones de notificación.....	1-5
Administración de NT y NetWare.....	1-5
Integración de aplicaciones DIGITAL y de terceros.....	1-6

2 Uso de SNMP con ServerWORKS Manager

Acerca de SNMP.....	2-2
Componentes del sistema SNMP.....	2-2
MIBs.....	2-2
Programas de administradores de redes	2-3
Agentes	2-3
Agente de extensión SNMP de DIGITAL.....	2-5
Cómo la consola utiliza SNMP para comunicarse	2-6
Configuración de SNMP para el reenvío de capturas	2-7
Configuración de la seguridad de SNMP	2-8
Configuración de SNMP Traps.....	2-9

3 Instalación

Requisitos de configuración de la red	3-2
Plataformas soportadas de SNMP.....	3-3

Hardware de la consola de administración	3-4
Software de la consola de administración	3-5
Hardware de agente	3-6
Software de agentes	3-6
Soporte de clúster de red.....	3-8
Consideraciones previas a la instalación para ServerWORKS.....	3-8
Orden de instalación	3-8
Instalaciones incompletas	3-10
Cerrar otros programas antes de la instalación	3-10
Conservar una base de datos de ServerWORKS anterior.....	3-11
Manipulación de la base de datos.....	3-11
Integración de ServerWORKS con administradores de empresas	3-11
Utilización de ManageWORKS	3-11
Agentes y servicio de SNMP.....	3-12
Agentes proporcionados con ServerWORKS.....	3-12
Agentes proporcionados con un sistema operativo	3-13
Instalación de un agente en el dispositivo de consola.....	3-13
Consideraciones previas a la instalación para ClientWORKS	3-13
Consideraciones previas a la instalación para RSM.....	3-14
Consideraciones previas a la instalación para RMC.....	3-14
Primeros pasos para instalar todos los componentes	3-15
Instrucciones para la instalación de componentes.....	3-17
Instalación de agentes de ServerWORKS Manager.....	3-17
¿Planea supervisar la consola de administración?	3-18
Instalación de ServerWORKS Manager Console	3-18
Inicio de la instalación para Windows NT 4.0	3-19
Inicio de la instalación para Windows NT 95	3-19
Instalación de la consola.....	3-20

Finalización de la instalación	3-22
Instalación de ServerWORKS Console Integration	3-22
Instalación de ClientWORKS	3-23
Instalación de RAID Storage Management	3-24
Instalación de StorageWorks	3-24
Instalación de Mylex GAM.....	3-25
Instalación de Integración de Remote Management.....	3-25
Tutorial	3-26
Documentación.....	3-26
Opciones posteriores a la instalación.....	3-26
WatchDog Timer en plataformas múltiples	3-27
WatchDog Timer en SCO UNIX	3-28

4 Descubrimiento de redes y objetos

Visualizaciones de la red.....	4-2
Visualización de ServerWORKS Explorer	4-2
Visores de mapas de IP Discovery.....	4-3
Elementos de las ventanas del visor	4-4
La Barra de menús	4-4
La Barra de herramientas de comandos	4-6
La Paleta del Visor de mapas	4-6
Abrir y salir de ServerWORKS.....	4-7
Navegar por visores de mapas y Explorer.....	4-8
Visualización de opciones en mapas individuales.....	4-9
Supresión y eliminación de objetos.....	4-10
Cómo IP Discovery encuentra objetos	4-11
Descubrimiento de redes	4-11
¿Qué ha descubierto?.....	4-13

Descubrimientos posteriores	4-13
Descubrimiento de clústers	4-14
Impresión de informes de información sobre IP Discovery	4-16
Informes de IP Discovery	4-16
Informes de dirección IP	4-17
¿Cómo opera la red?	4-17
Verificaciones de estado codificadas con colores	4-18
Verificaciones rápidas desde la Barra de estado	4-19
Cómo aprender del visor de alarmas	4-19
Guardar e imprimir la lista de alarmas	4-20
Filtro de alarmas para visualización	4-21

5 Definición de alarmas

La ventana Alarm Configuration y la Barra de herramientas	5-2
Actualización de la lista de alarmas configuradas	5-6
Impresión de la lista de alarmas	5-7
Configuración de alarmas	5-7
Minimal Health	5-7
Comprensión de alarmas de Minimal Health	5-8
Alarmas de consola definidas por el usuario	5-9
Configuración de SNMP y el destino de capturas	5-10
Alarmas de estado de componente	5-10
Alarmas de umbral de componente	5-10
Respuesta a indicaciones durante la configuración de alarmas	5-11
Configuración de capturas múltiples para alarmas de umbral	5-12
Definición de capturas múltiples con versiones de agente múltiples	5-12
Definición de capturas para paquetes de entrada y paquetes de salida de red	5-13
Alarmas de estado del sistema	5-13

Alarmas de SNMP Trap	5-13
Creación de alarmas y acciones de notificación.....	5-13
Creación de alarmas de estado de componente	5-14
Creación de alarmas componente	5-15
Creación de alarmas de estado de sistema.....	5-16
Creación de alarmas de SNMP Trap	5-17
Modificación de una alarma.....	5-17
Adición de la acción de notificación en una alarma.....	5-18
Configuración de una acción de notificación de Pager	5-18
Cambio del tiempo de espera predeterminado de Pager para Pager numérico	5-20
Configuración de una acción de notificación de correo electrónico	5-21
Configuración del perfil predeterminado ‘Configuraciones de Microsoft Exchange’	5-22
Configuración de una acción de inicio de aplicación	5-23
Configurar la notificación para capturas de Minimal Health.....	5-24
Definición de alarmas en clústers y recursos de clúster	5-24
Supervisión de transiciones.....	5-26

6 Administración desde la consola

System Browser para hosts DIGITAL.....	6-2
Visualización de datos de nodos con System Browser	6-5
Comparación de sistemas y componentes	6-6
Definir números asignados de FRU.....	6-6
Elaboración de gráficas de la actividad en tiempo real	6-7
Recopilación de la historia de un nodo.....	6-10
MIB Browser para objetos de SNMP.....	6-12
Administración de un objeto desde MIB Browser	6-13
Modificación de variables.....	6-13

Utilización de los aceleradores de consulta	6-15
Visualización de información sobre el clúster desde MIB Browser	6-16
MIF Browser.....	6-17
MIB Compiler.....	6-17
MIB Profiler.....	6-18
MIB Enroller.....	6-18
Tareas de segundo plano.....	6-18
Ping Server	6-19
Poller	6-19
Data Collector, Event Logger e Event Dispatcher.....	6-19

7 Obtención de los datos deseados

Opciones personalizables para un visor o un mapa	7-2
Iniciar con contexto	7-5
Descubrimiento y administración de impresoras	7-8
Uso de máscaras de red para refinar descubrimientos	7-9
Uso de colecciones y dominios para verificaciones de estado.....	7-9
Realización de encuestas efectiva.....	7-10
Creación de un grupo de encuesta	7-11
Definición de parámetros de encuesta de grupo	7-12
Visualización de información encuestada	7-13
Cambio de variables desde propiedades de objeto	7-13
Trabajo con la base de datos de ServerWORKS Manager	7-14
Utilización de DB Utility	7-17
Creación de tipos de objeto y perfiles personalizados.....	7-18
Definición del nuevo tipo de objeto	7-18
Acerca del nombramiento de objetos	7-19
Acerca de la selección de mapas de bits	7-19

Acerca de la forma de segundo plano	7-19
Almacenamiento de MIBs en la base de datos de ServerWORKS	7-20
Acerca de variables de grupo de MIB y su propósito	7-21
Asignación de grupos de MIB al tipo de objeto.....	7-21
Desplazamiento rápido por las listas de ServerWORKS Manager.....	7-22
Adición manual del objeto al mapa de red	7-23
Verificación del objeto.....	7-23
Asociación de objetos desconocidos a tipos de objeto conocidos	7-24
Edición del Registro para reconocer el nuevo objeto	7-26
Edición del Registro con un archivo por lotes.....	7-27
Configuración de destinos de capturas y SNMP	7-28
Seguridad de SNMP.....	7-29
Configuración de SNMP y el destino de capturas en Windows NT 4.0	7-29
Configuración de SNMP en Windows 95.....	7-32
Instalación del software SNMP.....	7-32
Configuración del destino de capturas en Windows 95	7-33
Configuración del destino de capturas desde la consola.....	7-34
Reenvío de capturas.....	7-37
Uso del Visor de sucesos de NT para seguir alarmas	7-40

8 Administración de redes Windows NT y NetWare

Descubrimiento del Administrador de servidores de NT.....	8-2
Antes de administrar NT desde ServerWORKS.....	8-2
Utilización de Administrador de servidores de NT para dominios Windows NT ...	8-3
Más acerca de Administración de NT.....	8-4
Novell NetWare Server Manager	8-5

A Procedimientos e información adicionales

Presentación general de subagentes de DSM.....	A-4
Configuración del sistema para utilizar agentes de DSM.....	A-4
Instalación de agentes SNMP para OS/2	A-6
Restricciones de datos ambientales: Sistemas AlphaServer 8200 y 8400	A-7
Dispositivo IIA0: ahora configurado en sistemas AlphaServer 4100.....	A-8
Dispositivo OPA1: ahora configurado en sistemas AlphaServer 8200 y 8400.....	A-8
Ejecución de una segunda versión de ServerWORKS	A-9
¿Tiene ManageWORKS instalado?	A-9
Después de actualizar a ServerWORKS Manager	A-10

B Solución de problemas

Problemas comunes y soluciones.....	B-1
Configuración de un módem y puerto de comunicaciones para comunicación por Pager.....	B-3
Edición del Registro.....	B-4
Supresión de claves de registro	B-4
Claves de Registro para ServerWORKS	B-5
Claves de Registro para agentes.....	B-6
Claves de Registro para ClientWORKS	B-7

C Referencias

Bibliografía	C-1
Sitio Web	C-4
Glosario	C-4

Figuras

Figura 2-1 Agentes de extensión en SNMP	2-4
Figura 4-1 Visores de mapas y Explorer de una red	4-5
Figura 4-2 Paleta de mapas	4-7
Figura 4-3 Mapa de clústers desplegados	4-14
Figura 4-4 Visor de alarmas.....	4-19
Figura 4-5 Cuadro de diálogo Filtro de Visor de alarmas	4-20
Figura 5-1 Ventana Alarm Configuration	5-2
Figura 5-2 Barra de herramientas de Alarm Configuration.....	5-3
Figura 6-1 Ventana System Browser	6-3
Figura 6-2 Gráficas de ServerWORKS	6-7
Figura 6-3 MIB Browser Window.....	6-13
Figura 7-1 Insight Manager iniciado desde ServerWORKS Manager Console	7-7
Figura 7-2 Entradas en el cuadro de diálogo Agregar Tipos de objeto de SNMP definen un tipo de objeto	7-20
Figura 7-3 Grupos de MIB asignados al nuevo tipo de objeto	7-22
Figura 7-4 Nuevo tipo de objeto descubierto en visores jerárquicos y de mapas	7-24
Figura 7-5 Cuadro de diálogo Tipos para asociar objetos desconocidos a objetos existentes.....	7-26
Figura 7-6 Selección de un agente de SNMP desde la página Servicios de Red.....	7-30
Figura 7-7 Destino de captura especificado en la página de Propiedades de captura.....	7-31
Figura 7-8 Cuadro de diálogo Trap Control.....	7-35
Figura 7-9 Cuadro de diálogo Trap Control.....	7-38

Tablas

Tabla 3-1 Agentes SNMP y DMI.....	3-3
Tabla 3-2 Requisitos de hardware mínimos para ServerWORKS Manager Console	3-4
Tabla 3-3 Requisitos de software mínimos para ServerWORKS Manager Console ...	3-5
Tabla 3-4 Requisitos de hardware mínimos para agentes.....	3-6
Tabla 3-5 Requisitos de software para agentes	3-7
Tabla 3-6 Requisitos para el soporte de clústers de red	3-8
Tabla 4-1 Indicadores de colores de estado en visores jerárquicos y de mapas	4-18
Tabla 5-1 Iconos de host de Alarm Configuration	5-4
Tabla 6-1 Información sobre System Browser	6-4
Tabla B-1 Claves de Registro para la clave HKEY_LOCAL MACHINE de ServerWORKS.....	B-5
Tabla B-2 Claves de Registro para la clave HKEY_LOCAL MACHINE de agentes	B-6
Tabla B-3 Claves de Registro para la clave HKEY_LOCAL MACHINE de ClientWORKS	B-7
Tabla B-4 Claves de Registro para la clave HKEY_CURRENT_USER de ClientWORKS	B-8

Prefacio *P*

Este documento explica cómo utilizar el producto ServerWORKS Manager de Digital para administrar servidores y otros dispositivos DIGITAL. Además, proporciona procedimientos detallados para instalar, configurar y utilizar ServerWORKS Manager Console.

Lectores

Este manual está hecho para el administrador de redes o administrador de servidores que está instalando y configurando ServerWORKS Manager Console y agentes. Este manual supone que está familiarizado con los fundamentos de redes y el protocolo SNMP.

Información relacionada

Consulte las fuentes siguientes para obtener más información

- Apéndice C, que contiene una bibliografía y un glosario
- *DIGITAL ServerWORKS Manager Enterprise Management Integration Guide*
- *Using the ClientWORKS® Management Suite with DIGITAL PCs: A Guide for Network Administrators*

Convenciones utilizadas en este manual

Los términos "Seleccionar" y "Elegir" se utilizan frecuentemente en los procedimientos. Ambos términos se refieren a a operaciones específicas con el puntero del ratón o el teclado:

Prefacio

- **Seleccione**—Mueva el puntero del ratón a un elemento (icono, comando, nombre) y haga clic una vez con el botón del ratón o utilice el conjunto de teclas especificado para indicar una selección.
- **Elija**—Mueva el puntero del ratón a un elemento y haga doble clic con el botón del ratón o utilice el conjunto de teclas especificado para iniciar una acción en el elemento seleccionado.

Se utilizan los iconos siguientes en el manual:



Nota: Indica información útil. La nota puede ser una recomendación, técnica especial, acceso rápido u otra información para ayudarlo a utilizar el producto. Una nota no es un aviso o una precaución de consecuencias serias.



Precaución: Indica información importante. Si no se utiliza la información, se pueden tener problemas.



Aviso: Indica información significativa o instrucciones que se deben tener en cuenta. Si no se utiliza la información, se pueden perder datos o pueden haber otras fallas catastróficas.

Convenciones del teclado

Para	Pulse estas teclas:
Desplazarse una ventana antes o una ventana después	AV PÁG. o RE PÁG.
Ir al principio de la lista	CTRL+INICIO
Ir al final de la lista	CTRL+FIN
Mover el área de activación a la izquierda o la derecha	FLECHA IZQUIERDA o FLECHA DERECHA
Mover el área de activación una línea arriba o una abajo	FLECHA ARRIBA o ABAJO
Mover a la ventana siguiente	CTRL+TAB
Mover a una ventana anterior	CTRL+MAYÚS+TAB
Ir al campo siguiente	FLECHA ABAJO o TAB
Ir al campo anterior	FLECHA ARRIBA o MAYÚS+TAB
Ir al grupo siguiente	CTRL+FLECHA ABAJO
Ir al grupo anterior	CTRL+FLECHA ARRIBA
Mover el área de activación hacia arriba o hacia abajo sin afectar el estado de la línea anterior (para agregar o suprimir líneas de un conjunto seleccionado)	MAYÚS+FLECHA ARRIBA o MAYÚS+FLECHA ABAJO
Cambiar el estado del elemento de la zona de activación	BARRA ESPACIADORA
Ver la Ayuda	F1
Ver la Ayuda (desde una ventana de la consola)	CTRL+ALT+F1

Prefacio

Introducción *1*

DIGITAL ServerWORKS Manager es una herramienta de administración para administradores de redes y servidores. Puede supervisar y administrar los objetos siguientes utilizando agentes de ServerWORKS y la consola:

- Servidores DIGITAL y no DIGITAL y clústers que ejecutan una gran variedad de sistemas operativos
- Objetos de no servidor y componentes de redes de proveedores múltiples
- Sistemas de escritorio DIGITAL

Las ventajas de ServerWORKS Manager

ServerWORKS Manager es una herramienta de administración de redes que facilita el diagnóstico y la supervisión de la red. ServerWORKS utiliza SNMP (Simple Network Management Protocol) como mecanismo principal de comunicación con servidores y objetos administrados. Al utilizar ServerWORKS, puede encontrar, supervisar y administrar dispositivos que soportan SNMP desde una sola consola de administración.

Los agentes de ServerWORKS Manager que se ejecutan en sistemas DIGITAL proporcionan el canal de comunicación con la consola de administración en una red. Los agentes proporcionan datos de rendimiento y sistema en tiempo real además de información sobre las alarmas.

ServerWORKS utiliza Desktop Management Interface (DMI) para su comunicación con sistemas móviles y de escritorio. Los agentes DIM de DIGITAL proporcionan datos de configuración sobre sistemas móviles o de escritorio DIGITAL.

ServerWORKS Manager utiliza IP Discovery, un proceso que primero encuentra objetos de red y luego devuelve información sobre los objetos a una estación de administración, la consola. ServerWORKS Manager Console es una estación de administración que se basa en Windows de la que puede acceder a toda la red y ver la configuración actual de la red en su vista lógica o real en una lista jerárquica o un mapa gráfico.

Los objetos que descubre ServerWORKS

ServerWORKS descubre:

- Servidores, incluyendo todos los servidores DIGITAL y que no sean DIGITAL cuyos MIBs se compilan en ServerWORKS. Por ejemplo, los MIBs de servidores Compaq ya están compilados en ServerWORKS.

Introducción

- Clústers, incluyendo clústers de NT de DIGITAL y NT de Microsoft. Un icono del clúster aparece en el visor de mapas o jerárquico. El despliegue del icono revela los servidores y los recursos en el clúster.
- Componentes de red, como encaminadores, puentes, hubs y concentradores.
- Nodos que no sean de servidor, como sistemas de escritorio, impresoras, controladores RAID y fuentes de alimentación no interrumpibles (UPS).

Integración con herramientas de administración a nivel de empresa

Como ServerWORKS Manager utiliza SNMP, ServerWORKS se integra con productos de administración de redes de empresa estándar de la industria, por lo que puede supervisar y administrar de manera eficaz servidores DIGITAL desde un administrador de empresas. Por otra parte, puede compilar MIBs que no sean DIGITAL en ServerWORKS Manager, lo que le permite supervisar servidores y objetos de red de otros proveedores desde ServerWORKS Manager Console.

Los agentes de servidores DIGITAL utilizan la pila de protocolos SNMP nativos y el agente SNMP extensible del sistema operativo. Puede configurar los agentes SNMP de servidores DIGITAL para enviar capturas (traps) a un sistema de administración de redes como ServerWORKS Manager Console. Entonces ServerWORKS puede enviar capturas a un administrador de empresas.

ServerWORKS se integra con:

- Insight Manager de Compaq
- OpenView de Hewlett-Packard
- Tivoli TME 10 NetView
- Computer Associates Unicenter TNG
- NetWare ManageWise

Introducción

Puede encontrar detalles completos para integrar MIBs de DIGITAL en administradores de empresas en el manual *DIGITAL ServerWORKS Manager Integration Guide*.

Minimal Health

ServerWORKS Minimal Health establece un sistema de alerta temprana en el momento de la instalación con parámetros predeterminados para la plataforma y los componentes. Los agentes de ServerWORKS proporcionan una configuración sofisticada de las alarmas para componentes de hardware comunes como los ventiladores y discos de servidores DIGITAL. El agente Minimal Health define alarmas para condiciones ambientales—fuentes de alimentación, tensión, ventiladores y temperatura— y, para el estado de los procesadores, discos y componentes de memoria.

Supervisión inteligente

Los agentes ServerWORKS recopilan información sobre servidores y componentes de manera inteligente. En vez de depender de la realización de encuestas constante desde la consola de administración, los agentes ServerWORKS que están instalados en sistemas administrados se interrogan entre sí y notifican a la consola cuando una unidad alcanza un umbral de alarma, ahorrando un ancho de banda de red considerable.

Uso detallado de componentes

ServerWORKS reúne estadísticas vitales actuales como el nombre y la dirección IP de un dispositivo, que ServerWORKS muestra en un mapa de IP Discovery en la vista jerárquica de ServerWORKS Explorer. ServerWORKS también recopila información sobre dispositivos de red, como estadísticas de adaptadores de red, almacenamiento en el disco y uso de la CPU, que puede ver desde System Browser.

Puede definir alarmas en objetos de red. Cuando el valor de un parámetro de la alarma excede el umbral que ha definido, se le notifica. Entonces puede hacer los ajustes antes de que los problemas pequeños se conviertan en mayores.

Puede registrar la actividad en tiempo real utilizando gráficas, ver los datos en una gráfica dinámica y acumular los datos para el análisis posterior. Los datos históricos analizados le pueden ayudar a solucionar problemas. Si sospecha de un problema en un componente, puede ejecutar la gráfica durante varias horas o días y volver a llamar los datos cuando esté listo para analizarlos.

Opciones de notificación

ServerWORKS le permite definir la acción precisa que se debe tomar cuando la consola recibe una captura o alarma. Puede enviar el correo electrónico, comunicarse con un administrador con un Pager numérico o alfanumérico o lanzar una aplicación que inicie una solución al problema del dispositivo con alarmas.

Administración de NT y NetWare

ServerWORKS supervisa y administra Windows NT desde la consola, eliminando la necesidad de utilizar herramientas de administración de NT múltiples. ServerWORKS descubre automáticamente los dominios NT y le permite visualizar el contenido y las propiedades de los objetos en el explorador como parte de una colección o vista personalizada.

En el Visor de mapas, puede arrastrar y soltar objetos entre dominios o servidores y realizar operaciones en grupo de manera sencilla. Por ejemplo, puede seleccionar varios grupos y modificar sus privilegios o administrar colas de impresora.

Si ejecuta servidores Novell NetWare en la red, puede ver los servidores NetWare de la red utilizando ServerWORKS Explorer. También puede administrar esos servidores, usando las utilidades de NetWare cuyos iconos aparecen en la Barra de herramientas de ServerWORKS.

Cuando selecciona un servidor NetWare, los iconos para las utilidades NetWare siguientes se muestran en la Barra de herramientas de ServerWORKS Manager: Filer, Pconsole, Printcon, Rconsole, Syscon, Userdef y NWAdmin. Si se hace clic en el botón, se inicia la utilidad.

Integración de aplicaciones DIGITAL y de terceros

ServerWORKS integra las aplicaciones de terceros por lo que puede administrar los dispositivos en los que están instalados sus agentes. La integración con ServerWORKS realiza las tareas siguientes:

- Activa ServerWORKS Manager para asociar la aplicación con objetos en los que están instalados agentes de terceros
- Agrega una opción de menú en el menú Console que lanza la aplicación de terceros desde el menú Console
- Agrega un icono a la Barra de herramientas de Console que lanza la aplicación
- Agrega un icono a la Barra de herramientas cuando un objeto de terceros se descubre en una vista.

Puede integrar las aplicaciones siguientes:

ClientWORKS — ClientWORKS es la herramienta de administración de sistemas de escritorio DIGITAL que se basa en DMI (Desktop Management Interface: Interfaz de administración de escritorios). ClientWORKS encuentra PCs que soportan DMI y recupera información de manera tanto local, como remota. ClientWORKS también crea instantáneas del sistema (archivos MIF) para utilizarlas con SMS (Microsoft Systems Management Server: Servidor de administración de sistemas Microsoft).

StorageWORKS Command Console — Supervisa, administra y soluciona los problemas de subsistemas de gran almacenamiento conectados a un controlador StorageWORKS RAID de DIGITAL.

Remote Server Manager (RSM) — Proporciona administración por módem para servidores DIGITAL con RSM instalado.

Remote Management Console (RMC) — Supervisa y administra sistemas Alpha configurados con la funcionalidad de RMC o el hardware opcional KRCM.

Global Array Manager — Supervisa y administra los subsistemas de cargadores de discos conectados a un controlador MYLEX RAID.

Introducción

APC PowerNet — PowerNet es el administrador de dispositivos para fuentes de alimentación no interrumpibles (UPS) de American Power Conversion. PowerNet proporciona información sobre dispositivos APC UPS. La integración con ServerWORKS coloca un icono en la Barra de herramientas y un comando de menú para lanzar PowerNet desde la consola.

Exide OnliNet® — OnliNet es software de administración de alimentación para fuentes de alimentación no interrumpibles por parte de Exide Electronics Corporation. Los dispositivos UPS Exide están disponibles de sistemas Alpha de DIGITAL. OnliNet para ServerWORKS le permite iniciar OnliNet desde la Barra de herramientas de ServerWORKS.

Introducción

Uso de SNMP con ServerWORKS Manager **2**

ServerWORKS Manager utiliza SNMP, agentes SNMP, y MIBs para supervisar y administrar una red. Si ya se conoce un poco SNMP es útil antes de comenzar a utilizar ServerWORKS Manager.

Este capítulo describe Simple Network Management Protocol (SNMP V1.0) que ServerWORKS Manager utiliza y explica cómo SNMP trabaja con agentes de DIGITAL para ampliar la información que necesita para realizar una administración profética.

Acerca de SNMP

SNMP es un protocolo de capa de aplicación para intercambiar información sobre administración entre dispositivos de red. SNMP es el protocolo que se utiliza con mayor frecuencia para administrar diversas redes que ejecutan una variedad de sistemas operativos. ServerWORKS Manager utiliza el protocolo SNMP V1.0 como medio de comunicación principal con servidores.

Componentes del sistema SNMP

SNMP recupera datos de una o más *Management Information Bases* (*Bases de información sobre administración*) (MIBs) que describen los objetos que se pueden administrar en un host determinado. Además de los MIBs suministrados por el sistema, otros proveedores pueden definir MIBs adicionales que permiten supervisar y administrar desde la consola de administración de SNMP los dispositivos desarrollados por otros proveedores. ServerWORKS Manager compila los MIBs de recursos de host (RFC1514), MIBs de DIGITAL y el MIBs de numerosos vendedores en su base de datos para proporcionar una recopilación de información sobre objetos de red.

ServerWORKS Manager implementa MIBs basados en SNMP y un componente de agente de extensión SNMP que permite:

- Controlar de manera remota sistemas a través de las operaciones de SNMP
- Definir capturas y alarmas de agentes SNMP utilizando agentes de ServerWORKS en los objetos que se están administrando
- Encuestar variables de SNMP para crear alarmas de umbral basadas en la consola

MIBs

MIB incluye la información siguiente sobre cada objeto que describe:

- Un identificador de objeto, conocido como OID, que identifica de manera única el objeto administrado en la red

Uso de SNMP con ServerWORKS Manager

- Una definición del tipo de datos utilizados para definir el objeto
- Una descripción textual del objeto
- Un método de índice utilizado para objetos que tienen un tipo de datos complejo
- El acceso en lectura o escritura que se permite en el objeto

MIBs se han definido para hosts y encaminadores de TCP/IP, tipos de interfaz como Token Ring y FDDI y, dispositivos como servidores y puentes.

Programas de administradores de redes

Un *administrador* es un programa que solicita datos desde otras computadoras de la red. Una *consola de administración de SNMP* es cualquier computadora que ejecuta el software de administración de SNMP. Cuando un administrador desde la consola de administración solicita información sobre un objeto administrado, el programa de administración de SNMP pide información sobre el objeto utilizando su identificador de objeto.

Agentes

El *agente* es el programa que recibe las peticiones de administración y luego envía dicha información al programa de administración de SNMP que inició la petición.

Los objetos de red que son supervisados deben tener un agente que resida en ellos o que interactúe con ellos. El agente realiza cuatro operaciones:

GET y **GET NEXT**— Recuperan información sobre el objeto administrado y la devuelven a la consola de administración.

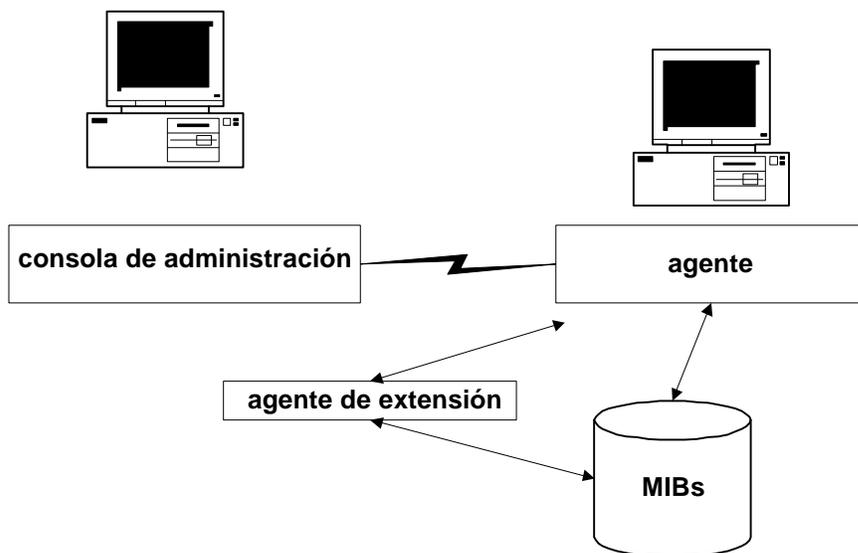
SET — Cambia el valor de una variable del objeto administrado. Sólo es posible definir las variables cuyas definiciones de objeto permiten el acceso en lectura/escritura.

TRAP — Envía mensajes a la consola de administración de SNMP cuando ocurre un cambio o error en un objeto administrado. La operación trap (captura) es la única iniciada por el agente sin necesidad de una petición específica desde un programa de administración.

Uso de SNMP con ServerWORKS Manager

Un agente de extensión es el software que extiende la funcionalidad del agente principal de SNMP del sistema. Cuando el agente recibe una petición de información sobre uno de los objetos manejados por un agente de extensión, pasa la petición al agente de extensión para procesarlo. El agente de extensión devuelve la información al agente SNMP, que a su vez la devuelve a la consola de administración que solicitó la información, como se muestra en la Figura 2-1.

Figura 2-1 Agentes de extensión en SNMP



Agente de extensión SNMP de DIGITAL

La mayoría de los sistemas operativos proporcionan subsistemas de agente SNMP que le permiten construir módulos de extensión para hardware y software específicos. El agente de servidor de DIGITAL utiliza la pila de protocolos SNMP nativos del sistema operativo y los mecanismos de distribución para devolver información sobre el hardware y software DIGITAL y, para exportar capturas (traps) a otros sistemas.

Uso de SNMP con ServerWORKS Manager

Un agente SNMP se puede configurar para que envíe sus capturas (traps) directamente a cualquier consola de administración de SNMP, como ServerWORKS Manager Console o, a sistemas de administración de redes de empresa, como HP OpenView o Tivoli TME10, que utilizan SNMP como mecanismo de capturas (traps) y alarmas.

Cómo la consola utiliza SNMP para comunicarse

ServerWORKS Manager Console funciona como una consola de administración sin el servicio SNMP Trap. Como utiliza su propia pila SNMP para decodificar capturas de SNMP, no requiere que SNMP esté instalado en el sistema de la consola.

Sin embargo, los sistemas que deben ser vistos por la consola de administración *deben* tener agentes SNMP instalados y configurados. Si la consola de administración se utilizará para ver el sistema en el que está instalada, entonces también se deberá instalar y configurar SNMP en la consola de administración.

ServerWORKS Manager Console depende de los componentes SNMP del sistema operativo para proporcionar el número de puerto de IP de la captura de SNMP (por lo general 162). Esta entrada se puede encontrar en el archivo de servicios. En un sistema Windows NT, este archivo por lo general se encuentra en `c:\winnt\system32\drivers\etc\services`. En un sistema UNIX, este archivo está en `\etc\services`.



Nota: ServerWORKS Manager tratará de utilizar el puerto de captura (trap) si todavía no se está utilizando. Event Dispatcher de ServerWORKS Manager recibe capturas del puerto de capturas de SNMP. Para ejecutar un administrador de empresas en el mismo sistema que ServerWORKS Manager, debe cerrar el proceso Event Dispatcher.

Es posible que se haya suprimido la entrada `snmp-trap` en algunos sistemas Windows 95 y Windows NT. Asegúrese de que la línea siguiente esté en el archivo de servicios:

```
snmp-trap 162/udp snmp
```

Si se cambia esta entrada, se dice a EventDispatcher que utilice otro

Uso de SNMP con ServerWORKS Manager

número de puerto para escuchar las capturas.

Configuración de SNMP para el reenvío de capturas

SNMP es un protocolo sin conexiones, lo que significa que no hay mecanismo en SNMP para solicitar y confirmar una sesión formal de la conexión. Si el sistema de agente y el sistema de consola de administración no están de acuerdo con el número de puerto de capturas y otros detalles sobre la comunicación, no pasará ningún mensaje entre ambos sistemas. No se detectará ningún error y no se generará ningún mensaje de excepción.

Un sistema que ejecuta sistemas operativos Windows no tiene instalado el servicio SNMP instalado de forma predeterminada. Debe agregar el servicio SNMP explícitamente desde el Panel de control y, luego, configurar el agente SNMP con la seguridad y el acceso correctos. No recibirá capturas en la consola de destino si no configura correctamente los servicios de SNMP.

Encontrará la configuración de SNMP en el Panel de control, bajo el icono Red. Necesita configurar el servicio de SNMP y especificar un destino de captura en el servidor administrado. Consulte la sección "*Configuración de SNMP y destinos de captura*" en el Capítulo 7 para obtener instrucciones sobre la configuración de SNMP para Windows NT y Windows 95. Los procedimientos son diferentes en las dos versiones, pero ambos requieren la misma información:

- El nombre o nombres de comunidad que se utilizarán
- El nombre de red o la dirección IP de cada consola de administración de SNMP que será el destino de los mensajes de captura generados dentro de una comunidad específica

Las secciones siguientes explican estos temas con más detalles.

Configuración de la seguridad de SNMP

El servicio de seguridad SNMP utiliza *nombres de comunidad* para autenticar mensajes. Todos los mensajes de SNMP deben contener un nombre de comunidad. El agente SNMP que recibe el mensaje verifica el nombre de comunidad en relación con la lista de nombres con los cuales el servicio de SNMP está configurado. Si el mensaje contiene un nombre de comunidad conocido, se procesa el mensaje. Si ningún nombre de comunidad corresponde al del mensaje, éste se rechaza. El cuadro de verificación "Enviar captura de autenticación" de la ventana de configuración determina si el servicio SNMP debe o no enviar un mensaje de captura al servidor solicitante cuando se produce una falla de autenticación.

El nombre de comunidad predeterminado cuando el servicio SNMP está instalado en una computadora que utiliza Windows NT es Public. Puede agregar o eliminar los nombres de comunidad como sea necesario.



Nota: Si suprime todos los nombres de comunidad, incluyendo el nombre predeterminado, el servicio de SNMP en dicha computadora autenticará y procesará los mensajes de SNMP que contengan cualquier nombre de comunidad.

No hay relación entre los nombres de comunidad y los nombres de dominio o grupo de trabajo. Los nombres de comunidad son una contraseña compartida para los grupos de hosts y los debe seleccionar y cambiar de la misma manera en que procede con cualquier otra contraseña.

Sólo los agentes y programas de administración que están configurados con el mismo nombre de comunidad pueden comunicarse entre sí. Si el agente no reconoce el nombre de comunidad contenido en los mensajes de SNMP procedentes de la consola de administración, no recibirá capturas del agente.

Configuración de SNMP Traps

El agente SNMP genera mensajes de capturas, que se envían a una consola de administración de SNMP llamada *destino de capturas*. Si desea que un sistema envíe capturas de SNMP a una consola de administración, debe asegurarse de que ambos sistemas estén configurados correctamente:

- El nombre de comunidad de la consola de administración debe ser el mismo que el nombre definido en el sistema de agente.
- El sistema de agente debe especificar el sistema de consola de administración como un destino de captura.

Si configura una alarma sin haber configurado los servicios de SNMP, se le pide que configure SNMP y un destino de captura de SNMP en el sistema administrado antes de continuar.

Cuando se produce una condición de captura de agente en el sistema que envía, el agente envía el mensaje de SNMP Trap apropiado hacia el sistema de consola de administración. Si no se configuran ambos sistemas correctamente, no pasa ninguna captura.

Las capturas por lo general notifican a la consola de administración sobre sucesos tales como el inicio o la parada de un servicio, la existencia de una condición de error grave u otro suceso que sea importante para el agente. El agente SNMP o agente de extensión y su MIB asociado definen qué condiciones provocan la generación de un mensaje de captura, pero el usuario controla dónde se envía el mensaje.

El destino de la captura debe ser un host que esté ejecutando un programa de administrador de SNMP, como ServerWORKS Manager o un administrador de empresas.

Aunque puede identificar el destino de captura por su nombre único, la utilización de la dirección IP numérica es más eficiente. No se recomienda DHCP (Dynamic Host Configuration Protocol: Protocolo de configuración de hosts dinámicos) debido a la incertidumbre de la traducción de la dirección de DHCP. No utilice una dirección de subred para el destino de la captura.

Uso de SNMP con ServerWORKS Manager

Instalación 3

ServerWORKS Manager facilita la administración de redes, un proceso complejo con los requisitos de configuración de la red, el software y el hardware. Este capítulo describe el entorno que necesita para hacer funcionar ServerWORKS Manager, incluyendo

- Requisitos de configuración de la red
- La lista de plataformas soportadas para agentes SNMP y DMI del sistema operativo que vienen con ServerWORKS Manager
- Los requisitos de hardware y software para ejecutar ServerWORKS Manager Console
- Los requisitos de hardware y software para ejecutar agentes en dispositivos administrados
- Los requisitos para la administración de clústers
- Instrucciones para la instalación

Requisitos de configuración de la red

Cada dispositivo de la red tiene una dirección Media Access Control (MAC) y una dirección IP numérica única. ServerWORKS Manager utiliza la dirección IP para encontrar objetos en la red. SNMP utiliza la dirección MAC para comunicar información sobre el objeto de red.

Para resolver los conflictos entre nombres y dirección, instale un servidor Domain Name Service (DNS). DNS enlaza un nombre a una dirección. Como una consola que se desplaza tiene una dirección IP asignada dinámicamente y no puede mantener un destino de captura fácilmente, se recomienda que no utilice DHCP para la consola.

