

WebSphere™ Edge Server para multiplataformas



Network Dispatcher Guía de administración

Versión 2.0

WebSphere™ Edge Server para multiplataformas



Network Dispatcher Guía de administración

Versión 2.0

Nota

Antes de utilizar esta información y el producto al que se refiere, lea la información general del “Apéndice I. Avisos” en la página 397.

Contenido

Tablas	xi	¿Por qué se necesita Network Dispatcher?	26
Figuras	xiii	¿Cuáles son las nuevas funciones?	28
Bienvenido	xv	¿Cuáles son los componentes de Network Dispatcher?	33
Cómo enviar sus comentarios	xv	Visión general del componente Dispatcher	33
Capítulo 1. Iniciación rápida	1	Visión general del componente Content Based Routing (CBR)	36
¿Qué se necesitará?	2	Visión general del componente Mailbox Locator	38
¿Cómo se debe preparar?	2	Visión general del componente Site Selector	39
Configuración del componente Dispatcher	3	Visión general del componente Consultant para Cisco CSS Switches	41
Configuración mediante la línea de mandatos	3	Acerca de la alta disponibilidad Dispatcher	44
Configuración mediante el asistente para configuración	4	CBR, Mailbox Locator, Site Selector	44
Configuración mediante la interfaz gráfica de usuario (GUI)	5	Capítulo 4. Planificación del componente Dispatcher	45
Comprobación de la configuración	7	Requisitos de hardware y de software	45
Tipos de configuraciones de clusters, puertos y servidores	7	Consideraciones referentes a la planificación Alta disponibilidad	47
Capítulo 2. Instalación de Network Dispatcher	11	Alta disponibilidad simple	47
Requisitos para AIX	12	Alta disponibilidad mutua	48
Instalación en AIX	13	Método de reenvío mac del Dispatcher	49
Antes de la instalación	14	Método de reenvío nat del Dispatcher	50
Pasos de instalación	14	Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)	52
Requisitos para Red Hat Linux o SuSe Linux	16	Capítulo 5. Configuración del componente Dispatcher	55
Instalación en Linux	17	Visión general de las tareas de configuración	55
Antes de la instalación	18	Métodos de configuración	55
Pasos de instalación	18	Línea de mandatos	56
Requisitos para Solaris	19	Scripts	56
Instalación en Solaris	20	GUI	57
Antes de la instalación	20	Asistente de configuración	58
Pasos de instalación	20	Configurar la máquina Dispatcher	58
Requisitos para Windows 2000	22	Paso 1. Iniciar la función de servidor	60
Instalación para Windows 2000	23	Paso 2. Iniciar la función de ejecutor	60
Paquetes de instalación	23	Paso 3. Definir la dirección de no reenvío (si es diferente del nombre de sistema principal)	61
Antes de la instalación	23	Paso 4. Definir un cluster y establecer las opciones de cluster	61
Pasos de instalación	23		
Capítulo 3. Presentación de Network Dispatcher	25		
¿Qué es Network Dispatcher?	25		

Paso 5. Crear un alias para la tarjeta de interfaz de red	61
Paso 6. Definir los puertos y establecer las opciones de puerto.	63
Paso 7. Definir los servidores con reparto del tráfico.	64
Paso 8. Arrancar la función gestor (opcional).	64
Paso 9. Arrancar la función asesor (opcional).	64
Paso 10. Establecer las proporciones del cluster según sea necesario	65
Configuración de las máquinas servidor para el reparto del tráfico	65
Paso 1. Crear un alias para el dispositivo de bucle de retorno	65
Paso 2. Comprobar si existe una ruta sobrante	68
Paso 3. Eliminar las rutas sobrantes	69
Paso 4. Comprobar que el servidor está configurado debidamente	69
Instalación del parche del kernel de Linux (para suprimir las respuestas a arp en la interfaz de bucle de retorno)	70

Capítulo 6. Planificación del componente

Content Based Routing	75
Requisitos de hardware y de software	75
Consideraciones referentes a la planificación	75
Reparto del tráfico a través de conexiones SSL totalmente seguras	78
Reparto del tráfico entre el cliente y el proxy en CBR y entre el proxy y el servidor en HTTP	78

Capítulo 7. Configuración del componente

Content Based Routing	81
Visión general de las tareas de configuración	81
Métodos de configuración	81
Línea de mandatos.	82
Scripts	84
GUI.	84
Asistente de configuración	85
Configuración de la máquina CBR	86
Paso 1. Configurar Caching Proxy para utilizar CBR	87
Paso 2. Iniciar la función del servidor	88
Paso 3. Iniciar la función del ejecutor	89
Paso 4. Definir un cluster y establecer las opciones de cluster.	89

Paso 5. Crear un alias para la tarjeta de interfaz de red (opcional)	89
Paso 6. Definir los puertos y establecer las opciones de puerto.	90
Paso 7. Definir las máquinas servidor sujetas a reparto del tráfico	90
Paso 8. Añadir normas a la configuración	91
Paso 9. Añadir servidores a las normas	91
Paso 10. Iniciar la función del gestor (opcional).	91
Paso 11. Iniciar la función del asesor (opcional).	91
Paso 12. Establecer las proporciones del gestor según sea necesario	91
Paso 13. Iniciar Caching Proxy	92
Ejemplo de configuración de CBR.	92

Capítulo 8. Planificación para el componente Mailbox Locator

Requisitos de hardware y de software	95
Consideraciones referentes a la planificación	95
Uso de la función de afinidad	97
Alteración del temporizador de inactividad de POP3/IMAP.	97

Capítulo 9. Configuración del componente

Mailbox Locator	99
Visión general de las tareas de configuración	99
Métodos de configuración	100
Línea de mandatos	100
Scripts	101
GUI	101
Asistente de configuración	102
Configuración de la máquina Mailbox Locator	103
Paso 1. Iniciar la función de servidor	103
Paso 2. Definir un cluster y establecer las opciones de cluster	103
Paso 3. Definir los puertos y establecer las opciones de puerto	103
Paso 4. Definir servidores de reparto del tráfico.	104
Paso 5. Iniciar la función del gestor (opcional)	104
Paso 6. Iniciar la función del asesor (opcional)	104
Paso 7. Establecer las proporciones del cluster según sea necesario.	104

Capítulo 10. Planificación para el componente Site Selector 107

Requisitos de hardware y de software . . .	107
Consideraciones referentes a la planificación	107
Consideraciones sobre TTL.	110
Utilización de la función de Proximidad en la Red	110

Capítulo 11. Configuración del componente Site Selector 113

Visión general de las tareas de configuración	113
Métodos de configuración	113
Línea de mandatos	114
Scripts	114
GUI	115
Asistente de configuración	116
Configuración de la máquina Site Selector	116
Paso 1. Iniciar la función de servidor . .	117
Paso 2. Iniciar el servidor de nombres . .	117
Paso 3. Definir un nombre de sitio y establecer las opciones de nombre de sitio	117
Paso 4. Definir servidores de reparto del tráfico.	117
Paso 5. Iniciar la función del gestor (opcional)	118
Paso 6. Iniciar la función del asesor (opcional)	118
Paso 7. Definir la métrica del sistema (opcional)	118
Paso 8. Establecer las proporciones del nombre de sitio según sea necesario. . .	118
Configuración de las máquinas servidor para el reparto del tráfico	118

Capítulo 12. Planificación para el componente Consultant para Cisco CSS Switches 119

Requisitos de hardware y de software . . .	119
Consideraciones referentes a la planificación	119

Capítulo 13. Configuración del componente Consultant para Cisco CSS Switches 125

Visión general de las tareas de configuración	125
Métodos de configuración	126
Línea de mandatos	126
Scripts	127
GUI	127
Configuración de la máquina Consultant para Cisco CSS Switches	128

Paso 1. Iniciar la función de servidor . . .	128
Paso 2. Configurar la función del ejecutor	129
Paso 3. Definir un cluster y establecer las opciones de cluster	129
Paso 4. Definir los puertos y establecer las opciones de puerto	129
Paso 5. Definir servidores con reparto del tráfico.	129
Paso 6. Iniciar la función del gestor . . .	130
Paso 7. Iniciar la función del asesor (opcional)	130
Paso 8. Establecer las proporciones del cluster según sea necesario.	130
Paso 9. Iniciar Metric Server (opcional)	130
Comprobación de la configuración	130

Capítulo 14. Funciones avanzadas de Network Dispatcher 131

Optimización del reparto del tráfico proporcionado por Network Dispatcher . .	134
Grado de importancia dado a la información de estado	135
Pesos	136
Intervalos de gestor	137
Umbral de sensibilidad	138
Índice de corrección	138
Utilización de scripts para generar una alerta o registrar un error de servidor . .	139
Asesores	139
Cómo funcionan los asesores	140
Inicio y detención de un asesor	140
Intervalos de asesor	141
Tiempo de caducidad del informe del asesor.	142
Tiempo de espera de conexión y de recepción del asesor para servidores . .	142
Lista de asesores	143
Creación de asesores personalizados (personalizables)	145
Asesor WebSphere Application Server .	146
Convenio de denominación	146
Compilación	146
Ejecución	147
Rutinas necesarias	147
Orden de búsqueda	148
Nomenclatura y vía de acceso	148
Asesor de ejemplo	149
Asesor de Workload Manager.	149
Restricción de Metric Server	150
Metric Server	150

Restricción de WLM	150	Utilización de normas basadas en el ancho de banda reservado y en el ancho de banda compartido	177
Requisitos previos	150	Norma de la métrica total	179
Cómo utilizar Metric Server	150	Norma de la métrica promedio	180
Particionamiento del servidor: servidores lógicos configurados para un solo servidor físico (dirección IP)	152	Utilización de normas que son siempre ciertas.	180
Opción de petición/respuesta del asesor HTTP (URL)	154	Utilización de normas basadas en el contenido de la petición.	181
Utilización de servidores de ubicación compartida	155	Adición de normas a la configuración	182
Para el componente Dispatcher	155	Opción de evaluación de servidor para normas	182
Para el componente CBR	156	Utilización de enlaces explícitos	183
Para el componente Mailbox Locator	156	Utilización de una configuración de red privada	184
Para el componente Site Selector	157	Utilizar el cluster comodín para combinar configuraciones de servidores.	185
Para el componente Cisco Consultant	157	Utilizar el cluster comodín para repartir el tráfico de los cortafuegos	186
Configurar el soporte de Dispatcher para área amplia	157	Utilización del cluster comodín con Caching Proxy para proxy transparente	187
Sintaxis de los mandatos	158	Utilización del puerto comodín para dirigir el tráfico de puertos no configurados	187
Utilización de asesores remotos con soporte de área amplia	159	La función de afinidad de Network Dispatcher	188
Ejemplo de configuración	161	Comportamiento con la afinidad inhabilitada	188
Notas	163	Comportamiento con la afinidad habilitada	188
Soporte de GRE (Generic Routing Encapsulation).	163	API de afinidad dirigida por el servidor (SDA) para controlar la afinidad cliente-servidor	188
Utilización del asesor self en una configuración WAND de dos niveles	164	Afinidad entre puertos	189
Alta disponibilidad	165	Máscara de dirección de afinidad	190
Configurar la característica de alta disponibilidad	166	Alteración temporal de afinidad de norma	191
Posibilidad de detección de anomalías mediante pulsos y el destino de acceso	169	Desactivación de conexiones persistentes	192
Estrategia de recuperación	169	Opción de afinidad en la norma	193
Utilización de scripts.	170	Afinidad activa de cookie	193
Configurar el reparto del tráfico basado en normas	173	Afinidad pasiva de cookie	194
¿Cómo se evalúan las normas?	174	Afinidad de URI	195
Utilización de normas basadas en la dirección IP del cliente	175	Detección de ataques de denegación de servicio	197
Utilización de normas basadas en la hora del día	175	Utilizar las anotaciones en binario para analizar las estadísticas del servidor	198
Utilización de normas basadas en las conexiones por segundo de un puerto	175	Información adicional sobre las funciones avanzadas de Cisco Consultant	200
Utilización de normas basadas en el total de conexiones activas en un puerto	176	Pesos de Cisco Consultant	202
Utilización de normas basadas en el puerto del cliente	177		
Utilización de normas basadas en el tipo de servicio (TOS)	177		

Capítulo 15. Utilización y gestión de Network Dispatcher	205
Administración autenticada remota	205
Utilización de los archivos de anotaciones de Network Dispatcher	207
Cambio de la vía de acceso de los archivos de anotaciones	208
Utilización del componente Dispatcher	209
Inicio y detención de Dispatcher	209
Utilización del valor de tiempo de espera de inactividad	209
Utilización del número de conexiones finalizadas (FIN) para controlar la recogida de basura	210
GUI de notificación — la opción de menú Supervisor	210
Utilización de SNMP (Simple Network Management Protocol) con el componente Dispatcher	211
Utilización de ipchains o iptables para rechazar todo el tráfico para (reforzar) el recuadro Network Dispatcher (en Linux)	216
Utilización del componente Content Based Routing	217
Inicio y detención de CBR	217
Control de CBR	217
Utilización de archivos de anotaciones de CBR	217
Utilización del componente Mailbox Locator	217
Inicio y detención de Mailbox Locator	217
Control de Mailbox Locator	218
Utilización de los archivos de anotaciones de Mailbox Locator	218
Utilización del componente Site Selector	218
Inicio y detención de Site Selector	218
Control de Site Selector	218
Utilización de los archivos de anotaciones de Site Selector	218
Utilización del componente Cisco Consultant	219
Inicio y detención de Cisco Consultant	219
Controlar Cisco Consultant	219
Utilización de los archivos de anotaciones de Cisco Consultant	219
Utilización del componente Metric Server	219
Inicio y detención de Metric Server	219
Utilización de los archivos de anotaciones de Metric Server	219
Capítulo 16. Resolución de problemas	221
Tablas de resolución de problemas	221

Comprobar los números de puerto de Dispatcher	227
Comprobación de los números de puerto de CBR	228
Comprobación de los números de puerto de Mailbox Locator	228
Comprobación de los números de puerto de Site Selector	229
Comprobación de los números de puerto de Cisco Consultant	230
Resolución de problemas habituales—Dispatcher	230
Problema: Dispatcher no funcionará	230
Problema: Dispatcher y el servidor no responderán	230
Problema: no se realiza el reparto del tráfico para las peticiones de Dispatcher	231
Problema: la modalidad de alta disponibilidad de Dispatcher no funciona	231
Problema: no se puede añadir pulso (Windows 2000)	231
Problema: rutas sobrantes (sólo Windows 2000)	232
Problema: los asesores no funcionan correctamente	232
Problema: SNMPPD no se ejecuta correctamente (Windows 2000)	232
Problema: Dispatcher, Microsoft IIS y SSL no funcionan (Windows 2000)	232
Problema: conexión de Dispatcher a una máquina remota	232
Problema: el mandato ndcontrol o ndadmin da error	232
Problema: se visualiza el mensaje de error del tipo “No se puede encontrar el archivo...” al intentar visualizar la ayuda en línea (Windows 2000)	233
Problema: mensaje falso de error al iniciar ndserver en Solaris 2.7	234
Problem: la interfaz gráfica de usuario (GUI) no arranca correctamente	234
Problema: error al ejecutar Dispatcher cuando Caching Proxy está instalado	234
Problema: la interfaz gráfica de usuario (GUI) no se visualiza correctamente	234
Problema: en Windows 2000, las ventanas de ayuda algunas veces quedan ocultas detrás de otras ventanas abiertas	234
Problema: Network Dispatcher no puede procesar y reenviar una trama	235