Para que objetos de red se comuniquen con ServerWORKS Manager Console utilizando SNMP:

- Instale un agente de SNMP en cada servidor administrado
- Asegúrese de que el servicio de SNMP esté instalado y ejecutándose en todos los objetos de red que se van a supervisar
- Especifique la dirección IP de la consola de administración como el destino de captura cuando configure SNMP en el dispositivo administrado

Como administrador de una red NT, necesita dos tipos de privilegios de administrador:

- Privilegios de administrador en el dominio
- Relaciones de confianza que permiten la administración de dominios en otros dominios que se desean administrar desde la consola

Familiarícese con el sistema operativo NT. NT impone restricciones poco conocidas en cuentas de usuario. Típicamente el administrador tiene todas las capacidades administrativas, pero a los que están designados como operadores de cuenta se les deben asignar derechos de manera explícita para realizar tareas en cuentas de usuario. Entre los derechos de usuario que se asignan explícitamente están los derechos de acceder a un sistema local desde la red, hacer copias de seguridad de archivos y directorios, acceder de manera local a un sistema, cerrar el sistema y tomar posesión de archivos u otros objetos.

Finalmente, entienda los fundamentos y protocolos de red. Para aprender más sobre esto, consulte la bibliografía en el Apéndice C.

Plataformas soportadas de SNMP

La tabla siguiente lista los agentes SNMP y DMI que se proporcionan con ServerWORKS Manager o como parte del sistema operativo.

Tabla 3-1 Agentes SNMP y DMI

Versión mínima soportada del sistema operativo	Agente SNMP para recursos de host	Agente SNMP de servidores DIGITAL con procesador X86	Agente SNMP de servidores DIGITAL con procesador Alpha	Agente de DMI de DIGITAL
NetWare® V3.12, V4.11 (sólo servidores DIGITAL con procesador X86)	Sí	Sí	N/D	N/D
Estación de trabajo y servidor Windows NT ® V4.0 (para todos los servidores DIGITAL)	Sí	Sí	Sí	Sí
Windows 95 ¹ (sólo servidores DIGITAL con procesador X86)	Sí	N/D	N/D	Sí
SCO® UNIX Open Server V5.x	Sí	Sí	N/D	N/D
DIGITAL UNIX V4.0	Sí	N/D	Si	N/D

¹ Proporcionado con ClientWORKS en computadoras portátiles DIGITAL.

Instalación

DIGITAL OpenVMS 6.2 ² o superior (sólo servidores con procesador Alpha)	Sí	N/D	Futuro	N/D
OS/2 Warp 3.0 proporcionado con el sistema operativo ³ (sólo servidores DIGITAL con procesador X86)	Sí	N/D	N/D	N/D

Hardware de la consola de administración

Necesita el hardware siguiente para ejecutar ServerWORKS Manager.

Tabla 3-2 Requisitos de hardware mínimos para ServerWORKS Manager Console

Componente	Requisitos mínimos
Procesador	Pentium 133 MHz
Dispositivos de almacenamiento	Unidad de disco duro de 1 GB Unidad de CD-ROM Unidad de disquete de 3,5"
Tarjeta de interfaz de red	Adaptador de red con soporte de TCP/IP instalado
Monitor	SVGA 800 x 600 (resolución 1024x768 que se recomienda en un monitor de 18")
Memoria	32 MB

² Disponible con DIGITAL TCP/IP Services for Open VMS V4.2 (antes se conocía como UCX).

³ Proporcionado como parte del sistema operativo OS/2.

Software de la consola de administración

Necesita el software siguiente para ejecutar ServerWORKS Manager Console.

Tabla 3-3 Requisitos de software mínimos para ServerWORKS Manager Console

Componente	Requisitos mínimos
Sistema operativo	Uno de los sistemas operativos siguientes en procesadores X86 <ul style="list-style-type: none"> • Windows NT V4.0 • Windows 95
Protocolo de administración	El servicio de SNMP proporcionado con el sistema operativo (ServerWORKS Manager requiere el servicio de SNMP sólo si un agente SNMP del sistema DIGITAL se está instalando en el sistema de consola de administración).
Protocolos de transporte y de red	Uno de los siguientes: <ul style="list-style-type: none"> • El servicio de TCP/IP proporcionado con el sistema operativo • El servicio de IPX proporcionado por Novell

Instalación

Hardware de agente

Necesita el hardware mínimo siguiente para soportar agentes de ServerWORKS. Algunas opciones del área de parámetros del sistema (por ejemplo información sobre FRU o números asignados), dependen del hardware.

Tabla 3-4 Requisitos de hardware mínimos para agentes

Componente	Requisitos mínimos
Servidores DIGITAL con procesadores X86	Servidores LX, MX, XL, HX y ZX Familia de servidores DIGITAL 500, 1000, 3000, 5000, 7000 y 9000
Sistemas Alpha	AlphaServer 300, 400, 800, 1000, 1000A, 1200, 2000, 2100, 2100A, 4000, 4100, 8200 y 8400 Servidor DIGITAL 3000, 5000, 7000 (Windows NT)
Computadoras de escritorio	Venturis FX, Venturis GL-6xxx, Venturis 486, Venturis 486 LP, Venturis Pentium, Venturis Pentium LP, Celebris XL 6xxx, DIGITAL PC 5500 y DIGITAL PC 5400
Notebooks	HiNote Ultra 2000
Tarjeta de interfaz de red	Servidores DIGITAL con procesador X86 — Adaptador TCP/IP (Ethernet, Token Ring o RAS) NetBEUI Sistemas Alpha - Todos los adaptadores de red TCP/IP

Software de agentes

Necesita el software siguiente para ejecutar agentes de ServerWORKS Manager.

Tabla 3-5 Requisitos de software para agentes

Componente	Requisitos
Sistema operativo de red	
Para servidores DIGITAL con procesadores X86	Un sistema operativo: <ul style="list-style-type: none"> • Novell NetWare V3.12 o V4.11 • SCO OpenServer V5.02, V5.04 (no en clústers) • Windows NT V4.0 • OS/2 V3.0
Para sistemas Alpha	Un sistema operativo: <ul style="list-style-type: none"> • DIGITAL UNIX V4.0 • OpenVMS 6.2 o superior • Windows NT V4.0 para Alpha (sólo agentes)
Protocolos de red	SNMP TCP/IP o IPX (sólo para servidores NetWare)

Instalación

Soporte de clúster de red

Necesita los elementos siguientes configurados en miembros de clúster para administrar clústers.

Tabla 3-6 Requisitos para el soporte de clústers de red

Tipo de clúster	Requisitos
DIGITAL Clusters V1.1	Windows NT Enterprise, V4.0 con Service Pack 3 ejecutándose en servidores DIGITAL Agente Common Cluster MIB Agente Cluster Extension MIB
Clústers de Microsoft NT	Windows NT Enterprise, V4.0 con Service Pack 3 ejecutándose en servidores DIGITAL Agente Common Cluster MIB Agente Cluster Extension MIB Microsoft Cluster Server (MSCS)

Consideraciones previas a la instalación para ServerWORKS

Lea las secciones siguientes para obtener información sobre los antecedentes de los componentes de ServerWORKS Manager antes de instalarlo.

Orden de instalación

Puede instalar el software siguiente del CD-ROM de ServerWORKS. Instálelos en el orden en que aparecen:

- Agentes
- ServerWORKS Manager Console
- ServerWORKS Console Integration

Instalación

- ClientWORKS
- Remote Server Manager (RSM)
- Remote Management Console (RMC)
- StorageWorks Command Console (SWCC)

Siempre desinstale las versiones anteriores de ServerWORKS, ClientWORKS o ManageWORKS antes de instalar ServerWORKS V4.0. Consulte el Apéndice B, “*Solución de problemas*” para obtener detalles.

DIGITAL recomienda que instale los componentes en los directorios predeterminados como se sugiere en la instalación. Evite ejecutar dos versiones en directorios diferentes.

Elija un idioma para instalar y desinstalar. Sólo una copia del programa de desinstalación se conserva en el directorio de Windows. Por lo tanto, siempre está en el idioma seleccionado durante la última instalación en ese sistema.

Asegúrese de tener privilegios de administrador local y de dominio si está instalando y configurando ServerWORKS con Windows NT. Recuerde que las reglas y restricciones de administración de Windows NT para grupos y usuarios se siguen aplicando cuando trabaja desde el Administrador de servidores de NT de ServerWORKS Manager.

Necesita 100 MB de espacio temporal en el disco para instalarlo. La instalación utiliza el directorio definido por la variable TEMP o, si TEMP no está definida, el directorio Windows. Para la variable de entorno ‘TEMP,’ especifique un directorio con un mínimo de 100 MB de almacenamiento para guardar los archivos temporales utilizados durante la instalación. Además, especifique un directorio TEMP que no esté en la RUTA. De otra manera, pueden ocurrir resultados impredecibles. En Windows NT, utilice en el Panel de Control, Propiedades del sistema→Entorno para modificar la variable TEMP.

Instalación

Instalaciones incompletas

Si interrumpe una instalación antes de que se complete, cierre el programa de instalación por completo y vuelva a empezar. Para mejores resultados, utilice Panel de control→Agregar o quitar programas para suprimir cualquier archivo de la instalación incompleta antes de hacer otra instalación. El programa de desinstalación sólo suprime archivos que se cambiaron la última vez que se estaba ejecutando una instalación. No se suprimen los archivos cambiados de instalaciones previas.

Los archivos de sistema copiados en el directorio Windows del sistema no se eliminan cuando se desinstala ServerWORKS Manager Console. Se conservan para evitar un problema con el programa de desinstalación InstallShield, que suprime los archivos de sistema Windows que ya no son utilizados por otro programa que se esté ejecutando sin pedir confirmación. Si el programa de desinstalación de ServerWORKS eliminara los archivos de sistema, se suprimirían algunos DLLs requeridos, causando problemas posteriormente cuando se inicien otros programas.

Cerrar otros programas antes de la instalación

Cierre todos los programas que se estén ejecutando, incluyendo programas de correo y la barra de acceso directo de Microsoft Office.

Si está actualizando ServerWORKS, cierre todos los procesos de segundo plano de ServerWORKS Manager (Event Logger, Event Dispatcher, Poller, Ping Server, Data Collector) antes de instalar o integrar cualquier aplicación de terceros.

Para instalar ServerWORKS Manager en un sistema que tenga Tivoli TME 10 NetView instalado, primero cierre los demonios de NetView. Los demonios se siguen ejecutando en el segundo plano después de que sale de NetView. Para parar los demonios, seleccione la opción del menú Server Management (Administración de servidores) del grupo de programas NetView. Luego seleccione Stop Server (Parar servidor) para parar los demonios.

Conservar una base de datos de ServerWORKS anterior

El programa de instalación verifica si una versión de ServerWORKS Manager Console ya existe en el sistema. Si es así, puede tener las opciones siguientes:

Conservar la base de datos — Fusiona una base de datos V3.2 o superior en una nueva base de datos de Microsoft Access, conservando toda la información de la versión anterior, incluyendo archivos de datos históricos.

Suprimir la versión anterior — Elimina bases de datos creadas de ServerWORKS V3.0 o inferior.

Puede actualizarse una base de datos Versión 3.0 si primero instala la Versión 3.2. Luego instale la Versión 4.0.

Manipulación de la base de datos

Si crea sus propios informes de Access, actualice Microsoft Access 95 o inferior a Access 97 antes de que se instale ServerWORKS Manager Console.

Integración de ServerWORKS con administradores de empresas

La integración de ServerWORKS Console fusiona agentes de ServerWORKS en administradores de empresas. Los agentes de DIGITAL pueden proporcionar detalles precisos a los administradores de empresas acerca de servidores DIGITAL. Antes de integrar ServerWORKS Manager, el administrador de empresa se debe instalar correctamente.

Utilización de ManageWORKS

ServerWORKS Manager Console y OpenVMS Management Station se pueden instalar y ejecutar *por separado* en el mismo sistema. Siga utilizando ManageWORKS como interfaz para OpenVMS Management Station.

Instalación

Agentes y servicio de SNMP

Instale SNMP en los sistemas administrados y configure un destino de captura si desea recibir mensajes de captura generados por los agentes SNMP. Consulte la sección “Configuración de destinos de capturas y SNMP” en el Capítulo 7.

Los agentes SNMP se pueden suministrar con el sistema operativo o con la instalación. Instale los agentes SNMP del CD-ROM de ServerWORKS Manager incluso si el sistema operativo viene con agentes SNMP.

Agentes proporcionados con ServerWORKS

Se proporcionan y están instalados agentes para los sistemas siguientes en ServerWORKS Manager:

- Windows NT 4.0 o superior

Se proporcionan agentes para los sistemas operativos siguientes en el CD-ROM de ServerWORKS Manager. Instálelos utilizando las instrucciones que vienen en el kit de instalación de ServerWORKS.

- NetWare V3.12 o V4.11
- SCO UNIX 5.x

Con ServerWORKS Manager, se proporcionan agentes para las opciones siguientes para procesadores X86 que ejecuten Windows NT. Seleccione uno o ambos agentes durante la instalación:

- Agentes de DIGITAL Server Management, incluyendo el agente de Minimal Health de ServerWORKS V4.0 para procesadores X86 que ejecuten NT. Se recomienda esta opción.
- DIGITAL Server Agents para Insight Manager. Estos agentes le permiten ver información sobre servidores DIGITAL que usan utilidades de ServerWORKS Manager desde Compaq Insight Manager.

Agentes proporcionados con un sistema operativo

Se proporcionan y están instalados agentes con los sistemas operativos siguientes:

- DIGITAL UNIX 4.0
- El agente SNMP de OpenVMS para sistemas Alpha se incluye en el producto DIGITAL TCP/IP Services for OpenVMS V4.2 o superior y es un componente de NAS Client/Server Package. El agente de SNMP se instala cuando se instala TCP/IP.
- Se incluyen agentes SNMP de IBM OS/2 con el sistema operativo. Consulte la documentación de OS/2 para obtener detalles.

Consulte la documentación del sistema operativo y el Apéndice A “*Procedimientos e información adicionales*” para obtener más información sobre la instalación de agentes SNMP en estos sistemas operativos.

Instalación de un agente en el dispositivo de consola

Si está instalando el software ServerWORKS Manager Console en un servidor con procesador X86 que este ejecutando NT 4.0 en el que también desea instalar un agente para supervisión local, primero instale el software del agente, luego instale ServerWORKS Manager Console.

Consideraciones previas a la instalación para ClientWORKS

Para obtener más información sobre ClientWORKS, consulte “*Using the ClientWORKS® Management Suite with DIGITAL PCs: A Guide for Network Administrators*” y el archivo README.TXT de ClientWORKS V3.0.

Instalación

Consideraciones previas a la instalación para RSM

RSM consta de componentes de hardware y software. Están instalados en servidores DIGITAL con procesador X86 que ejecutan Windows NT o nodos que ejecutan Windows 95. Para integrar RSM con ServerWORKS Manager Console, el software RSM debe estar instalado en el mismo sistema que el software ServerWORKS Manager Console.

El software RSM debe estar instalado en un servidor DIGITAL con procesador X86 en su directorio predeterminado:

```
<unidad windows>:\rs_mgr
```

Se proporciona un procedimiento de integración separado para integrar SRM en ServerWORKS Manager Console. La integración es automática si RSM se instaló en su directorio predeterminado. Si RSM se instaló en otro sitio, la herramienta de integración de RSM pedirá el directorio de destino donde estaba instalado RSM.

Consideraciones previas a la instalación para RMC

Esta sección describe cómo acceder a Remote Management Console (RMC) en un sistema con procesador Alpha. Después de configurar RCM, puede iniciarlo desde ServerWORKS Manager.

RMC es una funcionalidad de hardware/firmware de servidores con procesador Alpha. RMC le permite controlar y supervisar un sistema AlphaServer desde una ubicación remota. Los comandos de RMC se utilizan para reinicializar, parar y encender o apagar el sistema supervisado.

La lógica de control para RMC es parte del hardware del sistema en sistemas AlphaServer 800, 1200, 4000 y 4100. En la documentación del usuario de estos sistemas consulte las instrucciones sobre la configuración y utilización de RMC. Los sistemas AlphaServer 1000 y 1000A proporcionan funcionalidades de RMC mediante una opción de hardware, KCRCM AlphaServer Remote Console Module, que se puede pedir por separado. El módulo KCRCM está conectado a una ranura EISA/ISA en el sistema AlphaServer 1000 o 1000A. Consulte la documentación proporcionada con el módulo para obtener instrucciones sobre la instalación y configuración.

Instalación

Para llamar RMC desde ServerWORKS, instale HyperTerminal (HYPERTRM.EXE) en Windows NT V4.0 y Windows 95. Para integrar RMC en ServerWORKS Manager Console, HyperTerminal debe estar instalado en el directorio predeterminado seleccionado por la instalación del sistema operativo. Instálelo como se indica para Windows 95 y Windows NT.

Llame RMC desde ServerWORKS Manager de la manera siguiente:

1. Si está utilizando HyperTerminal, configúrelo como desee, utilizando los menús que se muestran en la pantalla. Si está utilizando otro programa de terminal, instálelo y configúrelo de acuerdo con la documentación.
2. Ejecute IP Discovery para identificar los servidores en la red.
3. Seleccione un objeto de AlphaServer en el mapa de descubrimiento o Explorer.
4. Seleccione la opción del menú RMC del menú Herramientas o haga clic en el icono de integración de RMC de la Barra de herramientas para iniciar el programa de terminal.

El programa de terminal se conecta a través del puerto COM1 a un módem, interruptor de terminal o PBX, dependiendo de cómo lo ha configurado. Si la conexión es por módem, llame al número telefónico configurado para el módem. Desde puerto COM1, introduzca la secuencia de escape para llamar RMC.

Cuando se completa la integración de RMC, el programa de instalación confirma que los enlaces entre RMC y ServerWORKS Manager Console se lograron con éxito.

Primeros pasos para instalar todos los componentes

La instalación de cada componente empieza desde la pantalla principal después de que selecciona un idioma de instalación. Los pasos siguientes abren la pantalla principal.

1. Inserte el CD-ROM en la unidad de CD-ROM. Por ejemplo, insértelo en la unidad de CD-ROM de un sistema administrado si va a instalar agentes. (No puede instalar desde una unidad de red).

Instalación

2. En sistemas Windows NT o Windows 95, tan pronto como se coloca el CD-ROM, aparece la pantalla principal. Si no se inicia automáticamente, haga lo siguiente:
 - Desde el escritorio, haga clic en el menú Inicio.
 - Elija Ejecutar. Introduzca la ruta de la manera siguiente y haga clic en Aceptar.

En sistemas Windows: <unidad de CD-ROM>:\Autoplay.exe

En sistemas Alpha: <unidad de CD-ROM>:\Alpha\Autoplay.exe-{-
3. Elija el idioma preferido. El idioma seleccionado es el idioma predeterminado la próxima vez que instale o desinstale cualquier componente del CD-ROM. Se abre la pantalla principal con las opciones siguientes:
 - **Bienvenida.** Muestra información general sobre el producto.
 - **Instalar.** Muestra los componentes que puede instalar.
 - **Tutorial.** Ejecuta el tutorial en línea. Puede instalar el tutorial o visualizarlo en cualquier momento desde el CD-ROM.
 - **Documentación.** Muestra los manuales y otros documentos impresos utilizando Adobe® Acrobat™ Reader que se encuentra en el CD-ROM. (No necesita instalar Adobe Acrobat en el sistema). Puede abrir el manual desde el CD-ROM. La ayuda en línea se instala con las aplicaciones.
 - **Finalizar.** Cierra la instalación y ofrece iniciar ServerWORKS Manager Console (si estaba instalado) o salir.
4. Siga uno de estos pasos:
 - Haga clic en Instalar para abrir la pantalla de componentes. Desde esta pantalla puede elegir otros componentes para instalarlos.
 - Haga clic en cualquiera de las demás opciones y siga las instrucciones para navegar por la opción. Por ejemplo, haga clic en el Tutorial para abrir el tutorial y visualizarlo. Cuando sale del tutorial, se regresa a la pantalla principal donde puede elegir instalar un componente o salir.

Instrucciones para la instalación de componentes

Utilice las instrucciones paso por paso en las secciones siguientes para instalar componentes específicos. Empiece por instalar los agentes de ServerWORKS en todos sistemas que desea administrar. Luego instale ServerWORKS Manager Console en la estación de administración.

Instalación de agentes de ServerWORKS Manager

Instale los agentes antes de instalar cualquier otro componente. Instale los agentes en los sistemas remotos que administrará desde ServerWORKS Manager Console. El programa de instalación proporciona sólo los agentes que son adecuados para el sistema operativo y la plataforma en la que está ejecutando el CD-ROM de ServerWORKS Manager.

1. Abra la pantalla principal siguiendo el procedimiento en "Primeros pasos para instalar todos los componentes".
2. Haga clic en Instalar para abrir la pantalla de componentes.
3. Desde la pantalla de componentes, haga clic en ServerWORKS Manager Agents.
4. Elija una opción:
 - Haga clic en Instalar para instalar los agentes en un sistema que ejecuta Windows NT. Luego continúe con el Paso 5.
 - Haga clic en el botón Leer para aprender más acerca de cómo instalar un agente en otros sistemas operativos. Siga las instrucciones para el sistema operativo y salga de las instrucciones siguiendo las indicaciones.
5. Confirme las indicaciones a medida que aparezcan.
 - Haga clic en Siguiente en la pantalla de licencia.
 - Si el servicio de SNMP se está ejecutando, haga clic en Sí apagarlo.
6. En la pantalla de operación de la configuración de agentes Digital, seleccione una opción: y haga clic en Siguiente.
 - **Install the Server SNMP Agents V4.0** (Instalar Server SNMP

Instalación

Agents V4.0). Elija esta opción para instalar o actualizar. Luego haga clic en Siguiente.

- **Suprimir los agentes SNMP de servidor** Elija esta opción para suprimir los agentes instalados.
7. En la pantalla Select Optional Agent Components (Seleccionar componentes adicionales de agente), seleccione una o ambas opciones y haga clic en Siguiente:
- **Digital Server Management Agent.** Instala el agente de administración de servidores de ServerWORKS V4.0, incluyendo Minimal Health. Este agente reemplaza todas las alarmas que se definieron antes con ServerWORKS V3.x o inferior.
 - **Digital Server Agents for Insight Manager.** Instala los agentes para supervisar y administrar servidores DIGITAL desde Insight Manager.
8. Confirme la indicación para reiniciar el servicio de SNMP ahora o más tarde u otras indicaciones para continuar.

En la pantalla de componente, elija el componente siguiente que se va a instalar. Si no va a instalar otros componentes, haga clic en Cerrar y luego haga clic en Terminar en la pantalla principal.

¿Planea supervisar la consola de administración?

Puede instalar un agente y el software de consola en una consola de administración que ejecute Windows NT 4.0. Utilice las instrucciones anteriores para la instalación de agentes.

Instalación de ServerWORKS Manager Console

El proceso de instalación de ServerWORKS Manager Console consta de los segmentos siguientes, que contienen pasos múltiples:

- Inicio de la instalación, eligiendo la instalación de Windows NT 4.0 o Windows 95
- Instalación de la consola
- Finalización de la instalación

Inicio de la instalación para Windows NT 4.0

1. Abra la pantalla principal siguiendo el procedimiento en "Primeros pasos para instalar todos los componentes".
2. Haga clic en Instalar para abrir la pantalla de componentes.
3. Desde la pantalla de componentes, elija ServerWORKS Manager Console.
4. Elija de las opciones siguientes en la pantalla de instalación intermedia:
 - **Paso 1 Instalar.** Instala los agentes de NT en sistemas que ejecutan Windows NT 4.0. Sátese esta opción a menos de que esté instalando un agente en el sistema de consola.
 - **Paso 2 Leer.** Muestra información sobre Data Access Components de Microsoft. Elija este paso para asegurar que esté utilizando la versión correcta de controladores de Microsoft. Elija Archivo→Salir para volver a la pantalla de instalación intermedia.
 - **Paso 3 Instalar.** Instala el Data Access Pack de Microsoft que se requiere. Para instalarlo:
 - a. Siga las indicaciones para la instalación de MDAC.
 - b. Cuando se indique, elija la instalación Típica. (Para una instalación personalizada, debe elegir Data Sources y MDAC Core Files).
 - c. Reinicie el sistema, como lo recomienda Microsoft.
 - d. Vuelva a la pantalla de instalación intermedia.
5. Elija Paso 4 Instalar para empezar la instalación de ServerWORKS Manager Console.

Continúe la instalación con el procedimiento de la sección "*Instalación de la consola*".

Inicio de la instalación para Windows NT 95

1. Abra la pantalla principal siguiendo el procedimiento en "Primeros pasos para instalar todos los componentes".
2. Haga clic en Instalar para abrir la pantalla de componentes.

Instalación

3. Desde la pantalla de componentes, elija ServerWORKS Manager Console.
4. Elija de las opciones siguientes en la pantalla de instalación intermedia:
 - **Paso 1 Instalar.** Muestra información sobre Data Access Components de Microsoft, incluyendo ODBC. Elija este paso para asegurarse de que esté utilizando ODBC 3.5 o superior. Elija Archivo→Salir para volver a la pantalla de instalación intermedia.
 - **Paso 2 Leer.** Muestra información sobre Data Access Components de Microsoft. Elija este paso para asegurar que está utilizando la versión correcta de controladores de Microsoft. Elija Archivo→Salir para volver a la pantalla de instalación intermedia.
 - **Paso 3 Instalar.** Instala Data Access Pack de Microsoft que se requiere. Para instalarlo:
 - a. Siga las indicaciones para la instalación de MDAC.
 - b. Cuando se indique, elija la instalación Típica. (Para una instalación personalizada, debe elegir Data Sources y MDAC Core Files).
 - c. Reinicie el sistema, como lo recomienda Microsoft.
 - d. Vuelva a la pantalla de instalación intermedia.
5. Elija Paso 4 Instalar para empezar la instalación de ServerWORKS Manager Console.

Continúe la instalación con el procedimiento de la sección “*Instalación de la consola*”.

Instalación de la consola

Puede actualizar desde ServerWORKS Manager Console V3.2 o V3.3. No se soportan las actualizaciones de versiones anteriores.

1. En la pantalla Bienvenida, haga clic en Siguiente para aceptar los términos y las condiciones de la licencia.

Instalación

2. Para una nueva instalación, registre el nombre y la empresa en la pantalla ServerWORKS Manager Console, siga las indicaciones y haga clic en Siguiente.
3. En la pantalla Elija ubicación de destino, haga clic en Siguiente para colocar los archivos en el directorio predeterminado especificado. (En una instalación posterior, es posible que tenga problemas al compartir archivos entre las dos versiones si una versión reside en otro directorio). Si desea cambiar el directorio, utilice el comando Examinar para seleccionar la ubicación y regresar a la pantalla Elija ubicación de destino. Luego haga clic en Siguiente para continuar.
4. Si esta es la primera instalación, sáltese al Paso 5. Si está volviendo a instalar, siga uno o ambos de los pasos siguientes:
 - Seleccione "Usar la base de datos existente". Esta opción conserva la base de datos actual y la fusiona en una nueva base de datos. Si no selecciona esta opción, la base de datos anterior se guarda en:
`\Archivos de programas\Digital\SWMgr\database\old`
 - Seleccione "Quitar ServerWORKS existente". Siga los mensajes que se indican referentes a la desinstalación de versiones anteriores del software.

Luego haga clic en Siguiente.

5. Elija una de las opciones siguientes:
 - **Iniciar automáticamente las tareas de segundo plano.** Las tareas de segundo plano empiezan a ejecutarse inmediatamente después de la instalación. Si la consola está dedicada a ServerWORKS y administración es posible que desee ejecutarlos automáticamente.
 - **Iniciarlas manualmente cada vez.** Las tareas de segundo plano se ejecutan sólo cuando está abierto ServerWORKS.

Luego haga clic en Siguiente y siga las indicaciones para continuar.

Instalación

Finalización de la instalación

1. Elija aceptar o rechazar la opción “Ver ahora README.TXT”. Si selecciona la opción, lea el archivo y salga de éste utilizando Archivo→Salir.
2. Haga clic en Finalizar. Cierre el grupo de programas si es necesario. Siga los mensajes para cerrar los cuadros de diálogo que sigan abiertos. Aparece la pantalla de instalación intermedia.
3. Haga clic en Cerrar.
4. En la pantalla de componentes, haga clic en Cerrar de nuevo para volver a la pantalla principal.
5. En la pantalla principal, haga clic en Finalizar.
6. En la indicación siguiente, seleccione "Iniciar ServerWORKS Manager inmediatamente" o haga clic en Salir.
7. Al salir se regresa a la pantalla de componentes. Si no piensa instalar ningún otro componente, haga clic en Cerrar.
8. En la pantalla principal, haga clic en Finalizar.

Instalación de ServerWORKS Console Integration

La instalación de ServerWORKS comienza el proceso de integración con el administrador de empresas. Las instrucciones varían para administradores de empresas y plataformas diferentes.

1. Abra la pantalla principal siguiendo el procedimiento en "Primeros pasos para instalar todos los componentes".
2. Haga clic en Instalar para abrir la pantalla de componentes.
3. Desde la pantalla de componentes, elija ServerWORKS Manager Integration.
4. Elija de las opciones siguientes en la pantalla de instalación intermedia:
 - HP Open/view/ServerWORKS
 - HP OpenView/HPUX

Instalación

- Tivoli TME 10 NetView for Windows NT/ServerWORKS
 - Tivoli TME 10/NetView for DIGITAL UNIX
 - +CA Uni/Center TNG/ServerWORKS
5. Siga las instrucciones para el administrador de empresas y la plataforma específicos. Cuando la instalación se complete, haga clic en Cerrar para volver a la pantalla de componentes de ServerWORKS.

Instalación de ClientWORKS

Para obtener detalles completos de la actualización de ClientWORKS, consulte el archivo readme.txt de ClientWORKS.

1. Abra la pantalla principal siguiendo el procedimiento en "Primeros pasos para instalar todos los componentes".
2. Haga clic en Instalar para abrir la pantalla de componentes.
3. Haga clic en ClientWORKS Components. Puede instalar dos componentes de ClientWORKS. Ambos son opcionales.
 - De la pantalla de componentes, elija ClientWORKS DMI Explorer para instalar el explorador para el sistema local. Siga las indicaciones para completar la instalación.
 - De la pantalla de componentes elija ClientWORKS DMI Explorer and Agents para instalar los componentes para administrar y examinar la red. Siga las indicaciones para completar la instalación.
4. Continúe con la parte de instalación de ClientWORKS. Siga las indicaciones. Luego haga clic en Siguiente.
5. En la primera pantalla de confirmación de licencia, haga clic en Siguiente. En la segunda pantalla de licencia, haga clic en Sí.
6. En la pantalla de componentes de ClientWORKS, seleccione la(s) opción(es) y luego haga clic en Siguiente.
7. En la pantalla de opción de idioma, elija el mismo idioma que utilizó para instalar ServerWORKS Manager y haga clic en Siguiente para continuar.

Instalación

8. Elija el destino para ClientWORKS y haga clic en Siguiente.
9. Elija el nombre de carpeta predeterminada o introduzca su propio nombre de carpeta. Luego haga clic en Siguiente. Siga las indicaciones referentes al servicio de SNMP.

Instalación de RAID Storage Management

Si no está instalando una aplicación de administración de controladores RAID, ignore las secciones “*Instalación de StorageWorks*” e “*Instalación de MYLEX GAM*”.

Instalación de StorageWorks

StorageWorks Command Console consta de un cliente para la consola de administración y agentes para los servidores administrados. El cliente de StorageWorks Command Console está instalado en un nodo de Windows NT o Windows 95. Los agentes de StorageWorks están instalados en servidores que están conectados a un controlador StorageWorks RAID que ejecuten Windows NT, NetWare o SCO UNIX.

StorageWorks se instala desde el CD-ROM. StorageWorks cliente se puede instalar en un sistema de administración. Los agentes de StorageWorks se pueden instalar en servidores administrados a los que esté conectado un controlador RAID. Si StorageWorks no se puede instalar automáticamente en el sistema, se muestra más información. StorageWorks se debe volver a instalar con la versión proporcionada en el CD-ROM de ServerWORKS Manager (o una versión más reciente).

1. Abra la pantalla principal siguiendo el procedimiento en "*Primeros pasos para instalar todos los componentes*".
2. Haga clic en Instalar para abrir la pantalla de componentes.
3. Desde la pantalla de componentes, haga clic RAID Storage Management.
4. Elija StorageWORKS Command Console.
5. En la pantalla siguiente, haga clic en Agente o Cliente y siga las indicaciones para volver la pantalla principal.

6. En la pantalla principal, elija el componente siguiente para instalarlo. Si no va a instalar ningún otro componente, haga clic en Finalizar.

Instalación de Mylex GAM

Mylex GAM consta de un cliente que está instalado en la consola de administración que ejecuta Windows NT o Windows 95 y agentes que están instalados en servidores que están conectados a controladores Mylex GAM RAID.

GAM se instala desde el CD-ROM. Si GAM no se puede instalar automáticamente en el sistema, aparece información sobre cómo hacerlo. Mylex GAM se debe volver a instalar con la versión proporcionada en el CD-ROM de ServerWORKS Manager o una versión más reciente.

1. Abra la pantalla principal siguiendo el procedimiento en "*Primeros pasos para instalar todos los componentes*".
2. Haga clic en Instalar para abrir la pantalla de componentes.
3. Desde la pantalla de componentes, elija RAID Storage Management.
4. Elija Mylex GAM.
5. En la pantalla siguiente, haga clic en Instalar y siga las indicaciones para volver a la pantalla principal.
6. En la pantalla principal, elija el componente siguiente para instalarlo. Si no va a instalar ningún otro componente, haga clic en Finalizar.

Instalación de Integración de Remote Management

Si no va a instalar Integración de Remote Management, ignore esta sección.

Su selección de administración remota depende del sistema operativo de la consola de administración donde está instalando el componente. Instale el software de RSM antes de instalar la integración de RSM. Consulte la documentación de RSM para obtener detalles.

Instalación

1. Abra la pantalla principal siguiendo el procedimiento en "*Primeros pasos para instalar todos los componentes*".
2. Haga clic en Instalar para abrir la pantalla de componentes.
3. Desde la pantalla de componentes, elija un servicio de administración remota para el sistema.
4. Siga las indicaciones y haga clic en Finalizar cuando la integración se realice de manera satisfactoria.
5. En la pantalla principal, elija el componente siguiente para instalarlo. Si no va a instalar ningún otro componente, haga clic en Finalizar.

Tutorial

El Tutorial de ServerWORKS Manager se instala como parte del software ServerWORKS Manager Console. Este tutorial contiene información básica sobre ServerWORKS Manager. Puede terminar el tutorial en unos 20 minutos. Si es primera vez que lo utiliza, DIGITAL recomienda que utilice el tutorial como introducción.

Documentación

Durante la instalación de ServerWORKS Manager Console, los archivos readme.txt e install.txt se copian en la raíz del directorio de instalación. La ayuda en línea se instala con los productos. Puede ver o imprimir los documentos desde el CD-ROM con Adobe Acrobat.

Opciones posteriores a la instalación

Varias funcionalidades de ServerWORKS se instalan o configuran manualmente después de que se instala ServerWORKS.

WatchDog Timer en plataformas múltiples

WatchDog Timer es una opción que puede instalarse en servidores con procesador X86 después de que se instala ServerWORKS Manager. Watchdog Timer es una utilidad que recupera automáticamente un sistema operativo interrumpido reiniciando el servidor. En la instalación, Watchdog Timer está desactivado por defecto. Por razones de seguridad ServerWORKS V4.0 soporta la activación y desactivación de esta funcionalidad en el sistema de agente desde el indicador de sistema.

En los sistemas operativos NT, NetWare y SCO UNIX, ServerWORKS Manager ofrece soporte de Watchdog Timer para servidores ZX6000, HX6000, MX6000 y XL6000 y DIGITAL Server Series 3000, 5000 y 7000.

Para activar WatchDog Timer:

1. Vaya al indicador de sistema.
2. Introduzca el nombre del programa seguido de un espacio y el número de minutos que se deben esperar antes de que se reinicie el sistema. Por ejemplo:

- En un sistema NT:

```
sw_wdt 4
```

- En un sistema NetWare:

```
load ServerWORKS_wdt 4
```

El sistema muestra un mensaje que describe el resultado. Por ejemplo, un sistema NT muestra el mensaje “WatchDog enabled for a one to four minute wait before reset after system hang” (WatchDog activado para esperar de uno a cuatro minutos antes de reiniciarse después de que se interrumpa el sistema).

Para desactivar WatchDog Timer:

1. Introduzca el nombre del programa en el indicador de sistema.
2. Suprima el número de minutos.

Instalación

Si se utiliza `sw_wdt` se define Watchdog Timer permanentemente en un servidor. Si Watchdog Timer provoca que un sistema se reinicie, la pantalla de mensaje confirma el reinicio y también muestra la razón del último cierre.

WatchDog Timer en SCO UNIX

Puede activar WatchDog Timer en la instalación cuando instala agentes de ServerWORKS en sistemas SCO UNIX. En respuesta al indicador, introduzca el número de minutos que se van a esperar antes de que se reinicie el sistema. Debe haber iniciado una sesión como `/root` o como administrador para activar WatchDog Timer en SCO UNIX. Para ManageWORKS V2.2, edite la línea de la manera siguiente:

```
INI file=<path of previous installation>\MWORKS.INI
```

Descubrimiento de redes y objetos **4**

IP Discovery con ServerWORKS Manager recopila volúmenes de información en todos los objetos de red. Puede ver la información de pantallas de nodos de red en la visualización de la lista de la ventana de ServerWORKS Explorer o en el visor geográfico de mapas IP Discovery.

Este capítulo

- Describe los elementos en el Explorer y la ventana de Visor de mapas
- Explica cómo manipular objetos en las ventanas
- Explica cómo descubrir la red
- Describe el Visor de alarmas y cómo puede utilizarlo para comprobar el estado de objetos de red

Descubrimiento de redes y objetos

Visualizaciones de la red

IP Discovery encuentra objetos de TCP/IP y SNMP en la red y coloca la información en la base de datos de ServerWORKS Manager. La información sobre la base de datos se utiliza para crear los mapas de IP Discovery y las vistas de ServerWORKS Explorer que representan la red. Figura 4-1 ilustra las dos visualizaciones.

Visualización de ServerWORKS Explorer

ServerWORKS Explorer es la entrada principal a ServerWORKS Manager y es la visualización predeterminada. Explorer se abre con una lista o vista arborescente que consta de objetos raíz para cada tipo de objeto de la red.

NT Server Management — Incluye todos los servidores que ejecutan Windows NT. Esta categoría aparece sólo cuando la consola de administración está ejecutando Windows NT Server o NT Workstation.

Objetos de NetWare — Incluye servidores de archivos NetWare de Novell. Esta categoría aparece sólo cuando la consola de administración está ejecutando Novell NetWare Client para Windows NT.

Objetos de servidor — Incluye todos los servidores DIGITAL (procesadores X86 y Alpha) que ejecuten Windows NT, Novell NetWare, SCO UNIX, OS/2, DIGITAL UNIX y OpenVMS. Se deben instalar los agentes adecuados. (Consulte la Tabla 3-1).

Objetos de IP y SNMP — Incluye puentes, encaminadores, nodos centrales, servidores (incluyendo servidores que no sean DIGITAL cuyos MIBs se almacenan en la base de datos de ServerWORKS), sistemas de escritorio, impresoras, Token Rings y FDDI y redes Ethernet.

Objetos de clúster — Incluye clústers de Microsoft NT y clústers de DIGITAL NT. Un clúster es representado por un objeto de clúster en un mapa o una lista. La expansión del objeto de clúster revela los miembros del clúster y los recursos—almacenamiento, aplicaciones, etc.— asociados a cada miembro de clúster. Consulte la Figura 4-1.

Descubrimiento de redes y objetos

La visualización de ServerWORKS Explorer es un visor permanente de sólo lectura que no puede modificar, eliminar ni cambiarle el nombre. El contenido del Explorer es temporal y se actualiza cuando lo abre. Sin embargo, puede crear y guardar otras visualizaciones de la lista.

La visualización del Explorer puede incluir colecciones, que contienen objetos múltiples de un tipo. Utilice la visualización de Explorer para mostrar nodos individuales y su estado. La visualización de Explorer es una ventana adecuada de la que se administran operaciones diarias porque siempre es actual.

Visores de mapas de IP Discovery

El Visor de mapas es una representación gráfica de la disposición de la red. ServerWORKS hace un descubrimiento y elabora el mapa.

Tiene las opciones siguientes para trabajar con visores de mapas:

- Ejecutar descubrimientos múltiples que se filtran para descubrir los tipos de objeto especificados
- Guardar visualizaciones actualizadas en mapas existentes
- Guardar nuevos objetos descubiertos en nuevos mapas
- Cambiar el nombre a o eliminar el Visor de mapas
- Agregar objetos manualmente en Visor de mapas

En Explorer o el Visor de mapas, los objetos de IP están codificados con colores para representar su estado actual. Las alarmas que se accionaron se indican mediante un icono de alarma enlazado al objeto. Los objetos de clúster de un mapa muestran un icono de campana si uno de los miembros o recursos ha accionado una alarma. La Figura 4-1 ilustra objetos con iconos de campana de alarma.

Descubrimiento de redes y objetos

La visualización del Explorer a la izquierda muestra los objetos de raíz de los tipos de objeto predeterminados. El signo (+) indica que hay objetos bajo el objeto raíz. Haga doble clic para desplegar el objeto raíz. El signo (-) indica que se ha desplegado la raíz. En esta ilustración están desplegados los objetos de Cluster, Printer y Server.

Este Visor de mapas muestra servidores, clústers y una impresora en una subred. Un servidor ha accionado una alarma, que es indicada por el icono pequeño de la campana.

Un objeto puede aparecer bajo varios objetos raíz. Por ejemplo, un servidor DIGITAL que ejecuta Microsoft Windows NT aparece bajo Objetos de servidor, Objetos de SNMP y Objetos de NT Server Management porque cumple con los requisitos de cada uno.

Debajo de las ventanas de visores está la Barra de estado de la alarma. Puede ver el número y tipo de alarmas con sólo echar un vistazo. Cuando hace clic en un botón de estado, abre el Visor de alarmas.

Elementos de las ventanas del visor

Cuándo está abierta la ventana Explorer o la ventana de Visor de mapas, la consola muestra:

- La Barra de menús
- La Barra de herramientas
- La Barra de estado de alarma

La Barra de menús

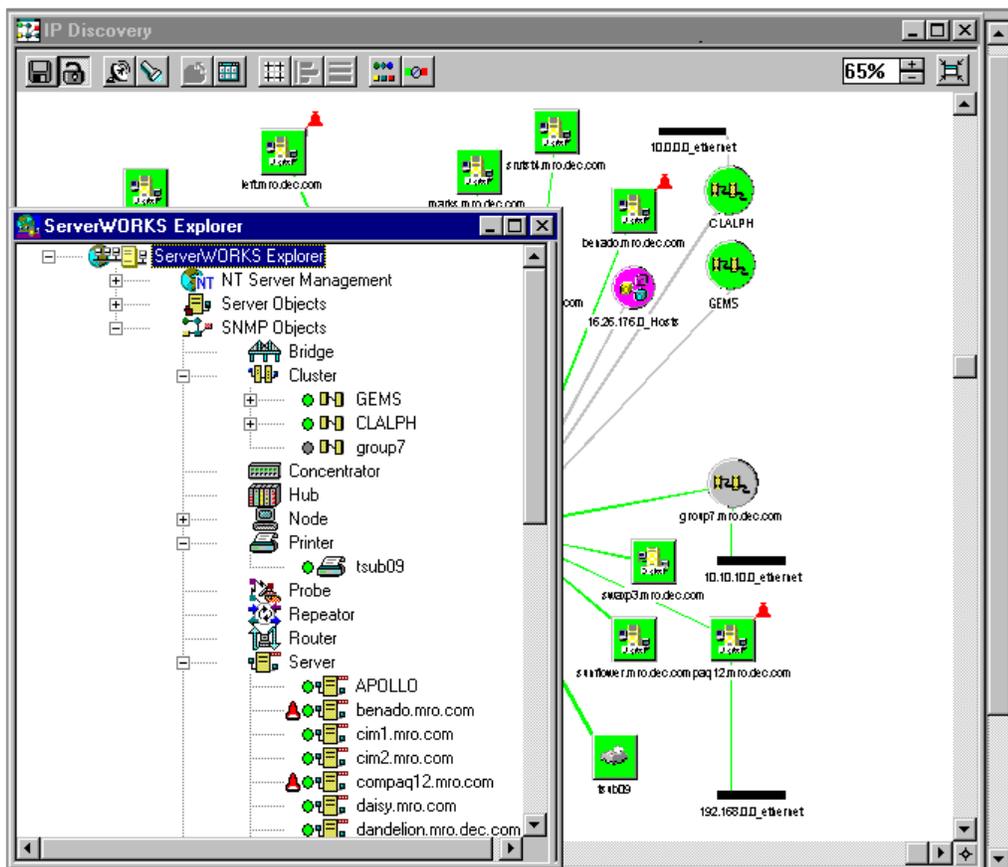
La Barra de menús contiene las opciones del menú para hacer funcionar la consola. Una descripción breve de una opción del menú aparece en la Barra de estado del menú en la parte inferior de la ventana. A medida que desplaza el cursor por las opciones del menú, la descripción cambia para cada comando. Puede leer las descripciones completas de los comandos del menú en la ayuda en línea de ServerWORKS Manager Console.

Para abrir el tema de ayuda de la Barra de menús

Descubrimiento de redes y objetos

1. Elija Ayuda→Temas de Ayuda→Índice.
2. Haga doble clic en tema de Barra de menús de ServerWORKS.

Figura 4-1 Visores de mapas y Explorer de una red



Descubrimiento de redes y objetos

La Barra de herramientas de comandos

ServerWORKS contiene una Barra de herramientas de comandos que aparece tanto en la ventana de Explorer, como en la de Visor de mapas. Las Barras de herramientas cambian dinámicamente según los objetos de red que aparecen en la lista o el mapa. Por ejemplo, los botones de la Barra de herramientas para NetWare y NT no aparecen si la red no tiene servidores que estén ejecutando estos sistemas operativos. Para una descripción completa de las Barras de herramientas, consulte la ayuda en línea.

Para abrir el tema de ayuda de la Barra de herramientas de Explorer y el Visor de mapas

1. Elija Ayuda→Temas de Ayuda→Índice.
2. Haga doble clic en el tema de la Barra de herramientas de ServerWORKS.

Para cambiar el tamaño de los botones de la Barra de herramientas de la Barra de herramientas de comandos

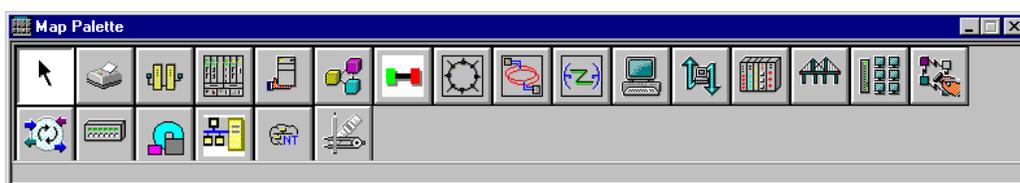
- Elija Ver→Iconos pequeños o Ver→Iconos grandes

La Paleta del Visor de mapas

El Visor de mapas también contiene una paleta de objetos para insertar objetos en un mapa. La paleta contiene los tipos de objeto genéricos y cualquier tipo de objeto que haya creado. A medida que desplaza el cursor sobre los botones de Paleta, el nombre del tipo de objeto aparece en la Barra de estado.

La Paleta es útil cuando está creando un visor de mapas especializado porque puede asociar un icono a un tipo de objeto. Por ejemplo, todos los servidores del departamento de Ingeniería pueden ser servidores DIGITAL, pero para un mapa especializado, puede asignar el logotipo del departamento de Ingeniería, un conjunto de herramientas. La Figura 4-2 ilustra la Paleta de mapas.

Figura 4-2 Paleta de mapas



Abrir y salir de ServerWORKS

Para abrir ServerWORKS Manager Console

- Desde el escritorio, elija Iniciar→Programas→ ServerWORKS Manager Console→ServerWORKS Manager.

Puede cerrar un visor o un mapa y dejar ServerWORKS Manager Console abierto o puede salir de ServerWORKS Manager Console. Si se sale, se cierran todos los visores y mapas.

Para cerrar un mapa o un visor

1. Haga clic en el mapa o el visor para seleccionarlo.
2. Elija Archivo→Cerrar visor.

Para salir de ServerWORKS Manager Console

- De la ventana Explorer o Visor de mapas, elija Archivo→Salir.

Para salir de ServerWORKS y cerrar todos los procesos

1. Elija Herramientas→Opciones→Acciones predeterminadas.
2. Seleccione Cerrar todas las aplic. al salir y haga clic en Aceptar.

Descubrimiento de redes y objetos

Navegar por visores de mapas y Explorer

Puede manipular los objetos de un mapa para ver mejor o agrupar de manera lógica y desplazarse de un mapa a otro y listar visores de varias maneras.

Puede ajustar el tamaño de un mapa porque una subred grande vista a 100% puede ser demasiado grande para el monitor.

Para ajustar un mapa a la ventana actual

- Haga clic en el botón de escala.

Para ajustar a escala un mapa a un tamaño específico

- Haga clic en el signo (+) o (-) o introduzca un número en el campo % y pulse Intro.

Por otro lado, si desea conservar el visor como está, puede ver otras partes del mapa.

Para ver las partes del mapa que se despliegan fuera de la ventana actual

- Haga clic y arrastre la barra de desplazamiento horizontal o vertical hasta que se vea la parte oculta del mapa.

Para seleccionar una parte del mapa para visualizarla

1. Elija Ver→Navegador
2. Haga clic en la sección del mapa que desea. Entonces aparece esa sección en el Visor de mapas.

Una subred ocupada puede tener cientos de conexiones y objetos. Una vez que ha establecido que las conexiones son válidas y que desea concentrarse en objetos específicos, puede ocultar las conexiones.

Para cambiar de conexiones visibles a ocultas

- Elija Ver→Mostrar conexiones o Ver→Ocultar conexiones

Descubrimiento de redes y objetos

La visualización del Explorer es de sólo lectura. Sin embargo, puede volver a crear el visor de la lista en otros visores de la lista o transferir objetos entre Visores de mapas.

Para copiar un objeto a otro visor

- Haga clic y arrastre el objeto de un mapa a otro mapa o de un visor de la lista a otro visor de la lista. (No puede arrastrar y colocar entre un visor de la lista y un Visor de mapas).

Para desplazar un objeto a otro mapa

1. Seleccione el objeto.
2. Pulse CTRL+X.
3. Haga clic en el mapa de destino.
4. Pulse CTRL+V.

Visualización de opciones en mapas individuales

Tiene varias opciones de presentación y alineación para ver mejor. La cuadrícula proporciona la orientación horizontal y vertical.

Para mostrar u ocultar la cuadrícula

1. Elija Archivo→Propiedades de visor.
2. En el cuadro de diálogo Propiedades de Visor de mapas, haga clic en Ajustar a cuadrícula o Pantalla de cuadrícula y elija las dimensiones de la celda.

La colocación automática determina la mejor distribución para un mapa específico.

Para colocar objetos de manera automática

- Elija Edición→Posicionamiento automático.

La presentación en mosaico alinea todos los objetos de manera horizontal y vertical.

Descubrimiento de redes y objetos

Para presentar los objetos en mosaico

- Elija Ver→Mosaico.

La alineación acomoda objetos seleccionados en la orientación que elija (por el extremo superior, inferior, derecho o izquierdo de los objetos).

Para alinear objetos seleccionados

1. Elija Edición→Alinear objetos.
2. En el cuadro de diálogo Alinear objetos, haga clic en la opción de alineación.
3. Haga clic en Aceptar.

Supresión y eliminación de objetos

También puede suprimir o eliminar objetos. La supresión de un objeto lo quita del visor, pero lo deja en la red. Eliminar quita *permanentemente* objetos de Windows NT, como dominios, usuarios, grupos y directorios de la red. Asegúrese de que desea eliminar el objeto.

Para quitar un objeto de un visor

1. Seleccione el objeto.
2. Elija Edición→Suprimir.

Para eliminar un objeto de NT de la red

1. Seleccione el objeto.
2. Elija Edición→Cortar o CTRL+X.

Cómo IP Discovery encuentra objetos

IP Discovery identifica objetos utilizando una secuencia específica. Primero se utiliza IP Discovery, seguido de una consulta al Descriptor de sistema de MIB II de SNMP (el sysDesc). IP Discovery también verifica si un agente de DIGITAL se está ejecutando en el objeto. Si es así, IP Discovery busca la cadena del descriptor de sistema de agente de base DIGITAL (svrSystemDescr). Al encontrar esta cadena, IP Discovery identifica el objeto como un Server.Digital.

Descubrimiento de redes y objetos

IP Discovery sigue consultando el objeto e investiga

- Si el objeto es un servidor, IP Discovery determina si el objeto es un servidor de clústers.
- Si el objeto es un servidor de clústers, IP Discovery determina si el objeto es un clúster de Microsoft o un clúster de NT de DIGITAL.
- Si IP Discovery no encuentra la información anterior, el objeto se identifica como Node.Generic. (La mayoría de los objetos aparecen como nodos genéricos porque SNMP no está configurado en los dispositivos (administrados). Los objetos también se clasifican como Node.Generic si tienen una capa de SNMP, pero no son identificables de su lista de tipos de objetos de SNMP conocidos.
- Si un objeto tiene adaptadores múltiples y no está ejecutando el agente de DIGITAL, el objeto se identifica como Router (Encaminador).

Descubrimiento de redes

El descubrimiento comienza con una búsqueda de la subred del sistema en la que está instalada la consola, utilizando la comunidad predeterminada Public. Discovery Wizard detecta la subred local que se basa en la dirección IP del sistema local. En descubrimientos posteriores, puede especificar otras subredes y guardar cada una como un Visor de mapas separado. Descubrir por subredes es una manera ordenada de descubrir una red entera.

Para el primer descubrimiento, empiece con la máscara de red y subred predeterminada.

1. Desde ServerWORKS Manager, elija Acciones→Descubrir objetos IP. Se abre el cuadro de diálogo Redes para descubrir.
2. Si este es el primer descubrimiento, haga clic en Siguiente. Si es un descubrimiento posterior, introduzca una dirección IP de subred o una dirección IP única (para descubrir un objeto conocido y colocarlo en un visor) en el campo Red.
3. En el campo Máscara de red, introduzca la máscara de subred.
4. Haga clic en Agregar para colocar la nueva red o sistema en la lista.

Descubrimiento de redes y objetos

5. Haga clic en la subred para seleccionarla para descubrirla.
6. Haga clic en Siguiente.
7. En el cuadro de diálogo Seguridad de IP Discovery, siga uno de estos pasos:
 - Haga clic en Siguiente para aceptar Public, la comunidad predeterminada.
 - Introduzca un nombre de comunidad. IP Discovery entonces encuentra sólo los objetos que pertenecen a la misma comunidad como el sistema de consola de administración.
8. En el cuadro de diálogo Tipos para descubrir, siga uno de estos pasos:
 - Haga clic en Siguiente para descubrir Todos los tipos de objetos.
 - Seleccione los tipos de objetos específicos que desea descubrir. Luego haga clic en Siguiente.
9. En el cuadro de diálogo Opciones de IP Discovery, elija el método de descubrimiento. A menos de que esté familiarizado con la subred y pueda especificar un Host de inicio para empezar el descubrimiento, elija Ping Spray. Si ha creado mapas o visores jerárquicos, seleccione uno para los resultados del descubrimiento de la lista “Seleccionar un Visor de mapas para resultados de descubrimiento:” .
10. Haga clic en Finalizar.
11. Elija Sí o No para indicar si desea ver el informe de descubrimiento.
12. Elija Sí o No para agregar nuevos objetos a la visualización actual.



Nota: El tiempo de descubrimiento varía de 15 segundos para un solo nodo a más de 30 minutos para una subred grande. Observe el cuadro de diálogo Descubrimiento de TCP/IP en curso. La Barra de estado muestra la actividad actual. Cuando el tiempo de finalización aparece, el descubrimiento está completo.

¿Qué ha descubierto?

Después del primer descubrimiento, tiene una lista o una representación gráfica de la subred. El mapa contiene iconos para los tipos de objeto predeterminados en la red.

Descubrimientos posteriores

El proceso de descubrimiento es ascendente. Puede ejecutar un descubrimiento cada vez que abre ServerWORKS Explorer para actualizar la información en la base de datos y en un mapa. Cuando abre Explorer hace un descubrimiento posterior en un visor:

- Nuevas conexiones y nodos se agregan al mapa
- La información sobre la configuración se actualiza para nodos descubiertos previamente
- Se conservan los mapas personalizados

Para realizar un descubrimiento posterior desde Explorer

- Haga clic en un tipo de objeto en el árbol de Explorer o haga clic en un signo + junto a un tipo de objeto. Se abre el cuadro de diálogo IP Discovery. Siga uno de estos pasos:
 - Haga clic en Descubrir para volver a ejecutar un descubrimiento en la subred del visor
 - Haga clic en Mostrar objetos ya descubiertos para abrir el visor sin actualizarlo.

Descubrimiento de clústers

ServerWORKS encuentra clústers en una red y los muestra con un icono de clúster en el Visor de mapas o en Explorer. La Figura 4-3 muestra un mapa de un dominio de clúster desplegado en los visores de mapas y jerárquico.

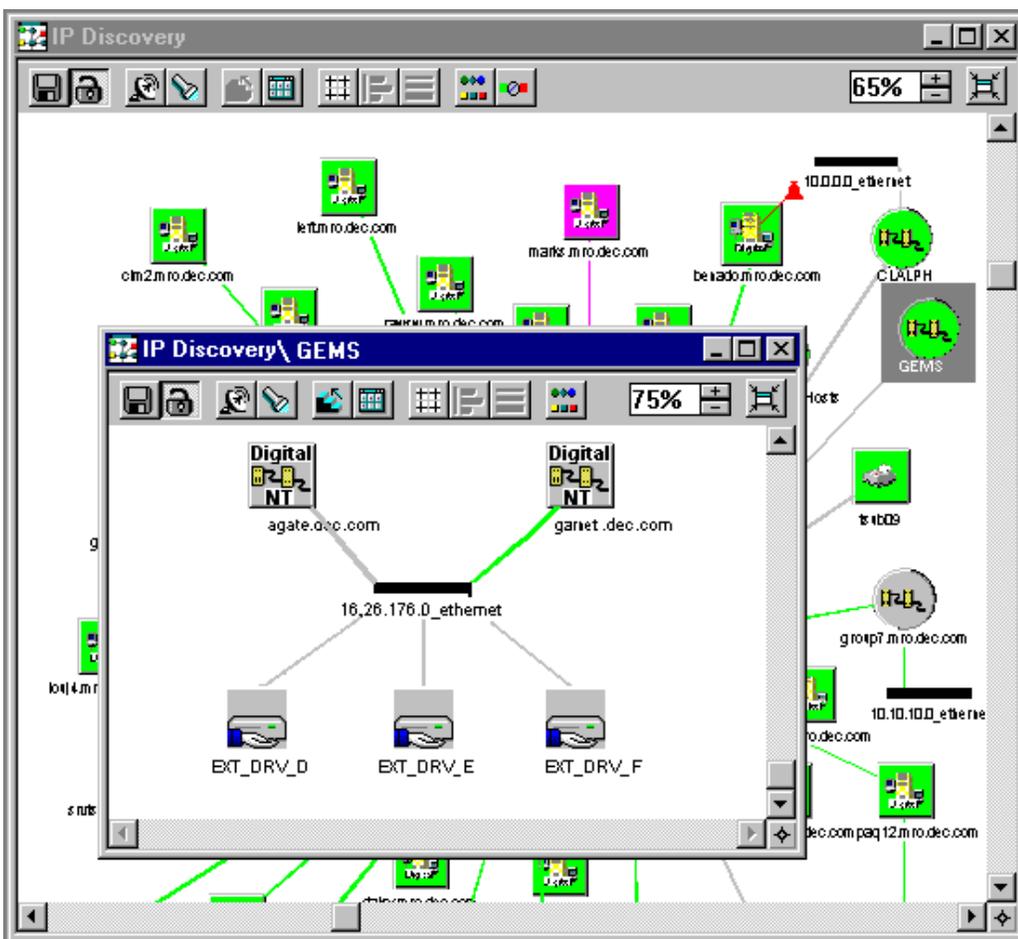
Para mostrar a los miembros y recursos de clúster

Siga uno de estos pasos:

Descubrimiento de redes y objetos

- Haga doble clic en el objeto de clúster en el mapa. Las ventanas temporales listan los servidores y los recursos.
- Haga doble clic en el tipo de objeto de clúster en la vista de Explorer, que despliega el objeto de clúster para mostrar sus servidores y recursos.

Figura 4-3 Mapa de clústers desplegados



Descubrimiento de redes y objetos

Impresión de informes de información sobre IP Discovery

IP Discovery se actualiza cada vez que abre un visor en ServerWORKS. Puede guardar la información en un informe. Los informes son archivos de texto que puede ver e imprimir en un editor como Bloc de notas. Puede elegir un Informe de IP Discovery o un informe de dirección IP. Los informes proporcionan información diferente.

Informes de IP Discovery

Los informes de IP Discovery son generados por IP Discovery y contienen información sobre los objetos descubiertos. Cuando se completa una operación de descubrimiento, el informe lista nuevos hosts de IP descubiertos, los cambios de configuración, las direcciones IP duplicadas y, los dispositivos mal configurados. Puede imprimir

- Desde IP Discovery a medida que concluye el descubrimiento. Siga las indicaciones para imprimir el informe.
- Del archivo de texto guardado, que puede abrir en el Bloc de notas. Los archivos guardados se encuentran en el directorio siguiente:

```
\Archivos de  
programas\DIGITAL\SWMGR\database\IPREPORT
```

Con el formato del nombre de archivo

```
<mes><fecha><hora><minutos>.txt
```

Por ejemplo, el informe para el 31 de marzo de 1998, aparece así

```
03311998.txt
```

Para definir una salida específica para el informe

1. Continúe mediante un descubrimiento (vea la sección “*Descubrimiento de redes*” en este capítulo) al cuadro de diálogo Opciones de Descubrimiento.
2. Elija el botón Avanzadas.
3. En el cuadro de diálogo Opciones avanzadas de TCP/IP, elija la ficha Resultados.

Descubrimiento de redes y objetos

4. Especifique el nombre del archivo de resultados y haga clic en los tipos de información que desea en un informe y haga clic en Aceptar.
5. Termine el descubrimiento.

Para crear un Informe de IP Discovery

1. Desde la consola, elija Herramientas→Informes de IP Discovery.
2. Haga doble clic en el archivo que desea imprimir.
3. En el Bloc de notas, elija el Archivo→Imprimir.

Informes de dirección IP

Los informes de dirección IP se crean a partir de la base de datos después de completar un descubrimiento. La información del informe incluye la dirección IP, el nombre y la dirección MAC de cada objeto descubierto. Este informe es útil para resolver conflictos entre direcciones IP y direcciones MAC.

Para imprimir un Informe de dirección IP

1. Desde la consola, elija Herramientas→Informe de dirección IP.
2. De la ventana DumpObject, elija Archivo→Guardar. El archivo se guarda como Report.txt.
3. Para imprimir el archivo, ubique el archivo en

```
\Archivos de programas\DIGITAL\SWMGR\database\report.txt
```
4. Haga doble clic en el archivo.
5. En el Bloc de notas, elija el Archivo→Imprimir.

¿Cómo opera la red?

Después de hacer un descubrimiento y desde cualquier visor, ServerWORKS muestra el estado completo de sistema de un vistazo. Puede utilizar cualquiera de los métodos siguientes para comprobar rápidamente el estado.

Descubrimiento de redes y objetos

- Iconos de alarma y estados codificados con colores en Explorer y el Visor de mapas
- Barra de estado de la alarma
- Visor de alarmas

Verificaciones de estado codificadas con colores

Puede supervisar los cambios de estado en objetos del visor por color. En un visor jerárquico, el estado es indicado por un círculo a la izquierda del objeto. En un visor de mapas, el estado es indicado por el color de fondo del icono del objeto. Para objetos de clúster, el estado Desactivado o Ninguna respuesta en un recurso o miembro se indica a nivel del grupo de clúster. El despliegue del icono del clúster revela la fuente del problema.

Tabla 4-1 Indicadores de colores de estado en visores jerárquicos y de mapas

Color	Significado
Verde	El objeto está funcionando.
Rojo	El objeto se desactivó (pero esto puede ser una acción intencional de un administrador).
Amarillo	Una encuesta de SNMP indica que el dispositivo es anormal de alguna manera, por ejemplo, es posible que una interfaz esté inactiva.
Magenta	El sistema no responde.

Puede cambiar los colores predeterminados. Consulte la sección “Opciones personalizables para un visor o mapa” en el Capítulo 7.

Verificaciones rápidas desde la Barra de estado

Utilice un visor de mapas o Explorer actualizado diario para verificaciones de alarmas diarias utilizando la Barra de estado del Visor de alarmas (Figura 4-1). Los botones Desactivado y Ninguna respuesta de la izquierda, le indican con sólo echar un vistazo si algún objeto está fuera de línea o no se está comunicando. A la derecha, los botones contadores de alarmas muestran el número de alarmas accionadas de en cada nivel de severidad.

Cómo aprender del visor de alarmas

El Visor de alarmas lista todas alarmas actuales. Utilice el Visor de alarmas para ver los detalles de la alarma. Utilice el Filtro de Visor de alarmas para personalizar el visor.

Para abrir el Visor de alarmas y comprobar los mensajes

- Haga clic en un botón de severidad de la alarma o elija Acciones→Ver alarmas.

En el Visor de alarmas (consulte la Figura 4-4), puede analizar los mensajes de la alarma de varias maneras:

- Elija Todas las alarmas no confirmadas para ver cada alarma de cualquier tipo en todos los sistemas.
- Clasifique las columnas del visor alfabéticamente por dispositivo o por severidad, fecha, en orden ascendente o descendente. Para ordenar una columna, haga clic en la etiqueta de la columna. La información de la hilera adyacente cambia a medida que se ordena la columna. Es posible que desee ordenar por severidad y primero ver todas las alarmas altas.
- Haga clic en una sola alarma para leer el mensaje de la alarma en la ventana Detalles.

Descubrimiento de redes y objetos

- Arrastre diagonalmente de la esquina de la ventana para desplegar o plegar la ventana Visor de alarmas. Las tres primeras columnas contienen la información más significativa (nombre de objeto, severidad, fecha y hora). Si necesita los demás detalles sobre la alarma, puede desplazar o desplegar la ventana. El Visor de alarmas de la Figura 4-4 está desplegado para ver más columnas.
- Filtre las alarmas para obtener información más precisa.

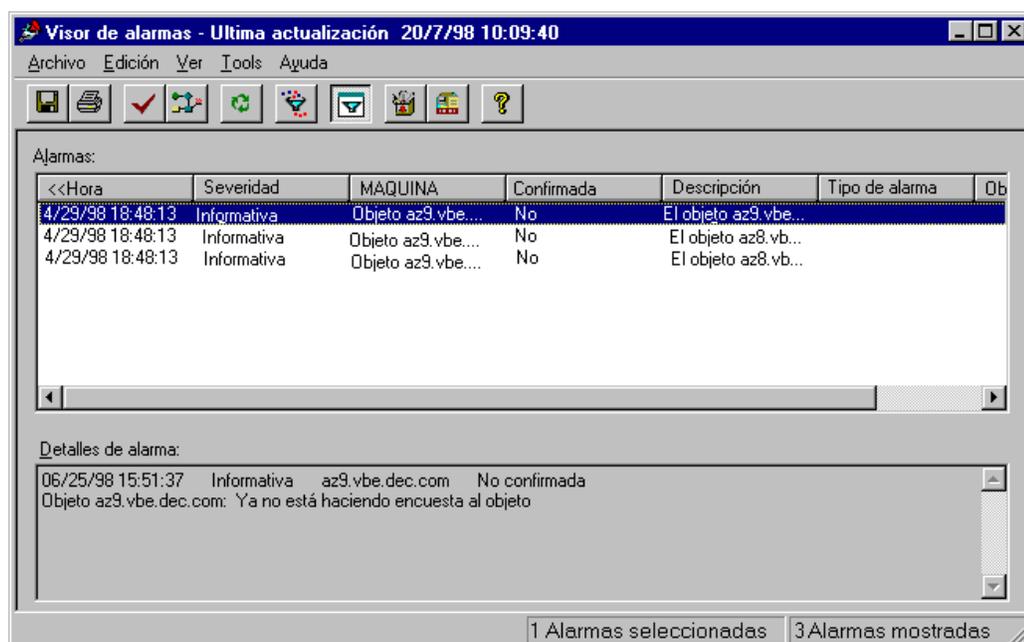
Guardar e imprimir la lista de alarmas

Puede guardar las alarmas como se han ordenado en la ventana Visor de alarmas. Después puede importar el archivo en Microsoft Excel.

Para guardar la lista de alarmas

1. Elija Archivo→Guardar como.
2. Introduzca un nombre de archivo y haga clic en Guardar. El archivo se guarda en un formato tabular para importarlo en programas de hojas de cálculo.

Figura 4-4 Visor de alarmas



Para importar la lista de alarmas a Microsoft Excel

- En el Explorador de Windows, haga clic en el archivo guardado y arrástrelo a un acceso directo de Excel en el escritorio. Excel se abre e inserta los archivos de texto en una hoja de cálculo.

Filtro de alarmas para visualización

El filtro de alarmas le permite elegir qué alarmas aparecerán en la ventana Visor de alarmas. El Filtro de Visor de alarmas en la Figura 4-5 está configurado para mostrar todas las alarmas de estado de componente no confirmadas de severidad alta en todos los tipos de objeto de red. Para el análisis de un cierto período, se definieron las horas y las fechas. Sólo aparecen alarmas que ocurrieron durante el período de tiempo.

Descubrimiento de redes y objetos

Figura 4-5 Cuadro de diálogo Filtro de Visor de alarmas



Definición de alarmas **5**

La verificación del estado de objetos de red es útil, pero el estado actual no es un indicador del rendimiento futuro. Por ejemplo, un estado Activado sólo indica que la operación es adecuada en este momento. Para estar prevenido de los problemas de desarrollo, utilice Alarm Configuration de ServerWORKS. Este capítulo explica:

- La ventana Alarm Configuration y la Barra de herramientas
- Alarmas predeterminadas de Minimal Health
- Alarmas de la consola (definidas por el usuario)
- Acciones de notificación de alarmas

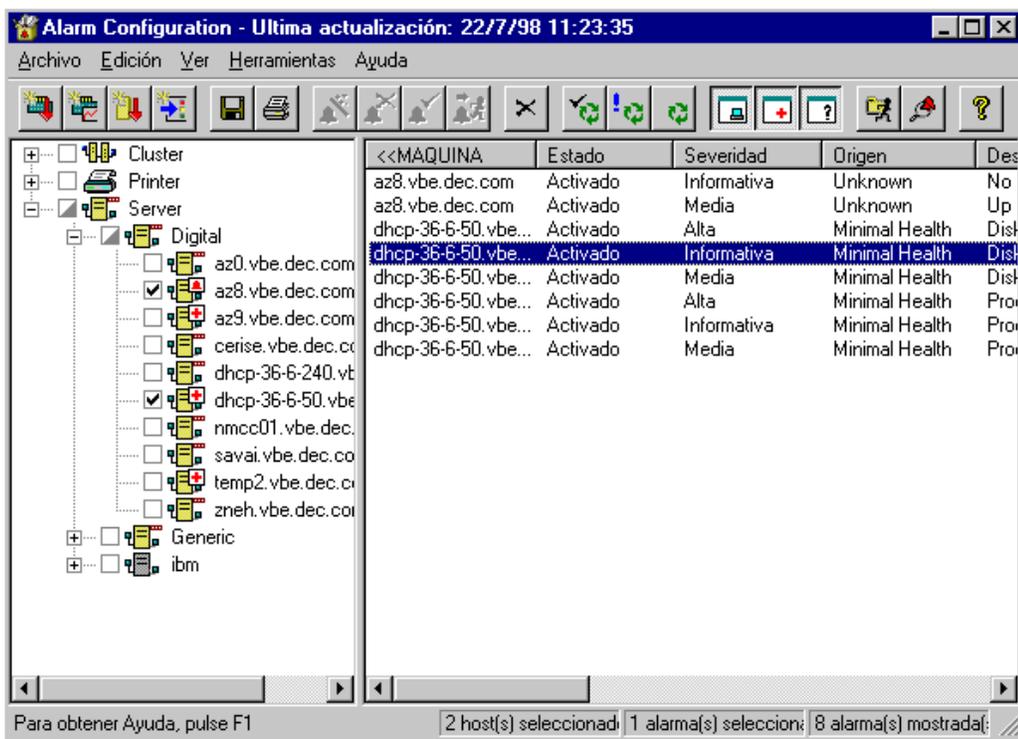
Definición de alarmas

La ventana Alarm Configuration y la Barra de herramientas

Esta sección explica Alarm Configuration, que se utiliza para crear y ver detalles sobre las alarmas definidas en hosts de red. (Utilice el Visor de alarmas para ver todas las alarmas que se accionaron).

La ventana Alarm Configuration muestra los nombres de host de red en la sección izquierda. La sección derecha contiene la descripción y los detalles de la alarma, como el nombre de host, la dirección IP, el tipo de objeto, una descripción, la severidad de la alarma, la fuente de la alarma, la categoría y su estado activado. La Figura 5-1 ilustra la ventana Alarm Configuration.

Figura 5-1 Ventana Alarm Configuration



Definición de alarmas

Puede utilizar las opciones del menú o la Barra de herramientas correspondiente para trabajar con las alarmas. (Consulte la Figura 5-2).

Figura 5-2 Barra de herramientas de Alarm Configuration



Cualquiera de los diferentes iconos junto al nombre de host en la sección izquierda indica si hay alarmas configuradas en el host.

Tabla 5-1 Iconos de host de Alarm Configuration

Este icono	Indica que
	Una o más alarmas de consola o de otras fuentes están configuradas para este host.
	Una o más alarmas de Minimal Health están configuradas para este host. Alarmas de consola o de otras fuentes también pueden estar configuradas.
	Una de las condiciones siguientes: <ul style="list-style-type: none"> El host se acaba de descubrir. Nunca ha habido comunicación con el host para determinar si las alarmas están configuradas. La comunicación de SNMP con el host no fue satisfactoria para esta sesión (por ejemplo, debido a los tiempos de espera) por lo que la lista no puede ser actual. Las alarmas que aparecen en la lista son alarmas que se informaron de la última comunicación satisfactoria con el host.
	Ninguna alarma de cualquier tipo está configurada en este host.

Definición de alarmas

Puede elegir qué datos se muestran y el orden en el que aparecen en la sección derecha y ordenar los datos de la columna alfabéticamente.

Para ordenar los datos de la columna

- Haga clic en la etiqueta de la columna en la parte superior de la columna.

Para configurar los datos de la columna y guardar el esquema de la pantalla

1. Elija Ver→Visualización de columnas. Se abre el cuadro de diálogo Visualización de columnas.
2. Para seleccionar una columna de datos para el pantalla, haga clic en el cuadro de verificación de la columna de datos.
3. Para cambiar el orden de las columnas, seleccione el nombre de la columna de datos y haga clic en Arriba o Abajo para volver a colocar la columna.
4. Para guardar el pantalla, haga clic en Guardar como. Luego introduzca un nombre en el cuadro de diálogo Guardar como nombre de visualización y haga clic en Aceptar.
5. Haga clic en Aceptar para cerrar el cuadro de diálogo Visualización de columnas.

Para ver alarmas definidas en hosts seleccionados

- Seleccione el host y uno de los comandos de menú siguientes:
 - Elija Ver→Mostrar alarmas de consola para ver alarmas definidas por el usuario.
 - Elija Ver→Mostrar alarmas de Minimal Health para ver alarmas de Minimal Health V2.x.
 - Elija Ver→Mostrar alarmas de otras fuentes para ver alarmas generadas por programas de administración de empresas (por ejemplo, HP OpenView).