Problema: aparece una pantalla azul al iniciar el ejecutor de Network Dispatcher .	235	Problema: el mandato lbcccontrol o ndadmin falla	242
Problema: la vía de acceso de descubrimiento impide la devolución de tráfico con Network Dispatcher	235	Problema: No se puede crear el registro para el puerto 14099	242
Problema: los asesores muestran que todos los servidores están inactivos . .	236	Resolución de problemas habituales—Metric Server.	243
Problema: la alta disponibilidad en la modalidad de área amplia de Network Dispatcher no funciona	237	Problema: excepción de E/S de Metric Server en Windows 2000 al ejecutar los archivos de métrica del usuario .bat o .cmd	243
Problema: la GUI se cuelga (o se comporta de forma inesperada) cuando se intenta cargar un archivo de configuración grande	237	Problema: Metric Server no notifica cargas a la máquina Network Dispatcher . . .	243
Resolución de problemas habituales—CBR	238	Problema: las anotaciones de Metric Server indican que "se necesita una firma para poder acceder al agente".	244
Problema: CBR no funcionará.	238		
Problema: el mandato cbrcontrol o ndadmin falla	238		
Problema: no se realiza el reparto del tráfico para las peticiones	239		
Problema: en Solaris, el mandato cbrcontrol executor start falla	239		
Problema: error sintáctico o de configuración	239		
Resolución de problemas habituales—Mailbox Locator	239		
Problema: Mailbox Locator no funcionará	239		
Problema: el mandato mlserver está detenido	240		
Problema: el mandato mlcontrol o ndadmin falla	240		
Problema: no se puede añadir un puerto	240		
Problema: se recibe un error de proxy al intentar añadir un puerto	241		
Resolución de problemas habituales—Site Selector	241		
Problema: Site Selector no funcionará . .	241		
Problema: Site Selector no efectúa un reparto rotatorio para el tráfico procedente de clientes Solaris	241		
Problema: el mandato sscontrol o ndadmin falla	241		
Problema: ssserver no se inicia en Windows 2000	241		
Problema: Site Selector no reparte el tráfico correctamente si hay rutas duplicadas	242		
Resolución de problemas habituales —			
Consultant para Cisco CSS Switches . . .	242		
Problema: lbccserver no arranca	242		
		Apéndice A. Cómo leer un diagrama de sintaxis	245
		Símbolos y puntuación	245
		Parámetros	245
		Ejemplos de sintaxis	246
		Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator . . .	249
		Diferencias de configuración entre CBR, Mailbox Locator y Dispatcher.	250
		ndcontrol advisor — controlar el asesor . .	252
		ndcontrol cluster — configurar clusters . .	258
		ndcontrol executor — controlar el ejecutor	263
		ndcontrol file— gestionar archivos de configuración	268
		ndcontrol help — visualizar o imprimir ayuda para este mandato	270
		ndcontrol highavailability — controlar la alta disponibilidad	272
		ndcontrol host — configurar una máquina remota	277
		ndcontrol log — controlar el archivo de anotaciones en binario	278
		ndcontrol manager — controlar el gestor . .	279
		ndcontrol metric — configurar métricas del sistema	285
		ndcontrol port — configurar puertos . . .	287
		ndcontrol rule — configurar normas . . .	294
		ndcontrol server — configurar servidores	302
		ndcontrol set — configurar anotaciones de servidor	308
		ndcontrol status — visualizar si el gestor y los asesores están en funcionamiento . . .	309

ndcontrol subagent — configurar subagente SNMP	310
---	-----

Apéndice C. Sintaxis de la norma de contenido (patrón):. 313

Sintaxis de la norma de contenido (patrón):	313
Palabras clave reservadas	313

Apéndice D. Consulta de mandatos de Site Selector 317

sscontrol advisor — controlar el asesor. . .	318
sscontrol file — gestionar archivos de configuración	324
sscontrol help — visualizar o imprimir ayuda para el mandato	326
sscontrol manager — controlar el gestor . .	327
sscontrol metric — configurar métricas del sistema	332
sscontrol nameserver — controlar el servidor de nombres	333
sscontrol rule — configurar normas.	334
sscontrol server — configurar servidores . .	338
sscontrol set — configurar archivo de anotaciones del servidor	340
sscontrol sitename — configurar un nombre de sitio	341
sscontrol status — visualizar si el gestor y los asesores están en ejecución	345

Apéndice E. Consulta de mandatos de Consultant para Cisco CSS Switches . . 347

lbcontrol advisor — controlar el asesor . .	348
lbcontrol cluster — configurar clusters . .	353
lbcontrol executor — controlar el ejecutor	355
lbcontrol file — gestionar archivos de configuración	357
lbcontrol help — visualizar o imprimir ayuda para el mandato	359
lbcontrol host — configurar una máquina remota	360

lbcontrol log — controlar el archivo de anotaciones en binario	361
lbcontrol manager — controlar el gestor	362
lbcontrol metric — configurar métricas del sistema	368
lbcontrol port — configurar puertos . . .	370
lbcontrol server — configurar servidores	372
lbcontrol set — configurar archivo de anotaciones del servidor	374
lbcontrol status — visualizar si el gestor y los asesores están en ejecución	375

Apéndice F. Ejemplos de archivos de configuración. 377

Archivos de configuración de ejemplo para Network Dispatcher	377
Archivo de configuración de Dispatcher—para AIX, Red Hat Linux y Solaris	377
Archivo de configuración de Dispatcher—Windows	381
Asesor de ejemplo	384

Apéndice G. Ejemplo de una configuración de alta disponibilidad de 2 niveles utilizando Dispatcher, CBR y Caching Proxy 391

Configuración de la máquina servidor . . .	391
--	-----

Apéndice H. Otros recursos 395

Acceso desde la línea de mandatos	395
Obtención de ayuda en línea	395
Información de consulta	395

Apéndice I. Avisos 397

Marcas registradas	398
------------------------------	-----

Glosario 401

Índice 413

Tablas

1.	Imágenes installp de AIX	13
2.	Mandatos de instalación de AIX	15
3.	Tareas de configuración de la función Dispatcher	55
4.	Mandatos para unir el dispositivo de bucle de retorno (lo0) por medio de un alias para Dispatcher	66
5.	Mandatos para eliminar rutas sobrantes para Dispatcher	69
6.	Tareas de configuración para el componente CBR	81
7.	Mandatos para unir el NIC por medio de un alias	89
8.	Tareas de configuración para el componente Mailbox Locator	99
9.	Tareas de configuración para el componente Site Selector	113
10.	Términos de configuración de Consultant y Cisco CSS Switch	121
11.	Ejemplo de configuración de Cisco CSS Switch y la correspondiente configuración de Consultant	123
12.	Tareas de configuración para el componente Consultant para Cisco CSS Switches	125
13.	Tareas avanzadas de configuración para Network Dispatcher	131
14.	Tabla de resolución de problemas de Dispatcher	221
15.	Tabla de resolución de problemas de CBR	224
16.	Tabla de resolución de problemas de Mailbox Locator	224
17.	Tabla de resolución de problemas de Site Selector	225
18.	Tabla de resolución de problemas de Consultant para Cisco CSS Switches	226
19.	Tabla de resolución de problemas de Metric Server	226

Figuras

1. Configuración local simple de Dispatcher	1
2. La interfaz gráfica de usuario (GUI)	5
3. Ejemplo de Dispatcher configurado con un cluster individual y 2 puertos	7
4. Ejemplo de Dispatcher configurado con 2 clusters, cada uno con 1 puerto	8
5. Ejemplo de Dispatcher configurado con 2 clusters, cada uno con 2 puertos	9
6. Ejemplo de representación física de un sitio Web que utiliza Dispatcher para gestionar servidores locales	34
7. Ejemplo de sitio Web que utiliza Dispatcher y Metric Server para gestionar servidores	35
8. Ejemplo de sitio Web en el que se utiliza Dispatcher para gestionar servidores locales y remotos	36
9. Ejemplo de sitio Web que utiliza CBR para gestionar servidores locales	37
10. Ejemplo de sitio Web que utiliza Mailbox Locator para gestionar servidores locales	39
11. Ejemplo de sitio Web donde se utilizan Site Selector y Metric Server para gestionar servidores locales y remotos	40
12. Ejemplo de sitio que utiliza Cisco Consultant y Metric Server para gestionar servidores locales	43
13. Ejemplo de Dispatcher utilizando la alta disponibilidad simple	47
14. Ejemplo de Dispatcher utilizando la alta disponibilidad mutua	48
15. Ejemplo de las direcciones IP que se necesitan para la máquina Dispatcher	60
16. Archivo de configuración CBR para AIX	87
17. Archivo de configuración de CBR para Linux	88
18. Archivo de configuración de CBR para Solaris	88
19. Archivo de configuración de CBR para Windows 2000	88
20. Ejemplo de un entorno DNS	108
21. Ejemplo de Consultant configurado con 2 clusters, cada uno con 3 puertos	122
22. Ejemplo de configuración formada por un sólo segmento de LAN	157
23. Ejemplo de configuración utilizando servidores locales y remotos	158
24. Ejemplo de configuración de área amplia con Network Dispatchers remotos	161
25. Ejemplo de configuración de área amplia con plataforma de servidor que da soporte a GRE	164
26. Ejemplo de configuración WAND de dos niveles con utilización del asesor self	165
27. Ejemplo de una red privada mediante Dispatcher	185
28. Mandatos SNMP para AIX y Solaris	212
29. Mandatos de SNMP para Windows 2000	213
30. Ejemplo de una configuración de alta disponibilidad de 2 niveles utilizando Dispatcher, CBR y Caching Proxy	391

Bienvenido

Este manual explica la forma de planificar, instalar, configurar, utilizar y resolver problemas de IBM® WebSphere Edge Server Network Dispatcher para AIX, Linux, Solaris y Windows 2000. Anteriormente, este producto se llamaba SecureWay Network Dispatcher, eNetwork Dispatcher e Interactive Network Dispatcher.

En el sitio Web de WebSphere Edge Server hallará la versión más reciente del presente manual en formato HTML y PDF. Para acceder a la publicación en línea, vaya al URL siguiente:

<http://www.ibm.com/software/webservers/edgeserver/library.html>

En el sitio Web de WebSphere Edge Server encontrará la información detallada más reciente referente a la manera de utilizar Network Dispatcher, a fin de aumentar al máximo el rendimiento de los servidores. Se incluyen casos prácticos y ejemplos de configuración. Para acceder a este sitio Web, vaya al URL siguiente:

<http://www.ibm.com/software/webservers/edgeserver>

Para obtener las actualizaciones más recientes y consejos sobre la utilización de Network Dispatcher, visite la página Web de soporte de WebSphere Edge Server y pulse *Search for Network Dispatcher hints and tips*. Para acceder a esta página Web, vaya al URL siguiente:

<http://www.ibm.com/software/webservers/edgeserver/support.html>

Cómo enviar sus comentarios

La información que nos proporcione nos ayuda a mejorar la precisión y la calidad de la información. Si desea realizar comentarios sobre este manual o cualquier otro documento de WebSphere Edge Server:

- Envíe sus comentarios por correo electrónico a fsdoc@us.ibm.com. Asegúrese de incluir el nombre del manual, el número de pieza del mismo, la versión de WebSphere Edge Server, y, si procede, la ubicación específica del texto sobre el que realiza el comentario (por ejemplo, el número de página o el número de tabla).

Capítulo 1. Iniciación rápida

¿Con qué rapidez puede hacer que Network Dispatcher trabaje para usted? Considere lo siguiente:

Supongamos que usted es el administrador del sitio Web de Intersplash Corporation. Se encarga de gestionar un sitio Web local con dos servidores HTTP. Ha estado utilizando un método rotatorio para gestionar el tráfico de los dos servidores, pero el negocio ha crecido recientemente y los clientes comienzan a quejarse de que no pueden acceder al sitio Web. ¿Qué puede hacer?

Diríjase a <http://www.ibm.com/software/webservers/edgeserver> y baje la última versión de Network Dispatcher. Este producto tiene cinco componentes: Dispatcher, Content Based Routing (CBR), Mailbox Locator, Site Selector y Consultant para Cisco CSS Switches (Cisco Consultant). De momento, sólo trataremos el componente **Dispatcher**.

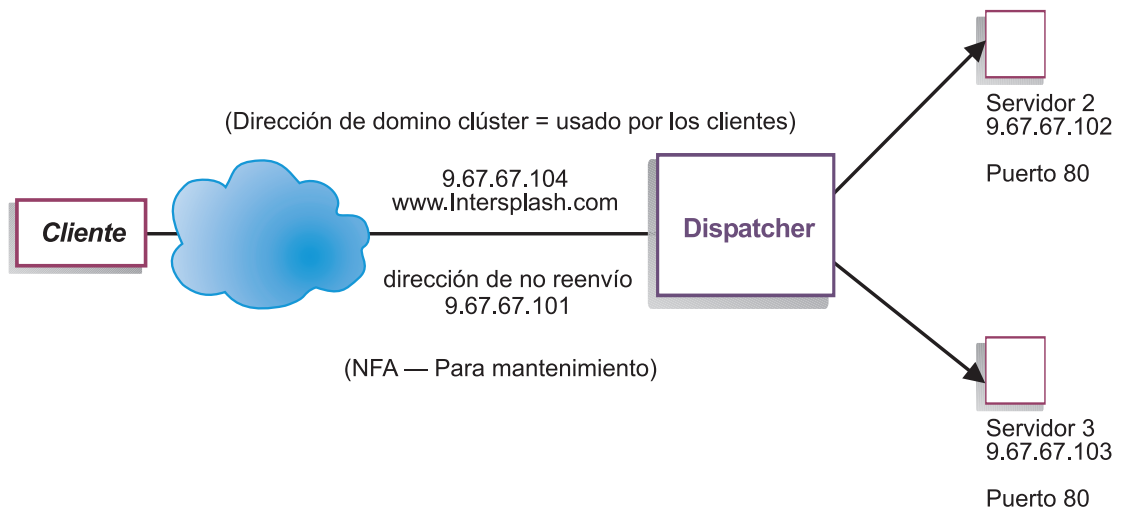


Figura 1. Configuración local simple de Dispatcher

Este ejemplo de iniciación rápida muestra cómo configurar tres estaciones de trabajo conectadas localmente utilizando el método de reenvío MAC del componente Dispatcher para repartir el tráfico Web entre dos servidores Web.

La configuración debe ser fundamentalmente la misma para distribuir cualquier otro tráfico de aplicación TCP o UDP sin estados.

Nota: Con la versión de Dispatcher para AIX, Linux o Solaris, la configuración podría completarse solamente utilizando dos estaciones de trabajo con Dispatcher ubicado en una de las estaciones de trabajo de servidor Web. Representa una configuración de ubicación compartida. Los procedimientos para poner a punto configuraciones más complejas se encuentran en “Configurar la máquina Dispatcher” en la página 58.

¿Qué se necesitará?

Para el ejemplo de iniciación rápida, necesitará tres estaciones de trabajo y cuatro direcciones IP. Una estación de trabajo se utilizará como Dispatcher; las otras dos estaciones de trabajo se utilizarán como servidores Web. Cada servidor Web necesita una sola dirección IP. La estación de trabajo de Dispatcher necesita una dirección real y una dirección para repartir el tráfico.