Definición de alarmas

Puede guardar la lista de alarmas como archivo de texto. El archivo que contiene la lista de alarmas configuradas actualmente, se guarda en el directorio SWMGR.

Para guardar una lista de alarmas

1. Elija Archivo→Guardar como.
2. Introduzca un nombre de archivo y haga clic en Guardar. El archivo se guarda en un formato de tabla para importarlo en programas de hojas de cálculo.

Para importar la lista de alarmas en Microsoft Excel

- Localice el archivo en el Explorador de Windows y arrástrelo a un acceso directo de Excel en el escritorio.

Actualización de la lista de alarmas configuradas

Se recomienda que se actualice la lista de alarmas configuradas para que la lista incluya nodos cuyas alarmas se definieron o modificaron desde otras estaciones de administración y nuevos nodos descubiertos.

Para actualizar la lista de alarmas configuradas

Siga uno de estos pasos:

- Elija Ver→Actualizar todos los hosts para actualizar las alarmas de todos los hosts. Esta acción se puede tardar un poco.
- Elija Ver→Actualizar hosts seleccionados para actualizar las alarmas definidas en hosts seleccionados. El tiempo que se requiere para actualizar aumenta con el número de hosts seleccionados.
- Elija Ver→Actualizar nuevos hosts descubiertos para actualizar alarmas definidas en hosts que nunca se incluyeron en una visualización de Alarm Configuration. Esta actualización incluye nodos que se insertaron manualmente y es más rápida que actualizar todos los nodos. Estos nodos son indicados por un signo de admiración (como se muestra en la Figura 5-1) por lo que no es necesaria la selección de nodos.

Impresión de la lista de alarmas

Puede imprimir la lista de Alarmas actual, clasificada por el contenido de una columna seleccionada. Sólo la información que se muestra aparece en el informe. Por ejemplo, si muestra las columnas de la Figura 5-1, y ordena la dirección IP, el informe contiene la información sobre el host y las alarmas de los hosts, empezando con el host que tiene la dirección IP más baja.

Para imprimir una lista de alarmas

1. Configure la lista de alarmas.
2. Haga clic en una columna.
3. Elija Archivo→Imprimir.

Configuración de alarmas

La herramienta Alarm Configuration se utiliza para definir alarmas en servidores, computadoras de escritorio y sistemas móviles. La consola recibe las alarmas y los mensajes de captura. Puede configurar la misma alarma para más de un objeto de host siempre y cuando el parámetro del sistema al que se está asignando una alarma (por ejemplo, un disco), esté presente en todos los hosts que se seleccionaron.

Minimal Health

Minimal Health es la primera línea de defensa para servidores. Minimal Health proporciona un conjunto de umbrales específicos de hardware en las plataformas con procesadores X86 siguientes en las que está instalado:

- Las condiciones de ambiente en fuentes de alimentación, ventiladores, tensión y temperatura y, las condiciones de funcionamiento en discos duros, procesadores y componentes de memoria para plataformas que ejecutan Windows NT
- Las condiciones de fuentes de alimentación, ventiladores, tensión y temperatura en plataformas que ejecutan Novell NetWare.

Definición de alarmas

Los hosts con Minimal Health son indicados por el icono de cruz roja junto al nombre de host en la ventana de Alarm Configuration. (Consulte la Figura 5-1).

Comprensión de alarmas de Minimal Health

Minimal Health es una opción de la instalación en un host. Las pautas siguientes describen cómo utilizar las alarmas de Minimal Health.

- Si elige Minimal Health cuando instala agentes de ServerWORKS, una plantilla que define las alarmas y los umbrales se aplica cuando se instalan los agentes de Minimal Health V2.x de ServerWORKS. Si no instala Minimal Health con el kit de instalación de ServerWORKS, puede instalarlo posteriormente con el kit. No puede activar las condiciones de protección mínima hasta que instale Minimal Health.
- Minimal Health reemplaza todos umbrales que fueron definidos por los agentes de la Versión 1.x en versiones anteriores de ServerWORKS.
- Las alarmas de Minimal Health y de consola pueden coexistir. Puede tener múltiples alarmas en un componente o una condición de ambiente.
- Una vez instalado, puede activar y desactivar Minimal Health desde el menú. Cuando se desactiva, se eliminan todos los umbrales de Minimal Health. La activación de Minimal Health vuelve a activar los umbrales.
- Minimal Health permanece desactivado hasta que lo vuelve a activar de una de las maneras siguientes:
 - En el menú Alarm Configuration, elija las opciones Archivo→Minimal Health activado.
 - Vuelva a instalar Minimal Health en el host.
 - Cambie la variable de activación de Minimal Health desde MIB Browser. (Para hacerlo debe estar familiarizado con MIB).

Definición de alarmas

- Cuando selecciona hosts múltiples en dónde activar alarmas de Minimal Health, compruebe que los agentes de Minimal Health se hayan instalado previamente en los hosts seleccionados. Si los hosts seleccionados contienen agentes Versión 1.x y Versión 2.x, Minimal Health sólo se aplica a los hosts que tienen agentes Versión 2.x.
- Puede especificar acciones para nombres de acciones predefinidos que estén asociados a alarmas de Minimal Health. Consulte la sección “Asociación de una acción a una captura de Minimal Health” en este capítulo.
- La modificación de alarmas de Minimal Health no se permite en Alarm Configuration. Sin embargo, puede eliminar alarmas individuales de Minimal Health y luego restaurarlas activando Minimal Health desde la consola.

Alarmas de consola definidas por el usuario

ServerWORKS permite crear cuatro clases de alarmas definidas por el usuario:

Alarmas de estado de componente —Informan sobre el estado de un objeto de nodo o servidor DIGITAL.

Alarmas de umbral de componente —Informa cuando una característica de un servidor DIGITAL reúne una condición especificada. Por ejemplo, la temperatura excede un valor o un disco excede su capacidad.

Alarmas de estado del sistema (interfaz) —Informan cuando un sistema o una interfaz, como un adaptador, cambia su estado. Por ejemplo, un sistema se desactiva.

SNMP Traps —Envía mensajes de SNMP que son accionados por el agente de SNMP.

Definición de alarmas

Configuración de SNMP y el destino de capturas

Si no lo ha hecho, debe configurar el servicio SNMP en cada sistema en el que esté instalado un agente de ServerWORKS y especifique la dirección IP de destino de la captura. La consola no recibe ninguna captura de un dispositivo administrado si no se especifica un destino de consola.

Puede tener múltiples destinos de capturas especificadas en la configuración de SNMP y puede enviar capturas de la consola de destino a otras consolas o a administradores de empresas. Consulte la sección del Capítulo 7 para obtener detalles sobre la configuración de SNMP y la definición de destinos de capturas.

Alarmas de estado de componente

Las alarmas de estado se envían cuando falla un dispositivo, envía una alerta o regresa a en línea. Puede definir alarmas de estado en los componentes siguientes:

- Procesadores
- Discos
- Sensores de ventiladores
- Sensores de tensión
- Sensores de fuente de alimentación
- Sensores de temperatura
- Estado de la memoria
- Estado de los grupos de clúster

Alarmas de umbral de componente

En una alarma de umbral se especifica un valor para una condición o característica mensurable. Cuando la condición de alarma alcanza el valor especificado, se acciona la alarma. Puede definir alarmas de umbral en las condiciones o características siguientes:

Definición de alarmas

- Utilización de la CPU, utilización del sistema de archivos y uso del almacenamiento de disco
- Estado de tensión, temperatura y ventiladores
- Número total de paquetes, errores de entrada, errores de salida, paquetes de entrada, paquetes descartados de entrada, errores de protocolo desconocido

Cuando configura el umbral, también especifica un valor que reinicia la alarma cuando las condiciones vuelven a un valor razonable. El valor de reinicio debe estar fuera del margen de alarma. Dependiendo del operador de relación (mayor que, menor que, etc.) que utilice, el reinicio puede ser más alto o más bajo que el umbral.

Por ejemplo, si está definiendo alarmas para un dispositivo para la temperatura excesiva, puede definir el umbral para temperaturas de más de 60° y reiniciar la alarma a 50°. Evitará las alarmas en picos momentáneos cerca del nivel de 60° ya que la unidad está volviendo al estado normal. Por otro lado, si está mirando las temperaturas bajas, puede definir el valor umbral a menos de 32° con un valor de reinicio de 40°.

También puede definir la alarma de umbral para enviar capturas múltiples en la misma alarma aplicando un modo de repetición, que envíe la captura hasta que se alcance el valor de reinicio.

Respuesta a indicaciones durante la configuración de alarmas

Alarm Configuration muestra varios cuadros de mensaje si está enviando capturas múltiples. Estos se explican en las secciones siguientes. A medida que se familiariza con los mensajes y sabe cómo piensa contestarlos, puede apagar los indicadores. Puede restaurarlos en cualquier momento.

Para administrar las indicaciones

- En el cuadro de mensaje, haga clic en "No volver a mostrar".

Para restaurar las indicaciones

- Elija Edición→Volver a activar todos los mensajes desactivados para ver los indicadores otra vez.

Definición de alarmas

Configuración de capturas múltiples para alarmas de umbral

Puede estar ejecutando agentes Versión 1.x y agentes de administración de servidores Versión 2.x en dispositivos de la red. Las versiones de agente se comportan de manera diferente cuando está definiendo umbrales y modos de repetición para capturas múltiples. Aparece un mensaje que explica las opciones.

- Puede enviar capturas múltiples desde dispositivos en los que estén instalados agentes Versión 1.x. Para hacerlo, los agentes permiten un valor de reinicio que esté dentro del margen de alarma, que a su vez enviará capturas múltiples a un destino de captura por un suceso de alarma. La frecuencia de las capturas enviadas es el intervalo de encuesta.
- Puede enviar capturas múltiples desde dispositivos en los que estén instalados agentes Versión 2.x accediendo a un modo de repetición cuando define la alarma. Agentes Versión 2.x no permiten un número de reinicio que no sea válido para un umbral. Si introduce un número no válido, se le pide que lo cambie.

Definición de capturas múltiples con versiones de agente múltiples

En general, evite definir alarmas simultáneamente en dispositivos múltiples que ejecuten alarmas Versión 1.x o Versión 2.x. Sin embargo, si selecciona dispositivos múltiples, aparece un mensaje que explica las opciones:

- Siga definiendo las alarmas. Para hacerlo, elija Sí en el mensaje. El valor de reinicio de umbral en dispositivos Versión 1.x se utilizará como modo de repetición y, el valor de reinicio para dispositivos Versión 2.x será igual al valor de accionamiento de la alarma.
- Deje de definir las alarmas. Para hacerlo, elija No. Luego empiece el proceso otra vez, definiendo las alarmas por separado para versiones de agente diferentes.

Definición de capturas para paquetes de entrada y paquetes de salida de red

Los paquetes de entrada y de salida de red no son afectados por la versión del agente. Si los agentes son Versión 1.x o Versión 2. x, el valor de reinicio de umbral es igual al intervalo de encuesta. Cuando se le pida, elija Sí para seguir definiendo las alarmas.

Alarmas de estado del sistema

Las alarmas de estado del sistema informan sobre un estado Activado, Desactivado, Ninguna respuesta o Prueba en un servidor. (El estado de la prueba puede aparecer si utiliza SNMP en vez de ICMP para la encuesta. Se devuelve un mensaje de Prueba como un estado en una interfaz, por ejemplo, en prueba de loopback de una interfaz).

Alarmas de SNMP Trap

Las alarmas de SNMP Traps se envían cuando el agente de SNMP detecta un cambio de estado. Alarm Configuration proporciona una lista de SNMP Traps válidas para definir las alarmas en componentes.

Para aprender más acerca de las variables de SNMP que se supervisan para capturas, lea el MIB del proveedor para el dispositivo particular.

Creación de alarmas y acciones de notificación

Cuando cree una alarma, complete las tareas siguientes. Cada una de ellas está compuesta de varios pasos más pequeños.

- Seleccione los hosts.
- Elija el tipo de la alarma y especifique el parámetros para la alarma.
- Actualice la lista de alarmas cuando agregue o modifique una alarma.

Además, si está creando una notificación opcional para la alarma, asocie una acción a la alarma. Puede crear notificaciones utilizando las acciones de la manera siguiente:

Definición de alarmas

- Puede volver a utilizar la acción para tipos de objeto diferentes o para tipos de alarma diferentes.
- Puede asignar múltiples acciones a un nombre de acción.
- Puede asignar nombres de acciones múltiples a una alarma.

Creación de alarmas de estado de componente

1. Del menú ServerWORKS Manager Console, elija Herramientas→Alarm Configuration.
2. Seleccione los hosts de la lista de objetos de red.
3. De Alarm Configuration, elija Archivo→Nueva alarma→Estado de componente.
4. En el cuadro de diálogo Agregar alarmas de estado del nuevo componente, ficha Categoría, seleccione una categoría de alarma y los elementos que se van a supervisar. Los elementos a los que puede definir una alarma se basan en el tipo de objeto. A su vez, los subelementos a los que puede definir una alarma cambian con la categoría. La sección Resumen de alarma, como su nombre lo indica, muestra un resumen de la alarma.
5. De la ficha Estados de la lista Estados posibles:, seleccione los estados que desea en la definición de alarma (por ejemplo No funcional) y haga clic en el botón con flecha derecha para agregar el estado a la lista Estados de alarma:.
6. En la ficha Severidad , elija la importancia de la alarma que se está definiendo.
7. En la ficha Encuesta seleccione el intervalo de encuesta para el objeto. Una alarma con severidad alta debe tener un valor de encuesta frecuente, por ejemplo un minuto.
8. Si está especificando una acción, siga uno de estos pasos:
 - En la ficha Acciones elija una acción existente del Directorio de acciones y haga clic en Aceptar para terminar de definir la alarma.
 - Haga clic en Agregar nueva y consulte la sección "Adición de

Definición de alarmas

la acción de notificación en una alarma" y la subsección que describe la acción que desea:

Acción de Pager Configurar una acción de notificación de Pager

Acción correo elec. Configurar una acción de notificación de correo electrónico

Inicio de aplicación Configurar un inicio de aplicación

9. Elija Aceptar.

Creación de alarmas componente

1. Del menú ServerWORKS Manager Console, elija Herramientas→Alarm Configuration.
2. Seleccione el(los) host(s) para asignar alarmas de la lista de objetos de red.
3. Desde Alarm Configuration, elija Archivo→Nueva alarma→Estado de componente.
4. En el cuadro de diálogo Agregar alarmas de umbral del nuevo componente, ficha Categoría, seleccione una categoría de alarma y los elementos que se van a supervisar. La categoría de alarma lista los elementos a los que puede definir una alarma basada en el tipo de objeto. A su vez, los subelementos a los que puede definir una alarma cambian con la categoría. La sección Resumen de alarma, como su nombre lo indica, muestra un resumen de la alarma.
5. En la ficha Umbral, seleccione un valor absoluto o relativo de la lista de Métodos de computación de alarma. Luego defina el cómputo de umbral, eligiendo un operador (por ejemplo, mayor que) y una línea base. Haga clic en el botón Valor actual para ver el uso actual. En Volver a activar alarma, elija un accionador de repetición opcional. Introduzca el valor en el cual accionar los estados que desea en la definición de alarma (por ejemplo No funcional) y haga clic en el botón con flecha derecha para agregar el estado a la lista Estados de alarma:.

Definición de alarmas

6. En la ficha Severidad , elija la importancia de la alarma que se está definiendo.
7. En la ficha Encuesta seleccione el intervalo de encuesta para el objeto. Una alarma con severidad alta debe tener un valor de encuesta frecuente, por ejemplo un minuto.
8. Si está asociando una acción a esta alarma, en la ficha Acciones, siga uno de estos pasos:
 - Elija una acción existente del Directorio de acciones y haga clic en Aceptar para terminar de definir alarma.
 - O haga clic en Agregar nueva y consulte la sección "Adición de la acción de notificación en una alarma" y la subsección que describe la acción que desea:
9. Elija Aceptar.

Creación de alarmas de estado de sistema

1. Del menú ServerWORKS Manager Console, elija Herramientas→Alarm Configuration.
2. Seleccione el objeto (host) de la lista de objetos de red para asignarle una alarma.
3. En Alarm Configuration, elija Archivo→Nueva alarma→Estado de sistema.
4. En el cuadro de diálogo Agregar alarmas de estado del nuevo sistema, especifique lo siguiente:
 - Estado de sistema: Elija uno: Activado, Desactivado, Ninguna respuesta y Prueba.
 - Elija una severidad de Alta, Baja, Media o Informativa.
 - Elija una acción del Directorio de Acciones o elija Agregar nueva para crear una nueva acción y continúe con la sección "Adición de la acción de notificación en una alarma".
5. Elija Aceptar.

Creación de alarmas de SNMP Trap

1. Del menú ServerWORKS Manager Console, elija Herramientas→Alarm Configuration.
2. Seleccione un objeto (host) de la lista de objetos de red para asignarle una alarma.
3. En Alarm Configuration, elija Archivo→Nueva alarma→Estado de componente→SNMP Trap.
4. En el cuadro de diálogo Agregar nuevas alarmas de SNMP Trap, especifique lo siguiente:
 - SNMP Traps: Elija cada elemento para el que desea que se envíe un mensaje de captura.
 - Elija una severidad de Alta, Baja, Media o Informativa.
 - Elija una acción del Directorio de Acciones o elija Agrega Nueva para crear una nueva acción y continúe con la sección "Adición de la acción de notificación en una alarma".
5. Elija Aceptar.

Modificación de una alarma

Es posible que necesite cambiar un parámetro, una acción o la severidad de una alarma.

1. De la sección de lista de alarmas, seleccione la alarma y elija Edición→Modificar alarma o haga doble clic en una alarma de la lista.
2. En el cuadro de diálogo que se abre, edite los parámetros de la alarma y haga clic en Aplicar después de cada cambio a una página de ficha de alarma o haga clic en Aceptar cuando se hayan realizado todos los cambios.

Definición de alarmas

Adición de la acción de notificación en una alarma

Puede elegir de varias acciones cuando ocurre una condición de alarma —notificación de Pager mediante Pagers numéricos o alfanuméricos, notificación de correo electrónico y el inicio de una aplicación. Para cualquier acción, también puede definir la frecuencia de la acción de las opciones siguientes en la página de propiedades Directivas:

- Siempre, para cualquier alarma, para cualquier acción, cuando se reúnan las condiciones de alarma
- Sólo una vez para la primera alarma
- En intervalos especificados para todas las alarmas, sin importar qué tan a menudo ocurre la condición
- En intervalos especificados para algunas alarmas individuales, hasta un número de veces máximo, sin importar qué tan a menudo ocurre la alarma

Para alarmas de alta severidad, puede elegir Siempre. Para alarmas con severidad menor, elija un intervalo para evitar la saturación de la cuenta de correo electrónico o el Pager con mensajes repetidos. Para alarmas menores, una vez es suficiente (suponiendo que actúa en la notificación antes de que el problema se vuelva grave).

Configuración de una acción de notificación de Pager

ServerWORKS Manager V4.0 soporta enviar por Pager mensajes numéricos y alfanuméricos.

El mensaje que recibe en una página numérica es el mensaje de Pager. Para enviar una página numérica, necesita:

- El número de Pager, que es el número telefónico para llamar a Pager.
- El Mensaje de Pager, un código numérico que representa el mensaje que está enviando

El mensaje que recibe de una página alfanumérica se recibe de la red y contiene la fecha, la hora, el nombre de nodo y una descripción de la condición que accionó la alarma. Para enviar una página alfanumérica, necesita:

Definición de alarmas

- El número de terminal de acceso telefónico, que es el número de teléfono del proveedor de Pager
- Un NIP (número de identificación personal), que es el número de Pager
- El mensaje que desea enviar
- La longitud máxima del mensaje que soporta Pager. Consulte la documentación de Pager.

Antes de que pueda utilizar Pager para notificación, debe verificar que tenga un módem y un puerto de comunicaciones configurado en la consola para marcar el número de teléfono correctamente. Consulte el Apéndice B para obtener más información.

1. En el cuadro de diálogo Agregar nuevas acciones, elija la ficha Pager y haga clic en Nuevo.
2. En el cuadro de diálogo Nuevo usuario, ficha General, introduzca el Nombre de usuario que se requiere y una dirección de correo electrónico y comentarios opcionales.
3. Haga clic en la ficha Pager.
4. Elija un modo de comunicación por Pager y complete la información:
 - Pager numérico. Introduzca el Número de Pager y el Mensaje de Pager Consulte la sección "Cambio del tiempo de espera predeterminado de Pager" para obtener detalles sobre el uso de comas con Pagets numéricos.
 - Pager alfanumérico. Introduzca el Número de terminal de acceso telefónico y el NIP. Luego seleccione la longitud del mensaje de la lista Longitud máx. mensaje.
5. En la ficha Pager, especifique la información sobre el módem. Seleccione el puerto de comunicación y la velocidad en baudios para la configuración del módem.
6. Haga clic en Aceptar. El nombre de usuario aparece en la lista Todos los usuarios con Pager. Haga clic en Agregar para incluir el nombre en la lista Acción asignada a usuarios de Pager.

Definición de alarmas

7. Haga clic en la ficha Directivas y elija el intervalo (como se describió anteriormente en esta sección) si desea especificar un intervalo para la notificación de Pager únicamente. Luego haga clic en Aceptar.
8. Introduzca el nombre de acción, por ejemplo, Enviar por Pager. Haga clic en Aceptar. Aparece la nueva acción Enviar por Pager en la lista Contenido de Directorio de acciones. Haga clic en Aceptar.

Cuando una condición de alarma se detecta en una alarma con una acción de Pager asociada, el módem marca al Pager y envía el mensaje al Pager.

Cambio del tiempo de espera predeterminado de Pager para Pager numérico

Los Pagers numéricos le permiten incluir un tiempo de espera para ajustar la sincronización entre la marcación de un número telefónico y el envío del mensaje numérico. El símbolo estándar es una coma. La alarma de Pager de ServerWORKS Manager Console tiene un tiempo de espera predeterminado de cinco comas. Puede cambiar el tiempo de espera si necesita más o menos tiempo de espera entre la marcación del número telefónico y el envío del mensaje numérico.

Para cambiar el tiempo de espera

1. Abra el archivo swmgr.ini y encuentre la sección [Setup].
2. Agregue lo siguiente a la sección:

```
PagerWaitTime=
```
3. Introduzca un número para el tiempo de espera de comunicación por Pager. Este tiempo de espera es el número de comas. Es posible que tenga que intentar varios números hasta que encuentre el intervalo de espera correcto para el sistema de comunicación por Pager.

Configuración de una acción de notificación de correo electrónico

Antes de poder utilizar el correo electrónico para notificación, debe verificar que tenga un perfil válido para el correo de Microsoft Exchange para que el destinatario obtenga la notificación y se esté ejecutando "Configuración del perfil predeterminado 'Configuraciones de Microsoft Exchange'Exchange. Primero verifique que el perfil para el correo sea 'Configuraciones de Microsoft Exchange'. Si no es así, debe especificarlo como el perfil predeterminado. Consulte la sección ". Vuelva a iniciar MS Exchange antes de configurar la acción de notificación por correo electrónico.

1. En el cuadro de diálogo Agregar nuevas acciones, elija la ficha Correo electrónico y haga clic en Nuevo.
2. En el cuadro de diálogo Nuevo usuario, ficha General, introduzca la información sobre el usuario. La dirección de correo electrónico es la dirección de correo Internet para el destinatario (por ejemplo, soporte@empresa.com). El mensaje al destinatario contiene la fecha y la hora, el nombre de nodo del objeto que accionó la alarma y una descripción de la condición de accionamiento. SNMP Traps puede incluir información adicional.
3. Haga clic en Aceptar. El nombre de usuario aparece en la lista Todos los usuarios con Pager.
4. Haga clic en la ficha Directivas y elija el intervalo (como se describió anteriormente en esta sección) si desea especificar un intervalo para la notificación de correo electrónico únicamente.
5. Haga clic en Agregar para incluir el nombre en la lista Acción asignada a usuarios de correo electrónico.
6. Introduzca el nombre de acción, por ejemplo Envíame correo electrónico y haga clic en Aceptar. Aparece la nueva acción Envíame correo electrónico en la lista Contenido de Directorio de acciones.

Cuando una condición de alarma se detecta en una alarma con una acción de correo electrónico asociada, el protocolo de correo envía un mensaje al destinatario en cuestión.

Definición de alarmas

Configuración del perfil predeterminado ‘Configuraciones de Microsoft Exchange’

Para configurar Exchange para notificaciones de correo electrónico, primero instale el protocolo de correo preferido en el mismo sistema en el que está instalado ServerWORKS Manager Console. (Consulte la documentación de instalación del protocolo de correo para obtener detalles. Las instrucciones para aplicaciones de correo específicas no se abarcan en este manual). Cuando ejecute ServerWORKS Manager, también ejecute Microsoft Exchange para recibir la notificación en la consola.

El perfil predeterminado ‘Configuraciones de Microsoft Exchange’ contiene información sobre el inicio de sesión y protocolo de correo. El perfil se requiere para la acción de notificación de correo electrónico.

1. Desde el escritorio de Windows, haga clic con el botón derecho del ratón en el icono Exchange Inbox y elija Propiedades.
2. Elija el botón Show Profiles (Mostrar perfiles). Si ‘Configuraciones de Microsoft Exchange’ aparece en la lista de perfiles y en el campo "When starting MS Exchange, use this profile" (Al iniciar Microsoft Exchange, utilice este perfil), elija Close (Cerrar). Si el perfil no se lista, créelo.
3. Antes de continuar, consulte al administrador del sistema para obtener información sobre el inicio de sesión y el nombre del protocolo de correo (como el nombre de usuario o buzón y si está utilizando Exchange Server, correo Internet u otros servicios de información).
4. Haga clic en el botón Add (Agregar). En el cuadro de diálogo Inbox Setup Wizard (Asistente para la Bandeja de entrada), seleccione la opción "Use the following information services" (Usar los siguientes servicios de información) y elija el protocolo de la lista de servicios de información.
5. Haga clic en el botón Next (Siguiente). En el cuadro de diálogo Profile Name (Nombre del perfil), seleccione ‘Configuraciones de Microsoft Exchange’ (o introduzca el nombre de ‘Configuraciones de Microsoft Exchange’ exactamente si no aparece. Debe utilizar este nombre). Luego vuelva a haga clic en Next (Siguiente).

Definición de alarmas

6. Siga las indicaciones de los cuadros de diálogo restantes. Éstos varían de acuerdo con el servicio de información que seleccionó pero incluirá información sobre el usuario y el protocolo.
7. Continúe siguiendo las indicaciones y elija Finish (Finalizar) en el último cuadro Wizard (Asistente).

El perfil de 'Configuraciones de Microsoft Exchange' se agrega a la lista de perfiles. Seleccione el perfil y elija Close (Cerrar).

Configuración de una acción de inicio de aplicación

La acción de inicio de aplicación puede llamar un archivo por lotes complejo o uno ejecutable sencillo. Por ejemplo, puede crear un archivo BAT con comandos múltiples. Tendrá que determinar la línea de comandos para cualquier procedimiento. A continuación se muestra un ejemplo sencillo.

1. En el cuadro de diálogo Agregar nuevas acciones, elija la ficha Inicio de aplicación.
2. Introduzca el nombre de archivo. Necesita el nombre de ruta completo y la extensión del archivo (por ejemplo, c:\netscape.exe para abrir una ventana de examinador).
3. Seleccione la información sobre la alarma (parámetros) que desea que se transmita a la aplicación que se va a iniciar. La aplicación se debe programar para utilizar los parámetros (por ejemplo, para ver una alerta animada y los parámetros transmitidos en una página HTML).
4. Haga clic en la ficha Directivas y elija el intervalo (como se describió anteriormente en este capítulo) si desea especificar un intervalo sólo para la notificación de inicio de aplicación. Luego haga clic en Aceptar.
5. En el cuadro de diálogo Nombre de acción, introduzca un nombre para la acción (por ejemplo, Avisarme). El nombre aparece en la lista Directorio de acciones.

Cuando una condición de alarma se detecta en una alarma con un inicio de aplicación asociado, se realiza la actividad especificada en la línea de comandos.

Definición de alarmas

Configurar la notificación para capturas de Minimal Health

La plantilla de Minimal Health se asocia los nombres de la acción para capturas de Minimal Health. El valor predeterminado es que ninguna acción esté asignada a los nombres. Si desea la notificación de un mensaje de Minimal Health, puede modificar las propiedades del nombre de acción asignando la elección de la(s) acción(es) para alarmas de Minimal Health siguientes.

- MhHigh
- MhMedium
- MhInformational
- MhLow

Para modificar un nombre de acción de Minimal Health con una acción

1. Elija Herramientas→Configuración de Directorio de acciones.
2. Seleccione un nombre de acción de Minimal Health y haga clic en Propiedades.
3. Seleccione de las páginas del cuadro de diálogo, Pager, Correo electrónico, Inicio de aplicación o Directivas y defina la acción. (Consulte los procedimientos que se presentan en este capítulo para obtener detalles).
4. Cuando todas acciones se definan, elija Aceptar para cerrar el cuadro de diálogo.

Definición de alarmas en clústers y recursos de clúster

Puede definir alarmas en un recurso servidor de clústers de la misma manera en la que define alarmas en otros objetos. Una condición de un recurso o servidor de clústers que los administradores encuentran útil es un mensaje que indica una falla de un servidor a otro. El agente de DIGITAL que controla clústers puede enviar los mensajes de captura siguientes, que indican la transición de control de un servidor a otro.

- Not Current Controller. El servidor que envía esta captura ha perdido el control de un recurso

Definición de alarmas

- **Current Controller.** El servidor que envía esta captura ha ganado el control de un recurso

En un clúster de dos servidores, A y B, puede definir alarmas de las maneras siguientes:

- Defina una captura para Not Current Controller on Server A para indicar que el control de un recurso del servidor A ha fallado con respecto al servidor B.
- Defina una captura para Current Controller on Server B para indicar que el servidor B está en control de un recurso.
- Defina alarmas de captura de Not Current Controller y Current Controller en el mismo recurso para recibir ambos mensajes. Al utilizar este esquema, puede determinar si ha ocurrido una falla de un servidor que no se está ejecutando. (Un servidor que se desactiva no puede enviar una captura de Not Current Controller, pero el servidor que ha asumido el control puede enviar una captura de Current Controller).

Para definir una alarma en un recurso o servidor de clústers

1. Desde ServerWORKS Manager Console, elija Herramientas→Alarm Configuration.
2. Seleccione el servidor en el que se está definiendo la alarma.
3. Elija Archivo→Nueva→Estado de componente.
4. En el cuadro de diálogo Agregar alarmas de nuevo componente, haga clic en la ficha Categoría.
5. De la lista desplegable Categoría de Alarma, elija Cluster Group Status (Estado de grupo de clústers).
6. En la lista Elementos para supervisar, seleccione los recursos de clúster en los que está definiendo las alarmas. Elija de:
 - Todos los grupos de clústers (todos los recursos que se definieron cuando creó el clúster)
 - Cualquiera o todos los grupos de recursos restantes. Los clústers diferentes tendrán selecciones diferentes.

Definición de alarmas

7. Haga clic en la ficha Estados y defina una alarma en los recursos seleccionados. Para mostrar la falla del servidor primario al servidor secundario, seleccione Not Current Controller. Luego haga clic en la flecha derecha para agregar el estado a la lista de estados de alarmas.
8. Haga clic en la ficha de Severidad y seleccione una severidad.
9. Haga clic en la ficha Encuesta y defina los parámetros de encuesta.
10. Haga clic en la ficha Acciones para configurar una notificación para la alarma. Esto es opcional. Consulte la sección anterior para obtener detalles sobre la definición de acciones de notificación.
11. Elija Aceptar.

Supervisión de transiciones

Utilice el Visor de alarmas para vigilar la actividad de transiciones en un clúster. Desde ServerWORKS Manager Console, haga clic en el botón de estado de Visor de alarmas para la severidad que eligió para la alarma Not Current Controller y Current Controller. Si ha ocurrido una transición de control, la alarma aparece en el Visor de alarmas.

Administración desde la consola **6**

ServerWORKS Manager utiliza los componentes siguientes para la administración de redes.

- System Browser para ver datos extensos acerca de servidores DIGITAL, incluyendo datos históricos
- MIB Browser para ver información sobre SNMP y realizar operaciones de SNMP en un objeto
- MIB Profiler, MIB Compiler y MIB Enroller, que trabajan juntos para integrar MIBs en ServerWORKS
- Otras herramientas de segundo plano que completan la capacidad de ServerWORKS Manager

Administración desde la consola

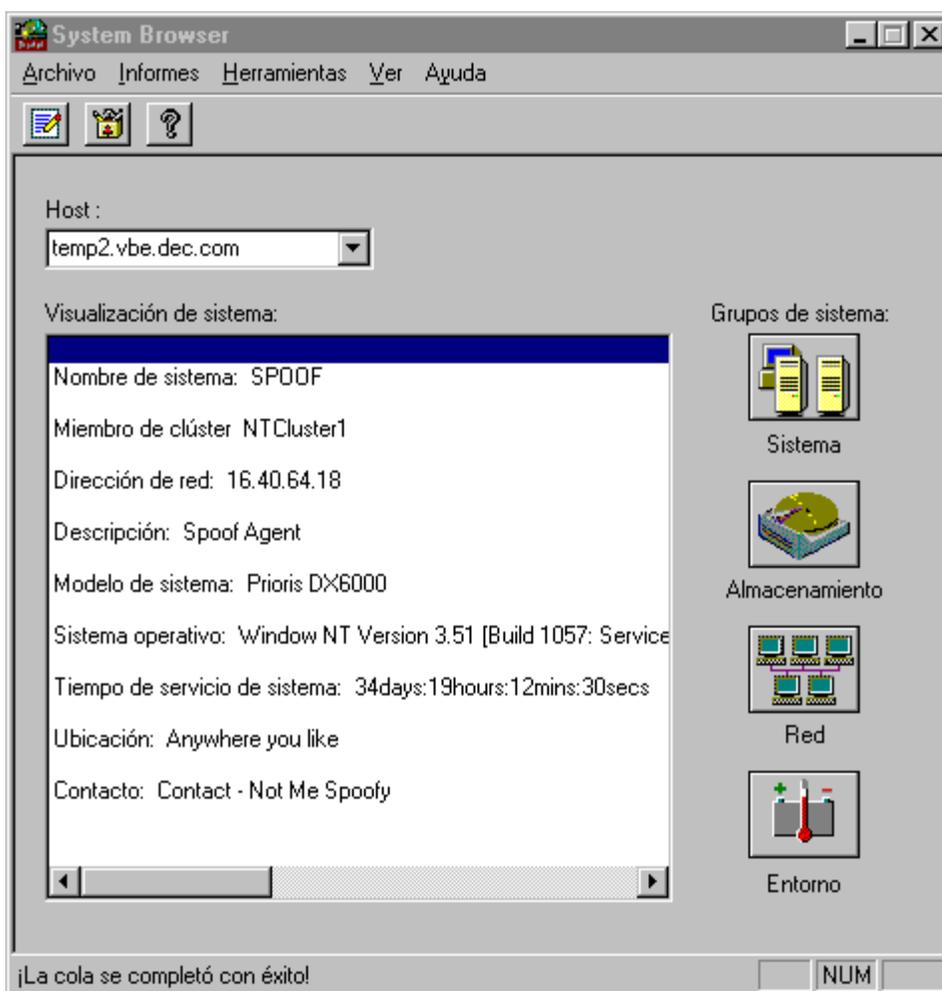
System Browser para hosts DIGITAL

System Browser proporciona información sobre los parámetros estáticos y dinámicos encontrados en los objetos de DIGITAL como servidores, clústers, sistemas de escritorio y dispositivos móviles. System Browser utiliza la información proporcionada por los agentes SNMP de DIGITAL cargados en el servidor, escritorio o sistema móvil.

System Browser muestra:

- La información sobre la configuración del sistema que por lo general no cambia.
- La información actual que se actualiza cada vez que examina un objeto desde System Browser. La Tabla 6-1 muestra el tipo de información encontrada en cada una de las ventanas de System Browser.
- Información histórica que se muestra cuando la información actual no está disponible debido a problemas en la red o el sistema. Esta información se recopiló antes y se guardó utilizando System Browser.
- La información acerca de miembros de clúster y recursos de clúster.
- Datos graficados históricos o dinámicos que muestran ejemplos de uso en discos y procesadores, definen fluctuaciones ambientales y supervisan estadísticas de transmisión de red.

Figura 6-1 Ventana System Browser



Administración desde la consola

Tabla 6-1 Información sobre System Browser

Esta ventana	Muestra esta información
System Browser	Nombre de host Dirección (IP) de red Descripción Ubicación y contacto físicos Modelo y sistema operativo* Longitud del sistema que se ha estado ejecutando (tiempo activo)
Sistema	Información general Dispositivo de E/S Procesador FRU* Clúster (cuando el servidor es un miembro de clúster)*
Almacenamiento	Discos Particiones de disco Sistema de archivos Almacenamiento Memoria* Ranuras de componentes de memoria (SIMMs y DIMMs)*
Red	Interfaz Estadísticas
Ambiente*	Sensores térmicos Sensores de tensión Sistema de enfriamiento (ventiladores)* Fuente de alimentación

*No siempre está presente en todos los sistemas

Visualización de datos de nodos con System Browser

Puede abrir System Browser para ver datos históricos o actuales. Si abre System Browser desde un visor jerárquico o de mapas, System Browser muestra información actual. Si el nodo no se puede alcanzar en la red, System Browser consulta la información histórica si está disponible. En la Figura 6-1 el nodo no está disponible y tiene marcado FUERA DE LINEA.

Cada vez que ve un nodo, el nombre de nodo se agrega a la lista desplegable y se recopilan datos sobre el nodo para cada grupo de sistema que visualiza.

Para lanzar System Browser desde un mapa o un visor

- Haga doble clic en un host DIGITAL de una visualización jerárquica o de mapas o elija Acciones→System Browser. La colección de datos comienza en cada nodo que examina.
Si no se puede acceder al nodo o la red y usted vio el nodo antes, puede seleccionar el nodo de la lista desplegable Host y ver sus datos históricos.

Para ver detalles acerca del servidor o el host

- Haga clic en uno de los botones de Grupos de sistema. (Consulte la Figura 6-1).

Para ver detalles sobre servidores o hosts adicionales a los que puede acceder en la red

Siga uno de estos pasos:

- Introduzca el nombre de host o la dirección IP o seleccione un nodo de la lista desplegable en el campo Host. Luego pulse Intro. En la Figura 6-1, se seleccionó garnet.dec.com de la lista desplegable. También podría introducir garnet o 16.34.112.234. Pero siempre utilice el mismo nombre de nodo cuando acceda a datos en un sistema porque se crea un nuevo archivo para cada nombre.
- Seleccione objetos múltiples del mapa o el visor y haga clic en el icono System Browser de la Barra de herramientas. System Browser se abre con información sobre el primer objeto seleccionado. Los



Administración desde la consola

objetos restantes aparecen en la lista desplegable.

Para ver información acerca de un clúster

1. Haga doble clic en un servidor de clústers desde una vista.
2. Haga clic en la ficha Clústers.

Comparación de sistemas y componentes

Puede utilizar System Browser para ver fuentes de datos múltiples.

- Seleccione un sistema. Luego abra todos los grupos de System Browser para ver todos los aspectos del sistema simultáneamente.
- Seleccione sistemas múltiples. Abra el mismo grupo para cada sistema para compararlos por categoría de información.

Definir números asignados de FRU

Puede cambiar el número asignado de FRU (Field replaceable unit: Unidad reemplazable de campo) en la tarjeta actual de un nodo que muestra información sobre FRU.

Para cambiar el número asignado

1. Desde System Browser, haga clic en la página FRU.
2. Seleccione una tarjeta actual de los componentes de la lista Tipos.
3. En la hilera resaltada, haga clic en la columna Núm. asignado e introduzca el número.
4. Haga clic en Definir núm. asignado.
5. Haga clic en Actualizar.

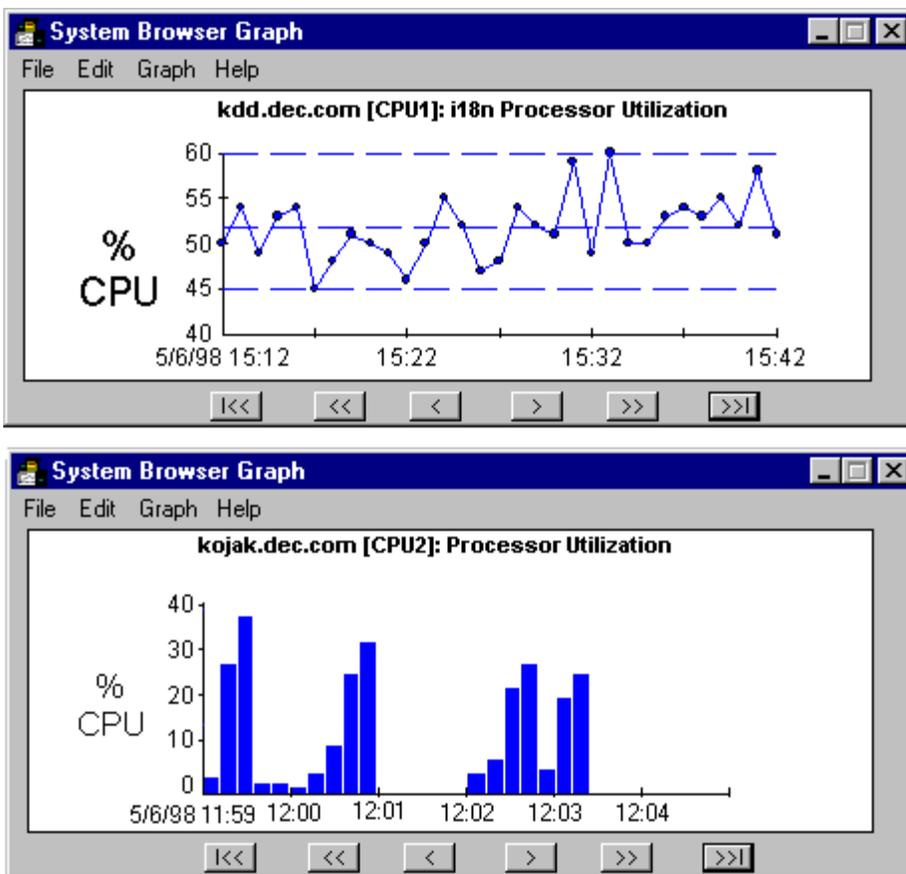
Elaboración de gráficas de la actividad en tiempo real

Puede registrar la actividad como una gráfica en tiempo real para la utilización de CPU, la utilización del sistema de archivos, estadísticas de variables de red y lecturas de los sensores térmico y de tensión y guardar la información como dato histórico. (No todos los sistemas soportan todos los tipos de gráficas). Puede ver datos graficados cuando el nodo está fuera de línea si ha graficado y guardado datos para la variable seleccionada.

Puede elegir entre gráficas de línea y de barras y definir un intervalo de ejemplo. La elaboración de gráficas empieza a guardar datos después del primer ejemplo. La gráfica muestra las horas de inicio y fin y tiene espacios para las horas en las que se no se guardaron los datos graficados. La Figura 6-2 muestra una gráfica de barras y de línea.

Administración desde la consola

Figura 6-2 Gráficas de ServerWORKS



Administración desde la consola

Para graficar información

1. Elija Acciones→System Browser o haga doble clic en un servidor.
2. De la ventana System Browser, elija uno de los botones:
 - Para la utilización del procesador de CPU que registra los modelos de utilización
 - a. Elija Sistema→Procesadores.
 - b. Seleccione una CPU y haga clic en Gráfica.
 - Para la utilización del sistema de archivos (uso del espacio de disco) que lo puedan ayudar a predecir los problemas potenciales del espacio de disco
 - a. Almacenamiento→Sistema de archivos.
 - b. Seleccione un sistema de archivos de la lista y haga clic en Gráfica.
 - Para estadísticas de la interfaz de red que muestran modelos de tráfico o disparidades en la transmisión
 - a. Elija Red→Estadísticas.
 - b. Seleccione una interfaz.
 - c. Seleccione un parámetro de transmisión y haga clic en Gráfica.
 - Para lecturas térmicas y de tensión que revelan fluctuaciones aleatorias o incrementos a largo plazo
 - a. Elija Ambiente→Sensores térmicos o Sensores de tensión
 - b. Seleccione el componente (chasis, fuente de alimentación) y haga clic en Gráfica.
3. Siga uno de estos pasos:
 - Elija Archivo→Cerrar y Guardar para guardar los datos de la gráfica.
 - Elija Archivo→Cerrar para descartar los datos actuales de la gráfica.
 - Elija Archivo→Eliminar y Cerrar para descartar

Administración desde la consola

permanentemente un archivo de gráficas obsoleto o innecesario.

Para cambiar el estilo de la gráfica

1. Elija Edición→Estilo.
2. Seleccione Gráfica de barras o de línea y los atributos para cada estilo.

Para cambiar el intervalo de tiempo y ejemplo

1. Elija Edición→Parámetros.
2. Introduzca el intervalo de ejemplo y el número de puntos de ejemplo.

Recopilación de la historia de un nodo

System Browser crea una carpeta de datos históricos para cada nodo que examina. La carpeta contiene un archivo INI que conserva una lista de los datos registrados de cada uno de los grupos de System Browser que ve. Por ejemplo, garnet.com.ini es el archivo para garnet.com. El archivo INI es un registro completo para un nodo. MIBs que corresponden al nodo proporcionan esta información.

En sesiones posteriores, los datos ya registrados se actualizan y los nuevos datos se agregan a los datos históricos. Si también grafica datos para una variable de nodo, se conserva un archivo de gráficas con los datos graficados guardados para ese parámetro y nodo. Puede importar los archivos de gráficas, que están en formato de tabla que utilizan TAB como carácter de delimitación, en Microsoft Excel.

Puede ver datos históricos cuando un nodo está fuera de línea utilizando el History Viewer si ya ha visto el nodo en línea desde System Browser. Si está viendo datos históricos, verá la etiqueta FUERA DE LINEA junto al nombre del sistema, como en la Figura 6-1.

Cuando el nodo está en línea y la red responde, los datos nuevos se agregan a la gráfica. La gráfica muestra interrupciones entre las recopilaciones de datos con ejemplos en blanco para el periodo de tiempo no registrado.

Administración desde la consola

Para empezar a recopilar datos históricos

1. Elija Acciones→System Browser.
2. Introduzca o seleccione el nombre de nodo.
3. Haga clic en las páginas de Grupos de sistema para los datos que desea recopilar.

Para ver datos históricos en un nodo

1. Desde el escritorio, elija Iniciar→Programas→ ServerWORKS→ History Viewer. System Browser abre y muestra una lista de nodos para los que se han recopilado datos históricos.
2. Seleccione un nodo.

Para recopilar datos de gráficas o ver datos históricos de gráficas

1. Elija Acciones→System Browser. System Browser abre y muestra una lista de nodos para los que se han recopilado datos históricos.
2. Introduzca o seleccione un nodo y haga clic en una página de Grupo de sistema desde la que haya recopilado gráficas.
3. Seleccione el elemento y haga clic en el botón Gráfica. Luego elija una flecha de dirección.

Para ver datos de gráficas	Haga clic en este botón
Retroceder al momento de inicio de la gráfica	
Retroceder una pantalla	
Retroceder el parámetro de ejemplo	
Adelantar desde la hora y fecha más recientes	
Avanzar una pantalla	
Avanzar el parámetro de ejemplo	

Administración desde la consola

MIB Browser para objetos de SNMP

Management Information Base Browser (MIB) (Examinador de base de información de administración) se utiliza para consultar variables GET y modificar variables SET de MIB en objetos que cumplen con SNMP en la red. MIB Browser lista todos los grupos de MIB que se aplican al objeto y las variables de MIB de cada grupo. Por ejemplo, si selecciona un puente, MIB Browser muestra las variables de MIB del puente.

Utilice MIB Browser para realizar las operaciones siguientes:

- Consultar agentes SNMP para realizar una operación GET o recuperar variables de MIB (Management Information Base), tales como el nombre del sistema, la ID del sistema y la hora de actividad para un encaminador, hub o puente desde los grupos estándar de MIB II o cualquier otro MIB almacenado con la base de datos de MIB
- Realizar operaciones SET de SNMP contra uno o más agentes SNMP
- Ver las propiedades de cualquier variable MIB (por ejemplo, el tipo de datos de la variable o el identificador de objeto, acceso en lectura/escritura y descripción)
- Abrir MIB Profiler para modificar o crear perfiles de MIB. Vea "Almacenamiento de MIBs en la base de datos de ServerWORKS" en el Capítulo 7
- Abrir MIB Enroller y MIB Compiler para compilar y almacenar nuevos grupos de MIB en la base de datos de ServerWORKS o modificar grupos existentes. Consulte "Herramientas adicionales" en este capítulo.

Para objetos de SNMP que no sean hosts DIGITAL, MIB Browser es la acción de administración predeterminada para ver el objeto.



Para iniciar MIB Browser

- Seleccione un objeto de un visor y elija Acción→MIB Browser.

Administración de un objeto desde MIB Browser

MIB Browser le permite ver información por grupo y variable de MIB. La Figura 6-3 ilustra la ventana MIB Browser. Cada uno de los botones de comando muestra información sobre el grupo de MIB en MIB II (RFC1213). Las variables de MIB contenidas en el grupo aparecen en la lista Variable.

Modificación de variables

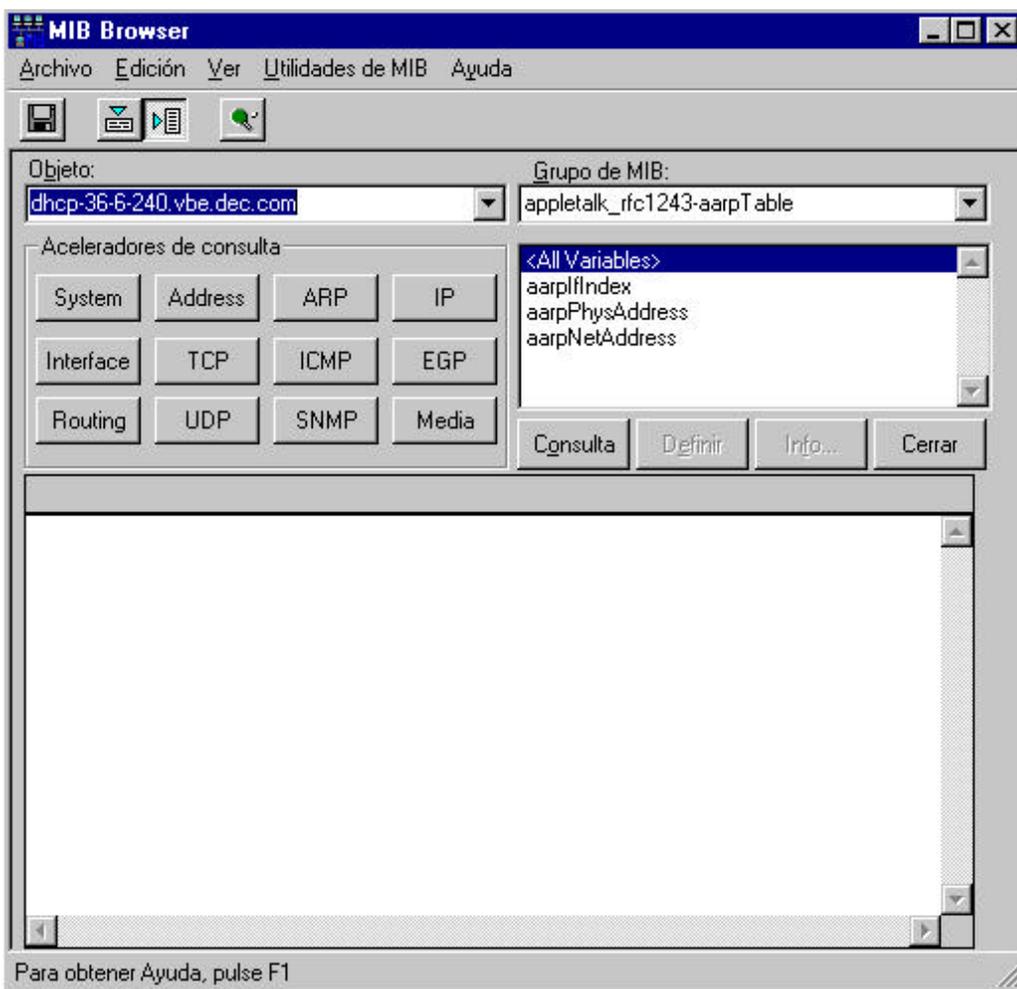
Puede utilizar MIB Browser para modificar variables. Algunas de las variables de MIB son de lectura/escritura. Una variable de lectura/escritura es una variable que puede modificar porque puede escribir o dar un nuevo valor, así como leerlo. Por ejemplo, sysLocation es una variable de lectura/escritura, lo que significa que puede introducir una nueva ubicación cuando el sistema se desplaza. El cambio se realiza en MIB. Otros usuarios que utilizan otro sistema de administración de redes también pueden cambiar las variables de lectura/escritura. Puede ver qué variables son de lectura/escritura utilizando MIB Enroller.

Para cambiar un valor de la variable desde MIB Browser

1. Seleccione la variable. Si el botón Definir está activo cuando se selecciona una variable, puede cambiar el valor.
2. Edite la variable y elija Aceptar.

Administración desde la consola

Figura 6-3 Ventana MIB Browser



Para ver la descripción de una variable

- Seleccione la variable de la lista de variables del grupo MIB y haga clic en el botón Info.

Para leer un MIB

1. Seleccione el objeto de un visor.
2. Elija Herramientas→MIB Enroller→MIB Compiler.
3. En MIB Compiler, elija Archivo→Abrir.
4. Seleccione el MIB y haga clic en Aceptar. MIB aparece en la ventana.

Utilización de los aceleradores de consulta

Los botones de consulta del MIB Browser corresponden a grupos de variables de MIB para el agente de MIB II. Cuando hace clic en un botón de consulta, está realizando una operación GET de SNMP, en el grupo de variables.

Si utiliza otro MIB en un objeto, puede cambiar un botón para consultar un grupo de variables desde un MIB diferente.

Para cambiar un botón de consulta

1. Elija Edición→Personalizar Aceleradores de consulta.
2. Seleccione el botón que desea cambiar.
3. En el campo Etiqueta de acelerador de consulta, introduzca una etiqueta para el botón.
4. En Grupo de MIB asociado, seleccione un grupo de MIB que sea adecuado para los tipos de objeto que supervisa, por ejemplo, servidores Compaq.
5. Haga clic en Aceptar.
6. Haga clic en Cerrar en el cuadro de diálogo Personalizar Aceleradores de consulta.

Administración desde la consola

Para ver todas variables en el grupo de consulta al mismo tiempo

- Elija All Variables (Todas las variables) de la lista de grupo de MIB y elija Ver→Visualización vertical Y desplácese por la lista.

Para ver todos los casos de una variable

- Elija Ver→Horizontal. Seleccione la variable. Por ejemplo, si está comprobando el número de interfaces, la orientación horizontal los mostrará todos.

Para ordenar la información sobre la variable alfabéticamente

- Elija Ver→Ordenar visualización.

Visualización de información sobre el clúster desde MIB Browser

MIB Browser muestra información acerca de servidores y recursos que forman parte de un clúster, que puede incluir los tipos de clúster, proveedor, versión de software, estado, recursos y miembros del grupo de clústers de NT, direcciones IP de miembros del clúster, alias para el clúster, OID de sistema, proveedor y versión. La información viene de las variables de los MIBs del clúster.

Para utilizar MIB Browser para ver datos del clúster

1. Elija Acciones→MIB Browser.
2. Seleccione una variable o un grupo de MIB en el grupo. Los MIBs de clúster tienen los prefijos SrvClu, SrvNTC y ntcmtg.
3. Introduzca el nombre de clúster o un nombre de servidor de clústers y pulse RETORNO.

MIF Browser

Management Information Format (MIF) Browser (Examinador de formato de información sobre administración) se utiliza de manera similar que MIB Browser para examinar MIFs proporcionados por el sistema. Se utiliza en sistemas de escritorio y móviles y también se puede utilizar en sistemas que ejecutan Windows NT o Windows 95. Con la capa de servicio DMI ejecutándose en el sistema que se va a examinar, puede ver un inventario de los diferentes software, hardware, parámetros y configuraciones del sistema. Esta información puede transmitirse a Microsoft System Management Server (SMS) a través del programa MIF Maker que se proporciona con ClientWORKS.

Se accede a MIF Browser con el icono de la Barra de herramientas y desde el menú. Para obtener detalles completos, consulte el manual *ClientWORKS Network Administrator's Guide* y la ayuda en línea de ClientWORKS.

MIB Compiler

Antes de que se pueda utilizar un tipo de objeto en ServerWORKS Manager Console, los grupos de MIB asociados al objeto se deben almacenar en la base de datos de ServerWORKS. MIB Compiler se utiliza para cargar un nuevo grupo de MIB y definiciones de variables MIB en la base de datos. Para obtener mayor información, consulte la sección "Creación de tipos de objeto y perfiles personalizados" en el Capítulo 7 para obtener detalles sobre la compilación y el almacenamiento de MIBs.

También puede leer un MIB compilado en MIB Compiler.

Para leer un MIB

1. Elija Acciones→MIB Enroller.
2. Elija Compilar→MIB Compiler.
3. Elija Archivo→Abrir y seleccione el MIB del cuadro de diálogo Elegir archivo de visualización de MIB.
4. Haga clic en Aceptar.

Administración desde la consola

MIB Profiler

MIB Profiler se utiliza para asociar MIBs a un tipo de objeto. Por ejemplo, un tipo de objeto de servidor DIGITAL tiene determinados MIBs que se han definido para asociarlos a dicho tipo de objeto.

Si los MIBs asociados a un objeto necesitan modificarse, esto se realiza utilizando MIB Profiler. MIB Profiler

- Asigna grupos de MIB a un tipo de objeto.
- Elimina (cancela la asociación) grupos de MIB desde un tipo de objeto.

MIB Profiler guarda las asignaciones de grupos de MIB en la base de datos para que puedan ser referenciadas por MIB Browser. Por ejemplo, después de seleccionar un objeto de SNMP determinado, MIB Browser obtiene el tipo de objeto y utiliza esta información para ver todos los grupos de MIB asociados desde la base de datos. Sólo los grupos de MIB aplicables se listan en el campo Grupos de MIB de la ventana MIB Browser. A continuación, se puede elegir ya sea un grupo o una o más variables para realizar operaciones GET y SET contra un objeto específico.

Consulte el Capítulo 7, “Obtención de los datos deseados” para aprender más sobre el uso de MIB Profiler.

MIB Enroller

MIB Enroller es una fuente de información de MIB. MIB Enroller muestra un grupo y sus variables, el identificador de objetos para la variable, tipo de datos y acceso en lectura/escritura. Los administradores confirmados pueden modificar una variable de MIB desde MIB Enroller.

Tareas de segundo plano

ServerWORKS Manager opera las tareas de segundo plano para recopilar y distribuir información sobre la red. Las tareas de segundo plano aparecen en la bandeja de sistema cuando se están ejecutando. Haga clic con el botón

Administración desde la consola

derecho del ratón en un icono para ver un menú.

Ping Server



ServerWORKS Manager Console tiene la capacidad de comunicarse con dispositivos o realizar operaciones “ping” de la red. Ping Server examina la red para ver si un dispositivo está activado, desactivado o no responde, utilizando una petición de ICMP y esperando una respuesta. Seleccione un dispositivo y realice ping con el botón de la Barra de herramientas. Ping Server observa esta actividad y el tiempo que tarda en hacer un viaje redondo de la consola al dispositivo y viceversa.

Poller

Poller solicita periódicamente información sobre estado (activado, desactivado, o ninguna respuesta) desde los objetos de red especificados y sus interfaces. Los objetos que se pueden encuestar son todas las interfaces que pertenecen a los objetos de red que tienen un agente SNMP o que soportan el protocolo IP (por ejemplo, encaminadores y nodos finales).

De forma predeterminada, Poller se inicia automáticamente después que se realiza un descubrimiento con IP Discovery. Utilizando los parámetros predeterminados, todos los objetos listados en la base de datos son encuestados en el mismo intervalo.

La encuesta también se puede realizar sobre un grupo definido por el usuario. Un grupo puede constar de una colección de objetos similares que se encuestarán en los mismos intervalos.

Data Collector, Event Logger e Event Dispatcher



Data Collector, Event Dispatcher e Event Logger se deben estar ejecutando para que la consola reciba alarmas.



Event Dispatcher y Event Logger se deben estar ejecutando para recibir notificaciones de alarma o para ejecutar automáticamente un archivo de

Administración desde la consola



comandos cuando se alcanza un umbral de alarma.

Si estas tres utilidades no están colocadas en el grupo de inicio de Windows NT o Windows 95, Event Dispatcher y Event Logger se inician automáticamente cuando se inicia ServerWORKS Manager Console.

Compruebe la bandeja de sistema en el extremo inferior derecho de la ventana para ver si se están ejecutando las tareas de ServerWORKS.

Obtención de los datos deseados **7**

IP Discovery con ServerWORKS presenta volúmenes de información sobre todos los objetos de la red. ServerWORKS le permite manipular datos y personalizar visores. Este capítulo explica cómo personalizar ServerWORKS para realizar las tareas siguientes:

- Adquirir datos que se basan en los requisitos de la red
- Presentar los datos de la manera que desea

Obtención de los datos deseados

Opciones personalizables para un visor o un mapa

Puede personalizar listas y visores de mapas para reunir requisitos específicos. Se pueden crear diferentes visores para diferentes propósitos. Por ejemplo, un visor podría contener todos los servidores de una empresa, mientras que otro puede mostrar archivos y aplicaciones en servidores múltiples, mientras que un tercero puede mostrar la topología de TCP/IP. Cualquier tipo de información puede agruparse en un visor, sin tener en cuenta la fuente o el contenido. ServerWORKS Explorer es un buen punto inicial para personalizar visores porque es una fuente de objetos para copiar en otros visores.

Una vez que crea un visor jerárquico o de mapas, puede modificarlo manualmente o ejecutar un descubrimiento posterior para actualizarlo.

Para cambiar el aspecto y el comportamiento de la ventana

1. Haga clic en un mapa para seleccionarlo.
2. Elija Archivo→Propiedades de visor.
3. Seleccione las preferencias para los parámetros siguientes en el cuadro de diálogo de Propiedades de Visor de mapas:
 - Elija un archivo opcional de segundo plano. Por ejemplo, seleccione un mapa de país y arrastre servidores en sus ubicaciones geográficas.
 - Elija una escala predeterminada para abrir un mapa.
 - Haga clic en Configurar. Luego seleccione los valores predeterminado para minimizar, cerrar o guardar mapas automáticamente y ocultar mapas de bits de nodo cuando el mapa se ajuste a una escala menor que el porcentaje especificado.
 - En el cuadro de diálogo Configurar, haga clic en Colores. Luego cambie los colores en los elementos del mapa.

Para obtener información básica rápidamente

- Haga doble clic en un objeto de la red para ver el examinador asociado. ServerWORKS Manager tiene objetos de servidores y red con System Browser, MIB Browser y MIF Browser.

Obtención de los datos deseados

Para crear un mapa de red lógico

Es posible que desee administrar objetos de red particulares en un mapa como un grupo porque tienen uso similar o para propósitos de la empresa. Puede aislarlos de manera sencilla. Sólo arrastre los objetos de red de mapa a mapa.

Para ver estadísticas vitales sobre un mapa

Puede agregar una etiqueta a un objeto de red para ver información específica sobre el mapa. Por ejemplo, es posible que desee ver el nombre, la dirección IP y la máscara de red de un objeto.

1. Desde el menú Herramientas, elija Opciones→Visualizar objetos.
2. Desde la lista Ocultos, seleccione la información que desea ver en una etiqueta.
3. Haga clic en Mostrar. Si desea poner las etiquetas en un orden específico, seleccione cada etiqueta y elija Delante o Detrás hasta que se coloquen las etiquetas.
4. Haga clic en Cerrar.

Para modificar los menús para el trabajo que hace

Puede editar el menú Herramientas para agregar o eliminar programas. Por ejemplo, puede crear un comando de menú que ejecute un archivo por lotes o inicie una aplicación.

1. Desde el menú Herramientas, elija Opciones→Herramientas.
2. Siga uno de estos pasos:
 - Haga clic en Agregar para agregar otra aplicación a la lista Herramientas. Introduzca el nombre de la herramienta (por ejemplo Bloc de notas) y la Ruta (por ejemplo, c:\windows\notepad.exe) y haga clic en Aceptar.
 - Seleccione una aplicación y haga clic en Suprimir para eliminar la aplicación.
 - Seleccione una aplicación y haga clic en Cambiar para modificar el nombre o la ruta de visualización de la herramienta.

Obtención de los datos deseados

3. Haga clic en Cerrar.

Para administrar objetos de red como un grupo

Un grupo es una colección de servidores u objetos de SNMP en los que puede realizar las operaciones de SNMP. Puede seleccionar un grupo lógico de objetos de red y aplicarles las mismas alarmas y opciones.

Primero, cree el grupo.

1. Desde un visor de mapas, seleccione el(los) objeto(s) realizando uno de los pasos siguientes:
 - Mantenga pulsada la tecla CTRL y haga clic en cada objeto que desee agregar al grupo.
 - Haga clic y arrastre por el mapa para dibujar un rectángulo de selección alrededor de los objetos que desea agregar al grupo.
2. Desde el menú Herramientas, elija Administración de grupos.
3. Siga uno de estos pasos:
4. Haga clic en Agregar grupo para crear un nuevo grupo que contenga los objetos seleccionados. Introduzca un nombre de grupo, propiedades de encuesta y el nombre de comunidad para operaciones Get y Set de SNMP en el grupo de Propiedades de grupo.
5. Seleccione uno de los grupos existentes. Copie sus propiedades de encuesta y el nombre de comunidad en el nuevo grupo y modifíquelos como sea necesario.
6. Seleccione de Objetos no en el grupo y haga clic en Agregar para colocarlos en la lista Objetos en el grupo. Para suprimir objetos del grupo, selecciónelos y haga clic en Suprimir.
7. Haga clic en Aceptar.

Iniciar con contexto

Los proveedores individuales de objetos que cumplen con SNMP pueden ofrecer herramientas adaptadas para ver sus propias propiedades del objeto e información. Por ejemplo, Compaq ofrece Insight Manager para ver servidores Compaq.

Una mejor manera de utilizar estas aplicaciones es iniciarlas desde la consola *con contexto*. Por ejemplo, cuando inicia Insight Manager con contexto, se abre con los datos para un objeto Compaq que haya seleccionado en ServerWORKS.

Para configurar una aplicación para que se inicie con el contexto, debe realizar los pasos siguientes:

- Configure la aplicación para asociarla con el tipo de objeto
- Especifique la aplicación como la acción predeterminada para el tipo de objeto

En los procedimientos siguientes, Insight Manager y el tipo de objeto Server.Compaq se utilizan como ejemplos.

Para configurar la aplicación

1. Desde la consola, elija Herramientas→Iniciar aplicación.
2. En el cuadro de diálogo Configurar Inicio de aplicación, seleccione o introduzca la información siguiente:
 - En el campo Objeto, seleccione el tipo de objeto (por ejemplo Server.Compaq).
 - En el campo Nombre de opción de menú, introduzca el nombre para la opción de menú (por ejemplo, Insight Manager).
 - En el campo Ruta de aplicación, haga clic en el botón para examinar y busque la aplicación. Asegúrese de utilizar la ruta completa y el espaciado exacto (por ejemplo: “c: \Archivos de programa\Compaq\Insight Manager\cim. exe”).
 - En el campo del botón de Barra de herramientas, elija cualquier mapa de bits de 16x16 píxeles.

Obtención de los datos deseados



3. En el grupo Configuración de línea de comandos de la aplicación del cuadro de diálogo, introduzca el comando que iniciará la aplicación. Siempre utilice el espaciado exacto y haga corresponder mayúsculas y minúsculas. Para iniciar Insight Manager, utilice la línea de comandos siguiente:

```
cim.exe -ObjIPAddress =<Internet Address>
```

Tiene la opción de seleccionar las declaraciones para la línea de comandos. La lista de selección de Parámetros de la línea de comandos permite elegir de parámetros que se utilizan comúnmente, que se agregan al campo Parámetros y modificadores. Si la línea de comandos incluye varios comandos, seleccione Permitir objetos múltiples e introduzca un tipo de delimitador.

4. Elija Agregar para colocar el nombre de menú en el menú Acciones y agregar el mapa de bits como un botón de la Barra de herramientas.
5. Elija Cerrar.

Para especificar la aplicación como la acción predeterminada

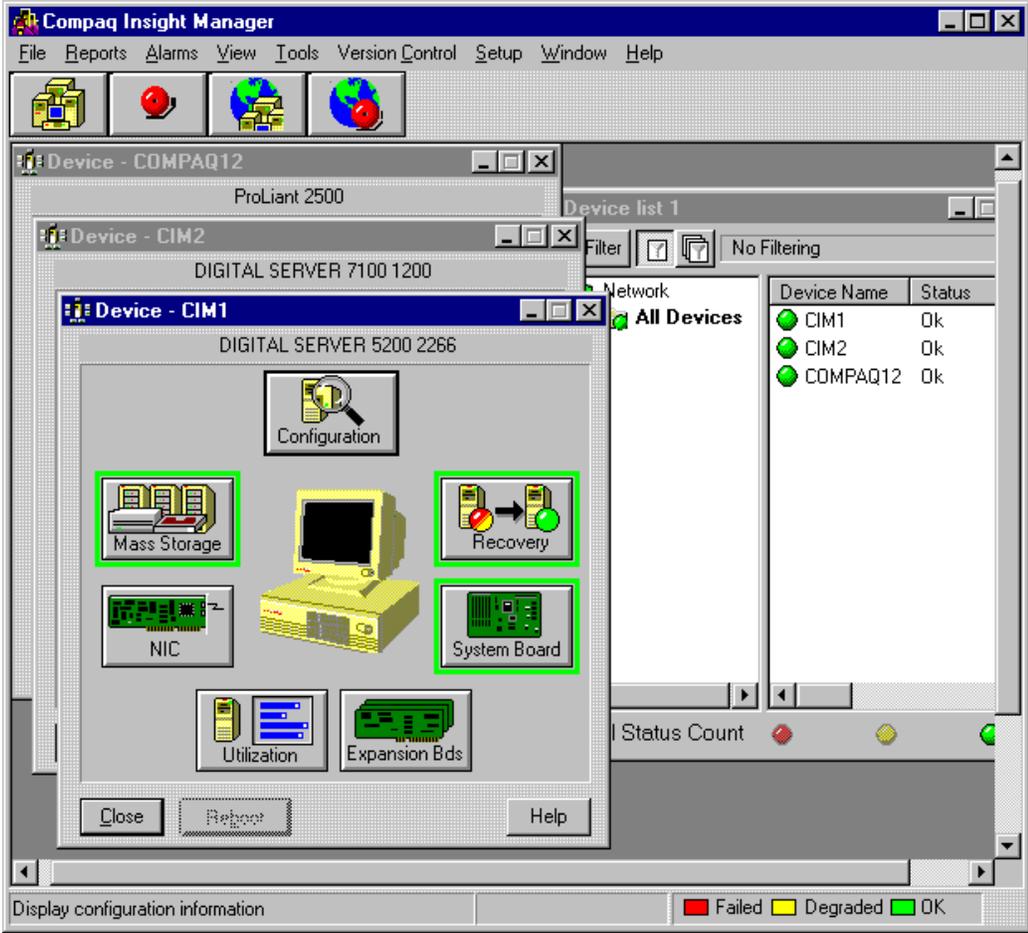
1. Elija Herramientas→Opciones.
2. En el cuadro de diálogo Opciones, haga clic en la página Acciones predeterminadas.
3. De la lista de objetos, seleccione el tipo de objeto.
4. De la lista Acción, seleccione la aplicación, en este caso, Insight Manager.
5. Elija Cerrar.

Para abrir la aplicación con el contexto

Desde un mapa de IP Discovery o un visor jerárquico, haga doble clic en un servidor Compaq. La Figura 7-1 ilustra un servidor Compaq como se ve a través de Insight Manager e iniciado desde un mapa de descubrimiento de ServerWORKS.

Obtención de los datos deseados

Figura 7-1 Insight Manager iniciado desde ServerWORKS Manager Console



Obtención de los datos deseados

Descubrimiento y administración de impresoras

Puede crear mapas o visores arborescentes de un tipo de objeto. Por ejemplo, es posible que desee supervisar impresoras, que son propensas a problemas de mantenimiento. ServerWORKS reconoce los identificadores de objetos del sistema para impresoras DIGITAL, Hewlett-Packard y Lexmark.

Para crear un mapa de impresoras

1. Desde la ventana de consola, elija Archivo→Nuevo visor y el visor jerárquico o de mapas.
2. Introduzca un nombre de mapa en el cuadro de diálogo Nuevo Visor. Un mapa vacío se abre con la Paleta.
3. Elija Acciones→Descubrir objetos IP.
4. Especifique la red y máscara de red y elija Siguiente.
5. Especifique la comunidad que se va a descubrir.
6. En el cuadro de diálogo Tipos para descubrir, seleccione los tipos de impresora y elija Siguiente.
7. En el cuadro de diálogo Opciones de IP Discovery, elija el visor y haga clic en Finalizar.
8. Elija Sí o No para indicar si desea ver el informe de descubrimiento.
9. Elija Sí o No para agregar nuevos objetos al visor actual.

Uso de máscaras de red para refinar descubrimientos

Si está familiarizado con redes, el direccionamiento de IP y el uso de máscaras de red, puede utilizar otras máscaras de red para limitar un descubrimiento. En un descubrimiento, la consola consulta subredes con dirección IP para una lista de sus nodos. Una dirección IP se compone de cuatro números, de 1 a 255, separados con decimales (puntos). La dirección 16.151.24.36 es un ejemplo. La dirección corresponde a cuatro octetos en formato binario. Una máscara de red identifica qué partes de una dirección IP especifican la red y cuáles especifican las partes del host. IP Discovery utiliza la combinación de la dirección IP y la máscara de red para buscar los nodos que están conectados a la red especificada.

La máscara de red predeterminada es 255.255.255.0 para un descubrimiento. Por ejemplo, si utiliza la dirección de red 16.151.24.0, el uso de la máscara de red 255.255.255.0, la máscara de red oculta los tres primeros números de la dirección e intenta descubrir todos los nodos de la parte host, hasta 254 nodos.

Utilice una máscara de red de un solo nodo para limitar un descubrimiento a un solo objeto de red (por ejemplo, uno que haya insertado manualmente). Para el nodo con la dirección 16.151.24.36, utilice la dirección de nodo exacta con la máscara de red 255.255.255.254. Esta máscara de red encuentra hasta dos nodos— 16.151.24.36 y 16.151.124.37, el nodo dirigido de manera consecutiva— debido a la interpretación de la dirección por IP Discovery.

Uso de colecciones y dominios para verificaciones de estado

En un descubrimiento, ServerWORKS encuentra los dominios de hosts y clúster. ServerWORKS muestra clústers y dominios de host por lo que puede ir hacia abajo para ver los miembros de clúster o nodos. Puede aplicar el mismo concepto si desea juntar objetos múltiples en un subconjunto llamado una colección.



Nota: Una colección o un dominio no es un grupo de SNMP, aunque los objetos de una colección o un dominio también se puedan encontrar en un grupo de SNMP. Un dominio en una vista no tiene relación con

Obtención de los datos deseados

un dominio de Windows NT.

Para crear una colección

1. Elija Edición→Insertar.
2. Haga clic en Colección e introduzca un nombre para la colección.
3. Abra una vista de lista y arrastre objetos del visor a la colección.