¿Cómo se debe preparar?

1. Asegúrese de que se cumplen los requisitos previos, enumerados en el “Capítulo 2. Instalación de Network Dispatcher” en la página 11.
2. Configure las estaciones de trabajo de manera que se encuentren en el mismo segmento de la LAN. Asegúrese de que el tráfico de red entre las tres máquinas no debe atravesar ningún encaminador o puente.
3. Configure los adaptadores de red de las tres estaciones de trabajo. En este ejemplo, supondremos que dispone de la siguiente configuración de red:

Estación de trabajo	Nombre	Dirección IP
1	servidor1.intersplash.com	9.67.67.101
2	servidor2.intersplash.com	9.67.67.102
3	servidor3.intersplash.com	9.67.67.103
Máscara de red = 255.255.255.0		

Cada una de las estaciones de trabajo contiene solamente una tarjeta de interfaz de red Ethernet estándar.

4. Asegúrese de que servidor1.intersplash.com puede enviar mensajes PING tanto a servidor2.intersplash.com como a servidor3.intersplash.com.
5. Asegúrese de que tanto servidor2.intersplash.com como servidor3.intersplash.com pueden enviar mensajes PING a servidor1.intersplash.com.
6. Asegúrese de que el contenido sea el mismo en los dos servidores Web (Servidor 2 y Servidor 3). Esto se puede llevar a cabo replicando los datos

en ambas estaciones de trabajo por medio de un sistema de archivos compartidos como NFS, AFS, DFS o por cualquier otro medio apropiado para su sitio Web.

7. Asegúrese de que los servidores Web de `servidor2.intersplash.com` y `servidor3.intersplash.com` son funcionales. Utilice un navegador Web para solicitar páginas directamente a **`http://servidor2.intersplash.com`** y **`http://servidor3.intersplash.com`**.
8. Obtenga una nueva dirección IP válida para este segmento de la LAN. Esta será la dirección que proporcionará a los clientes que deseen acceder al sitio Web. En este ejemplo utilizaremos:
Nombre= `www.intersplash.com`
IP=`9.67.67.104`
9. Configure las dos estaciones de trabajo de servidor Web para que acepten tráfico destinado a `www.intersplash.com`.
Añada un alias para `www.intersplash.com` a la interfaz de **bucle de retorno** en `servidor2.intersplash.com` y en `servidor3.intersplash.com`.
 - Para AIX:
`ifconfig lo0 alias www.intersplash.com netmask 255.255.255.0`
 - Para Solaris 7:
`ifconfig lo0:1 www.intersplash.com 127.0.0.1 up`
 - Para otros sistemas operativos, consulte la Tabla 4 en la página 66.
10. Suprima cualquier ruta sobrante que se haya podido crear como consecuencia de crear un alias para la interfaz de bucle de retorno. Consulte “Paso 2. Comprobar si existe una ruta sobrante” en la página 68. Ya ha realizado todos los pasos de configuración necesarios en las dos estaciones de trabajo de servidor Web.

Configuración del componente Dispatcher

Con Dispatcher, puede crear una configuración mediante la línea de mandatos, el asistente para la configuración o la interfaz gráfica de usuario (GUI).

Nota: Los valores de parámetros se deben escribir en caracteres ingleses. Las únicas excepciones son los valores de parámetros para nombres de sistema principal y nombres de archivo.

Configuración mediante la línea de mandatos

Si está utilizando la línea de mandatos, siga estos pasos:

1. Inicie el `ndserver` en Dispatcher:
 - Para AIX, Linux o Solaris, ejecute el mandato siguiente como usuario root: **`ndserver`**

- En Windows 2000, ndserver se ejecuta como servicio que se inicia automáticamente.
2. Inicie la función executor de Dispatcher:
ndcontrol executor start
 3. Añada la dirección del cluster a la configuración de Dispatcher:
ndcontrol cluster add www.intersplash.com
 4. Añada el puerto de protocolo http a la configuración de Dispatcher:
ndcontrol port add www.intersplash.com:80
 5. Añada cada servidor Web a la configuración de Dispatcher:
ndcontrol server add www.intersplash.com:80:servidor2.intersplash.com
ndcontrol server add www.intersplash.com:80:servidor3.intersplash.com
 6. Configure la estación de trabajo para aceptar el tráfico destinado a la dirección del cluster:
ndcontrol cluster configure www.intersplash.com
 7. Inicie la función manager de Dispatcher:
ndcontrol manager start
Dispatcher comenzará a realizar el reparto del tráfico basándose en el rendimiento del servidor.
 8. Inicie la función advisor de Dispatcher:
ndcontrol advisor start http 80
Dispatcher se asegurará ahora de que las peticiones de los clientes no se envíen a un servidor Web anómalo.

Ha finalizado la configuración básica con servidores conectados localmente.

Configuración mediante el asistente para configuración

Si está utilizando el asistente para configuración, siga estos pasos:

1. Inicie el ndserver en Dispatcher:
 - Para AIX, Linux o Solaris, ejecute el mandato siguiente como usuario root:
ndserver
 - En Windows 2000, ndserver se ejecuta como servicio que se inicia automáticamente.
2. Inicie la función asistente de Dispatcher, **ndwizard**.

El asistente le guía paso a paso a través del proceso de creación de una configuración básica para el componente Dispatcher. Se le harán preguntas acerca de su red. Se le guiará a través de la configuración de un cluster para que Dispatcher reparta el tráfico entre un grupo de servidores.

Con el asistente para configuración, verá los siguientes paneles:

- Introducción al asistente
- Qué va a ocurrir
- Preparación para la configuración
- Selección de un sistema principal para configurar (si es necesario)
- Definición de un cluster
- Adición de un puerto
- Adición de un servidor
- Inicio de un asesor
- Configuración de la máquina servidor

Configuración mediante la interfaz gráfica de usuario (GUI)

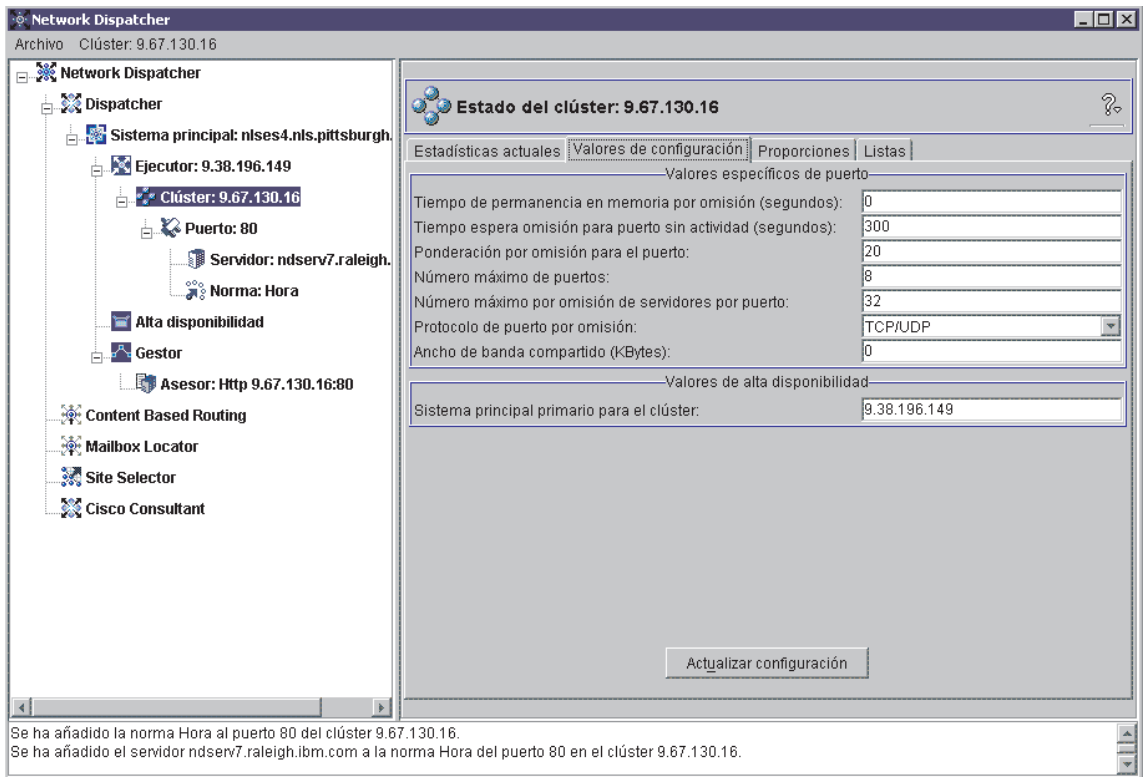


Figura 2. La interfaz gráfica de usuario (GUI)

Para iniciar la interfaz gráfica de usuario, siga estos pasos:

1. Asegúrese de que ndserver se está ejecutando:
 - Para AIX, Linux o Solaris, ejecute el mandato siguiente como usuario root:
ndserver

- En Windows 2000, ndserver se ejecuta como servicio que se inicia automáticamente.
2. A continuación, lleve a cabo una de las siguientes acciones:
- Para AIX, Linux o Solaris, ejecute el mandato **ndadmin**.
 - En Windows 2000, pulse **Inicio, Programas, IBM WebSphere, Edge Server, IBM Network Dispatcher** y finalmente **Network Dispatcher**.

Instrucciones generales para la utilización de la GUI

El lado izquierdo del panel muestra una estructura en árbol con Network Dispatcher en el nivel superior y Dispatcher, Content Based Routing, Mailbox Locator, Site Selector y Cisco Consultant como componentes. Consulte Figura 2 en la página 5.

Todos los componentes se pueden configurar desde la GUI. Puede seleccionar elementos de la estructura en árbol pulsando el botón uno del ratón (normalmente el izquierdo) y visualizar menús emergentes pulsando el botón dos del ratón (normalmente el derecho). También puede accederse a los menús emergentes de los elementos del árbol desde la barra de menús situada en la parte superior del panel.

Pulse sobre los signos más o menos para ampliar o contraer los elementos de la estructura en árbol.

En el lado derecho del panel se muestran las pestañas de los indicadores de estado para el elemento seleccionado actualmente.

- La pestaña **Estadísticas actuales** presenta información estadística sobre el elemento.
- El botón **Renovar estadísticas** visualiza los datos estadísticos más recientes. Si no aparece un botón Renovar Estadísticas, las estadísticas se renuevan dinámicamente y siempre son actuales.
- La pestaña **Valores de configuración** presenta los parámetros de configuración que se pueden establecer utilizando los procedimientos descritos en los capítulos de configuración correspondientes a cada componente. Esta pestaña no aparece para todos los elementos de la estructura en árbol.
- El botón **Actualizar configuración** aplica los cambios más recientes a la configuración que se está ejecutando actualmente.
- La pestaña **Proporciones** muestra parámetros de proporción (o ponderación) que se pueden establecer utilizando la información de “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131. Esta pestaña no aparece para todos los elementos de la estructura en árbol.

- La pestaña **Listas** presenta detalles adicionales sobre el elemento del árbol que se ha seleccionado. Esta pestaña no aparece para todos los elementos de la estructura en árbol.
- El botón **Eliminar** suprime elementos resaltados.

Puede acceder a la **Ayuda** pulsando el signo de interrogación, situado en la esquina superior derecha de la ventana de Network Dispatcher.

- **Ayuda para campos** — describe cada campo y sus valores por omisión
- **Cómo puedo** — lista tareas que pueden efectuarse desde la pantalla actual
- **Contenido** — es una tabla de contenido de toda la información de la Ayuda
- **Índice** — es un índice alfabético de los temas de la Ayuda

Comprobación de la configuración

Compruebe si la configuración es funcional.

1. Desde un navegador Web, vaya a la ubicación **<http://www.intersplash.com>**. Si aparece una página, todo está funcionando.
2. Vuelva a cargar la página en el navegador Web.
3. Observe los resultados del mandato siguiente: **ndcontrol server report www.intersplash.com:80**. La columna de conexiones totales de los dos servidores debe ascender a "2."

Tipos de configuraciones de clusters, puertos y servidores

Existen muchas formas de configurar Network Dispatcher para dar soporte a su sitio Web. Si el sitio Web tiene un solo nombre de sistema principal al que se conectan todos los clientes, se puede definir un único cluster de servidores. Para cada uno de estos servidores, configure un puerto a través del cual se comunica Network Dispatcher. Consulte Figura 3.

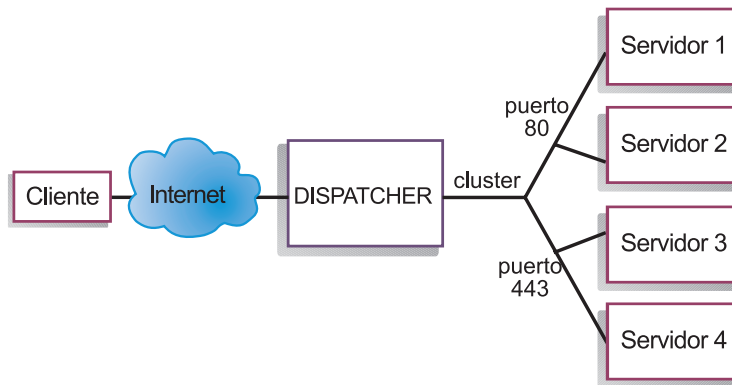


Figura 3. Ejemplo de Dispatcher configurado con un cluster individual y 2 puertos

En este ejemplo del componente Dispatcher, un cluster está definido en www.productworks.com. Este cluster tiene dos puertos: el puerto 80 para HTTP y el puerto 443 para SSL. El cliente que haga una petición a <http://www.productworks.com> (puerto 80) irá a un servidor diferente del que irá el visitante que solicite <https://www.productworks.com> (puerto 443).

Si el sitio Web es muy grande y tiene muchos servidores dedicados a cada uno de los protocolos soportados, otra forma de configurar Network Dispatcher resultaría más adecuada. En este caso, le interesaría definir un cluster para cada protocolo con un único puerto pero con varios servidores, tal y como se muestra en la Figura 4.

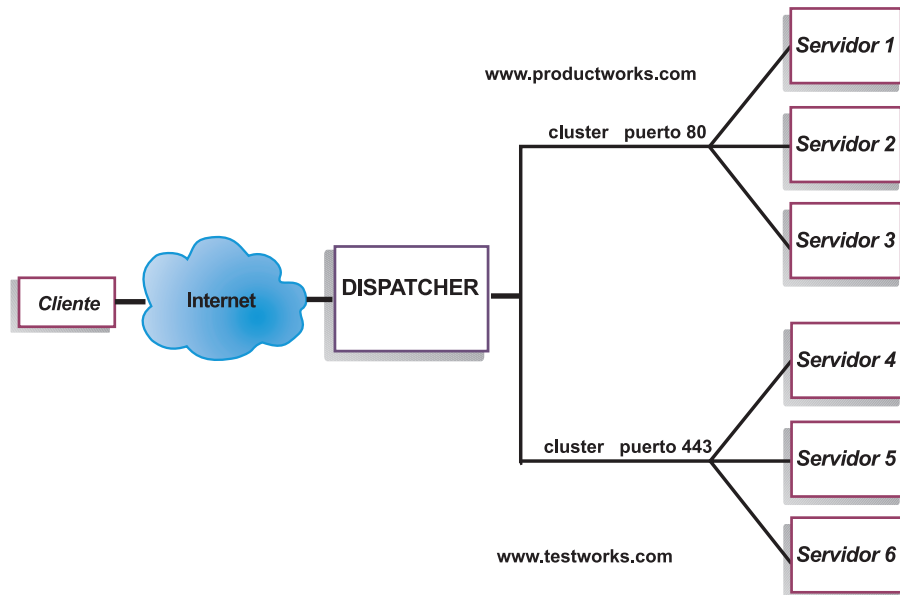


Figura 4. Ejemplo de Dispatcher configurado con 2 clusters, cada uno con 1 puerto

En este ejemplo del componente Dispatcher, hay 2 clusters definidos: www.productworks.com para el puerto 80 (HTTP) y www.testworks.com para el puerto 443 (SSL).