Para crear un dominio

1. Elija Edición→Insertar.
2. Haga clic en Dominio del cuadro de diálogo Insertar.
3. Introduzca un nombre de pantalla y elija el tipo de objeto en el dominio. Por ejemplo, para crear un dominio de clúster, elija Clúster.
4. Abra una vista y arrastre los objetos al dominio. Para un clúster, incluya a los miembros y recursos del clúster.

Para ver el contenido de una colección o dominio de host

- Haga doble clic en el icono de dominio. El contenido se abre en un mapa separado, temporal y presentado en forma de mosaico.

Realización de encuestas efectiva

La encuesta consume los recursos de la red si la frecuencia de encuesta es demasiado alta o la base del objeto que se está encuestando es demasiado amplia. La personalización de la encuesta le permite enfocarse en tan pocos o tantos objetos como desee encuestando el objeto como un grupo. El valor predeterminado es encuestar todos los objetos descubiertos e insertados.

Para encuestar por grupos, realice las tareas siguientes:

Obtención de los datos deseados

- Configure un grupo de encuesta. Puede iniciar con cualquiera de los dos grupos llamados Critical y Non-Critical que son establecidos por ServerWORKS o puede crear su propio grupo. Cada grupo tiene su propio periodo de tiempo de espera, número de reintentos e intervalos de encuesta. Cada grupo pertenece a una comunidad para la autenticación.
- Adapte los parámetros de encuesta.

Creación de un grupo de encuesta

1. Elija Herramientas→Administración de grupos.
2. En el cuadro de diálogo Administración de grupo de SNMP, elija Agregar grupo.
3. En el cuadro de diálogo Agregar grupo de encuesta
 - En el campo Nombre de grupo, introduzca un nombre nuevo.
 - En el campo Propiedades de grupo, introduzca un Reintento, Tiempo de espera e Intervalo. El Tiempo de espera y el Intervalo se miden en segundos. Como un ejemplo, el intervalo del grupo Critical es 60 segundos (un minuto) y el Non-Critical es 300 segundos (cinco minutos).
 - Introduzca el nombre de comunidad o utilice Public.
 - Elija Aceptar.
4. En el cuadro de diálogo de Administración de Grupo de SNMP, seleccione el nuevo grupo Nombre de grupo.
 - Las Propiedades de grupo se especificaron cuando creó el grupo. Para cambiar una propiedad, selecciónela e introduzca un nuevo valor.
 - Utilice Public como la Comunidad Set y Comunidad Get, a menos que haya creado otros nombres de comunidad.
 - En la lista Objetos no en el grupo, utilice CTRL+Clic para seleccionar miembros del grupo. Luego haga clic en Agregar.
5. Cuando todos miembros estén seleccionados, haga clic en Aceptar.

Obtención de los datos deseados

Definición de parámetros de encuesta de grupo

Pare Poller para volver a definir los parámetros de un grupo o para activar la encuesta de un nuevo grupo. Pare el Poller después de abrir la ventana de Poller.

Para abrir Poller

- Haga clic en el botón de la Barra de tareas de Poller o elija Herramientas→Poller.

Para parar la encuesta

- En la ventana de Poller, haga clic en Parar encuesta.

Para activar un grupo y definir parámetros de grupo

1. En la ventana de Poller en la columna Activar, haga clic en la casilla en la hilera de grupo. Se activa la casilla y el color de fondo cambia a verde. (Los parámetros de la frecuencia de encuesta se definieron cuando creó o modificó el grupo).
2. Elija las Opciones→Definir parámetros de encuesta. Defina los valores para los elementos siguientes:
 - Encuestas máximas pendientes a interfaces: Introduzca el número de interfaces que Poller puede colocar en la cola para encuestarlas en un momento dado.
 - Número máximo de sucesos: El número de operaciones Get y Set de SNMP, pings, mensajes de Event Logger y alarmas de estado que se pueden enviar por segundo.
3. Elija Aceptar.
4. En la ventana de Poller, elija las Opciones→Visualización de Poller. (Si el Poller está desactivado, no aparece ninguna salida en el campo). Elija el botón Opciones y haga clic en los tipos de información que desea de la encuesta. Haga clic en Aceptar para cerrar el cuadro de diálogo Visualización de Poller.
5. En la ventana de Poller, haga clic en Iniciar encuesta para encuestar los grupos seleccionados.

Visualización de información encuestada

Puede ver segmentos pequeños de información encuestada desde el cuadro de diálogo Visualización de Poller (como se describió en la sección anterior). Utilice el registro de Poller para ver el tiempo excesivo de encuesta e imprimir el archivo poller.log.

Para utilizar el archivo poller.log

- Del Explorador de Windows o Mi Computadora, haga doble clic en registro de Poller que se encuentra en,

```
\Archivos de  
programas\Digital\SWMgr\Database\poller.log
```

Cambio de variables desde propiedades de objeto

Las propiedades combinan varias actividades en un cuadro de diálogo. Las propiedades le dan una idea general del objeto y le permiten modificarlo, que es una operación Set de SNMP en el objeto.

Utilice Propiedades para ver detalles:

- Nombre de objeto, dirección IP, dirección MAC y tipo de objeto. Si conoce el nombre o la dirección IP, ServerWORKS encuentra el otro. Haga clic en Obtener direc. para encontrar la dirección IP o haga clic en Obtener nombre para encontrar el nombre de dispositivo.
- La persona de contacto responsable del objeto y los comentarios (por ejemplo, la ubicación) en la descripción del objeto.
- El destino de la captura si está configurado.
- Grupos a los que pertenece el objeto.
- Aplicaciones de terceros asociadas al objeto (por ejemplo, RSM o StorageWorks Command Console).

Utilice Propiedades para modificar la configuración de la red:

- Cambie el nombre global que se utiliza para la resolución del nombre

Obtención de los datos deseados

- Modifique la información de encuesta o el protocolo de encuesta
- Cambie el tipo de objeto.

Para ver y modificar las propiedades

1. Haga clic en un objeto en una vista de mapa o de lista.
2. Desde el menú, elija Acciones→Propiedades.
3. Modifique los campos editables.
4. Haga clic en Aceptar para cerrar el cuadro de diálogo Propiedades.

Trabajo con la base de datos de ServerWORKS Manager

La base de datos de ServerWORKS Manager es PCMGR.mdb. Es una base de datos de Access de Microsoft 97 que puede ver en Access. La base de datos se instala en el subdirectorio llamado `database` del kit de ServerWORKS Manager Console. Si elige el directorio predeterminado en la instalación, la ubicación es:

`/Archivos de programas/DIGITAL/SWMgr/database/PCMGR.mdb`

La base de datos contiene toda la información sobre objetos descubiertos en la red, información sobre alarmas y configuración de alarmas y datos de sucesos.

Si está familiarizado con Access y la estructura de la base de datos, puede modificar registros en la base de datos para crear informes de consulta, utilizar archivos de comandos o realizar operaciones de SNMP especializadas. La información de las tablas puede verse de manera más sencilla en los registros de la tabla de bases de datos que en los archivos de MIB.

La lista siguiente describe las tablas de bases de datos a las que más se accede:

Tabla 7-1 Registros de tabla de bases de datos de Access

Esta tabla	Contiene registros sobre
APPL_GR	Todas las aplicaciones de terceros. Existe un registro para cada aplicación integrada.
EVT_LOG	La tabla de registros de alarmas. Todas las alarmas, sucesos, IDs de objeto y mensajes asociados a cada suceso están almacenados ahí.
MIB_CLAS	El nombre de clase de MIB y el grupo al que pertenece MIB, para todos los MIBs compilados en la base de datos.
MIB_DESC	Una descripción de cada variable de MIB.
MIB_NAME	Nombres de los grupos de MIB.
MIB_PROF	Tipo de objeto y perfil de subtipo para cada MIB.
MIB_TABL	La ID de la variable de MIB interna para todos los grupos de MIB que estén compilados en ServerWORKS. La ID es útil para unir esta tabla a otras tablas.
OBJ_DEF	Nombre real y el intervalo de encuesta para cada máquina.
OBJ_IP	Información sobre el nombre global (incluyendo la dirección IP, dirección o subred alterna y máscara de red) de cada máquina.
OBJ_SNMP	Nombres de comunidades de SNMP.
TRAP_ENT	Definiciones de capturas y OID de empresa para todos los MIBs compilados en la base de datos.



Nota: La base de datos de ServerWORKS V4.0 es una base de datos de Access 97. Si ejecuta Access 95, puede seguir utilizando la base de datos de ServerWORKS V3.x. Sin embargo, si piensa utilizar archivos de comandos para crear informes de Access o para modificar la base de datos, debe utilizar Access 97 y seguir las instrucciones de Microsoft para convertir la base de datos al formato Access 97. Las bases de datos de V2.x se deben convertir después de instalar ServerWORKS Manager V3.2 y después utilizar Access 97 para convertirlas al formato ServerWORKS Manager V4.0.

Obtención de los datos deseados

La tabla siguiente lista los prefijos que se utilizan para nombrar las tablas de bases de datos.

Tabla 7-2 Prefijos de las tablas de bases de datos

Prefijo	Información sobre las tablas
ALM	Configuración de alarmas
APPL	Integración de aplicaciones de terceros
AUTO	Información sobre IP Discovery
COL	Información sobre Data Collector
DB	Información sobre la base de datos de ServerWORKS
EVT	Datos del registro de sucesos
GR	Información sobre grupos
LOG	Datos del registro de sucesos
LTBL	Reservado para uso futuro
MIB	Información sobre la variable de MIB II
NMDB	Contadores máximos para campos de la base de datos
NOTF	Información sobre notificación
OBJ	Información sobre el tipo de objeto que utiliza ServerWORKS
POD	Reservado para uso futuro
SUBT	Información sobre el subtipo de objeto
SYS	Asignación de SYSOID e información sobre subtipo para variables de MIB II
TRAP	Información sobre capturas
TYPE	Información sobre tipo de objeto
USR	Información sobre usuario
VIEW	Información sobre visores jerárquicos y de mapas
VWER	Información sobre el visor interno

Utilización de DB Utility

DB Utility realiza varias tareas de mantenimiento de la base de datos. Utiliza DB Utility en las situaciones siguientes:

- Si sospecha que la base de datos o una parte de ésta (por ejemplo, una tabla) está dañada.
- Si desea borrar una tabla y volver a empezar. Por ejemplo, si desea cambiar los niveles en todas las alarmas de umbral. (El borrado elimina todo en la tabla seleccionada, por eso asegúrese de que desea volver a crear la información en ServerWORKS Manager).
- Si desea modificar la tabla de registro de alarmas. Por ejemplo, si definió una alarma "falsa" que envió varios mensajes para una condición de no alarma y desea borrar el registro de entradas excesivas. También puede cambiar el tamaño de la tabla de registro (el número de líneas).

Cierre ServerWORKS Manager Console, incluyendo las tareas de fondo, antes de iniciar DB Utility.

Para abrir DB Utility

1. Del menú Inicio, elija Programas→ServerWORKS Manager Console→ServerWORKS DB Utility.
2. Siga uno de estos pasos:
 - En el grupo Tablas de bases de datos para borrar, seleccione una tabla y haga clic en Inicializar.
 - En la tabla Registro de alarmas, introduzca las líneas máximas que desea en la tabla (hasta 10 000, pero observe que 10 000 entradas de registro consumen espacio en el disco y la memoria).
3. Elija Archivo→Salir.

Obtención de los datos deseados

Creación de tipos de objeto y perfiles personalizados

ServerWORKS Manager le permite crear tipos de objeto personalizados y asignar grupos de variables de MIB para servidores que no sean DIGITAL para ampliar la administración de ServerWORKS para incluir objetos que no estén en el conjunto predeterminado o para incluir nuevos tipos de objeto que se podrían agregar a la red en el futuro.

Para crear el tipo de objeto y asignar las variables, debe completar las tareas siguientes. Cada una de ellas está compuesta de varios pasos más pequeños. Cuando ha completado las tareas, puede agregar manualmente el objeto al mapa de redes y empezar a administrarlo inmediatamente.

- Defina el tipo de objeto para que ServerWORKS reconozca objetos en la red que correspondan a la descripción
- Almacene los grupos de MIB
- Asigne los grupos de MIB que se concentran en la información que desea sobre el tipo de objeto

Utilice el procedimiento siguiente como guía para crear un tipo de objeto y perfil para cualquier elemento de la red. Este ejemplo crea un tipo de objeto para el servidor Compaq ProLiant 2500, asigna grupos de MIB y explica cómo agregar el tipo de objeto al mapa de redes manualmente y por parte del descubrimiento.

Definición del nuevo tipo de objeto

Desde el menú Herramientas de ServerWORKS, elija Herramientas→Tipos de objeto y haga clic en el botón Agregar. Se abre el cuadro de diálogo Agregar Tipos de objeto de SNMP. Aquí es donde introduce la definición del objeto. (Consulte la Figura 7-2).

1. En el cuadro de diálogo Agregar Tipos de objeto de SNMP, introduzca o seleccione:
 - El nombre del tipo de objeto, por ejemplo, Server
 - El nombre de subtipo del objeto, por ejemplo Compaq
 - Mapas de bits para representar los iconos de objetos (consúltese la Figura 7-2)
 - La forma de segundo plano del icono (por ejemplo, nodo final)

Obtención de los datos deseados

2. Haga clic en Aplicar.
3. Haga clic en Cerrar. Un mensaje le indica que salga de ServerWORKS Manager.
4. Elija Archivo→Salir.

Acerca del nombramiento de objetos

Puede dar el nombre que desee a un objeto. Por ejemplo, si piensa ver la red por organización, es posible que tenga tipos de objeto llamados Server.Finanzas o Node.Ventas1, Node.Ventas2.

Acerca de la selección de mapas de bits

Puede crear sus propios mapas de bits o puede seleccionarlos desde la colección de mapas de bits de ServerWORKS y modificarlos un poco para representar un nuevo objeto.

Puede encontrar los mapas de bits de ServerWORKS en:

```
<ServerWORKS directory>:\database\bitmaps
```

Un cambio de color es un cambio sencillo que se realiza fácilmente utilizando una herramienta como Paint. Los ejemplos de mapas de bits `serverg.bmp` y `server32.bmp` proporcionan un buen punto inicial para modificar mapas de bits porque son del tamaño correcto. Modifique y cambie el nombre a los mapas de bits en Paint. Por ejemplo, para un objeto de Compaq, utilice `serverc16.bmp` y `serverc32.bmp` y almacénelos con los mapas de bits de ServerWORKS.

Acerca de la forma de segundo plano

Cada elemento de la red que aparece en la lista de objetos (servidor, nodo, puente, etc.) tiene una forma predeterminada para el icono. Utilice el valor predeterminado.

Obtención de los datos deseados

Figura 7-2 Entradas en el cuadro de diálogo Agregar Tipos de objeto de SNMP definen un tipo de objeto



Almacenamiento de MIBs en la base de datos de ServerWORKS

Antes de que se pueda utilizar un tipo de objeto en ServerWORKS Manager Console, los grupos de MIB asociados al objeto se deben almacenar en la base de datos de ServerWORKS. ServerWORKS Manager ya ha almacenado cientos de grupos de MIB que están listos para asignarlos a nuevos tipos de objeto. Por ejemplo, si el tipo de objeto Nodo.Finanzas es un servidor DIGITAL, puede asignar MIBs de DIGITAL que ya estén almacenados para el tipo de objeto "Server.Digital". (Para la conveniencia de administradores de servidores Compaq, las variables MIB de Compaq ya están almacenadas en la base de datos de ServerWORKS).

Obtención de los datos deseados

Sin embargo, si está creando un tipo de objeto con MIBs que ha adquirido de un proveedor, un sitio Web o un servicio de boletines electrónicos, primero debe almacenarlos (compilarlos) en la base de datos de ServerWORKS.

1. Del menú ServerWORKS, elija Herramientas→MIB Enroller. Se abre el cuadro de diálogo MIB Enroller.
2. Del menú Compilar, elija MIB Compiler.
3. Elija Archivo→Abrir para examinar el MIB en el sistema.
4. Seleccione el MIB. El texto de MIB aparece en el cuadro de edición de MIB.
5. Haga clic en el botón Almacenar. Introduzca un nombre para MIB y elija Aceptar.
6. Elija Aceptar de nuevo en el indicador “¿Desea almacenar este MIB en la base de datos permanente?”

Acerca de variables de grupo de MIB y su propósito

¿Cómo saber qué grupo de MIB elegir? Se explica cada variable de grupo. Para aprender más sobre las variables de un grupo, elija el grupo de la lista de grupos de MIB. Seleccione una variable de MIB y haga clic en el botón Info sobre MIB para ver una explicación de la variable. También puede agregar comentarios a la definición y guardarlos.

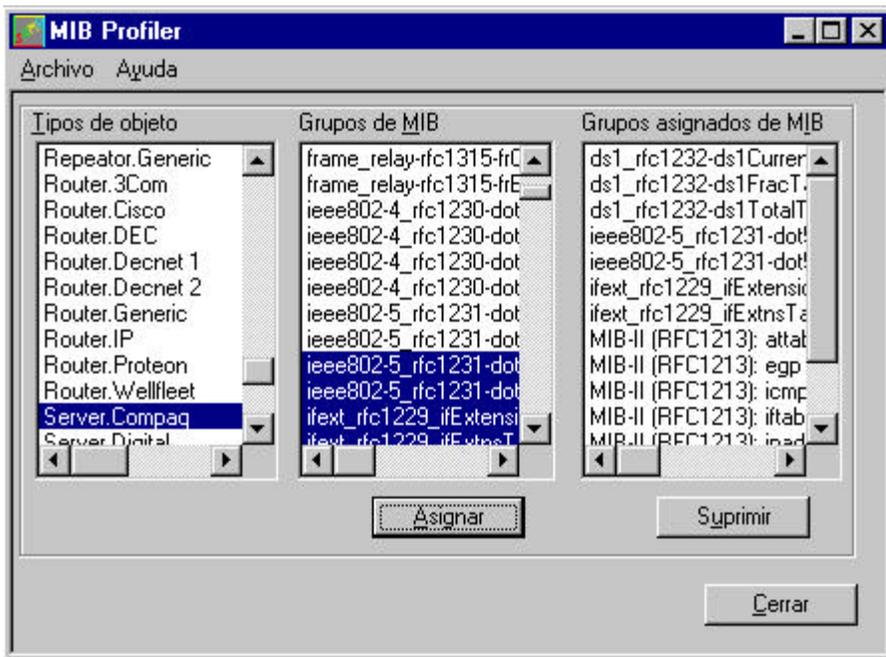
Asignación de grupos de MIB al tipo de objeto

1. Del menú ServerWORKS, elija Acciones→MIB Browser→Utilidades de MIB.
2. Del menú MIB Browser, elija Utilidades de MIB→MIB Profiler.
3. Seleccione el nombre del nuevo objeto de la lista Tipos de objeto, como se ilustra en la Figura 7-3.
4. Desplácese por la lista Grupos de MIB y seleccione los grupos de variables para asignarlos al tipo de objeto. En este caso, MIBs de Compaq se identifican con el prefijo cpq.

Obtención de los datos deseados

5. Elija Asignar para agregar los grupos a la lista Grupos asignados de MIB.
6. Haga clic en Cerrar.

Figura 7-3 Grupos de MIB asignados al nuevo tipo de objeto



Desplazamiento rápido por las listas de ServerWORKS Manager

Grupos de MIB y número de variables en los cientos. Para reducir el tiempo de búsqueda, haga clic en cualquier parte de la lista y luego introduzca la primera letra o dos de un nombre de grupo para ir a la sección de la lista que contiene las variables. Por ejemplo, introduzca s en la lista Tipos de objeto para ver los objetos de servidor, introduzca cp en la lista Grupos de MIB para encontrar grupos de Compaq.

Adición manual del objeto al mapa de red

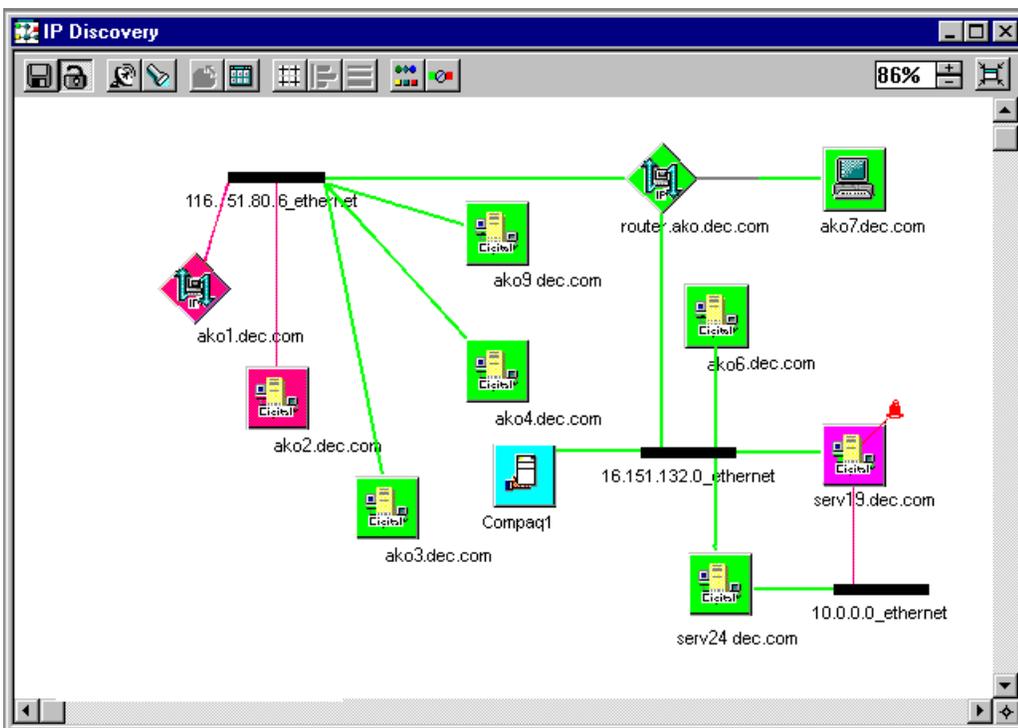
1. La adición de un elemento de red manualmente es la manera más rápida y menos compleja de empezar a administrar los objetos.
2. Del menú ServerWORKS Manager, elija Archivo→Nuevo visor para crear un nuevo mapa o elija Archivo→Abrir Visor para abrir un mapa existente donde agregará objetos del nuevo tipo de objeto, en este caso, el tipo Server.Compaq.
3. Elija Edición→Insertar y seleccione el tipo de objeto (Servidor) de la lista del cuadro de diálogo Insertar.
4. En el cuadro de diálogo Insertar: Server, introduzca un nombre de pantalla, por ejemplo Compaq1. Este nombre también es el nombre de IP predeterminado. Puede cambiar el nombre de IP. Elija un tipo de objeto de red de la lista Tipo. Para este ejemplo, es Server.Compaq.
5. Haga clic en Obtener dir. para ver la Dirección IP.
6. Haga clic en Aceptar. Se inicia un descubrimiento automático para insertar el nuevo objeto en el visor que seleccionó.

Verificación del objeto

Desde el mapa, haga doble clic en el objeto para abrir MIB Browser. El nuevo objeto se identifica con el nombre Compaq como parte del descriptor de sistema. Después de que ejecute IP Discovery, vea Informes de IP Discovery para ver la lista de nuevos objetos de Compaq. La Figura 7-4 muestra el visor de mapas de una red con el nuevo tipo de objeto.

Obtención de los datos deseados

Figura 7-4 Nuevo tipo de objeto descubierto en visores jerárquicos y de mapas



Asociación de objetos desconocidos a tipos de objeto conocidos

Cuando se está ejecutando SNMP, es posible que IP Discovery también encuentre objetos que no están asociados a un tipo de objeto conocido. Estos objetos se llaman Unknown.Type (tipo desconocido). La sysObjectID para el objeto no se asigna a un tipo de objeto existente, por lo que los MIBs adecuados no se aplican al objeto.

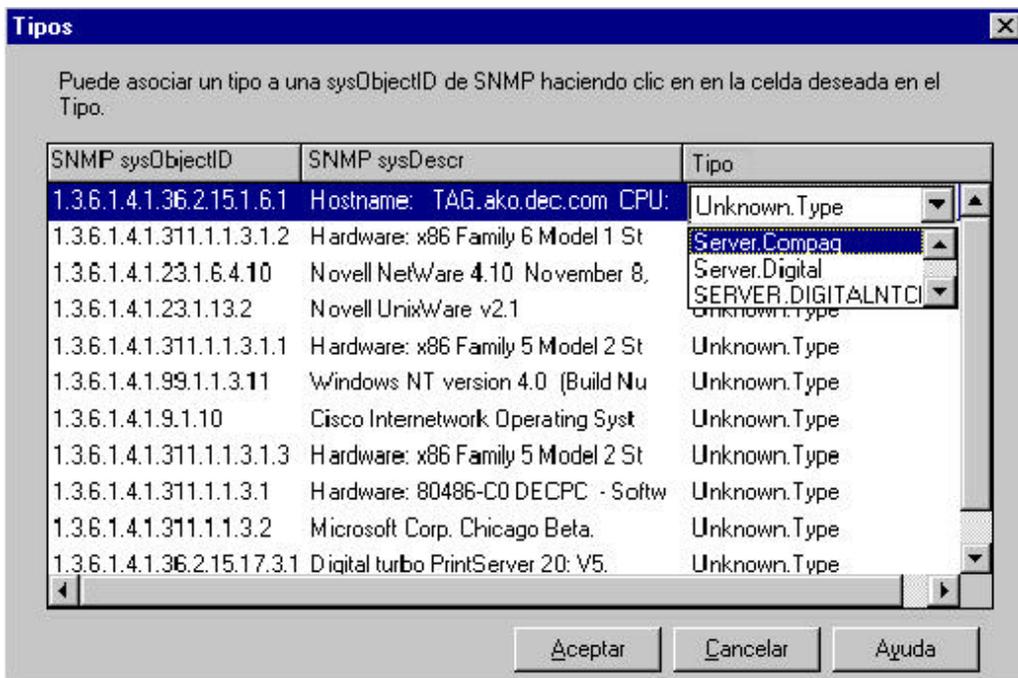
Obtención de los datos deseados

Para crear la asociación, debe asignar el tipo de objeto desconocido a un objeto de red existente. Puede realizar la asignación cuando ejecuta un nuevo descubrimiento.

1. Desde la ventana ServerWORKS Manager, elija Acciones→Descubrir objetos de IP.
2. En el cuadro de diálogo Redes para descubrir, seleccione la red y la máscara de red. Luego haga clic en Siguiente.
3. En el cuadro de diálogo Tipos para descubrir, haga clic en el botón Tipos.
4. En el cuadro de diálogo Tipos, puede ver la lista de objetos de tipo desconocido, Unknown.Type.
5. Seleccione un objeto para asociarlo a un tipo. Puede identificar el objeto por la sysObjectID o la sysDescr de SNMP. (Haga doble clic en el objeto de un mapa para abrir MIB Browser y encuentre la información).
6. Haga clic en la etiqueta de tipo desconocido, Unknown.Type, en la hilera del objeto. Aparece una lista desplegable con la lista de tipos de objeto existente. Seleccione el tipo de objeto. Como ha creado el objeto Server.Compaq, el nombre aparece en la lista.
7. Haga clic en Aceptar. Desde el cuadro de diálogo Tipos para descubrir, haga clic en Siguiente.
8. En el cuadro de diálogo Opciones de descubrimiento, seleccione la vista o el mapa que va a conservar el descubrimiento y haga clic en Finalizar.

Obtención de los datos deseados

Figura 7-5 Cuadro de diálogo Tipos para asociar objetos desconocidos a objetos existentes



Cuando se completa el descubrimiento, aparece el objeto desconocido en el mapa como el nuevo objeto de Server.Compaq. Haga doble clic en el objeto para ver detalles en MIB Browser.

Edición del Registro para reconocer el nuevo objeto

La inserción manual es una manera rápida de insertar uno o dos objetos, pero si está agregando objetos múltiples de un tipo, es posible que prefiera utilizar IP Discovery. En sistemas NT, IP Discovery utiliza una clave en el Registro de NT para identificar objetos. Puede cambiar la clave para reflejar una característica única del objeto para un visor de mapas particular (por ejemplo, un identificador específico de hardware o un identificador de organización).

Obtención de los datos deseados

1. Abra el editor de Registro regedit.exe. (Si utiliza Inicio→Buscar→Archivos o carpetas es una manera de ubicar el archivo).

2. En el Registro, encuentre la entrada

```
HKEY_LOCAL_MACHINE\  
    HARDWARE\  
        DESCRIPTION\  
            System\  
                CentralProcessor\  
                    
```

3. Haga doble clic en el valor del identificador y encuentre la cadena con Compaq, de la manera siguiente:

```
REG_SZ: Compaq - x86 Family 6 Model 1 Stepping 7
```

En este ejemplo, la expresión Compaq sólo identifica el tipo de objeto del servidor.

4. Haga clic en Aceptar y salga del Registro.

Edición del Registro con un archivo por lotes

La creación de un nuevo tipo de objeto cambia temporalmente el Registro. Como el cambio no es permanente, puede escribir un archivo por lotes para hacer este cambio cada vez que reinicia. Utilice Windows NT Resource Kit (Kit de recursos de Windows NT) regcgh.exe para obtener el valor de la clave para el Registro.

Obtención de los datos deseados

A continuación se presenta un ejemplo de un archivo por lotes que puede utilizar como pauta:

```
if "%1"==" " goto error
set tmpfile=C:\temp.reg
echo REGEDIT4>%tmpfile%
echo.>>%tmpfile%
echo [HKEY_LOCAL_MACHINE
    \HARDWARE
        \DESCRIPTIONS
            \System
                \CentralProcessor
                    \0]>>%tmpfile%
echo "Identifier"="Compaq Server">>%tmpfile%
call regedit %tmpfile%
del %tmpfile%
goto exit
echo Set of Compaq MIB II System Descriptor failed
:error
pause
:exit
```

Configuración de destinos de capturas y SNMP

Para recibir capturas de SNMP de dispositivos administrados en la consola, debe configurar el servicio de SNMP en el dispositivo administrado y especificar una dirección de destino. Puede haber configurado SNMP cuando instaló ServerWORKS o un agente en un dispositivo administrado.

Seguridad de SNMP

Puede dar mantenimiento a la seguridad cuando utiliza SNMP de la manera siguiente:

- Especifique nombres de comunidad GET y SET para la autenticación cuando configure el servicio de SNMP en el dispositivo administrado. El nombre de comunidad del dispositivo administrado debe ser el mismo que el nombre de comunidad de la consola para la autenticación.
- Un nombre de comunidad que esté asociado a un destino de captura se utiliza como un dispositivo de filtrado para enviar capturas sólo a destinos seleccionados. No se autentifica. Como ServerWORKS tiene la capacidad de ver los nombres de comunidad de los destinos de captura, utilice un nombre de comunidad diferente de los nombres de comunidad GET y SET.
- En sistemas operativos que soportan el control de acceso, especifique nombres de comunidad GET y SET diferentes para restringir el acceso en lectura y escritura a los dispositivos administrados.
- Bloquee la estación de trabajo de la consola cuando no esté presente.

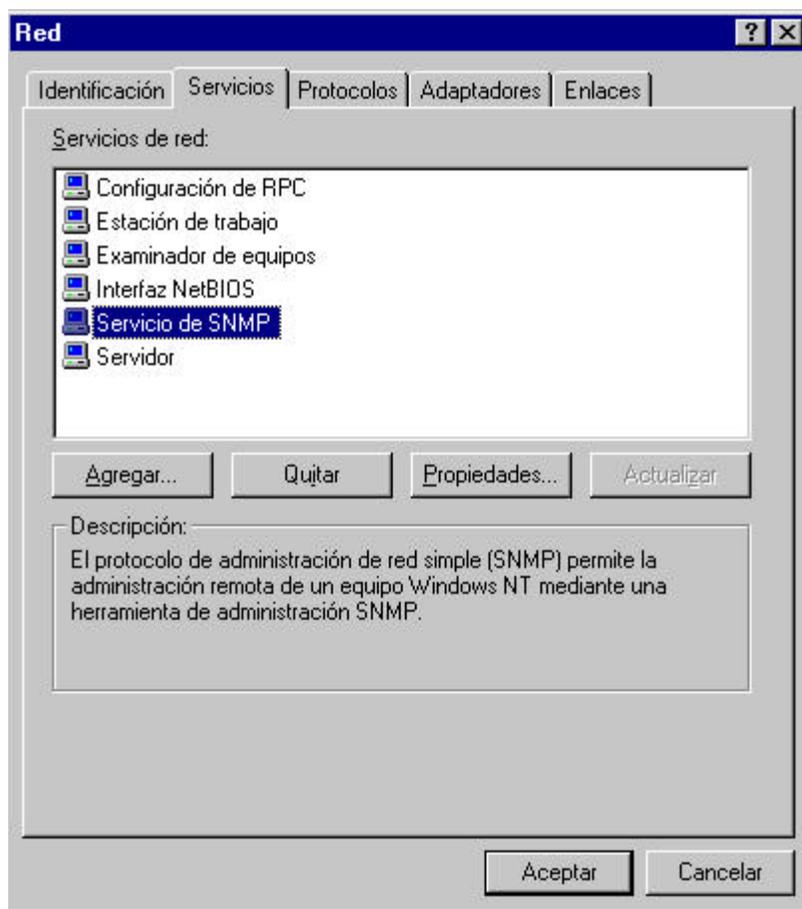
Configuración de SNMP y el destino de capturas en Windows NT 4.0

Puede configurar SNMP en dispositivos administrados desde el Panel de control del dispositivo administrado. Instale y configure el agente SNMP del servidor Windows NT 4.0 con la dirección IP o el nombre del cliente que recibirá las capturas.

1. En el Panel de control de Windows NT, seleccione la opción Red.
2. Seleccione la ficha Servicios de la página de propiedades Red.
3. Seleccione la opción Servicio de SNMP de la lista de servicios como se muestra en la figura siguiente. (Si el servicio no aparece en la lista, cargue el servicio de SNMP de los discos de instalación del sistema operativo). Consulte la documentación de sistema operativo.
4. Haga clic en el botón Propiedades.

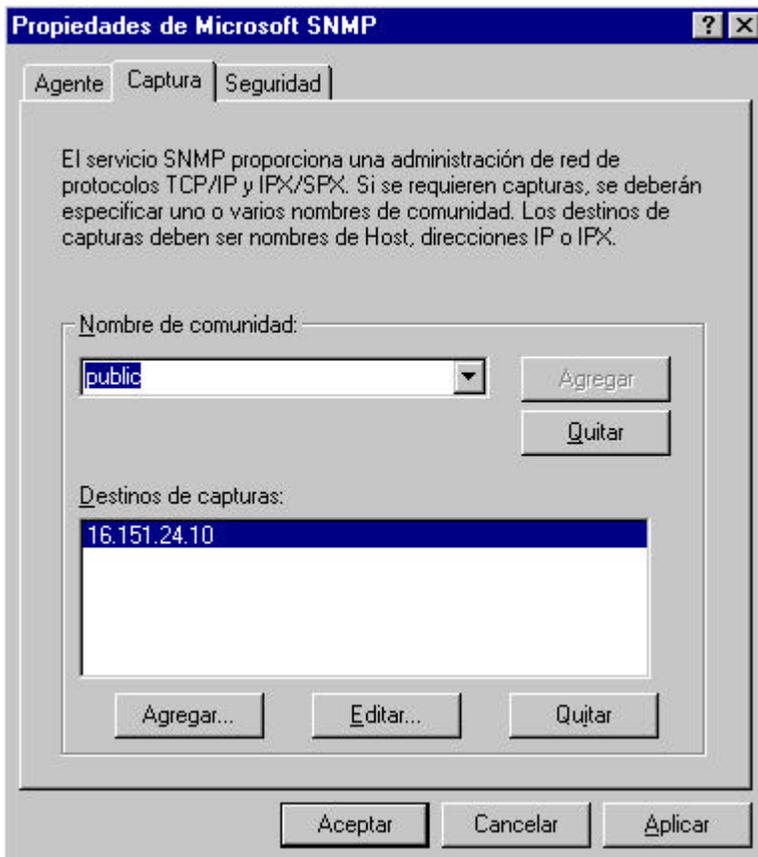
Obtención de los datos deseados

Figura 7-6 Selección de un agente de SNMP desde la página Servicios de Red



5. Seleccione la ficha Captura.
6. Seleccione el nombre de comunidad que desea modificar o introduzca un nuevo nombre de comunidad y haga clic en el botón Agregar. (Public es el nombre de comunidad predeterminado de Windows NT).

Figura 7-7 Destino de captura especificado en la página de Propiedades de Captura



7. Haga clic en el botón Agregar bajo el cuadro Destinos de capturas. El destino de la captura representa un nodo que ejecuta una aplicación (como ServerWORKS Manager) que está escuchando capturas en un puerto especificado en el archivo /Windows/Services (por lo general, puerto 162).
8. Introduzca la dirección IP o IPX única del host que recibirá capturas para esta comunidad. No utilice una dirección de subred.

Obtención de los datos deseados

9. Haga clic en el botón Agregar del cuadro de diálogo Configuración de servicios.
10. Según las recomendaciones de Microsoft, vuelva a instalar el último Service Pack.

Verifique que se esté ejecutando el servicio de SNMP. Utilice el Panel de control→Servicios en Windows NT o Panel de control→Red→Servicios en Windows 95. No inicie el servicio SNMP Trap en la consola de administración.

Consulte el Apéndice B para obtener detalles sobre la configuración de SNMP y el destino de una captura para Windows 95.

Configuración de SNMP en Windows 95

Instale y configure el agente SNMP del nodo Windows 95 con la dirección IP o el nombre del cliente que recibirá las capturas.

Instalación del software SNMP

1. Desde el Panel de control, haga clic en el icono Red.
2. Haga clic en el botón Agregar en la opción Red.
3. En el cuadro de diálogo Seleccionar tipo de componente de red, haga doble clic en Servicio.
4. En el cuadro de diálogo Seleccionar servicio de red, haga clic en el botón Utilizar disco.
5. En el cuadro de diálogo Instalar desde disco, introduzca la ruta al directorio ADMIN\NETTOOLS\SNMP en el CD de Windows 95, luego haga clic en Aceptar.
6. En el cuadro de diálogo Seleccionar servicio de red, haga clic en Agente SNMP de Microsoft en la lista Modelos y haga clic en Aceptar. Si se le pide que especifique a ubicación de archivos adicionales, especifique una ruta a los archivos en el CD-ROM o la unidad de red compartida.
7. Reinicie la computadora.