Sería necesaria una tercera forma de configurar Network Dispatcher si el sitio Web realiza hospedaje de contenidos para varias empresas o departamentos y cada uno de ellos accede al sitio Web con un URL diferente. En este caso, podría definir un cluster para cada empresa o departamento y luego definir varios puertos para las conexiones entrantes de cada URL, tal como se muestra en la Figura 5 en la página 9.

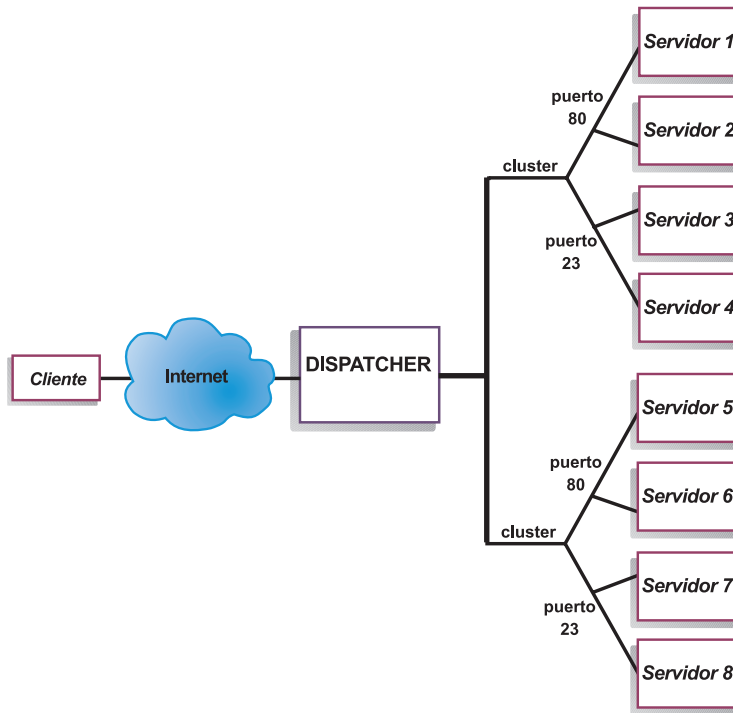


Figura 5. Ejemplo de Dispatcher configurado con 2 clusters, cada uno con 2 puertos

En este ejemplo del componente Dispatcher, hay 2 clusters definidos: www.productworks.com con el puerto 80 (para HTTP) y www.testworks.com con el puerto 23 (para Telnet).

Capítulo 2. Instalación de Network Dispatcher

Este capítulo describe los requisitos de hardware y la instalación de Network Dispatcher en AIX, Linux, Solaris y Windows 2000. Siga estas instrucciones empezando en:

- “Requisitos para AIX” en la página 12
- “Requisitos para Red Hat Linux o SuSe Linux” en la página 16
- “Requisitos para Solaris” en la página 19
- “Requisitos para Windows 2000” en la página 22

Notas:

1. Si desea hacer una migración desde una versión anterior del producto, tenga en cuenta que la estructura de directorios de instalación de Network Dispatcher ha cambiado. Deberá trasladar sus archivos de configuración al directorio `...nd/servers/configurations/componente` (donde *componente* es dispatcher, cbr, ml, ss o lbc). Además, debe trasladar sus scripts (tales como goldle y goStandby) al directorio `...nd/servers/bin` para poder ejecutarlos.
2. Si finaliza la sesión de una máquina una vez instalado Network Dispatcher, deberá reiniciar todos los servicios de Network Dispatcher cuando vuelva a iniciar una sesión.
3. El nivel de Java necesario para Network Dispatcher Release 2.0 es 1.3.0 o superior. Puesto que algunas aplicaciones ubicadas en el sistema de Network Dispatcher pueden requerir otras versiones de Java, es necesario tener instaladas las versiones correctas de Java en el sistema cuando actualice.

Para asegurarse de que los componentes de Network Dispatcher utilicen la versión correcta de Java cuando hay instaladas varias versiones, realice las acciones siguientes:

- a. Instale la versión correcta de Java 1.3 correspondiente al sistema operativo según se especifique en las secciones de requisitos de este capítulo.
- b. Edite los archivos de script de Network Dispatcher para el uso de Java 1.3. Por omisión, los archivos de script están ubicados en los directorios siguientes:

Basado en Unix

`/usr/bin/<archivoscript>`

Windows

`C:\WINNT\System32\<archivoscript.cmd>`

Edite los archivos de script de cada componente de Network Dispatcher que desee actualizar. Los archivos de script de cada componente son:

Administración

ndadmin

Dispatcher

ndserver, ndcontrol, ndwizard, ndkeys

Content Based Routing (CBR)

cbrserver, cbrcontrol, cbrwizard, cbrkeys

Site Selector

ssserver, sscontrol

Cisco Consultant

lbserver, lbcontrol

Nota: Por omisión, estos archivos son de sólo lectura, así que debe cambiar los permisos de estos archivos para poder guardar los cambios.

- c. Siempre que encuentre un mandato java o javaw en los archivos de script, añada una vía de acceso como prefijo que indique la ubicación del mandato en el directorio de instalación de Java 1.3.

Por ejemplo, en Windows 2000, si Java 1.3 se ha instalado en C:\Archivos de programa\IBM\Java13\jre\bin, cambie la línea de ndserver.cmd:

de ser: javaw %END_ACCESS%
-DEND_INSTALL_PATH=%IBMNDPATH% ..

por: C:\Archivos de programa\IBM\Java13\jre\bin\javaw
%END_ACCESS% -DEND_INSTALL_PATH=%IBMNDPATH%
...

Requisitos para AIX

- Una máquina basada en IBM RS/6000
 - IBM AIX 5.1 con APAR IY19177. Soporte para Power PC de 32 bits (*no* para el kernel de 64 bits).
- IBM AIX 4.3.3.10 junto con los APAR (para dar soporte a Java 1.3). Consulte el archivo README de IBM AIX Developer Kit para obtener una lista de los APAR de AIX necesarios.
- 50 MB de espacio libre de disco para la instalación

Nota: Se necesitará espacio de disco adicional para los archivos de anotaciones.

- Se da soporte a las siguientes tarjetas de interfaz de red (NIC):
 - Red en Anillo de 16 Mb
 - Ethernet de 10 Mb
 - Ethernet de 100 Mb
 - Ethernet de 1 Gb
 - FDDI (Fiber Distributed Data Interface)
 - Tarjetas de interfaz de red Ethernet multipuerto

Nota: La implementación de las tarjetas multipuerto puede variar de un proveedor a otro. Por tanto, el soporte para algunas tarjetas multipuerto puede ser limitado.

- IBM AIX Developer Kit, Java 2 Technology Edition, Versión 1.3.0 o superior para Java Runtime Environment. (Si desea información sobre la ejecución de varias versiones de Java, consulte la Nota número 3 en la página 11.)
- Edge Server Caching Proxy V2.0, si utiliza el componente CBR para repartir tráfico HTTP o SSL.
- Netscape Navigator 4.07 (o superior) o Netscape Communicator 4.61 (o superior) para ver la ayuda en línea
- Para Consultant para Cisco CSS Switches, ha de tener instalado y configurado Cisco CSS 11000 Series Switch.

Instalación en AIX

La Tabla 1 lista las imágenes installp de Network Dispatcher para AIX.

Tabla 1. Imágenes installp de AIX

Dispatcher (componente, administración, licencia y mensajes)	intnd.nd.driver intnd.nd.rte intnd.msg.nd.<language>.nd intnd.admin.rte intnd.msg.<idioma>.admin
Administración (sólo)	intnd.admin.rte intnd.msg.<idioma>.admin
Documentación	intnd.doc.rte
Licencia	intnd.nd.license
Metric Server	intnd.ms.rte

donde <idioma> es uno de los siguientes:

- en_US
- de
- es_ES
- fr
- it

- ja_JP
- Ja_JP
- ko_KR
- pt_BR
- zh_CN
- zh_TW
- Zh_TW

Si baja del sitio Web una copia de evaluación del producto, utilice las instrucciones de instalación de (<http://www.ibm.com/software/webserver/edgeserver/downloads/html>).

Antes de la instalación

Cuando instala el producto, puede instalar cualquiera de los elementos siguientes o todos ellos:

- Administración de ND
- Controlador de dispositivo de ND Dispatcher (necesario para ND Dispatcher)
- Licencia de ND (necesario para ND Dispatcher)
- Documentación de ND
- Metric Server de ND
- Licencia

Pasos de instalación

Nota: Si tiene instalada una versión anterior, deberá desinstalarla para poder instalar la versión actual. Primero compruebe que todos los ejecutores y servidores están detenidos. Seguidamente, para desinstalar el producto completo, entre **installp -u intnd**. Para desinstalar conjuntos específicos de archivos, lístelos explícitamente en lugar de especificar el nombre del paquete.

Siga estos pasos para instalar Network Dispatcher para AIX:

1. Inicie la sesión como usuario root.
2. Inserte el soporte del producto o, si va a instalar desde la Web, copie las imágenes de instalación en un directorio.
3. Instale la imagen de instalación. Se recomienda utilizar SMIT para instalar Network Dispatcher para AIX porque SMIT se asegurará de que se instalen todos los mensajes automáticamente.

Utilización de **SMIT**:

Seleccione

Mantenimiento e instalación de software

Seleccione

Instalar y actualizar software

Seleccione

Instalar y actualizar desde el último software disponible

Entre El nombre del dispositivo o directorio que contiene las imágenes installp.

Entre En la línea *SOFTWARE a instalar, la información pertinente para especificar las opciones (o seleccione List)

Pulse Aceptar

Cuando finalice el mandato, pulse **Hecho** y, a continuación, seleccione **Salir de Smit** en el menú Salir o pulse **F12**. Si utiliza SMITTY, pulse **F10** para salir del programa.

Con la línea de mandatos:

Si realiza la instalación desde CD, debe entrar los mandatos siguientes para montar el CD:

```
mkdir /cdrom  
mount -v cdrfs -p -r /dev/cd0 /cdrom
```

Consulte la tabla siguiente para determinar qué mandato o mandatos deben entrarse para instalar los paquetes de Network Dispatcher para AIX que desee:

Tabla 2. Mandatos de instalación de AIX

Network Dispatcher (con mensajes). Comprende: Dispatcher, CBR, Mailbox Locator, Site Selector y Cisco Consultant	installp -acXgd <i>dispositivo</i> intnd.nd.rte intnd.admin.rte intnd.nd.driver intnd.msg.<idioma>.nd intnd.msg.<idioma>.admin
Documentos	installp -acXgd <i>dispositivo</i> intnd.doc.rte intnd.msg.<idioma>.doc
Administración (sólo)	installp -acXgd <i>dispositivo</i> intnd.admin.rte intnd.msg.<idioma>.admin
Licencia	installp -acXgd <i>dispositivo</i> intnd.nd.license
Metric Server	installp -acXgd <i>dispositivo</i> intnd.ms.rte intnd.msg.<idioma>.admin

donde *dispositivo* es:

- /cdrom, si realiza la instalación desde CD.
- /dir (el directorio que contiene las imágenes installp), si realiza la instalación desde un sistema de archivos.

Asegúrese de que en la columna de resultado se indica la instalación satisfactoria de cada uno de los componentes de Network Dispatcher que se están instalando (aplicando). No siga hasta que todos los componentes que desee instalar se hayan aplicado satisfactoriamente.

Nota: Para generar una lista de los catálogos de archivos en cualquier imagen installp, incluidos todos los catálogos de mensajes disponibles, entre

```
installp -ld  
dispositivo
```

donde *dispositivo* es:

- /cdrom, si realiza la instalación desde CD.
- /dir (el directorio que contiene las imágenes installp), si realiza la instalación desde un sistema de archivos.

Para desmontar el CD, teclee:

```
umount /cdrom
```

4. Verifique que se ha instalado el producto. Entre el mandato siguiente:

```
lsipp -h | grep intnd
```

Si ha instalado todo el producto, este mandato devuelve lo siguiente:

```
intnd.admin.rte  
intnd.doc.rte  
intnd.ms.rte  
intnd.msg.en_US.admin.rte  
intnd.msg.en_US.doc  
intnd.msg.en_US.nd.rte  
intnd.nd.driver  
intnd.nd.license  
intnd.nd.rte
```

Las rutas de instalación de Network Dispatcher son las siguientes:

- Administración - **/usr/lpp/nd/admin**
- Componentes de Network Dispatcher- **/usr/lpp/nd/servers**
- Metric Server - **/usr/lpp/nd/ms**
- Documentación (*Guía de administración*) - **/usr/lpp/nd/documentation**

Requisitos para Red Hat Linux o SuSe Linux

- Red Hat Linux versión 7.1 (kernel de Linux versión 2.4.2-2) o SuSE Linux versión 7.1 (kernel de Linux versión 2.4.0-4 GB). Están soportados los kernels de uniprocador y multiprocador.

Nota: Si utiliza el método de reenvío MAC de Dispatcher junto con la modalidad de alta disponibilidad y la ubicación compartida, deberá instalar un parche para el kernel de Linux. Para conocer cómo bajar e instalar el parche, consulte “Instalación del parche del kernel de Linux (para suprimir las respuestas a arp en la interfaz de bucle de retorno)” en la página 70.

- 50 MB de espacio libre de disco para la instalación

Nota: Se necesitará espacio de disco adicional para los archivos de anotaciones.

- Se da soporte a las siguientes tarjetas de interfaz de red (NIC):
 - Ethernet de 10 Mb
 - Ethernet de 100 Mb
 - Ethernet de 1 Gb
 - Tarjetas de interfaz de red Ethernet multipuerto (Sólo puede utilizarse la Modalidad 1. No pueden utilizarse la tolerancia de errores (Modalidad 2) ni la agregación de puertos (Modalidad 3).)

Nota: La implementación de las tarjetas multipuerto puede variar de un proveedor a otro. Por tanto, el soporte para algunas tarjetas multipuerto puede ser limitado.

- Debe haber una versión de ksh (shell Korn) instalada
- IBM Runtime Environment para Linux, Java 2 Technology Edition, Versión 1.3.0 o superior. (Si desea información sobre la ejecución de varias versiones de Java, consulte la Nota número 3 en la página 11.)
- Las variables de entorno JAVA_HOME y PATH se deben establecer utilizando el mandato **export**. El contenido de la variable JAVA_HOME depende de dónde se ha instalado Java. A continuación se muestra un ejemplo:
 - JAVA_HOME=/opt/IBMJava2-13/jre
 - PATH=\$JAVA_HOME/bin:\$PATH
- Edge Server Caching Proxy V2.0, si utiliza el componente CBR para repartir el tráfico HTTP o SSL
- Netscape Navigator 4.07 (o superior) o Netscape Communicator 4.61 (o superior) para ver la ayuda en línea
- Para Consultant para Cisco CSS Switches, ha de tener instalado y configurado Cisco CSS 11000 Series Switch.

Instalación en Linux

Esta sección describe cómo instalar Network Dispatcher en Red Hat Linux o SuSe Linux utilizando el CD del producto o la copia de evaluación del producto que se puede bajar del sitio Web. Puede obtener instrucciones de

instalación en el sitio Web
(<http://www.ibm.com/software/webserver/edgeserver/download.html>).

Antes de la instalación

Antes de comenzar el procedimiento de instalación, asegúrese de que tiene la autorización de usuario root para instalar el software.

Pasos de instalación

Nota: Si tiene instalada una versión anterior, deberá desinstalarla para poder instalar la versión actual. Primero compruebe que todos los ejecutores y servidores están detenidos. Seguidamente, para desinstalar el producto completo, entre **rpm -e pkgname**. Cuando desinstale, invierta el orden que ha utilizado para la instalación del paquete asegurándose de desinstalar en último lugar los paquetes de administración.

Para instalar Network Dispatcher:

1. Preparativos de instalación.

- Inicie la sesión como usuario root.
- Inserte el soporte del producto o descargue el producto del sitio Web e instale la imagen de instalación utilizando RPM (Red Hat Packaging Manager).

Nota: Los paquetes de instalación de Red Hat Linux y SuSE Linux no se pueden ejecutar en ninguna otra versión del producto para Linux.

La imagen de instalación es un archivo con el formato **ndlinux-versión.tar**.

- Descomprima el archivo tar en un directorio temporal entrando el mandato siguiente: **tar -xf ndlinux-versión.tar**. El resultado es un conjunto de archivos con la extensión .rpm.

Lo siguiente es una lista de los paquetes RPM que se pueden instalar:

- **ibmnd-adm-release-versión.i386.rpm** (Administración de ND)
- **ibmnd-doc-release-versión.i386.rpm** (Documentación)
- **ibmnd-ms-release-versión.i386.rpm** (Metric Server)
- **ibmnd-srv-release-versión.i386.rpm** (versión ejecutable de Network Dispatcher)
- **ibmnd-lic-release-versión.i386.rpm** (Licencia)
- El orden en el que se instalan los paquetes es importante. A continuación se incluye una lista de los paquetes que se necesitan para cada componente y el orden en el que se deben instalar:
 - Administración (adm)

- Licencia (lic)
- Componentes de Network Dispatcher (srv)
- Metric Server (ms)
- Documentación (doc)

El mandato para instalar los paquetes se debe emitir desde el mismo directorio donde residen los archivos RPM. Emita el mandato siguiente para instalar cada paquete: **rpm -i *paquete.rpm***.

Nota: Como mínimo uno de los archivos RPM requiere que se haya instalado Java y registrado en la base de datos de RPM. Si ha instalado Java, pero no lo ha registrado en la base de datos de RPM, utilice el mandato con una opción de 'no dependencias' del modo siguiente:

rpm -i --nodeps *paquete.rpm*

- Las rutas de instalación de Network Dispatcher son las siguientes:
 - Administración - **/opt/nd/admin**
 - Componentes de Network Dispatcher - **/opt/nd/servers**
 - Metric Server - **/opt/nd/ms**
 - Documentación (*Guía de administración*) - **/opt/nd/documentation**
- Para desinstalar los paquetes, invierta el orden que ha utilizado para instalarlos, asegurándose de desinstalar en último lugar los paquetes de administración.

2. Verifique que se ha instalado el producto. Entre el mandato siguiente:

rpm -qa | grep ibmnd

Instalar todo el producto genera un listado similar a este:

- *ibmnd-adm-release-versión*
- *ibmnd-doc-release-versión*
- *ibmnd-ms-release-versión*
- *ibmnd-srv-release-versión*
- *ibmnd-lic-release-versión*

Requisitos para Solaris

- Cualquier estación de trabajo SPARC o servidor Ultra 60 soportado por Solaris Versión 7 o Solaris Versión 8. Network Dispatcher sólo da soporte a la modalidad de 32 bits para las plataformas Solaris.
- 50 MB de espacio libre de disco para la instalación

Nota: Se necesitará espacio de disco adicional para los archivos de anotaciones.

- Se da soporte a las siguientes tarjetas de interfaz de red (NIC):
 - Ethernet de 10 Mb
 - Ethernet de 100 Mb
 - Ethernet de 1 Gb (sólo en servidores Ultra 60)
 - Tarjetas de interfaz de red Ethernet multipuerto (Sólo puede utilizarse la Modalidad 1. No pueden utilizarse la tolerancia de errores (Modalidad 2) ni la agregación de puertos (Modalidad 3).)

Nota: La implementación de las tarjetas multipuerto puede variar de un proveedor a otro. Por tanto, el soporte para algunas tarjetas multipuerto puede ser limitado.

- Java 2 JRE, Standard Edition, Versión 1.3.0 o superior. (Si desea información sobre la ejecución de varias versiones de Java, consulte la Nota número 3 en la página 11.)
- Edge Server Caching Proxy V2.0, si utiliza el componente CBR para repartir el tráfico HTTP o SSL
- Para Solaris 7, Sun Microsystems HotJava Browser 1.0.1 o superior para visualizar la Ayuda en línea
Para Solaris 8, Netscape Navigator 4.07 (o superior) o Netscape Communicator 4.61 (o superior) para visualizar la Ayuda en línea
- Para Consultant para Cisco CSS Switches, ha de tener instalado y configurado Cisco CSS 11000 Series Switch.

Instalación en Solaris

Esta sección describe cómo instalar Network Dispatcher en Solaris utilizando el CD del producto. Si baja de Internet una copia de evaluación del producto, utilice las instrucciones que se proporcionan en el sitio Web (<http://www.ibm.com/software/webserver/edgeserver/download.html>).

Antes de la instalación

Antes de comenzar el procedimiento de instalación, asegúrese de que tiene la autorización de usuario root para instalar el software.

Pasos de instalación

Nota: Si tiene instalada una versión anterior, deberá desinstalarla para poder instalar la actual. En primer lugar, asegúrese de que ha parado el ejecutor y el servidor. A continuación, para desinstalar Network Dispatcher entre **pkgrm pkgname**. Network

Para instalar Network Dispatcher:

1. Preparativos de instalación.

- Inicie la sesión como usuario root.
- Inserte el CD-ROM que contiene el software de Network Dispatcher en la unidad correspondiente.

En el indicador de mandatos, entre **pkgadd -d** *vía de acceso*, donde -d *vía de acceso* es el nombre del dispositivo de la unidad de CD-ROM o el directorio del disco duro donde se encuentra el paquete; por ejemplo **pkgadd -d /cdrom/cdrom0/**.

Se mostrará una lista de los paquetes que puede instalar. Estos paquetes son:

- ibmdsp IBM ND para Solaris (componentes de Network Dispatcher)
- ibmndadm IBM ND Base Administration para Solaris
- ibmnddoc IBM ND Documentation para Solaris
- ibmndms IBM ND Metric Server para Solaris
- ibmdsplic Licencia para Solaris

Si desea instalar todos los paquetes, simplemente escriba "all" y pulse Intro. Si desea instalar algunos de los componentes, escriba los números correspondientes a los paquetes, separados por un espacio o una coma y pulse Intro. Se le pedirá si desea modificar permisos sobre directorios o archivos existentes. Simplemente pulse Intro o responda "yes". Tendrá que instalar paquetes necesarios (pues se instalan por orden alfabético, no por orden de dependencia). Si responde "all", luego sólo debe responder "yes" a todas las preguntas y la instalación se efectuará satisfactoriamente.

Todos los paquetes dependen del paquete común, ibmndadm. Este paquete común debe instalarse junto con cualquiera de los demás paquetes.

Si desea instalar el producto Network Dispatcher completo, debe instalar cinco elementos: ibmdsp, ibmdsplic, ibmndadm, ibmnddoc y ibmndms. Si desea instalar la administración remota, sólo es necesario instalar un elemento: ibmndadm.

Los componentes de Network Dispatcher residen en el directorio de instalación **/opt/nd/servers**.

2. El componente Administración se instala en el directorio **/opt/nd/admin**
3. El componente Metric Server se instala en el directorio **/opt/nd/ms**
4. La Documentación (*Guía de administración*) se instala en el directorio **/opt/nd/documentation**
5. Verifique que se ha instalado el producto. Emita este mandato:
pkginfo | grep ibm.

Si ha instalado el producto completo, debe obtener un listado similar al siguiente:

- ibmdsp
- ibmndadm
- ibmnddoc
- ibmndms
- ibmdsplic

Requisitos para Windows 2000

- Un PC Intel x86 soportado por Microsoft Windows 2000
- Windows 2000 Professional, Server o Advanced Server
- 50 MB de espacio libre de disco para la instalación

Nota: Se necesitará espacio de disco adicional para los archivos de anotaciones.

- Se da soporte a las siguientes tarjetas de interfaz de red (NIC):
 - Red en Anillo de 16 Mb
 - Ethernet de 10 Mb
 - Ethernet de 100 Mb
 - Ethernet de 1 Gb
 - Tarjetas de interfaz de red Ethernet multipuerto

Nota: La implementación de las tarjetas multipuerto puede variar de un proveedor a otro. Por tanto, el soporte para algunas tarjetas multipuerto puede ser limitado.

- IBM Cross Platform Technologies para Windows v2.0 (SDK 1.3.0 o superior)
Debe bajar los paquetes instalables del Developer Kit y de Runtime Environment para poder ejecutar el programa InstallShield. (Si desea información sobre la ejecución de varias versiones de Java, consulte la Nota número 3 en la página 11.)
- Edge Server Caching Proxy V2.0, si utiliza el componente CBR para repartir el tráfico HTTP o SSL.
- Asegúrese de que su navegador por omisión es Netscape Navigator 4.07 (o superior), Netscape Communicator 4.61 (o superior) o bien Internet Explorer 4.0 (o superior). El navegador por omisión se utiliza para ver la ayuda en línea.
- Para Consultant para Cisco CSS Switches, ha de tener instalado y configurado Cisco CSS 11000 Series Switch.

Instalación para Windows 2000

Esta sección describe cómo instalar Network Dispatcher en Windows 2000 utilizando el CD del producto. Si baja del sitio Web una copia de evaluación del producto, utilice las instrucciones de instalación de (<http://www.ibm.com/software/webservers/edgeserver/downloads/html>).

Paquetes de instalación

Se le mostrarán los paquetes que puede instalar.

Estos paquetes son:

- Unidad ejecutable
- Administración
- Licencia
- Documentación
- Metric Server

Antes de la instalación

La versión para Windows 2000 de Network Dispatcher está soportada en:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server

Nota: La versión para Windows 2000 de Network Dispatcher *no* es funcional en ninguna otra versión de Windows.

Restricciones: La versión para Windows 2000 de Network Dispatcher no se puede instalar en la misma máquina junto con IBM Firewall.

Antes de empezar el procedimiento de instalación, asegúrese de que se ha conectado como administrador o con un perfil de usuario que tenga privilegios de administrador.

Pasos de instalación

Si tiene instalada una versión anterior, deberá desinstalarla para poder instalar la versión actual. Para desinstalar utilizando la opción **Agregar o quitar programas**, haga lo siguiente:

1. Pulse **Inicio**→**Configuración**→**Panel de control**
2. Efectúe una doble pulsación en **Agregar o quitar programas**
3. Seleccione *Network Dispatcher*
4. Pulse el botón **Cambiar o quitar**

Para instalar Network Dispatcher:

1. Inserte el CD-ROM de Network Dispatcher en la unidad de CD-ROM y la ventana de instalación aparecerá automáticamente.
2. Sólo se requiere el paso siguiente si la ejecución automática del CD no funciona en su sistema. Haga lo siguiente pulsando el botón izquierdo del ratón:
 - Pulse en **Inicio**.
 - Seleccione **Ejecutar**.
 - Especifique la unidad de CD-ROM, seguida de setup.exe, por ejemplo:
 E:\setup
3. Seleccione el **Idioma** en el que desea leer el proceso de instalación.
4. Pulse con el ratón en **Aceptar**.
5. Siga las instrucciones del programa de instalación.
6. Si desea cambiar la unidad o el directorio destino, pulse con el ratón en **Examinar**.
7. Puede seleccionar "Todo el producto ND" o "su elección de componentes".
8. Una vez finalizada la instalación, aparecerá un mensaje en el que se indica que debe reiniciar el sistema para poder utilizar Network Dispatcher. Esto es necesario con el fin de garantizar que se han instalado todos los archivos y que se ha añadido la variable de entorno IBMNDPATH al registro.

Las rutas de instalación de Network Dispatcher son las siguientes:

- Administración – **c:\Progra~1\IBM\edge\nd\admin**
- Componentes de Network Dispatcher –
c:\Progra~1\IBM\edge\nd\servers
- Metric Server – **c:\Progra~1\IBM\edge\nd\ms**
- Documentación (Guía de administración) –
c:\Progra~1\IBM\edge\nd\documentation

Capítulo 3. Presentación de Network Dispatcher

Este capítulo ofrece una visión general de Network Dispatcher y comprende las secciones siguientes:

- “¿Qué es Network Dispatcher?”
- “¿Por qué se necesita Network Dispatcher?” en la página 26
- “¿Cuáles son las nuevas funciones?” en la página 28
- “¿Cuáles son los componentes de Network Dispatcher?” en la página 33
- “Acerca de la alta disponibilidad” en la página 44

¿Qué es Network Dispatcher?

Network Dispatcher es una solución de software para distribuir el tráfico entre servidores. Aumenta el rendimiento de los servidores encaminando las peticiones de sesión TCP/IP hacia distintos servidores dentro de un grupo de ellos; de esta forma, reparte las peticiones entre todos los servidores. El reparto del tráfico es transparente a los usuarios y a otras aplicaciones. Network Dispatcher resulta útil para aplicaciones tales como servidores de correo electrónico, servidores WWW (World Wide Web), consultas a bases de datos paralelas distribuidas y otras aplicaciones TCP/IP.

Utilizado con servidores, Network Dispatcher contribuye a maximizar el potencial de su sitio Web al ofrecer una solución potente, flexible y escalable a los problemas de picos de demanda. Si los visitantes de un sitio Web no pueden acceder a él en las horas de mayor demanda, Network Dispatcher busca automáticamente el servidor óptimo para gestionar las peticiones entrantes, con lo que aumenta la satisfacción de los usuarios y la rentabilidad.

Network Dispatcher consta de cinco componentes que se pueden utilizar por separado o juntos para lograr un mejor reparto del tráfico:

- El componente **Dispatcher** se puede utilizar individualmente para repartir el tráfico en los servidores de una red de área local o red de área amplia por medio de diversos valores de ponderación (pesos) y medidas definidos dinámicamente por Dispatcher. Este componente proporciona reparto del tráfico para servicios determinados, tales como HTTP, FTP, SSL, NNTP, IMAP, POP3, SMTP y Telnet. No utiliza un servidor de nombres de dominio para correlacionar los nombres de dominio con direcciones IP.

Para el protocolo HTTP, puede también utilizar el encaminamiento por contenido del Dispatcher para repartir el tráfico basándose en el contenido de la petición del cliente. El servidor elegido es el resultado de comparar el URL con una norma especificada.