Configuración del destino de capturas en Windows 95

También puede configurar el destino de la captura en Windows 95 con el Editor de planes de sistema. Este editor no es un componente instalado estándar para Windows 95.

1. Del menú Inicio, elija Panel de control.
2. Elija Agregar o quitar programas y haga clic en la ficha Instalación de Windows.
3. Haga clic en Utilizar disco y especifique la ruta \ADMIN\APPTOOLS\POLEDIT. Haga clic en Aceptar.
4. Seleccione Editor de planes de sistema desde el cuadro Componentes y haga clic en Instalar y salga de la herramienta Agregar o quitar programas.
5. Desde el menú Inicio, haga clic en Ejecutar e introduzca el comando
6. poledit
7. Haga clic en Aceptar para iniciar el programa.
8. En el Editor de planes de sistema, elija Archivo→Abrir registro.
9. Haga doble clic en PC local.
10. En el cuadro de diálogo Propiedades de PC local, haga doble clic en el icono Red.
11. Haga doble clic en SNMP para ver las propiedades para el agente de SNMP. Luego defina la comunidad, los administradores permitidos (las direcciones IP o IPX que están permitidas para obtener información de un agente SNMP) y el destino de capturas para la comunidad Public (la dirección IP o IPX de los hosts en la comunidad Public a la que desea que SNMP envíe capturas).



Nota: Para enviar capturas a una comunidad que no sea Public, debe editar el Registro directamente. Ese procedimiento se explica con detalle en la documentación de Windows 95 de Microsoft y este manual no lo puede explicar con más detalle.

Obtención de los datos deseados

Configuración del destino de capturas desde la consola

Se le pide que defina un destino de captura cuando configura una alarma en un dispositivo administrado. Puede especificar el destino de la Consola con la herramienta Trap Control Remote Destination si todavía no especifica un destino de captura en el sistema remoto.

Puede tener uno o más destinos de captura en el dispositivo administrado, pero el destino de la captura debe ser un sistema en el que esté instalado ServerWORKS Manager Console o un administrador de redes de la empresa.

Debe conocer los nombres de comunidades Get y Set de la máquina remota si no acepta las Comunidades predeterminadas. Los nombres de comunidad Get y Set proporcionan autenticación.

Para configurar la captura en un dispositivo administrado

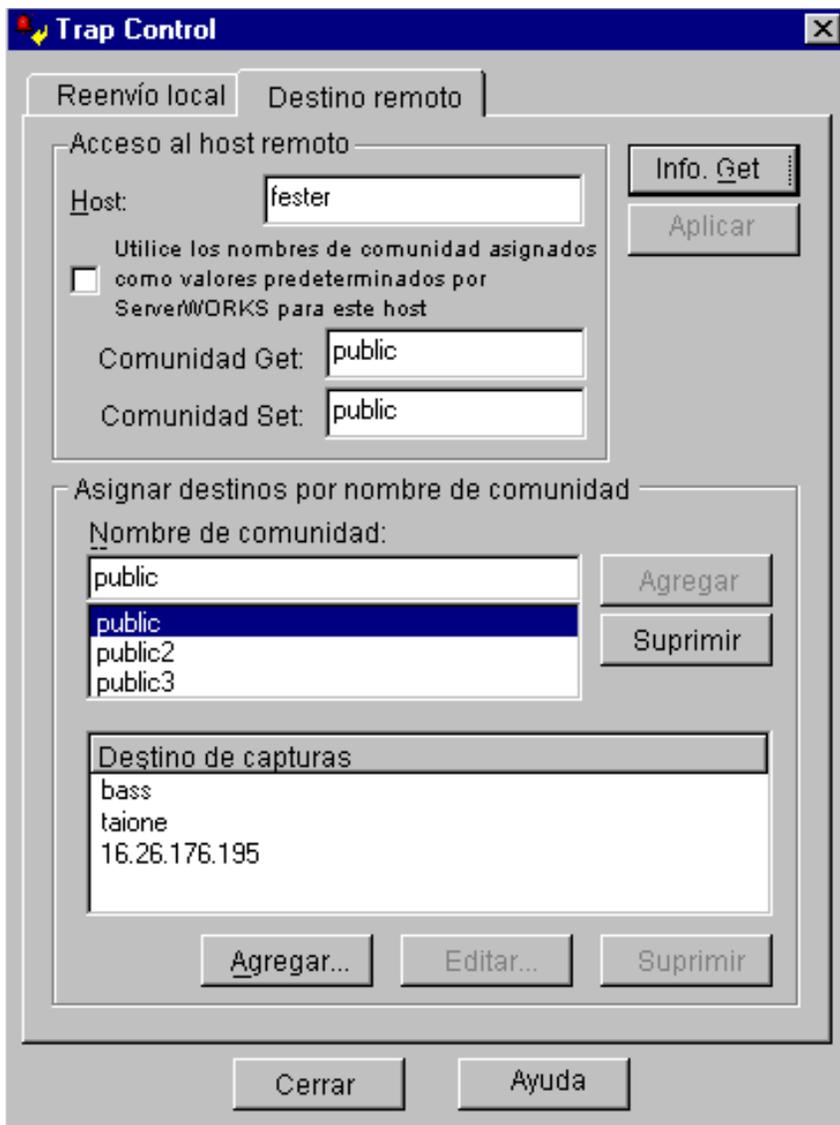
1. Elija Herramientas → Trap Control de la consola o de Alarm Configuration.
2. Haga clic en la ficha Destino remoto.
3. Introduzca el nombre de host (el nombre del dispositivo administrado). Consulte la Figura 7-8.
4. Elija uno de estos pasos:
 - Acepte la comunidad predeterminada (por ejemplo, Public para Windows NT)
 - Anule la selección de la opción predeterminada e introduzca los nombres de Comunidad Get y Comunidad Set.
5. Haga clic en Información sobre Get para ver información sobre el nombre de comunidad actual y el destino de captura para el host.
6. Especifique los destinos asignados por nombre de comunidad. Estos destinos se incluyen en el mensaje de captura y se envían sólo a los destinos de la comunidad actual.
7. Para agregar un nuevo nombre de comunidad, introduzca el nombre en la casilla de nombre de comunidad y haga clic en Agregar.

Obtención de los datos deseados

8. Para modificar la lista, seleccione un nombre de comunidad y un destino. Luego haga clic en Agregar, Edición o Suprimir. En el cuadro de diálogo Agregar o Edición, introduzca la dirección IP de destino y haga clic en Aceptar.
9. Haga clic en Aplicar para activar los cambios y Cerrar para descartar los cambios.

Obtención de los datos deseados

Figura 7-8 Cuadro de diálogo Trap Control



Reenvío de capturas

ServerWORKS Manager Console que recibe capturas, a su vez puede *reenviar* esas capturas a otros sistemas. Esto le permite a administradores de nivel de grupo de trabajo ejecutar ServerWORKS Manager, mientras que los administradores de nivel de empresa ejecutan programas de administrador como HP OpenView o Tivoli TME 10. Las capturas reenviadas son transmitidas por Event Dispatcher e Event Logger de ServerWORKS, no por el agente.

Para reenviar capturas desde la consola, defina los destinos de reenvío desde la utilidad Console Trap Control.

El reenvío de capturas ocurre sólo cuando Event Dispatcher e Event Logger se están ejecutando y sólo si ninguna otra aplicación ha abierto el puerto de captura 162. Por defecto, no ocurre ningún reenvío. Las capturas que se basan en agentes siempre se reenvían a la consola de administración. Las alarmas se pueden reenviar como capturas si lo especifica en la utilidad Trap Control.

Especifique un puerto y una dirección únicos para cada destino. Si no se especifica un nombre de puerto, entonces se supone que es el puerto 162 para evitar problemas con sistemas que tengan escuchadores de capturas de SNMP múltiples en éstos. Todas las capturas se reenviarán a cada destino que defina. ServerWORKS permite hasta diez direcciones de destino de reenvío.

Para especificar un destino de reenvío de capturas

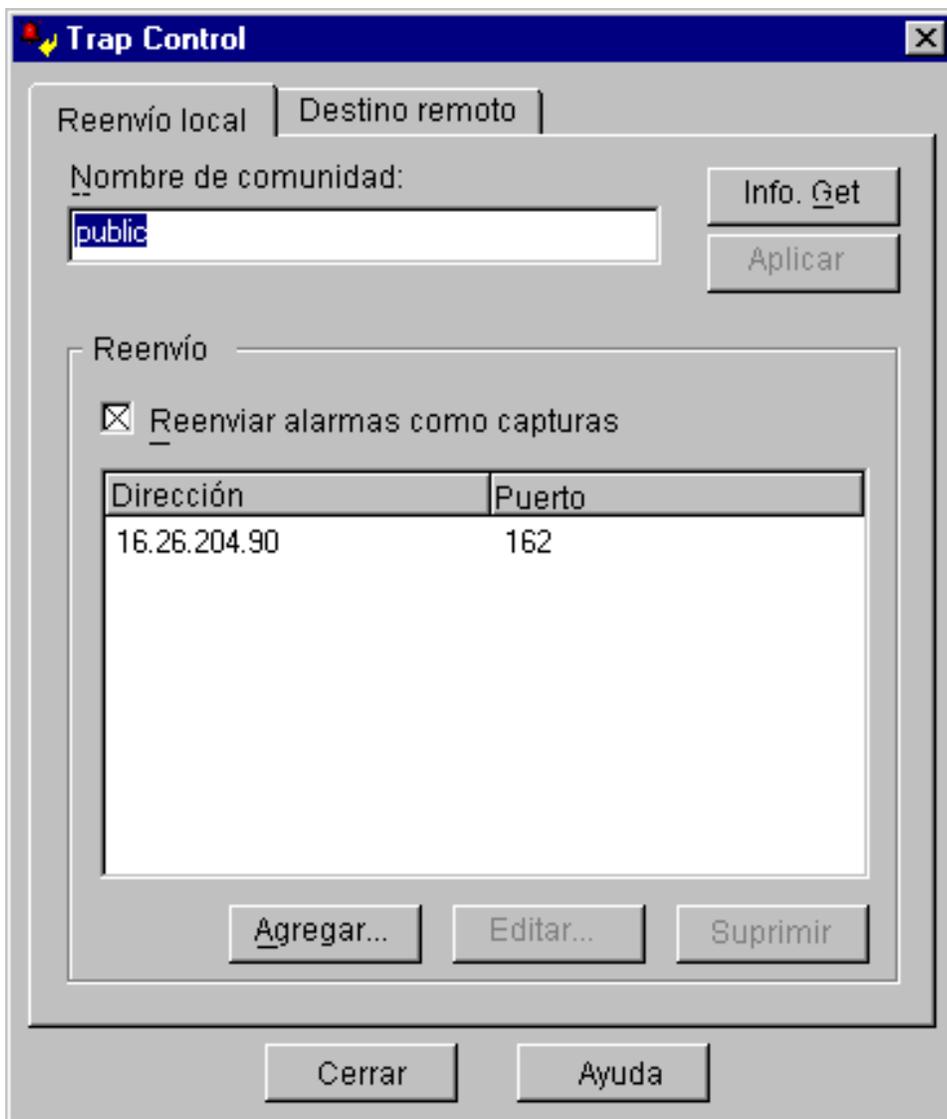
1. Desde el menú Consola, elija Herramientas→Trap Control.
2. Haga clic en la ficha Reenvío local y realice las tareas siguientes:
 - Introduzca el nombre de comunidad, si es necesario. Public es la comunidad predeterminada de NT. Puede cambiar el nombre de comunidad, pero el nombre que utilice se aplica a todos los destinos de reenvío de la lista.
 - Seleccione Reenviar alarmas como capturas.
 - Haga clic en Información sobre Get para ver una lista de direcciones de reenvío para la comunidad seleccionada.

Obtención de los datos deseados

3. Para agregar una dirección de reenvío, haga clic en Agregar. En el cuadro de diálogo Agregar, introduzca la Dirección y el Número de puerto. Por ejemplo, para reenviar todas las capturas recibidas en una consola de administración a la dirección IP 16.20.204.90, complete el cuadro de diálogo como se muestra en la Figura 7-9. Luego haga clic en Aceptar.
 - También puede eliminar o modificar una dirección de reenvío. Par eliminarla, seleccione una dirección y haga clic en Suprimir. Para modificarla, seleccione una dirección y haga clic en Edición. Luego cambie la información sobre Dirección y Puerto en el cuadro de diálogo Edición.
4. Haga clic en Aplicar para activar los cambios y Cerrar para cerrar el cuadro de diálogo.

Obtención de los datos deseados

Figura 7-9 Cuadro de diálogo Trap Control



Obtención de los datos deseados

Uso del Visor de sucesos de NT para seguir alarmas

Puede enviar alarmas al Visor de sucesos de Windows NT modificando el archivo de inicialización de ServerWORKS.

Para utilizar Visor de sucesos como un visor de alarmas

1. Desde el menú Inicio, elija Buscar→Archivos o carpetas.
2. Introduzca swgmr.ini en el campo Nombre y haga clic en Buscar.
3. Cuando se haya terminado la búsqueda, haga doble clic en swgmr.ini.
4. Busque la sección de parámetros [Setup] en el archivo.
5. Cambie el valor del parámetro siguiente
WriteTrapMsgToNTEventLog=1
6. Cierre el archivo swgmr.ini.

Administración de redes Windows y NetWare 8

Puede administrar una red Windows NT o una red Novell NetWare utilizando ServerWORKS Manager.

Al utilizar el componente Administrador de servidores de NT desde la consola, puede realizar la mayoría de las tareas administrativas de NT incluyendo configurar nuevas cuentas, dominios y grupos, administrar colas de impresión y directorios compartidos y administrar relaciones de confianza.

Las herramientas administrativas de NetWare están disponibles para utilizarlas desde la consola para redes con servidores NetWare.

Descubrimiento del Administrador de servidores de NT

El descubrimiento del Administrador de servidores de NT lista los objetos de Microsoft Network (los que ejecutan el protocolo LAN Manager V3.0). Esta categoría incluye todos los servidores DIGITAL de una LAN que ejecutan el sistema operativo Windows NT. Esta categoría también puede incluir servidores que no sean DIGITAL cuyas variables MIB II están almacenadas en la base de datos de ServerWORKS.

ServerWORKS Explorer muestra el objeto raíz, que puede desplegar para mostrar la red Microsoft completa. Los objetos encontrados pueden incluir más objetos que sólo servidores NT (como OS/2 o Windows 95). Es posible que los sistemas que responden no dispongan de las funcionalidades completas de Windows NT y, en tal caso, no tendrán todas sus capacidades.

Además, necesita el agente DIGITAL instalado en un sistema NT que esté supervisando para obtener la información completa sobre el sistema NT. Las herramientas de Administrador de servidores de NT se pueden utilizar para administrar algunas tareas de esos sistemas, pero no necesariamente todas.

Antes de administrar NT desde ServerWORKS

Necesita privilegios de administrador en el dominio que administre. Para modificar cuentas en otros dominios, la relación de la confianza entre dominios debe permitir la administración del dominio desde otros dominios.

Utilización de Administrador de servidores de NT para dominios Windows NT

Para administrar un dominio NT en la red, puede utilizar Administrador de servidores de NT de ServerWORKS en lugar de utilizar las utilidades de administración de NT. El procedimiento siguiente explica cómo crear un grupo Local y asignar derechos al grupo. Es sólo un ejemplo de una tarea administrativa de NT que puede realizar desde ServerWORKS Manager Console.

Administración de redes Windows NT

Para crear un grupo en Administrador de servidores de NT de ServerWORKS Manager

1. Desde el Explorador, elija Administrador de servidores de NT.
2. Seleccione el dominio NT. La lista se despliega para mostrar los objetos de Grupos, Servidores y Usuarios para el dominio.
3. Seleccione Servidores. La lista se despliega para mostrar los servidores en el dominio.
4. Seleccione el servidor o la estación de trabajo en donde desea crear el grupo.
5. Seleccione Grupos.
6. Del menú Acciones, elija Crear. Aparece el cuadro de diálogo Crear grupo.
7. Introduzca el nombre del grupo y un comentario breve que identifique el grupo. Luego seleccione Global o Local.
8. Haga clic en Aplicar para crear el grupo y permanecer en el cuadro de diálogo Crear grupo para crear más nuevos grupos o haga clic en Aceptar para crear el grupo y cerrar el cuadro de diálogo.
9. Se le pide que defina otros atributos para el nuevo grupo. Siga uno de estos pasos:
 - Seleccione No para aceptar los atributos predeterminados.
 - Seleccione Sí para abrir el cuadro de diálogo Propiedades de grupos para cambiar otros atributos.

Para modificar los derechos

1. Del Administrador de servidores de NT, seleccione el dominio y la máquina donde está asignando derechos a grupos.
2. Seleccione Grupos.
3. Elija Acciones→Propiedades.
4. En el cuadro de diálogo Propiedades de servidor, haga clic en la ficha Derechos de usuario.

Administración de redes Windows NT

5. En la página Derechos de usuario, seleccione un derecho de la lista desplegable Derecho. Por ejemplo, para permitir a los miembros del grupo que inicien una sesión localmente en la máquina seleccionada, haga clic en Iniciar sesión localmente.
6. Haga clic en Agregar.
7. En el cuadro de diálogo Agregar grupos y usuarios a..., seleccione el grupo y haga clic en Agregar para incluir este derecho para este grupo. Luego haga clic en Aceptar.
8. Repita los pasos 1 a 7 para cada derecho que esté asignando hasta que esté satisfecho que el grupo tenga los derechos adecuados.

Asignación de derechos a grupos múltiples al mismo tiempo

Sólo seleccione varios grupos de la lista Grupos. Pulse y mantenga pulsada la tecla CTRL y haga clic en los grupos que va a incluir. Todos los derechos asignados o eliminados se aplican a todos los grupos seleccionados.

Más acerca de Administración de NT

Para revisar los procedimientos administrativos que puede realizar de la consola, lea la Ayuda de Administrador de servidores de NT.

Para abrir la Ayuda

1. Elija Ayuda→Administrador de servidores de NT.
2. De la ventana Índice, haga doble clic en un tema de interés.

Novell NetWare Server Manager

Cuando está ejecutando NetWare de Novell en ServerWORKS Console, puede ver los servidores NetWare en la red. El descubrimiento de Novell NetWare es similar al descubrimiento de Administrador de servidores de NT en que se inicia desplegando el objeto raíz de NetWare en ServerWORKS Explorer. Esto da como resultado el encuentro dinámico de objetos de NetWare en la LAN. Observe que los sistemas NetWare V3.x y V4.x tienen funciones diferentes.

Administración de redes Windows NT

La información proporcionada por el descubrimiento de NetWare no se almacena en la base de datos, sino que se obtiene cada vez que se despliega el objeto de Novell NetWare.

Esta categoría incluye todos los servidores DIGITAL de una LAN que ejecuta el sistema operativo Novell NetWare y que se puede administrar utilizando herramientas NetWare Management.

Administración de una red de NetWare desde ServerWORKS

Puede descubrir y administrar todos los servidores DIGITAL de una LAN que ejecuta el sistema operativo Novell NetWare que utilizan las herramientas de NetWare estándar:

- Filer
- Pconsole
- Princon
- Rconcols
- Syscon
- Userdef
- NWAdmin

Cuando selecciona un servidor NetWare, las utilidades NetWare aparecen en la Barra de herramientas de ServerWORKS Manager: Para obtener detalles sobre la administración de una red de NetWare desde ServerWORKS, consulte la ayuda en línea.

Procedimientos e información adicionales



Esta sección contiene la información siguiente:

- Cómo instalar a agentes SNMP para los sistemas operativos siguientes:
 - DIGITAL UNIX V4.0
 - OpenVMS 7.1-1H1
 - IBM OS/2

Estos agentes forman parte de un sistema operativo y no se proporcionan con ServerWORKS Manager. Además de la información de las secciones siguientes, consulte las instrucciones de instalación y notas de revisión para el sistema operativo para cualquier cambio de último minuto al sistema operativo por parte del vendedor.

- Ejecución de una segunda versión de ServerWORKS en otro directorio

Instalación de agentes SNMP de DIGITAL UNIX

ServerWORKS Manager supervisa servidores Alpha que ejecutan DIGITAL UNIX V3.2d-1 y superior. Los agentes SNMP de DIGITAL UNIX y MIBs asociados se incluyen con el sistema operativo y están instalados de manera predeterminada en todos los servidores en los que instala DIGITAL UNIX. Los subagentes y los MIBs son una parte del subconjunto obligatorio OSFCLINETXX.

El MIB del Sistema de servidores Digital facilitará la supervisión de todo el estado de un Sistema de servidores Alpha, incluyendo hardware, firmware e información sobre entorno. El MIB del Administrador de servidores Digital ayudará a administrar los atributos de cualesquiera MIBs. Supervisará los valores del atributo, llamará acciones si exceden sus umbrales predefinidos y, si se especificó, encuestará los atributos en cada reinicio del subagente.

Los MIBs de definición del MIB del Sistema de servidores Digital (svrSystem.mib) y el MIB de Administración de servidores Digital (svrMgt mib) residen en

```
/usr/share/sysman/mibs.
```

Los agentes residen en

```
/usr/sbin/svrMgt_mib
```

```
/usr/sbin/svrSystem_mib
```

Instalación de agentes SNMP de OpenVMS

El agente SNMP de OpenVMS para sistemas Alpha se incluye en el producto DIGITAL TCP/IP Services for OpenVMS V4.2 o superior y es un componente de NAS Client/Server Package. El agente SNMP se instala cuando se instala TCP/IP. Consulte las instrucciones del sistema operativo, que también contienen instrucciones de instalación para TCP/IP.

Procedimientos e información adicionales

ServerWORKS Manager supervisa servidores Alpha que ejecutan OpenVMS Alpha Versión 7.1-1H1; el protocolo Extensible Simple Network Management Protocol (eSNMP) lo hace posible para administradores de redes para administrar muchos tipos de dispositivos diferentes en toda la red y límites de vendedores mediante el uso de bases de datos llamadas MIBs (Management Information Bases). Esencialmente, la información se intercambia entre subagentes y agentes principales, que son dispositivos tales como encaminadores y servidores de la red que se está administrando y administradores, que son los dispositivos de la red a través los cuales se realiza la administración.

DIGITAL Server MIB (DSM) consta de dos extensiones o subagentes:

- Sistema - Describe una interfaz de administración hacia la información de sistemas Alpha no definidos por MIBs estándar.
- Administración - Describe instrumentación del agente de extensión de DIGITAL, incluyendo la capacidad de detectar y supervisar umbrales en variables de entero.

La representación de DSM dentro de Structure of Managed Information (SMI: Estructura de información administrada) estándar es:

```
iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) 36
```

OpenVMS Alpha Versión 7.1-1H1 implementa los subagentes DSM en los sistemas AlphaServer 800, 1000, 4000, 4100, 8200 y 8400. Con los subagentes de DSM, los clientes pueden determinar y administrar de manera remota información importante:

- Números de revisión de firmware
- Descripciones de sistemas de base
- Información y descripciones de FRU (unidad reemplazable de campo)
- El estado del procesador y la memoria caché
- Configuraciones de interfaz
- Las condiciones ambientales en la caja del sistema que podrían perjudicar el hardware

Puede acceder a subagentes de DSM utilizando el software siguiente:

Procedimientos e información adicionales

- DIGITAL ServerWORKS Manager Versión 3.0 o superior o cualquier examinador de MIB que tenga acceso a definiciones de DSM.
- DIGITAL TCP/IP Services for OpenVMS Versión 4.2 (antes conocido como UCX). Los subagentes de DSM utilizan el agente de SNMP proporcionado con UCX para comunicarse con clientes de SNMP.

Presentación general de subagentes de DSM

Subagentes de DSM responden a peticiones de SNMP para:

- Un objeto de DSM—el elemento de datos con el que está relacionado el administrador de la red
- Una captura—información sobre un cambio de estado. Un subagente es responsable de informar y dar mantenimiento a los datos que pertenecen a estos objetos y capturas.

Una descripción completa de MIB y sus variables está disponible en las notas de revisión de OpenVMS Alpha Versión 7.1-H1.

Configuración del sistema para utilizar agentes de DSM

Para configurar SNMP en el sistema y activar el agente principal para aceptar comandos SET de SNMP cliente, envíe el comando de administración de UCX siguiente del indicador UCX>. Esta operación requiere privilegios de SYSPRV o BYPASS.

```
UCX> SET CONFIGURATION SNMP /FLAGS=SETS
```

Para activar o desactivar el tipo de acceso a los datos locales de MIB, utilice los comandos, calificadores y opciones de UCX siguientes:

Procedimientos e información adicionales

```
UCX> SET CONFIGURATION SNMP /[NO]COMMUNITY="name" -
_UCX> /[NO]ADDRESS=host address
      /TYPE=( [NO]READ, [NO]TRAP,
_UCX> [NO]WRITE)
```

Por ejemplo, el comando siguiente configura SNMP, especifica el nombre y la dirección de la comunidad, especifica que el agente puede aceptar comandos SET de miembros de la comunidad y, activa el agente principal para enviar mensajes de capturas a miembros de la comunidad. (Observe que el acceso de READ (lectura) se supone al especificar TRAP (captura) o WRITE (escritura).

```
UCX> SET CONFIGURATION SNMP /COMMUNITY="public"
/ADDRESS=128|45.2.8 - _UCX> /TYPE=(TRAP,WRITE)
```

Para iniciar los subagentes de DSM, el administrador de sistema o de red debe modificar dos archivos que se proporcionan en el kit del producto DIGITAL TCP/IP Services for OpenVMS, de la manera siguiente:

1. Agregue los comandos siguientes al final del archivo `SYSS$STARTUP:UCX$SNMP_STARTUP.COM`:

```
$ RUN      /DETACHED -
          /PROCESS_NAME="UCX$SERVER_MIB" -
          /OUTPUT=SYS$SYSDEVICE:[UCX$SNMP]UCX$SERVER_MIB.LOG
          -
          /ERROR=SYS$SYSDEVICE:[UCX$SNMP]UCX$SERVER_MIB.ERR -
          /UIC=UCX$SNMP -
          SYS$SYSTEM:SVR$SYSTEM_MIB

$ RUN      /DETACHED -
          /PROCESS_NAME="UCX$SVRMGT_MIB" -
          /OUTPUT=SYS$SYSDEVICE:[UCX$SNMP]UCX$SVRMGT_MIB.LOG
          -
          /ERROR=SYS$SYSDEVICE:[UCX$SNMP]UCX$SVRMGT_MIB.ERR -
          /UIC=UCX$SNMP -
          SYS$SYSTEM:SVRMGT_MIB
```

Procedimientos e información adicionales

2. Modifique el archivo
SYS\$MANAGER:UCX\$SNMP_SHUTDOWN.COM para activar los cierres. Las diferencias siguientes del archivo muestran las modificaciones hechas a UCX\$SNMP_SHUTDOWN.COM;2 para incluir el cierre del subagente de DSM:

```
File SYS$COMMON:[SYSMGR]UCX$SNMP_SHUTDOWN.COM;2
52  $ SUBAGT2 := ucx$server_mib
53  $ SUBAGT3 := ucx$svrmgt_mib
54  $ CONTEXT = ""
*****
```

Instalación de agentes SNMP para OS/2

Consulte las instrucciones de instalación del sistema operativo para instalar a agentes nativos de SNMP para OS/2.

En ServerWORKS Manager, los servidores OS/2 de DIGITAL se descubren como objetos de “servidor” y no como server.DIGITAL. Para administrar servidores O/2 de DIGITAL, cambie las propiedades del servidor de la manera siguiente:

1. Seleccione el servidor O/2 de DIGITAL en el visor de mapa o el Explorer.
2. Elija Acciones→Propiedades.
3. Haga clic en Propiedades→ficha Información general.
4. En el cuadro de lista Tipo, seleccione server.Digital.
5. Elija Aceptar.

Procedimientos e información adicionales

```
File SYS$COMMON:[SYSMGR]UCX$SNMP_SHUTDOWN.COM;1
53  $ CONTEXT = ""
*****

*****

File SYS$COMMON:[SYSMGR]UCX$SNMP_SHUTDOWN.COM;2
59  $   IF  (PRCNAM .EQS. AGENT) .OR. -
60      (PRCNAM .EQS. SUBAGT) .OR. -
61      (PRCNAM .EQS. SUBAGT2) .OR. -
62      (PRCNAM .EQS. SUBAGT3) THEN STOP /ID='P1'
63  $   GOTO _LOOP1
*****

File SYS$COMMON:[SYSMGR]UCX$SNMP_SHUTDOWN.COM;1
59  $   IF  (PRCNAM .EQS. AGENT) .OR. (PRCNAM .EQS.
      SUBAGT) THEN STOP /ID='P1'
60  $   GOTO _LOOP1
*****
```

Número de secciones diferentes que se encontró: 2

Número de registros diferentes que se encontró: 4

Restricciones de datos ambientales: Sistemas AlphaServer 8200 y 8400

Los reguladores de alimentación en sistemas AlphaServer 8200 no contienen sensores para condiciones ambientales. Por lo tanto, los datos no se pueden informar en los grupos de MIB de fuente de alimentación y térmico del subagente del sistema DSM.

Aunque los reguladores de alimentación en sistemas AlphaServer 8400 contienen sensores ambientales, es posible que algunas configuraciones no proporcionen información sobre el ambiente correctamente al subagente del sistema DSM. Este problema afecta los grupos MIB térmicos y de fuente de alimentación y se resolverá en una versión futura del software.

Procedimientos e información adicionales

Dispositivo IIA0: ahora configurado en sistemas AlphaServer 4100

OpenVMS Alpha Versión 7.1-1H1 configura el dispositivo IIA0 automáticamente: en sistemas AlphaServer 4100.

IIA0: dispositivo, que es controlado por SYS\$IIDRIVER. EXE, proporciona acceso a información sobre el estado del ventilador, la temperatura y la fuente de alimentación disponible a través del bus 12C integrado. El MIB del Sistema de servidores DIGITAL, que se describe en la Sección 1, proporciona información sobre el estado a la consola ServerWORKS. La interfaz al controlador de dispositivos está reservada para uso de DIGITAL únicamente.

Dispositivo OPA1: ahora configurado en sistemas AlphaServer 8200 y 8400

OpenVMS Alpha Versión 7.1-1H1 configura el dispositivo OPA1 automáticamente: en sistemas AlphaServer 8200 y 8400. OPA1: dispositivo, que es controlado por SYS\$OPDRIVER. EXE proporciona acceso a información sobre el estado de la temperatura y la fuente de alimentación disponible a través de los reguladores de alimentación integrados H7263. El MIB del Sistema de servidores DIGITAL, que se describe en la Sección 1, proporciona la información sobre el estado a la consola ServerWORKS. La interfaz al controlador de dispositivos está reservada para uso de DIGITAL únicamente.

Ejecución de una segunda versión de ServerWORKS

Si desea una segunda versión, primero cambie el nombre a los archivos de la versión anterior en los directorios del menú de inicio. Utilice el procedimiento siguiente:

Para Windows NT 4.0 o Windows 95:

1. Desde el Escritorio, elija Iniciar→Configuración→Barra de tareas.
2. Seleccione Programas del menú Inicio y haga clic en el botón Opciones avanzadas.
3. Elija Herramientas→Buscar→Archivos o carpetas. Luego introduzca Inicio en el campo Nombre.

Examine el árbol de directorios para los directorios de ServerWORKS, ClientWORKS o ManageWORKS y cambie el nombre a los archivos.

¿Tiene ManageWORKS instalado?

ServerWORKS Manager Console y OpenVMS Management Station se pueden instalar y ejecutar *por separado* en la misma máquina. Siga utilizando ManageWORKS como interfaz para OpenVMS Management Station.

Si no tiene ManageWORKS instalado, puede saltarse esta sección.

Sólo ManageWORKS V2.2 se soporta para actualizar a ServerWORKS Manager 3.x. La instalación verifica si está instalado ManageWORKS. Si es así, puede conservar los mapas de IP Discovery desde ManageWORKS V2.2. Sólo se conservan los objetos de la vista de IP Discovery. Las preferencias del usuario y las vistas de SVN personalizadas de ManageWORKS se deben volver a aplicar a los nuevos visores jerárquicos que cree en ServerWORKS Manager. No se conserva la demás información sobre inicio de aplicaciones, acciones predeterminadas, información sobre encuesta y alarmas y vistas de ManageWORKS. Si no suprime ManageWORKS después de actualizar a ServerWORKS Manager, puede seguir utilizándolo *por separado* desde ServerWORKS Manager.

Después de actualizar a ServerWORKS Manager

Ocurrirán las condiciones siguientes:

- La primera vez que ejecuta ServerWORKS Manager después de actualizar de ManageWORKS V2.2, aparece el mensaje siguiente "¡Se detectó una inconsistencia en la base de datos!". Elija el botón Ignorar. En el cuadro de diálogo siguiente, elija el botón Ignorar siempre para evitar ver el mensaje cada vez que ejecuta ServerWORKS Manager.
- Cuando está descubriendo una red utilizando IP Discovery Wizard después de hacer una actualización, se le pide que elija una vista de mapas para los resultados de descubrimiento. Los visores de mapas son equivalentes, por lo que puede seleccionar cualquiera.
- Si conserva la base de datos de ManageWORKS, se crea un visor de sólo lectura que se llama Examinador. No puede eliminarlo.
- Para inicializar una base de datos de ManageWORKS después de actualizar a ServerWORKS Manager V3.x, primero cierre todos los componentes de ServerWORKS Manager (Event Logger, Event Dispatcher, Poller, Ping Server y Data Collector).

Luego inicialícelo utilizando la utilidad ServerWORKS Manager DB Utility con el procedimiento siguiente:

1. Desde el menú Iniciar, elija Programas→ServerWORKS DB Utility.
2. Seleccione "Toda la base de datos excepto MIB".
3. Haga clic en Inicializar.
4. Elija Aceptar para salir de la utilidad.

Procedimientos e información adicionales

Si conserva la versión V2.2 de ManageWORKS y la ejecuta sin toda la línea de comandos (incluyendo el archivo de inicialización SWMGR.INI), obtendrá punteros de la ruta de la base de datos incorrectos de la nueva versión además de los mensajes siguientes:

```
CODEBASE ERROR
Wrong DB version 0.0.0
Expected DB version 2.0.X
```

Si no suprime las opciones del menú de ManageWORKS del menú Inicio, puede ocurrir el mismo comportamiento.

Procedimientos e información adicionales

Solución de problemas *B*

Esta sección describe ocurrencias comunes cuando una instalación no se realiza de manera satisfactoria y sugiere soluciones. Revise la lista para esta situación precisa si no está satisfecho con la instalación. Si todavía realiza la instalación, se recomienda que revise la lista antes de continuar.

Problemas comunes y soluciones

Condición	No se inicia ServerWORKS Manager. Es posible que la última vez que se salió de ServerWORKS Manager u otro componente que utiliza el archivo PCMGR.MDB no haya sido normal o que el cierre del sistema no haya sido correcto (por ejemplo, una anomalía en la alimentación).
Acción	<p>El archivo .MDB de la base de datos necesita corregirse. Para hacerlo, siga los pasos siguientes:</p> <ol style="list-style-type: none">1. Inicie la utilidad de administración de ODBC desde el Panel de control.2. Haga clic en la página DSN de usuario.3. Seleccione SWMgrDB.4. Haga clic en el botón Configure (Configurar).

Solución de problemas

5. Haga clic en el botón Repair (Corregir).
6. Elija OK (Aceptar) para salir.
7. Vuelva a iniciar y pruebe ServerWORKS Manager de nuevo.

Condición

Event Logger de ServerWORKS Manager no registra sucesos como se esperaba.

Acción

Esta condición puede tener una de las causas siguientes:

1. Si Event Logger se finaliza de manera anormal (por ejemplo, se cierra desde System Tray), no se registran los nuevos sucesos y no se confirman los sucesos existentes. El reiniciar la consola de administración puede corregir este problema.
2. Si sucesos no confirmados llenan el registro, el búfer del registro alcanza el límite y nuevos sucesos se agregan al registro desde la parte superior del búfer, sobrescribiendo los sucesos existentes. Incremente el tamaño del archivo de búfer con la utilidad ServerWORKS Manager DB Utility.
3. Event Logger reconoce nombres de comunidad desde SNMP Traps de sólo hasta seis caracteres. Los nombres más largos se truncan. Revise la documentación del sistema operativo para obtener información sobre la definición de nombres de comunidad.

Condición

El servicio de SNMP no se inicia a partir del programa de instalación o desde el comando NET START SNMP.

Acción

Primero verifique el Visor de sucesos y busque uno de los mensajes siguientes:

En NT 4.0: Servicio de SNMP está ignorando el destino de captura <nombre de nodo> porque no es válido.

Si ve estos mensajes, utilice el procedimiento siguiente:

1. Suprima el nodo que está causando el problema de la lista de destino de capturas en el cuadro de diálogo SNMP Service Configuration (Configuración del servicio SNMP).

Solución de problemas

2. Inicie SNMP desde el indicador de DOS con el comando NET START SNMP. Repita este procedimiento para cada nodo que tenga una falla en la lista.
3. Si hay muchos destinos de capturas listados, haga lo siguiente:
4. Desde el indicador de DOS, introduzca NET STOP SNMP para asegurar que se ha parado el servicio SNMP.
5. Inicie el servicio con el comando SNMP.
6. Verifique si Event Log tiene errores y suprima de la lista de destino de capturas cualquier nodo que se haya agotado

Hay otros errores de SNMP que pueden hacer que el error 1 específico del servicio se envíe al registro de sucesos. Si el procedimiento anterior no cambia la condición, considere las alternativas siguientes:

- Verifique la configuración de DNS y WINS. Asegúrese de que la búsqueda de LMHOSTS esté activada si trata de resolver el problema utilizando LMHOSTS.
- Un solo destino no válido puede causar un tiempo de espera si la red se está ejecutando lentamente. La espera de tiempos de espera múltiples causará este problema en una red sin problemas.