- Para el protocolo HTTP y HTTPS (SSL), puede utilizar el componente **Content Based Routing (CBR)** para repartir el tráfico basándose en el contenido de la petición del cliente. Los clientes envían peticiones a Caching Proxy y éste envía las peticiones al servidor apropiado. El servidor elegido es el resultado de comparar el URL con una norma especificada.
- Para los protocolos IMAP o POP3, puede utilizar el componente **Mailbox Locator**, que actúa como proxy y selecciona un servidor apropiado basándose en el ID de usuario y la contraseña proporcionados por el cliente.
- Puede utilizar el componente **Site Selector** para repartir el tráfico entre servidores de una red de área local o de área amplia, utilizando un método rotatorio basado en DNS o un método más avanzado especificado por el usuario. Site Selector trabaja en combinación con un servidor de nombres para correlacionar nombres de DNS con direcciones IP.
- Puede utilizar el componente **Consultant para Cisco CSS Switches** para generar métricas de ponderación de servidor que se envían al Cisco CSS Switch para ayudar en la selección óptima del servidor, la optimización del reparto del tráfico y la tolerancia a los errores.

Para obtener más información sobre los componentes Dispatcher, CBR, Mailbox Locator, Site Selector y Consultant para Cisco CSS Switches, consulte “¿Cuáles son los componentes de Network Dispatcher?” en la página 33.

¿Por qué se necesita Network Dispatcher?

El número de usuarios y de redes conectadas a Internet crece de forma exponencial. Este crecimiento origina problemas de escala que pueden restringir el acceso de los usuarios a los sitios Web más populares.

En la actualidad, los administradores de red utilizan diversos métodos para intentar ampliar al máximo el acceso. Algunos de estos métodos permiten a los usuarios elegir aleatoriamente un servidor distinto si el seleccionado anteriormente resulta lento o no responde. Esta forma de abordar la cuestión es incómoda, molesta e ineficaz. Otro método es el rotatorio estándar, en el que el servidor de nombres de dominio selecciona los servidores por turnos para que manejen las peticiones. Este método es mejor, pero sigue siendo poco eficiente, pues el tráfico se reenvía a ciegas sin tomar en cuenta la carga de trabajo de los servidores. Además, aunque falle un servidor, se siguen enviando peticiones a él.

La necesidad de una solución más eficaz ha dado lugar a Network Dispatcher. Este producto ofrece numerosas ventajas con respecto a soluciones anteriores:

Escalabilidad

A medida que aumenta el número de peticiones de los clientes, puede añadir servidores de forma dinámica, con lo que se puede dar soporte a decenas de millones de peticiones al día en decenas, o incluso cientos, de servidores.

Uso eficiente del equipo

El reparto del tráfico asegura que cada grupo de servidores utilice el hardware de forma óptima gracias a que se minimizan las zonas de actividad continua que se producen habitualmente con un método rotatorio estándar.

Facilidad de integración

Network Dispatcher utiliza protocolos TCP/IP estándar. Se puede añadir a la red existente sin tener que realizar cambios físicos en ella. Resulta sencillo de instalar y configurar.

Reducción de la actividad general

Gracias a la utilización de un método de reenvío simple a nivel MAC, Dispatcher sólo necesita observar los flujos entrantes de cliente a servidor. No necesita observar los flujos salientes de servidor a cliente. Esto reduce significativamente el efecto que tiene sobre la aplicación en comparación con otros métodos y puede originar una mejora del rendimiento de la red.

Alta disponibilidad

Dispatcher ofrece una función incorporada de alta disponibilidad, ya que utiliza una máquina de reserva que permanece lista para asumir el control en caso de producirse una anomalía en la máquina Dispatcher principal. Dispatcher también ofrece la característica de alta disponibilidad mutua que permite que dos máquinas estén activas y en espera entre sí. Consulte el apartado “Acerca de la alta disponibilidad” en la página 44.

encaminamiento basado en contenido (uso del componente CBR o del componente Dispatcher)

En combinación con Caching Proxy, el componente CBR tiene la capacidad de reenviar peticiones HTTP y HTTPS (SSL) hacia servidores determinados basándose en el contenido de las páginas solicitadas. Por ejemplo, si una petición contiene la cadena de caracteres `"/cgi-bin/"` en la porción del URL correspondiente al directorio y el nombre del servidor es un servidor local, CBR puede dirigir la petición hacia el servidor más apropiado de un grupo de servidores que están asignados específicamente para gestionar peticiones de cgi.

El componente Dispatcher también proporciona encaminamiento basado en el contenido, pero no necesita que el Caching Proxy esté instalado. Debido a que el encaminamiento basado en contenido del componente Dispatcher se realiza en el kernel a medida que se reciben los paquetes, el componente Dispatcher puede proporcionar un encaminamiento basado en contenido *más rápido* que el componente CBR. El componente Dispatcher realiza encaminamiento por contenido para HTTP (utilizando la norma de tipo "content") y HTTPS (utilizando la afinidad del ID de sesión de SSL).

Nota: Sólo el componente CBR puede utilizar la norma de contenido para HTTPS (SSL) cuando se reparte el tráfico tomando como base el contenido de la petición HTTP, lo cual exige descifrar y volver a cifrar mensajes.

¿Cuáles son las nuevas funciones?

Network Dispatcher para IBM WebSphere Edge Server Versión 2.0 contiene varias funciones nuevas. A continuación se listan las más importantes.

- **Soporte de AIX v5.1**

Esta función es aplicable a todos los componentes de Network Dispatcher. Network Dispatcher ahora da soporte a una versión más reciente de AIX: AIX v5.1. En "Requisitos para AIX" en la página 12 hallará más información.

- **Soporte de SuSE Linux v7.1**

Esta función es aplicable a todos los componentes de Network Dispatcher. Network Dispatcher ahora da soporte a SuSE Linux v7.1 (versión de kernel 2.4.0-4GB). Anteriormente, Network Dispatcher sólo daba soporte a Red Hat Linux. En "Requisitos para Red Hat Linux o SuSe Linux" en la página 16 hallará más información.

- **Soporte de Red Hat Linux v7.1**

Esta función es aplicable a todos los componentes de Network Dispatcher. Network Dispatcher ahora da soporte a una versión más reciente de RedHat Linux: Red Hat Linux v7.1. (versión de kernel 2.4.2-2). En "Requisitos para Red Hat Linux o SuSe Linux" en la página 16 hallará más información.

- **Soporte de idioma nacional para Linux y Solaris**

Esta función es aplicable a todos los componentes de Network Dispatcher. En los sistemas operativos Linux y Solaris, Network Dispatcher proporciona soporte de idioma nacional para los países del Grupo 1.

- **Nuevo soporte estándar de idioma nacional para el chino**

Esta función es aplicable a todos los componentes de Network Dispatcher.

Network Dispatcher proporciona soporte de idioma nacional para el nuevo estándar GB 18030 del chino.

- **Componente Consultant para Cisco CSS Switches (Cisco Consultant)**

Esta función es un nuevo componente de Network Dispatcher.

El trabajo conjunto con Cisco y su Content Distribution Network (CDN) ha originado el desarrollo de un componente adicional de Network Dispatcher: Cisco Consultant. Este componente (que primero se presentó como Avance autónomo) permite a Network Dispatcher generar valores de ponderación y tomar decisiones sobre el reparto del tráfico para Cisco CSS Switch.

Consulte el “Capítulo 12. Planificación para el componente Consultant para Cisco CSS Switches” en la página 119 y el “Capítulo 13. Configuración del componente Consultant para Cisco CSS Switches” en la página 125 para obtener más información.

- **Componente Site Selector**

Esta función es un nuevo componente de Network Dispatcher.

El componente Site Selector reparte el tráfico entre un grupo de servidores seleccionando la dirección IP del servidor “apropiado” para una petición de servicio de nombres. Este permite que el cliente se conecte directamente con el servidor para todas sus comunicaciones. Site Selector sustituye a Interactive Session Support (ISS), que en releases anteriores era un componente de Network Dispatcher. Site Selector proporciona funciones similares a las de ISS, pero necesita menos pasos para configurar el reparto del tráfico de DNS.

Consulte el “Capítulo 10. Planificación para el componente Site Selector” en la página 107 y el “Capítulo 11. Configuración del componente Site Selector” en la página 113 para obtener más información.

- **Metric Server**

Esta función es aplicable a todos los componentes de Network Dispatcher.

Metric Server proporciona a Network Dispatcher información sobre el tráfico de los servidores en forma de métrica específica del sistema. El agente de Metric Server es un componente de Network Dispatcher que puede instalarse y ejecutarse en los servidores para los que Network Dispatcher realice el reparto del tráfico. Metric Server sustituye a System Monitoring Agent (SMA), que en releases anteriores estaba soportado en Linux. Metric Server está soportado en todas las plataformas. Es recomendable utilizar Metric Server junto con el componente Site Selector. En “Metric Server” en la página 150 hallará más información.

- **Componente Mailbox Locator**

Esta función es un nuevo componente de Network Dispatcher.

Anteriormente el componente Mailbox Locator era una función dentro del componente CBR que repartía el tráfico entre servidores de correo IMAP y POP3 basándose en el ID de usuario y la contraseña. Separar CBR en dos

componentes permite ejecutar Mailbox Locator (antes denominado "CBR para IMAP/POP3") y CBR con Caching Proxy en la misma máquina.

Consulte el "Capítulo 8. Planificación para el componente Mailbox Locator" en la página 95 y el "Capítulo 9. Configuración del componente Mailbox Locator" en la página 99 para obtener más información.

- **Mejoras en el manejo del componente Content Based Routing (CBR)**

Se ha simplificado la definición del archivo de configuración de Caching Proxy (ibmproxy.conf) para utilizar CBR y se ha mejorado CBR para poder ejecutar simultáneamente varias instancias de Caching Proxy en la misma máquina mientras se interactúa con CBR. Para obtener más información sobre cómo configurar CBR con Caching Proxy, consulte "Configuración de la máquina CBR" en la página 86.

- **Soporte para Network Address Translation (NAT) y Network Address Port Translation (NAPT)**

Esta función es aplicable al componente Dispatcher.

Gracias a NAT/NAPT ya no es necesario que los servidores de fondo estén situados en una red conectada localmente. También permite que Dispatcher reparta el tráfico de las peticiones TCP del cliente hacia varios daemons de servidor que se ejecutan en la misma máquina física. Existen dos maneras de configurar servidores con varios daemons. Con NAT, puede configurar varios daemons de servidor para responder a peticiones dirigidas a diferentes direcciones IP. Esto se denomina vincular un daemon de servidor con una dirección IP. Con NAPT, puede configurar varios daemons de servidor para recibir las peticiones en diferentes números de puerto.

La ventana del método de reenvío nat de Dispatcher es que se configura a nivel de puerto, lo que ofrece mucho mejor granularidad.

Nota: Para Network Dispatcher, NAT/NAPT no es efectivo con los protocolos de aplicación, tales como FTP, que incluyen las direcciones o números de puerto en la porción de datos de los mensajes. Esta es una limitación bien conocida del NAT/NAPT basado en el uso de cabeceras.

En "Método de reenvío nat del Dispatcher" en la página 50 hallará más información.

- **Función de encaminamiento por contenido del Dispatcher (con uso de norma de contenido y afinidad de ID de sesión de SSL)**

Esta función es aplicable al componente Dispatcher.

En versiones anteriores de Network Dispatcher, el encaminamiento por contenido sólo podía utilizarse al usar el componente CBR en combinación con Caching Proxy. Ahora el componente Dispatcher permite realizar encaminamiento por contenido para HTTP (utilizando la norma de tipo "content") y para HTTPS (utilizando la afinidad del ID de sesión de SSL),

sin tener que utilizar Caching Proxy. Para el tráfico de HTTP y HTTPS, el componente Dispatcher puede proporcionar un encaminamiento por contenido más rápido que el componente CBR.

Consulte “Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)” en la página 52 para obtener más información sobre el uso de la norma de contenido y la afinidad del ID de sesión de SSL.

- **Afinidad pasiva de cookie**

Esta función es aplicable al encaminamiento por contenido del componente Dispatcher (método de reenvío CBR) y al componente CBR.

La afinidad pasiva de cookie le permite repartir el tráfico Web con afinidad por un mismo servidor basándose en los cookies autodefinidos generados por los servidores. En “Afinidad pasiva de cookie” en la página 194 hallará más información.

- **Afinidad de URI (reparto del tráfico para caching proxies)**

Esta función es aplicable al encaminamiento por contenido del componente Dispatcher (método de reenvío CBR) y al componente CBR.

La afinidad de URI le permite repartir el tráfico Web hacia servidores caching-proxy y aumentar de forma efectiva el tamaño de la antememoria. En “Afinidad de URI” en la página 195 hallará más información.

- **Proporciones específicas del cluster (o sitio Web)**

Esta función es aplicable a todos los componentes de Network Dispatcher.

En versiones anteriores, se utilizaba la función del gestor para definir la proporción de importancia (asignado a conexiones activas, conexiones nuevas, puertos y métricas del sistema) y realizar el reparto del tráfico. Estas proporciones se aplicaban a cada cluster de la configuración para el componente. Todos los clusters se evaluaban utilizando las mismas proporciones, con independencia del sitio Web donde se hacía el reparto del tráfico.

Gracias a esta mejora, la proporción de importancia se puede definir para cada cluster (o sitio Web). En “Grado de importancia dado a la información de estado” en la página 135 hallará más información.

- **Particionamiento del servidor**

Esta función es aplicable a todos los componentes de Network Dispatcher.

Ahora Network Dispatcher proporciona la capacidad de particionar un servidor físico en varios servidores lógicos. Esto permite, por ejemplo, consultar un determinado servicio de la máquina para detectar si un motor de servlet o petición de base de datos se está ejecutando más rápidamente o no se está ejecutando. Esta mejora permite repartir el tráfico de una forma más precisa, de acuerdo con el servicio. En “Particionamiento del servidor: servidores lógicos configurados para un solo servidor físico (dirección IP)” en la página 152 hallará más información.

- **Opción de petición/respuesta del asesor HTTP (URL)**

Esta función es aplicable a los componentes Dispatcher y CBR.

Con esta mejora para el asesor HTTP, puede evaluar el estado de servicios individuales dentro de un servidor. Para cada servidor lógico del puerto HTTP, puede especificar un URL exclusivo para un cliente HTTP, que sea específico del servicio que desea consultar en el servidor. En “Opción de petición/respuesta del asesor HTTP (URL)” en la página 154 hallará más información.

- **Asesores específicos del cluster (o sitio Web)**

Esta función es aplicable a todos los componentes de Network Dispatcher.

Network Dispatcher le permite iniciar varios asesores en un mismo puerto, pero que están configurados en clusters (sitios Web) diferentes. Por ejemplo, esta función le permite utilizar un asesor HTTP en el puerto 80 para un cluster (sitio Web) y un asesor personalizado en el puerto 80 para otro cluster (sitio Web). En “Inicio y detención de un asesor” en la página 140 hallará más información.

- **Detección de ataques de denegación de servicio**

Esta función es aplicable al componente Dispatcher.

Con esta mejora, Dispatcher permite detectar posibles ataques de denegación de servicio y avisar al administrador mediante una alerta. Para ello, Dispatcher comprueba si las peticiones entrantes contienen un volumen importante de conexiones semiabiertas, lo cual es una característica habitual de los ataques simples de denegación de servicio.

En “Detección de ataques de denegación de servicio” en la página 197 hallará más información.

- **Salidas de usuario mejoradas**

Esta función se aplica a todos los componentes excepto a Consultant para Cisco CSS Switches y Site Selector.

Network Dispatcher proporciona nuevas salidas de usuario que provocan la ejecución de scripts, los cuales puede personalizar. Puede crear scripts para realizar acciones automatizadas, tales como iniciar la sesión cuando cambie un estado de alta disponibilidad o avisar al administrador cuando se detecte un servidor fuera de servicio. Network Dispatcher proporciona los nuevos archivos de script siguientes:

- serverDown, serverUp, managerAlert y managerClear — (en “Utilización de scripts para generar una alerta o registrar un error de servidor” en la página 139 encontrará más información)
- highavailChange — (en “Utilización de scripts” en la página 170 encontrará más información)
- halfOpenAlert — se ha detectado un posible ataque de denegación de servicio (en “Detección de ataques de denegación de servicio” en la página 197 encontrará más información)

- halfOpenAlertDone — el ataque de denegación de servicio ha finalizado (en “Detección de ataques de denegación de servicio” en la página 197 encontrará más información)
- **Asesor DB2**
Esta función es aplicable al componente Dispatcher.
Dispatcher proporciona un asesor DB2 que se comunica con los servidores DB2. En “Lista de asesores” en la página 143 hallará más información sobre el asesor DB2.

¿Cuáles son los componentes de Network Dispatcher?

Los cinco componentes de Network Dispatcher son: Dispatcher, Content Based Routing (CBR), Mailbox Locator, Site Selector y Consultant para Cisco CSS Switches. Network Dispatcher le proporciona la flexibilidad de utilizar estos componentes por separado o juntos, dependiendo de la configuración de su sitio Web. Esta sección proporciona una visión general de estos componentes.

Visión general del componente Dispatcher

El componente Dispatcher reparte el tráfico entre los servidores mediante una combinación exclusiva de software de gestión y de reparto del tráfico. Dispatcher también puede detectar un servidor anómalo y reenviar el tráfico hacia otros servidores. Dispatcher da soporte a HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3, Telnet, y a cualquier aplicación basada en TCP o UDP sin estados.

Todas las peticiones de los clientes enviadas a la máquina Dispatcher se dirigen al “mejor” servidor, según los pesos que se establecen de forma dinámica. Se pueden utilizar los valores por omisión de dichos pesos o cambiarlos durante el proceso de configuración.

Dispatcher proporciona tres métodos de reenvío (especificados para el puerto):

- Método de reenvío MAC (**mac**). Mediante este método de reenvío, Dispatcher reparte la petición entrante hacia el servidor. El servidor envía la respuesta directamente al cliente, sin que intervenga Dispatcher.
- Método de reenvío NAT/NAPT (**nat**). Gracias al recurso NAT (network address translation)/NAPT (network address port translation) de Dispatcher se elimina la limitación que supone que los servidores de fondo deban estar situados en una red conectada localmente. Si desea tener servidores en ubicaciones remotas, puede utilizar la técnica nat en lugar de la técnica de encapsulación GRE/WAND. Con el método de reenvío nat, Dispatcher reparte la petición entrante hacia el servidor. El servidor devuelve la respuesta a Dispatcher. Luego la máquina Dispatcher devuelve la respuesta al cliente.

- El método de reenvío CBR (Content-Based Routing) (**cbr**). Sin utilizar Caching Proxy, el componente Dispatcher le permite realizar un encaminamiento por contenido para HTTP (utilizando la norma de tipo "content") y HTTPS (utilizando la afinidad del ID de sesión de SSL). Para el tráfico de HTTP y HTTPS, el componente Dispatcher puede proporcionar un encaminamiento por contenido *más rápido* que el componente CBR. Con el método de reenvío cbr, Dispatcher reparte la petición entrante hacia el servidor. El servidor devuelve la respuesta a Dispatcher. Luego la máquina Dispatcher devuelve la respuesta al cliente.

El componente Dispatcher es la clave para conseguir una gestión eficiente y estable de una red grande y escalable de servidores. Con Dispatcher, puede enlazar muchos servidores y crear lo que en apariencia es un único servidor virtual. De esta forma, el sitio Web aparece como una sola dirección IP para el entorno. Dispatcher trabaja de forma independiente del servidor de nombres de dominio; todas las peticiones se envían a la dirección IP de la máquina Dispatcher.

Dispatcher aporta ventajas claras al repartir el tráfico hacia servidores agrupados en cluster, lo que da como resultado una gestión estable y eficaz del sitio Web.

Gestión de servidores locales con Dispatcher

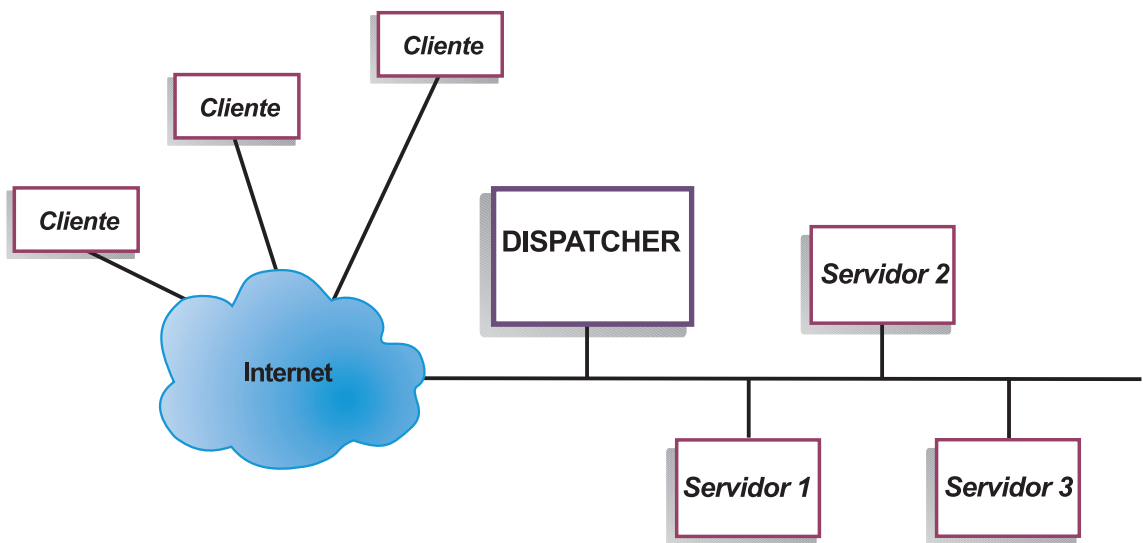


Figura 6. Ejemplo de representación física de un sitio Web que utiliza Dispatcher para gestionar servidores locales

La Figura 6 muestra una representación física del sitio Web con una configuración de red Ethernet. La máquina Dispatcher puede instalarse sin

necesidad de realizar ningún cambio físico en la red. Después de que Dispatcher encamina la petición de un cliente hacia el servidor óptimo, la respuesta se envía directamente del servidor al cliente sin la intervención de Dispatcher si se utiliza el método de reenvío MAC.

Gestión de servidores utilizando Metric Server

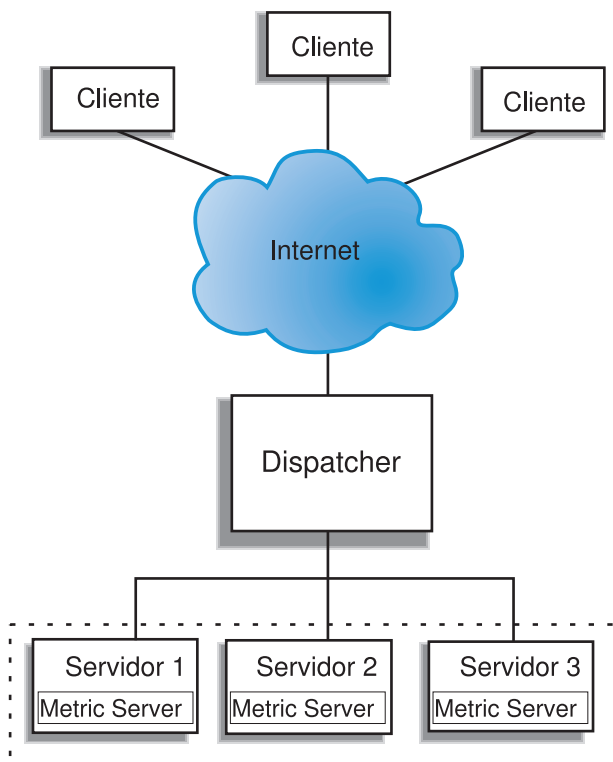


Figura 7. Ejemplo de sitio Web que utiliza Dispatcher y Metric Server para gestionar servidores

La Figura 7 muestra un sitio Web en el que todos los servidores están en una red local. Se utiliza el componente Dispatcher para reenviar peticiones y Metric Server para proporcionar información sobre el tráfico del sistema a la máquina Dispatcher.

En este ejemplo, el daemon de Metric Server está instalado en cada servidor de fondo. Puede utilizar Metric Server con el componente Dispatcher o con cualquiera de los demás componentes de Network Dispatcher.

Gestión de servidores locales y remotos con Dispatcher

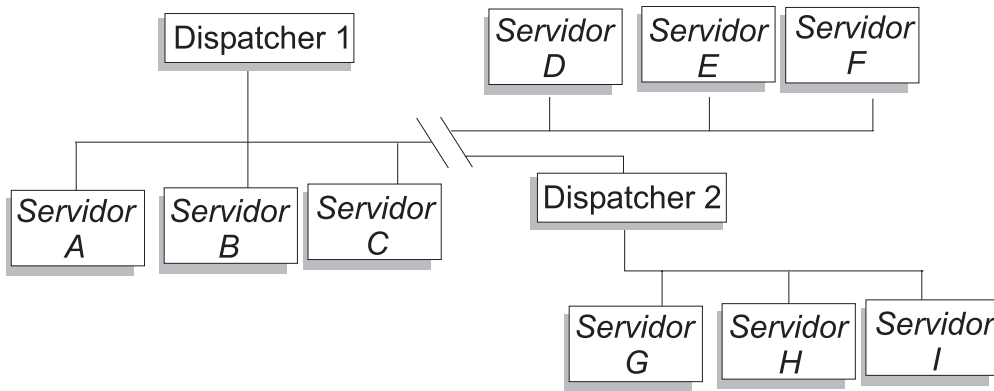


Figura 8. Ejemplo de sitio Web en el que se utiliza Dispatcher para gestionar servidores locales y remotos

El soporte de área amplia de Dispatcher le permite utilizar servidores tanto locales como remotos (servidores situados en subredes diferentes). La Figura 8 muestra una configuración donde un Dispatcher local (Dispatcher 1) sirve como punto de entrada para todas las peticiones. Este Dispatcher reparte las peticiones entre sus propios servidores locales (ServidorA, ServidorB, ServidorC) y el Dispatcher remoto, el cual reparte el tráfico entre sus servidores locales (ServidorG, ServidorH, ServidorI).

Cuando se utiliza el método de reenvío NAT o el soporte de GRE de Dispatcher, también se puede conseguir el soporte de área amplia con Dispatcher sin utilizar un Dispatcher en el sitio remoto (donde residen ServidorD, ServidorE y ServidorF). Consulte “Método de reenvío nat del Dispatcher” en la página 50 y “Soporte de GRE (Generic Routing Encapsulation)” en la página 163 para obtener más información.

Visión general del componente Content Based Routing (CBR)

CBR trabaja con Caching Proxy para encaminar las peticiones de los clientes hacia servidores HTTP o HTTPS (SSL) especificados. CBR le permite manipular datos de la gestión de antememoria para lograr una recuperación más rápida de documentos Web con pocos requisitos respecto al ancho de banda de red. CBR junto con Caching Proxy examina las peticiones HTTP utilizando los tipos de normas especificados.

CBR le permite especificar un conjunto de servidores que manejen una petición basándose en la comparación expresiones regulares del contenido de la petición. Puesto que CBR le permite especificar varios servidores para cada tipo de petición, se puede repartir el tráfico de las peticiones para optimizar la respuesta al cliente. CBR también detectará si falla un servidor de un grupo y detendrá el encaminamiento de peticiones hacia ese servidor. El algoritmo de

reparto del tráfico utilizado por el componente CBR es idéntico al algoritmo comprobado utilizado por el componente Dispatcher.

Cuando Caching Proxy recibe una petición, ésta se compara con las normas que se han definido en el componente CBR. Si se encuentra una coincidencia, se elige uno de los servidores asociados con esa norma para atender la petición. A continuación, Caching Proxy realiza su proceso normal para encaminar la petición hacia el servidor elegido.

CBR tiene las mismas funciones que Dispatcher, a excepción de la alta disponibilidad, el subagente, el área amplia y otros mandatos de configuración.

Caching Proxy debe estar en ejecución para que CBR pueda comenzar a repartir las peticiones de los clientes.

Gestión de servidores locales con CBR

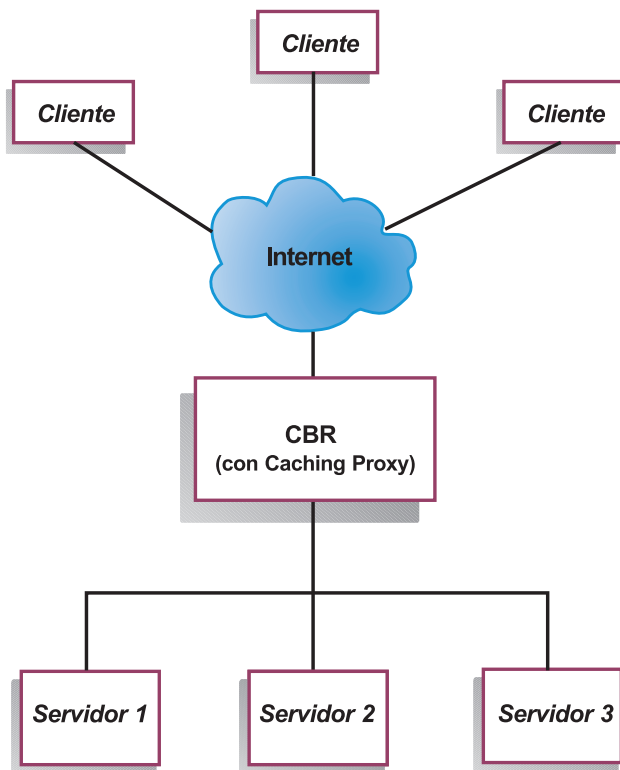


Figura 9. Ejemplo de sitio Web que utiliza CBR para gestionar servidores locales

La Figura 9 en la página 37 muestra una representación lógica de un sitio Web en el que se utiliza CBR para dirigir al proxy parte del contenido de los servidores locales. El componente CBR utiliza Caching Proxy para reenviar las peticiones de los clientes (HTTP o HTTPS) hacia los servidores basándose el contenido del URL.

Visión general del componente Mailbox Locator

Mailbox Locator puede proporcionar un único punto de presencia para varios servidores IMAP o POP3. Cada servidor puede tener un subconjunto de todos los servicios de correo de usuario para los que ofrece servicio el punto de presencia. Para el tráfico de IMAP y POP3 traffic, Mailbox Locator es un proxy que elige un servidor adecuado basándose en el ID de usuario y la contraseña proporcionados por el cliente. Mailbox Locator no da soporte al reparto del tráfico basado en normas.