Configuración de un módem y puerto de comunicaciones para comunicación por Pager

Si todavía no lo ha hecho, instale el hardware y software del módem siguiendo las instrucciones del fabricante.

Intente marcar del módem utilizando cualquier software de acceso telefónico. Si no puede conectarse y comunicarse con el número telefónico de la ubicación de prueba, vuelva a verificar la computadora: las conexiones computadora a módem y módem a teléfono y asegúrese de que esté encendido el módem. También verifique que el número telefónico, los códigos de área y de país sean los correctos. Consulte las instrucciones del fabricante de software de acceso telefónico para obtener detalles sobre el software.

Solución de problemas

Si no puede realizar la instalación con éxito, puede editar las claves de Registro para ServerWORKS Manager Console, ClientWORKS y los agentes.

Antes de editar el Registro, revise las pautas siguientes:

Edición del Registro

En algunos casos, la nueva instalación puede seguir fallando si las versiones anteriores de ServerWORKS , ManageWORKS y ClientWORKS no se instalaron correctamente. Algunas versiones anteriores de estos productos no se pueden suprimir completamente sin intervenir en el Registro.

Primero debe suprimir el software en el Panel de control→ficha Agregar o quitar programas. Luego puede suprimir elementos del Registro. Puede encontrar el Registro en las ubicaciones siguientes:

- En, Windows NT\Windows\Regedt32.exe
- En Windows 95 \Windows\Regedit.exe

Supresión de claves de registro

Siga los pasos que se presentan a continuación antes de editar el Registro.

- Siempre utilice la opción unInstallShield del menú ServerWORKS Manager Console o en el Panel de control→ficha Agregar o quitar programas primero para suprimir versiones anteriores de ServerWORKS Manager Console, ClientWORKS y los agentes.
- Siempre haga una copia de seguridad del Registro antes de editarla en caso de que deba restaurar un Registro dañado. Desde el editor de Registro, utilice Registro→Exportar archivo de Registro para guardar el archivo como un archivo .reg. La ayuda en línea de Registro describe cómo completar este procedimiento y restaurar la copia de seguridad del Registro.
- Es posible que las claves y los valores sean diferentes para sistemas Windows NT y Windows 95.

Solución de problemas

- No todas las claves y los valores aparecen en todos los sistemas. Es posible que las claves introducidas con versiones anteriores sean obsoletas aunque permanezcan en el sistema.
- Si el sistema no contiene un valor para una clave como se lista en las tablas siguientes, no suprima la clave.
- Las claves y los valores están sujetos a modificaciones entre las versiones.



Aviso: No edite el Registro, a menos que esté familiarizado con los sistemas operativos Windows NT o Windows 95. No suprima la ruta arborescente completa.

Claves de Registro para ServerWORKS

Tabla B-1 Claves de Registro para la clave HKEY_LOCAL MACHINE de ServerWORKS

HKEY_LOCAL_MACHINE\

 \\SOFTWARE\ODBC\ODBC.INI\ODBC Data Sources

 \\SOFTWARE\ODBC\ODBC.INI\SWMgrDB

 \\SOFTWARE\ODBC\ODBC.INI\SWMgrDBEmpty

HKEY_LOCAL_MACHINE

 \\SOFTWARE\DigitalEquipmentCorporation\ServerWORKS Manager Console\4.0

 \\SOFTWARE\Microsoft\Windows\CurrentVersion\AppPaths\pwMgmt.EXE

 \\SOFTWARE\Microsoft\Windows\CurrentVersion\AppPaths\smb.exe

Claves de Registro para agentes

Tabla B-2 Claves de Registro para la clave HKEY_LOCAL MACHINE de agentes

HKEY_LOCAL_MACHINE

\\SOFTWARE\\DigitalEquipmentCorporation\\CimHealthAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\CimHostAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\CimScsiAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\CimSinfoAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\CimStdeqAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\CimThresAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\DigitalClusterExtensionAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\DigitalCommonClusterAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\HostResourcesAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\ServerManagementAgent

\\SOFTWARE\\DigitalEquipmentCorporation\\ServerSystemAgent

\\System\\CurrentControlSet\\Services\\SNMP\\Parameters\\Extension Agents

\\System\\CurrentControlSet\\Services\\SNMP\\Parameters\\ServerSystemAgent
\\SvrCpuPIInterval

Claves de Registro para ClientWORKS

Tabla B-3 Claves de Registro para la clave HKEY_LOCAL_MACHINE de ClientWORKS

HKEY_LOCAL_MACHINE

- \\SOFTWARE\\DigitalEquipmentCorporation\\AssetWORKS LiveLINK
- \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS
- \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS\\CW Shared
- \\SOFTWARE\\DigitalEquipmentCorporation\\DMI\\2.00
- \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS DMI Browser
- \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS DMIExplorer
- \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS SMART
- \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS SNMP
- \\SOFTWARE\\DigitalEquipmentCorporation\\Host Resources Agent
- \\SOFTWARE\\DigitalEquipmentCorporation\\Server Management Agent
- \\SOFTWARE\\DigitalEquipmentCorporation\\Server System Agent
- \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS Init

HKEY_LOCAL_MACHINE

- \\SYSTEM\\CurrentControlSet\\Services\\DIGITAL DMI Instrumentation
- \\SYSTEM\\CurrentControlSet\\Services\\tvdddrv
- \\SYSTEM\\CurrentControlSet\\Services\\Win32sl
- \\SYSTEM\\CurrentControlSet\\Control\\VirtualDeviceDrivers\\VDD

Tabla B-4 Claves de Registro para la clave HKEY_CURRENT_USER de ClientWORKS

HKEY_CURRENT_USER

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall
 \\ClientWORKS

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\CWSNMP1.0

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\LiveLINK1.0

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\SMART1.0

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\DMIPATH

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\
 Digital DMI

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\
 Digital SmartMonitor

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Read BIOS

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\SNMP

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\CW SMARTMonitor

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\CW Shared

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\SecureOnClient

\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Win32SL

Referencias C

El hecho de familiarizarse con los fundamentos de la red y el sistema operativo es crítico para utilizar las funciones de ServerWORKS Manager a su potencial máximo. Se sugiere leer las fuentes siguientes.

Bibliografía

Tema	Fuente de información adicional
DIGITAL UNIX	Network Administration and Network Programmer's Guide
Descubrimiento de objetos en la red	Ayuda en línea, Capítulo 3 de este manual.
KCRCM	KCRCM AlphaServer Remote Console Module Installation and User's Guide (EK-KCRCM-IN) incluido con el producto KCRCM
Supervisión de sistemas	<u>The Simple Book</u> - An Introduction to Internet Management por Marshall T. Rose, publicado por Prentice Hall 1991, II Ed. SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards por William Stallings, publicado por Addison Wesley 1993

continúa

Referencias

Tema	Fuente de información adicional
Supervisión de sistemas (continuación)	<u>Internetworking with TCP/IP</u> , Volumen 2, Design, Implementation, and Internals por Douglas E. Comer y David L. Stevens, publicado por Prentice Hall 1991 <u>Internetworking with TCP/IP</u> , Volumen 1, Principles, Protocols, and Architecture por Douglas E. Comer; publicado por Prentice Hall 1991, II Ed.
Mylex GAM	Mylex Global Array Manager 2 Installation and User's Guide (ER-MYL02-IA) incluido en el CD-ROM de ServerWORKS Manager en la sección de documentación
Novell NetWare	Novell's Guide to Multiprotocol Internetworking, por Laura A. Chappell and Roger L. Spicer publicado por Novell Press NetWare, The Professional Reference, Tercera edición, publicado por News Rider Publishing 1994
OpenVMS	TCP/IP Networking on OpenVMS Systems and OpenVMS System Manager's Manual
RSM	RSM Installation Guide (ER-PCDSC-IA) y RSM Station Software User's Guide (ER-PCDSM-UA) incluido con el producto RSM
SCO UNIX	SCO OpenServer Handbook How to install, configure, and start using an SCO OpenServer system, publicado por The Santa Cruz Operation 1995

continúa

Referencias

Tema	Fuente de información adicional
Envío de SNMP Traps	Ayuda en línea, Capítulo 5 de este manual. The Simple Book - An Introduction to Internet Management por Marshall T. Rose, publicado por Prentice Hall 1991, II Ed. SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards por William Stallings, publicado por Addison Wesley 1993
Definir y recibir alarmas SNMP	Ayuda en línea, Capítulo 5 de este manual The Simple Book - An Introduction to Internet Management por Marshall T. Rose, publicado por Prentice Hall 1991, II Ed. SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards por William Stallings, publicado por Addison Wesley 1993 Internetworking with TCP/IP Volume 2 Design, Implementation, and Internals por Douglas E. Comer y David L. Stevens publicado por Prentice Hall 1991
SWCC	StorageWORKS Command Console Installation Guide (AA-ROHJB-TE) incluido en el CD-ROM de ServerWORKS Manager en la sección de documentación
Windows 95	Microsoft Windows 95 Resource Kit publicado por Microsoft Press 1995

continúa

Referencias

Tema	Fuente de información adicional
SNMP de Windows 95	Microsoft Windows 95 Resource Kit publicado por Microsoft Press 1995
Windows NT	Windows NT Networking Guide - Windows NT Resource Kit por y publicado por Microsoft Press
Windows NT SNMP Service	Windows NT Networking Guide - Windows NT Resource Kit publicado por Microsoft Press

Sitio Web

El sitio Web siguiente también puede proporcionar información adicional sobre ServerWORKS:

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

Glosario

Los términos siguientes se utilizan frecuentemente en cualquier discusión de administración de redes y de SNMP.

Término	Definición
Alarma	SNMP Trap generada por un agente o un suceso y accionada por los resultados de la encuesta de un agente.
Unidades de asignación	Tamaño en bytes para un dispositivo de almacenamiento determinado. Por ejemplo, las unidades de asignación para un disco por lo general son 512, 1024 o 2048 bytes y algunas veces se les denomina "tamaño de bloque".
Clúster	
Uso de la CPU	Porcentaje medio de tiempo en que este procesador no estuvo inactivo.

continúa

Referencias

Término	Definición
Data Collector	Proceso que se ejecuta en Manager Console y que encuesta objetos sobre los datos de SNMP. Collector analiza los datos y genera alarmas o pasa los datos a aplicaciones registradas como System Browser.
DMI	Desktop Management Interface (Interfaz de administración de escritorio).
FAT	File Allocation Table (Tabla de asignación de archivos, listada en la página Propiedades del sistema de archivos de System Browser).
Uso del sistema de archivos	Porcentaje del sistema de archivos que se está usando (sistemas de archivos locales).
IP	Internet Protocol (protocolo Internet) (véase también TCP/IP).
Dirección IP	Dirección de un objeto en una red. La dirección estándar está compuesta de cuatro números, cada uno de los cuales es inferior a 255.
Management Information Base (MIB)	Especificación de datos para pasar información utilizando el protocolo SNMP.
MIF	Management Information File (Archivo de información de administración) - Es un archivo de la base de datos que define una configuración de host dada, inventario de hardware, dispositivos de almacenamiento, procesadores, y memoria.
Punto de montaje	Nombre del nivel superior para un sistema de archivos montado.
MTU	Maximum Transmission Unit (Unidad de transmisión máxima).
Interfaz de red	Comunicación entre la máquina de Manager Console y la red. Normalmente completada a través de tarjetas de interfaz de red.
Errores de entrada de interfaz de red	Número de paquetes de entrada que contienen errores que les impiden ser transmitidos a un protocolo de la capa superior.

Referencias

Término	Definición
Paquetes de entrada rechazados de la interfaz de red	Número de paquetes de entrada que se han elegido para que se descarten, aún cuando no se ha detectado ningún error para evitar que se entreguen a un protocolo de la capa superior. Una razón posible para rechazar un paquete de este tipo podría ser liberar espacio en el búfer.
Paquetes de entrada de la interfaz de red	Número de paquetes entregados a un protocolo de la capa superior.
Errores de salida de la interfaz de red	Número de paquetes de salida que no pueden ser transmitidos debido a errores.
Errores de protocolo desconocidos de interfaz de red	Número de paquetes recibidos a través de la interfaz que fueron descartados debido a un protocolo desconocido o no soportado.
NOS	Network Operating System (Sistema operativo de red). Sistema operativo y protocolo usado para comunicarse entre los objetos de una red.
NTFS	NT File System (Sistema de archivos NT). Sistema de archivos usado en NT.
Intervalo de encuesta	Tiempo entre las consultas de encuesta de un dispositivo.
Valor de reactivación	Valor que se puede definir en la pantalla de umbral para activar automáticamente una alarma que se ha accionado previamente.
SNMP	Simple Network Management Protocol. El protocolo de aplicación que ofrece el servicio de administración de red en Internet.
SNMP Trap	Un suceso asíncrono generado por el agente y enviado al administrador de SNMP.
Alarma de estado	Alarma definida sobre los discos o los procesadores de servidor para indicar el estado del dispositivo (opciones en ejecución, no funcionales, y alerta).

Referencias

Término	Definición
Nombre de sistema	Nombre del objeto en la red IP según lo define el servidor de nombres o se encuentra en el archivo de hosts en la máquina de Manager Console.
Tiempo de activación del sistema	Tiempo que el sistema ha estado activado desde que se inició.
TCP/IP	Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisión/protocolo Internet). Conjunto de software de protocolos de comunicación ampliamente utilizado. TCP transmite datos en una conexión entre aplicaciones en diferentes computadoras de una red. IP controla cómo se transfieren los paquetes (unidades de datos) entre las computadoras de una red.
Alarma de umbral	Alarma accionada cuando un valor introducido en la pantalla de alarma de umbral cumple con una condición específica.
Valor de umbral	Valor en el cual se acciona una alarma (por ejemplo, 10000 paquetes por segundo).

Referencias

Índice

—A—

- Access, 7-14
- Acción alfanumérica de Pager, 5-18
- Acción de notificación
 - correo electrónico, 5-20
- Acción de notificación de Pager
 - procedimiento, 5-18
- Acción de Pager
 - resultados de obtención de alarma, 5-19
 - tiempo de espera predeterminado, 5-20
- Acción numérica de Pager, 5-18
- Acciones
 - correo electrónico, 5-21
 - correo electrónico, requisito de perfil predeterminado, 5-21
 - inicio de aplicación, 5-23
 - Pager, 5-18
- Acciones predeterminadas
 - especificar aplicación para iniciarla, 7-6
- Acciones, asociadas con Minimal Health, 5-9
- Actualización
 - lista de alarmas configuradas, 5-6
- Administración de grupos
 - objetos, 7-4
- Administración de servidores Novell NetWare, 4-2
- Administrador de servidores de NT
 - Descubrimiento, 8-2
- Adobe Acrobat Reader, 3-16
- Agente de extensión SNMP de DIGITAL, 2-5
- Agentes
 - administración de servidores, 3-12
 - controladores RAID, 3-24
 - DIGITAL UNIX, 3-13
 - extensión, proceso, 2-4
 - función, 1-2, 2-3
 - Insight Manager, 3-12
 - instalados en la máquina de consola, 3-13
 - instalar en la consola de administración, 3-18
 - Minimal Health, 5-8
 - NetWare, 3-12
 - OpenVMS, 3-13
 - OS/2, 3-13
 - proporcionados con ServerWORKS, 3-12
 - requisitos de hardware, 3-6
 - requisitos de software, 3-6
 - SCO UNIX 5. x, 3-12
 - Versión 1.x, 5-8
 - Versión 2.x, 5-9
 - Windows NT, 3-12
- Agentes de DSM, A-4
- Agentes DMI
 - proporcionados con ServerWORKS, 3-3
- Agentes SNMP
 - configurar antes de la instalación, 3-12
 - proporcionados con ServerWORKS, 3-3
- Agentes Versión 1.x, 5-12
- Agentes Versión 2.x, 5-12

Índice

- Ajustar mapas a escala, 7-2
- Alarm Configuration
 - (ordenar columnas), 5-5
 - Barra de herramientas (*ilus.*), 5-4
 - descripción de la ventana, 5-2
 - esquemas de la pantalla, 5-3
- Alarmas
 - acciones de notificación, 5-13
 - configurar, 5-7
 - creación, procedimiento, 5-13
 - definidas desde otras fuentes, 5-6
 - directivas de configuración, 5-18
 - estado de componente, 5-9
 - estado de componentes, procedimiento, 5-14
 - estado de sistema, procedimiento, 5-16
 - estado del sistema, 5-9
 - imprimir informe, 4-20
 - indicadores durante la configuración, 5-11
 - lista guardada, 5-6
 - Minimal Health, 5-7
 - Minimal Health, eliminar, 5-9
 - Minimal Health, ver, 5-5
 - modificar, 5-17
 - múltiples en host, 5-8
 - SNMP Traps, 5-9
 - SNMP Traps, procedimiento, 5-16
 - umbral de componente, 5-9
 - umbral de componente, procedimiento, 5-15
 - vistas por host, 5-5
- Alarmas ambientales, 1-4
- Alarmas de ambiente
 - Novell NetWare, Minimal Health, 5-8
 - Windows NT, Minimal Health, 5-7
- Alarmas de consola, 5-9
- Alarmas de estado de componente, 5-9, 5-10
- Alarmas de estado del sistema, 5-9, 5-13
- Alarmas de Minimal Health, 5-7
- Alarmas de SNMP Trap, 5-9, 5-13
- Alarmas de umbral de componente, 5-9, 5-10
- Alarmas definidas por el usuario, 5-9
- Alarmas múltiples en host, 5-8
- Alarmas predeterminadas. Consúltese Minimal Health
- Alarmas, accionadas
 - vistas Visor de alarmas, 5-2
- Alarmas, configuradas
 - en la consola, ver, 5-5
 - imprimir la lista de, 5-7
- Alarmas, definidas por el usuario
 - con umbrales, 5-10
- Alinear objetos, 4-10
- APPL_GR, 7-15
- APS PowerNet, 1-7
- Archivo de segundo plano
 - para visores de mapas, 7-2
- Archivo poller.log, 7-13
- Archivos por lotes
 - para modificar Registro, (*ej.*), 7-27
- Archivos Report.txt, 4-17
- Asociación
 - tipo de objeto con iconos, 4-6
 - tipo de objeto con MIB, 6-18

—B—

- Bandeja de sistema, 6-18, 6-19, 6-20
- Barra de estado de la alarma, 4-4
- Barra de herramientas, 4-6
 - cambiar en botones, 4-6

Índice

- Barra de menús, 4-4
- Base de datos
 - conservación, A-10
 - utilizar anterior, 3-11
 - versiones anteriores, conservar, 3-11
 - versiones soportadas, 3-11
- Base de datos de ServerWORKS Manager, 7-14
- Bases de datos
 - ManageWORKS, A-11
- Blancos, en gráficas, 6-10
- Botones de consulta
 - modificar, 6-15
- C—
- Capturas
 - configurar destinos, 2-9
 - identificación por la red, 2-9
 - requisitos, 2-9
- capturas múltiples
 - en dispositivos múltiples, agentes diferentes, 5-12
- Categorías para alarmas, 5-14
- Cerrar un mapa o un visor, 4-7
- Clasificación
 - alarmas configuradas, 5-5
- ClientWORKS, 1-6
 - desinstalar, 3-9
- Clusters
 - alarmed, viewed on map, 4-3
- Clústers
 - definir alarmas en, 5-24
 - descubiertos, en el mapa (*ilus.*), 4-15
 - descubrimiento, 4-2
 - en descubrimientos, 4-11
 - en visores de mapas, (*ilus.*), 7-26
 - en vista de Explorer, 4-14
 - información sobre variables de MIB, 6-16
 - presentación en un mapa, 4-14
 - requisitos de software, 3-8
- Códificación en color
 - estado, 4-18
- Colecciones, 4-3, 7-9
- Colores
 - modificar, 7-2
- Comas
 - utilizadas en Pager, 5-20
- Compaq ProLiant 2500, 7-18
- Compilación de MIBs, 6-17
- Comunicación
 - de escritorio, sistemas móviles, con ServerWORKS, 1-2
- Comunidad Public, 4-11
- Conducta de ventanas
 - en mapas, 7-2
- Conexiones
 - mostrar, ocultar, 4-9
- Configuración de alarmas, 5-7
- Configuración de SNMP
 - requisitos para ServerWORKS, 2-7
- Consola de administración, 2-3
- Contexto
 - en la aplicación, en el nodo, 7-5
- Controlador StorageWorks RAID de DIGITAL.
 - Consúltese StorageWorks Command Console.*
- Copiar objetos, entre visores, 4-9
- Cuadrícula

Índice

mostrar, ocultar, 4-9

—D—

Data Collector, 6-19, 6-20

Database Utility, 7-17

para reparar tablas de bases de datos, 7-17

procedimientos, 7-17

y tabla de registros de alarmas, 7-17

Datos de Fuera de línea, 6-5

Datos históricos

recopilación, 6-10

Demonios

NetView, 3-10

ServerWORKS, 3-10, 6-19, 6-20

Demonios de ServerWORKS, 3-10

Desactivar, activar Minimal Health, 5-8

Descubrimiento

clúster, 4-2

clústers, 4-14

objetos de IP, 4-2

objetos de NetWare, 4-2

objetos de NT, 4-2

objetos de SNMP, 4-2

tiempo requerido, 4-13

Descubrimiento de redes

procedimiento, 4-11

Descubrimientos

posteriores, 4-13

Desplazamiento de objetos, al mapa, 4-9

Destinos de captura

configurar para el dispositivo remoto desde

Consola, 7-34

Destinos de capturas

con DHCP, 2-9

especificar, 7-32

Detalles de alarma

visualizar, 4-19

DHCP, 2-9

DIGITAL OpenVMS

agentes de ServerWORKS, 3-4

DIGITAL UNIX, C-1

agentes de instalación, A-2

Dirección MAC, 3-2

Discovery

informes impresos, 4-16

DMI, 1-2

Domain Name Server, 3-2

Dominios, 7-9

Dominios, Windows NT, 7-10

—E—

Editor de planes de sistema, 7-33

Ejemplos de mapas de bits, 7-19

Elaboración de gráficas, 6-7

Eliminación de objetos

en Windows NT, 4-10

Encontrar

subredes, en un mapa, 4-8

Encuesta

crear grupo de administración para, 7-11

frecuencia, para alarmas, 5-14

parámetros de grupo, 7-12

por grupo, 6-19, 7-10

Especificar nombres de nodo

en System Browser, 6-5

Estado

de objetos, colores asignados por estado,

4-18

Índice

- de objetos, en la Barra de estado, 4-19
- de red, colas visuales en vistas, 4-17
- Estados
 - de alarmas, 5-14
- Event Dispatcher, 6-19, 6-20
 - reenvío de capturas, 7-37
- Event Logger, 6-19, 6-20
 - problemas, B-2
- EVT_LOG, 7-15
- Excel, 6-10

—F—

- Falla
 - definir alarma, procedimiento, 5-24
 - detección desde Visor de alarmas, 5-26
 - elecciones de mensajes de alarma, 5-24
- Filtro de alarmas, para visualizar, 4-21
- Formas de segundo plano, 7-19
- Frecuencia de encuesta
 - para alarmas, 5-15
- Fuera de línea
 - nodos, ver en System Browser, 6-10

—G—

- Global Array Manager. Consúltase Mylex GAM
- Graficar
 - procedimiento, 6-9
- Gráficas
 - como muestran condiciones, 6-2
 - navegar por datos históricos, 6-11
- Grupo
 - SNMP (*def.*), 7-4

- Grupo de almacenamiento
 - de System Browser, contenido, 6-4
- Grupo de ambiente
 - de System Browser, contenido, 6-4
- Grupo de red de System Browser, contenido, 6-4
- Grupo de sistema
 - de System Browser, contenido, 6-4
- Grupos de MIB
 - almacenar, 7-20
 - asignar a un objeto, 7-21
- Guardar alarmas, 5-6
- Guardar visores de mapas, 4-3

—H—

- Historia de nodo, 6-10
- Hosts DIGITAL
 - System Browser para, 6-2
- HyperTerminal
 - utilizado con RMC, 3-15

—I—

- Icono de campana
 - mostrar alarmas accionadas, 4-3
 - mostrar alarmas configuradas, 5-5
- Icono de cruz roja, 5-5
- Icono de punto de exclamación, 5-5
- Iconos
 - alarmas de Minimal Health en el host, 5-5
 - en Visor de mapas, 4-3
 - en vista Explorer, 4-4
 - host con cualquier alarma, 5-5
 - hosts nunca encuestados para alarmas, 5-5

Índice

- Importación
 - a Excel, desde el Visor de alarmas, 4-21
 - Impresoras
 - descubrimiento, 7-8
 - Información histórica
 - en System Browser, 6-2
 - Informe de dirección IP, 4-17
 - imprimir, 4-17
 - Informe de IP Discovery
 - imprimir, 4-17
 - Informes de IP Discovery, 4-16
 - Iniciar la consola, 4-7
 - Inicio de aplicaciones
 - con contexto, 7-5, 7-6
 - Inicio de aplicación
 - notificación, 5-23
 - Insight Manager, 7-5
 - Instalación
 - cerrar otros programas, 3-10
 - ClientWORKS, 3-23
 - ClientWORKS, 3-13
 - elección de directorio predeterminado, 3-9
 - instrucciones para todos los componentes, 3-15
 - kit, 3-16
 - Mylex GAM, 3-25
 - problema de no completar, 3-10
 - RCM, 3-14
 - requisitos de administrador de NT, 3-9
 - RSM, 3-14, 3-25
 - secuencia para instalar componentes, 3-8
 - selección del idioma, 3-9
 - ServerWORKS Console, 3-20
 - en Windows 95, 3-19
 - software de agente de ServerWORKS Manager, 3-17
 - StorageWORKS, 3-24
 - tareas realizadas después de, 3-26
 - Tutorial, 3-26
 - y privilegios de administrador, 3-9
 - Integración
 - MIBs, 1-4
 - programas de administración de empresas, 3-11
 - resultados de, 1-6
 - IP Discovery
 - elaboración de mapas, 4-2
 - explicación, 4-11
 - IPREPORT, 4-16
- K—**
- KCRCM, C-1
- L—**
- Líneas de comandos
 - acción de inicio de aplicación, 5-23
 - especificar para aplicaciones, 7-6
- M—**
- Management Information Base, 2-2
 - ManageWORKS
 - actualización, A-9
 - Mapa de IP Discovery, 4-3
 - Mapas
 - personalizados, 7-3
 - visores lógicos, 7-3
 - Mapas de bits

Índice

- ocultar, 7-2
 - ServerWORKS, ubicación, 7-19
 - Máscaras de red
 - elegir para descubrimientos, 7-9
 - Mensaje Current Controller, 5-24
 - Mensaje Not Current Controller, 5-24
 - Mensajes de Pager
 - contenido, 5-18
 - Menú Herramientas
 - personalizar, 7-3
 - MIB
 - detalles de variables, 7-21
 - variables, encontrar en listas, 7-22
 - MIB Browser
 - funcionamiento, 6-12
 - inicio, 6-12
 - ver datos de clúster, 6-16
 - MIB Compiler, 6-17
 - MIB de recursos de host (RFC1514), 2-2
 - MIB Enroller, 6-18
 - MIB II, 6-13
 - MIB Profiler, 6-18
 - MIB_CLAS, 7-15
 - MIB_DESC, 7-15
 - MIB_NAME, 7-15
 - MIB_PROF, 7-15
 - MIB_TABL, 7-15
- MIBs
- fuentes de variables de SNMP, 5-13
 - funciones, 2-2
 - modificar variables, 7-13
 - parámetros, 6-12
 - variables, 6-12
 - variables definidas, 7-21
 - variables, modificar, 6-13
 - ver contenido, 6-15
 - ver descripciones de variables, 6-15
- Microsoft Access
 - conflicto entre versiones, 3-11
 - Microsoft Excel, 6-10
 - MIF Browser, 6-17
 - Minimal Health
 - agentes, 5-8
 - alarmas
 - visualización para hosts múltiples, 5-9
 - descripción, 1-4
 - instalación, 5-8
 - nombres de acción
 - especificar acciones para, 5-24
 - nombres de configuración de acción, 5-24
 - plantilla, 5-23
 - Minimal Healthcomportamiento, 5-8
 - Módems
 - configurar, B-3
 - Modificación
 - alarmas, 5-17
 - variables de MIB, 6-18
 - Modificar
 - nombres globales, 7-13
 - números asignados de FRU, 6-6
 - objetos, permanentemente por cambio con el archivo por lotes, 7-28
 - propiedades de objeto, 7-14
 - tipos de objeto, 7-13
 - Mostrar, ocultar cuadrícula, 4-9
 - Mylex GAM, 1-6
 - más información, C-2

Índice

—N—

Navegador
 utilizar, 4-8

Navegar
 en visores, 4-8

NetView
 cerrar para instalar ServerWORKS, 3-10

NetWare
 agentes en ServerWORKS, 3-3
 utilidades, 8-6

NetWare Server Manager, 8-5

Nodos Generic
 en descubrimientos, 4-11

Nombre de comunidad
 recepción de capturas, 2-7

Nombre de comunidad Public, 2-8, 7-37

Nombres de comunidad, 2-8, 7-34
 en NT, 2-8
 en seguridad de SNMP, 7-29
 predeterminada, 7-37

Nombres de comunidades
 en IP Discovery, 4-11

Nombres de nodo
 especificar en System Browser, 6-5

Nombres globales
 modificar, 7-13

Notificación de alarma
 acciones, frecuencia de, 5-17
 correo electrónico, 5-21
 inicio de aplicación, 5-23

Notificación de alarma por correo electrónico,
 5-20

Notificación de alarmas

Pager, 5-19

Notificación de Pager
 procedimiento, 5-19

Novell NetWare, C-2.

NT Server Management, 4-2

Número de acceso telefónico de terminal, 5-18

Número de NIP, 5-18

Números asignados, 6-6

Números de FRU, 6-6

—O—

O/S2
 instalar agentes, A-6

O/S2 Warp 3.0
 agentes de ServerWORKS, 3-4

OBJ_DEF, 7-15

OBJ_IP, 7-15

OBJ_SNMP, 7-15

Objeto raíz, 8-2

Objetos
 administración de grupos, 7-4
 bajo un objeto raíz, 4-4
 eliminación, 4-10
 encontrados por ServerWORKS, 1-2
 insertar tipos manualmente en un mapa, 7-
 23
 manipular presentación en mapas, 4-9
 nombres, 7-19
 seleccionar mapas de bits, 7-19
 supresión, 4-10
 Unknown.Type (Tipo desconocido), 7-25
 ver propiedades, 7-13

Objetos de clúster
 expandir, 4-2

Índice

Objetos de IP
 descubrimiento, 4-2

Objetos de proveedores múltiples, 1-1

Objetos de servidor
 descubrimiento, 4-2

Objetos de SNMP
 descubrimiento, 4-2

Ocultar nodos, 7-2

OpenVMS, C-2
 instalar agentes, A-2

OpenVMS Management Station, 3-11, A-9

Operación Trap (de captura), 2-4

Operaciones de SNMP, 2-3

Operaciones Get, 2-3

Operaciones Set, 2-3
 en MIB Browser, 6-12

Ordenar
 alarmas, en el Visor de alarmas, 4-19

—P—

Página de propiedades Directivas, 5-17

Paleta, 4-6

Paleta del Visor de mapas. Consulte

Paquetes de entrada de red, 5-13

Paquetes de salida de red, 5-12

Parámetros de correo de Exchange, 5-21

PCMGR.mdb, 7-14

Perfil de configuración de Microsoft Exchange,
 5-20

Perfil de correo electrónico, 5-21
 configurar en Exchange, 5-21

Perfil predeterminado
 correo de Exchange, 5-21

Personalizar

 visores, mapas, 7-2

Peticiones de ICMP, 6-19

Peticiones de IP, 6-19

Pila del protocolo SNMP
 uso de ServerWORKS, 1-3

Ping, 6-19

POLEDIT.EXE, 7-33

Poller, 6-19

Posicionamiento automático de objetos, 4-9

Presentación de objetos en mosaico, 4-9

Primer descubrimiento, 4-11

Programas de administración de empresas
 integración con ServerWORKS, 3-22

Programas de administrador, 2-3

Programas de administrador de empresas,
 integración con ServerWORKS, 1-3

Puerto de comunicaciones, B-3

Puerto de SNMP Trap, 2-6

—R—

RCM
 instalación, 3-14

Recopilación de datos
 en System Browser, 6-5

Reenvío de capturas, 2-7, 7-37
 definición, 7-37

Registro
 modificar para el descubrimiento de nuevos
 objetos, 7-26

 problemas, B-2

Reinicio, 5-12

Relaciones de confianza, NT, 3-2

Remote Server Manager (RSM), 1-6

Requisito del protocolo TCP/IP, 3-5, 3-7

Índice

Requisitos de hardware

- agentes, 3-6
- para la Consola, 3-4

Requisitos de software

- agentes, 3-6
- clústers, 3-8
- ServerWORKS, 3-5

RFC1213, 6-13

RMC, 1-6

- sistemas soportados, 3-14

Router

- en descubrimientos, 4-11

RSM, C-2

- instalación, 3-14

—S—

Salir

- de ServerWORKS, todos los procesos, 4-7
- de un mapa o un visor, 4-7

SCO UNIX, C-2

- agentes en ServerWORKS, 3-3

Seguridad de SNMP, 7-29

ServerWORKS

- cerrar para instalar, 3-10
- requisitos de configuración de la red, 3-2, 7-13
- requisitos de hardware de la consola, 3-4
- requisitos de software de la consola, 3-5

ServerWORKS Explorer

- con descubrimiento de Administrador de servidores NT, 8-2
- con descubrimiento de NetWare, 8-5

ServerWORKS Manager

- actualizar de ManageWORKS, A-10

- agentes de extensión, 2-2

- falla al iniciarse, B-1

- integración con administradores de empresas, 1-3

- ventajas, 1-2

ServerWORKS Manager de DIGITAL.

- Consúltese ServerWORKS Manager

Servicio de SNMP

- falla en el inicio, B-2

- nombre de destino no válido, B-3

Servicio DMI, 6-17

Servicio SNMP

- instalar en Windows 95, 7-32

- instalar en Windows NT, 7-29

Servidor DNS, 2-9, 3-2

Severidad

- para alarmas, 5-14, 5-15

Sistema

- estadísticas vitales, 7-3

Sistemas Alpha

- instalar agentes SNMP, A-8

- restricciones en agentes SNMMP, A-7

Sistemas de escritorio, 1-1

SNMP, 1-2, 1-3, 2-2, C-4

- autenticación, 2-8

- configurar en sistemas, 2-6

- configurar, en Windows 95, 7-32

- usar para comunicarse, 2-6

SNMP Traps

- configurar correctamente, 5-9

- longitud del nombre de comunidad, B-2

- reenvío, 5-9

Solución de problemas, B-1

StorageWorks Command Console, 3-24

Índice

Subredes
 en descubrimientos, 4-11
Sucesos no confirmados, B-2
Supervisión inteligente, 1-4
Supresión de objetos, 4-10
svrSystemDescr, 4-11
SWCC, 1-6
 más información, C-3
SysDescr de SNMP, 7-25
SysObjectID de SNMP, 7-24, 7-25
System Browser, 6-2
 detalles disponibles, 6-4
 inicio, 6-5
 ver hosts múltiples, 6-6

—T—

Tabla de registros de alarmas, 7-17
Tablas de bases de datos
 contenido, 7-14
Tareas de segundo plano, 6-18, 6-19, 6-20
 inicio automático, 3-21
 ServerWORKS, 3-10
Tiempo de espera de Pager, 5-20
Tiempo de espera predeterminado de Pager, 5-20
Tipo de objeto
 en visor de mapas, (diag.), 7-26
Tipos de objeto
 asociar tipo desconocido a un tipo de objeto conocido, 7-25
 definir nuevo, 7-18
 impresoras, 7-8
 modificar, 7-14
 personalizados, 7-18

 personalizar, para la red, 7-18
TME 10 NetView, 3-10
TRAP_ENT, 7-15

—U—

Umbrales
 agentes de la Versión 1.x, 5-8
 definición de capturas múltiples, 5-12
 en dispositivos múltiples, 5-11
 operadores de relación para, 5-10
 para alarmas, 5-15
 y las versiones diferentes de agentes, 5-11

—V—

Valor de encuesta
 y reinicio, 5-12
Variable de entorno
 TEMP, 3-9
Variable de entorno TEMP, 3-9
Variables de MIB de clústers
 prefijos, 6-16
Variables de MIB II, 6-12
Variables de MIBs
 ver, 6-16
Ventana Alarm Configuration (*ilus.*), 5-4
Ventana MIB Browser (*ilus.*), 6-14
Ventana System Browser (*ilus.*), 6-3
Ver
 datos históricos, 6-11
 datos, en nodos múltiples, 6-5, 6-6
Ver alarmas
 accionadas en mapas, 4-3
Ver datos

Índice

- en nodos múltiples, 6-6
- Verificación de alarmas, 4-19
- Visor de alarmas
 - utilizar para verificar alarmas, 4-19
- Visor de alarmas, (*ilus.*), 4-20
- Visor de mapas
 - eliminar, 4-3
 - inserción de objetos, 4-3
 - modificar, 4-3
 - objetos con alarma en, 4-3
 - plegar y desplegar, 4-4
 - uso para encontrar objetos específicos, 4-3
- Visor de mapas (*ilus.*), 4-4
- Visor de sucesos de NT
 - utilizar para seguir alarmas, 7-40
- Visores
 - ajustar tamaño, 4-8
 - cerrar, 4-7
 - fuera de la ventana, 4-8
 - salir de, 4-7
- Visores de mapas
 - guardar, 4-3
- Vistas
 - navegar, 1-5

- opciones, 1-2
- Visualización de alarmas
 - actualizar lista, 5-6
 - configuradas, por host, 5-5
- Visualización de Explorer, 4-2
 - características, 4-3
- Visualización de ServerWORKS Explorer.
- Visualizaciones
 - Explorer, 4-2

—W—

- WatchDog Timer
 - desactivar, 3-28
 - en servidores DIGITAL, 3-27
 - en UNIX, 3-28
- Windows 95
 - agentes en ServerWORKS, 3-3
- Windows NT
 - agentes en ServerWORKS, 3-3
 - privilegios de administrador para instalar ServerWORKS, 3-9
 - requisitos de administrador, 3-2
 - y ServerWORKS, 3-2