Nota: Anteriormente el componente Mailbox Locator era una función dentro del componente CBR que repartía el tráfico entre servidores de correo IMAP y POP3. Al separar CBR en dos componentes, se *elimina* la limitación de que "CBR para IMAP/POP3" (Mailbox Locator) y "CBR para HTTP/HTTPS" (CBR con Caching Proxy) no se puedan ejecutar en la misma máquina.

Gestión de servidores locales con Mailbox Locator

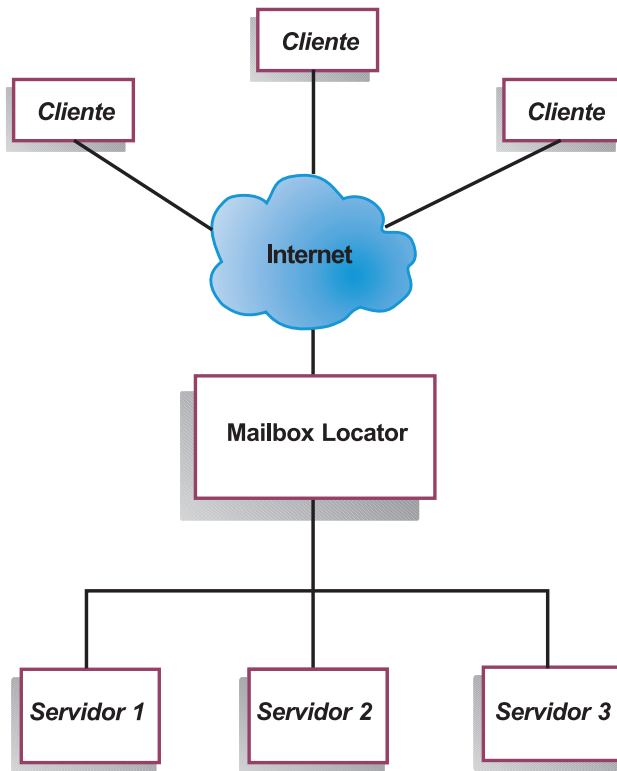


Figura 10. Ejemplo de sitio Web que utiliza Mailbox Locator para gestionar servidores locales

La Figura 10 muestra una representación lógica de un sitio Web donde se utiliza Mailbox Locator para encaminar las peticiones de los clientes (protocolo IMAP o POP3) hacia el servidor apropiado, basándose en el ID de usuario y la contraseña.

Visión general del componente Site Selector

Site Selector actúa como un servidor de nombres que funciona junto con otros servidores de nombres en un sistema de nombres de dominio para distribuir el tráfico entre un grupo de servidores utilizando medidas y pesos recopilados. Puede crear una configuración de sitio Web para poder repartir el tráfico entre un grupo de servidores basándose en el nombre de dominio utilizado para la petición de un cliente.

Un cliente envía una petición para resolver un nombre de dominio en un nombre de servidor dentro de su red. El servidor de nombres reenvía la petición a la máquina de Site Selector. A continuación, Site Selector resuelve el nombre de dominio y obtiene la dirección IP de uno de los servidores que se

ha configurado en el nombre de sitio. Site Selector devuelve la dirección IP del servidor seleccionado al servidor de nombres. El servidor de nombres devuelve la dirección IP al cliente.

Metric Server es un componente de Network Dispatcher, para la supervisión del sistema, que se debe instalar en cada servidor de la configuración hacia el que se reparte el tráfico. Mediante Metric Server, Site Selector puede supervisar el nivel de actividad de un servidor, detectar el servidor con menos tráfico y los servidores anómalos. El tráfico es una medida de la intensidad con que trabaja un servidor. Mediante la personalización de archivos de script de métricas del sistema, el usuario puede controlar el tipo de mediciones utilizadas para medir el tráfico. Se puede configurar Site Selector de acuerdo con el entorno, teniendo en cuenta factores tales como la frecuencia del acceso, el número total de usuarios y los tipos de acceso (por ejemplo, consultas breves, consultas de larga duración o cargas de datos que exigen un alto consumo de CPU).

Gestión de servidores locales y remotos mediante Site Selector y Metric Server

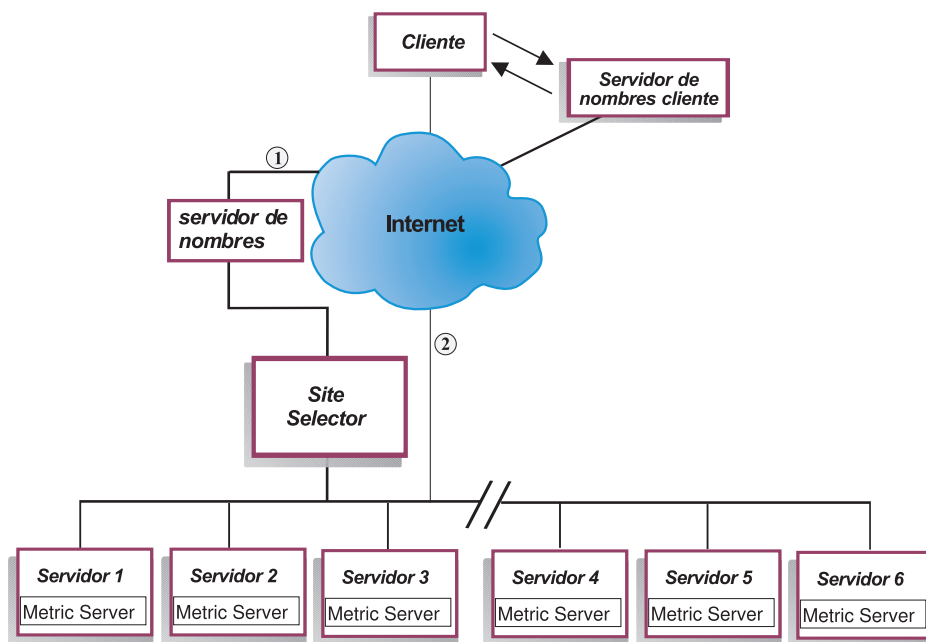


Figura 11. Ejemplo de sitio Web donde se utilizan Site Selector y Metric Server para gestionar servidores locales y remotos

La Figura 11 en la página 40 muestra un sitio Web donde se utiliza el componente Site Selector para responder a las peticiones. Servidor1, Servidor2 y Servidor3 son locales. Servidor4, Servidor5 y Servidor6 son remotos.

Un cliente envía una petición para resolver un nombre de dominio en un servidor de nombres dentro de su red. El servidor de nombres del cliente reenvía la petición a través del DNS a la máquina Site Selector (Ruta 1). A continuación, Site Selector resuelve el nombre de dominio y obtiene la dirección IP de uno de los servidores. Site Selector devuelve la dirección IP del servidor seleccionado al servidor de nombres del cliente. El servidor de nombres devuelve la dirección IP al cliente.

Después de recibir la dirección IP del servidor, el cliente envía las peticiones subsiguientes directamente al servidor seleccionado (Ruta 2).

Nota: En este ejemplo, Metric Server proporciona información sobre el tráfico del sistema a la máquina de Site Selector. El agente de Metric Server está instalado en cada servidor de fondo. Es conveniente utilizar Metric Server en combinación con Site Selector, pues de lo contrario Site Selector sólo puede utilizar un método de selección rotatorio para repartir el tráfico.

Visión general del componente Consultant para Cisco CSS Switches

Consultant para Cisco CSS Switches constituye una solución complementaria que actúa en combinación con la serie de conmutadores Cisco CSS 11000. Esta solución combinada integra los recursos de reenvío de paquetes y encaminamiento por contenido de la serie CSS 11000 con los complejos algoritmos de detección de Network Dispatcher para determinar información sobre la disponibilidad y la carga de trabajo de servidores de fondo, aplicaciones y bases de datos. La función de Cisco Consultant utiliza los asesores estándar, personalizados y del gestor de Network Dispatcher, y Metric Server para determinar las métricas, el estado y la carga de los servidores de fondo, aplicaciones y bases de datos. Con esta información, Cisco Consultant genera métricas de ponderación de servidores, la cual la envía a Cisco CSS Switch para seleccionar el servidor óptimo, optimizar el tráfico y habilitar la tolerancia a errores.

Cisco CSS Switch realiza decisiones sobre el reparto del tráfico basándose en criterios especificados por el usuario.

Cisco Consultant hace un seguimiento de muchos criterios, tales como:

- Conexiones activas y conexiones nuevas
- Información sobre la disponibilidad de aplicaciones y bases de datos, que se obtiene mediante el uso de asesores estándar y personalizados, y agentes residentes en servidores que están adaptados a la aplicación específica

- Utilización de la CPU
- Ocupación de la memoria
- Métricas de servidor personalizables por el usuario

Cuando Cisco CSS Switch, sin la utilización de Cisco Consultant, determina el estado de un servidor de contenidos, utiliza los tiempos de respuesta de las peticiones de contenido u otras medidas de la red. Cuando se utiliza Cisco Consultant, esas actividades se trasladan desde Cisco CSS Switch a Cisco Consultant. Cisco Consultant influye en la capacidad del servidor para atender las peticiones de contenido (el "peso" del servidor), y activa o detiene un servidor según convenga, cuando el servidor recupera o pierde su disponibilidad.

Cisco Consultant:

- Utiliza un interfaz SNMP publicada para obtener información sobre conexiones a partir de Cisco CSS Switch
- Utiliza datos procedentes de asesores para analizar la información sobre conexiones
- Utiliza información de Metric Server para analizar el estado relativo de los servidores
- Genera pesos para cada servidor de la configuración

Los pesos se aplican a todos los servidores de un puerto. Para un puerto determinado cualquiera, las peticiones se reparten entre los servidores según el peso relativo de los servidores. Por ejemplo, si un servidor tiene establecido un peso de 10 y otro tiene un peso 5, el servidor con peso 10 debe obtener el doble de peticiones que el servidor con peso 5. Estos pesos se proporcionan a Cisco CSS Switch utilizando SNMP. A medida que el peso de un servidor cualquiera se establece en un valor más alto, más peticiones envía Cisco CSS Switch hacia ese servidor.

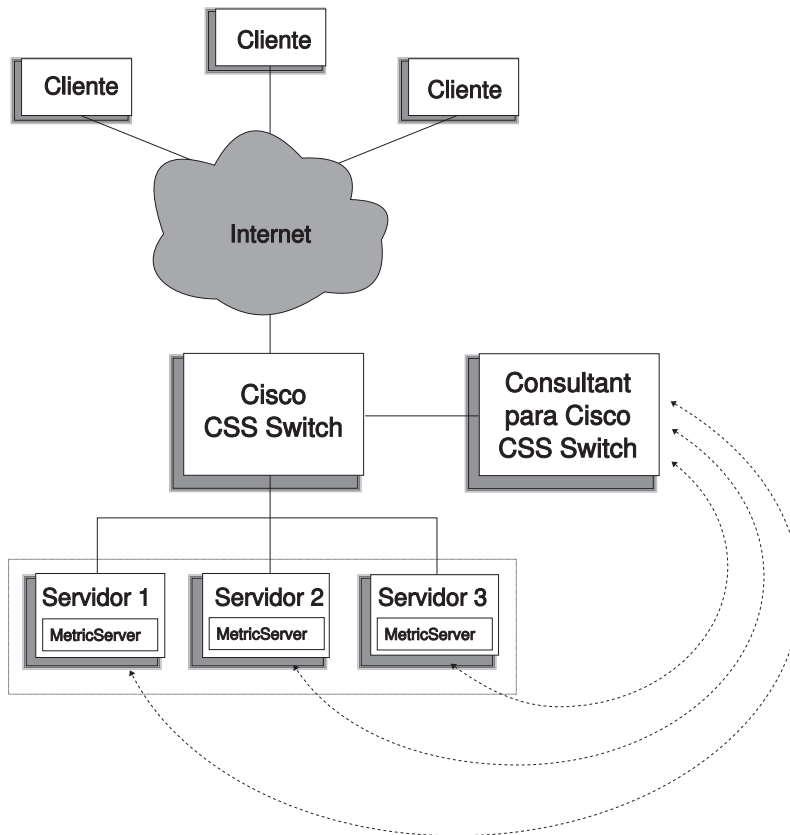


Figura 12. Ejemplo de sitio que utiliza Cisco Consultant y Metric Server para gestionar servidores locales

Cisco Consultant, junto con Cisco CSS Switch, proporciona una solución que combina la conmutación de contenidos con métodos complejos de identificación de aplicaciones, tolerancia a errores y optimización del tráfico de servidores. Cisco Consultant forma parte de una solución global complementaria entre Cisco CSS Switch y el producto WebSphere Edge Server de IBM.

Consulte el “Capítulo 2. Instalación de Network Dispatcher” en la página 11 para obtener una lista de los requisitos de Cisco Consultant.

Acerca de la alta disponibilidad

Dispatcher

El componente Dispatcher ofrece una función integrada de alta disponibilidad. Esta función supone el uso de una segunda máquina Dispatcher, cuya finalidad es supervisar a la máquina principal y estar a la espera para hacerse cargo del reparto del tráfico si falla la máquina principal. El componente Dispatcher también proporciona alta disponibilidad mutua, que permite que dos máquinas sean al mismo tiempo la máquina principal y la máquina de reserva la una respecto de la otra. Consulte “Configurar la característica de alta disponibilidad” en la página 166.

CBR, Mailbox Locator, Site Selector

Cuando utiliza una configuración de dos niveles con un Dispatcher que reparte el tráfico hacia dos o más servidores donde está instalado CBR, Mailbox Locator o Site Selector, puede conseguir un alto nivel de disponibilidad para estos componentes de Network Dispatcher.

Capítulo 4. Planificación del componente Dispatcher

En este capítulo se describen los aspectos que debe tener en cuenta la persona encargada de planificar la red antes de proceder a la instalación y configuración del componente Dispatcher.

- Consulte el “Capítulo 5. Configuración del componente Dispatcher” en la página 55 para obtener información sobre cómo configurar los parámetros de distribución de tráfico de Dispatcher.
- Consulte el “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131 para obtener información sobre cómo configurar Network Dispatcher para funciones más avanzadas.
- Consulte el “Capítulo 15. Utilización y gestión de Network Dispatcher” en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Este capítulo incluye las siguientes secciones:

- “Requisitos de hardware y de software”
- “Consideraciones referentes a la planificación”
- “Alta disponibilidad” en la página 47
- “Método de reenvío mac del Dispatcher” en la página 49
- “Método de reenvío nat del Dispatcher” en la página 50
- “Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)” en la página 52

Requisitos de hardware y de software

Requisitos de plataforma:

- Para AIX, vea “Requisitos para AIX” en la página 12
- Para Linux, vea “Requisitos para Red Hat Linux o SuSe Linux” en la página 16
- Para Solaris, vea “Requisitos para Solaris” en la página 19
- Para Windows 2000, vea “Requisitos para Windows 2000” en la página 22

Consideraciones referentes a la planificación

Dispatcher consta de las siguientes funciones:

- El **ndserver**, que maneja las peticiones procedentes de la línea de mandatos para el ejecutor, los asesores y el gestor.

- El **ejecutor**, que da soporte al reparto del tráfico basado en puertos para las conexiones TCP y UDP. El ejecutor puede reenviar las conexiones con servidores basándose en el tipo de petición recibida (por ejemplo, HTTP, FTP, SSL, etc.) El ejecutor se ejecuta siempre que se utiliza el componente Dispatcher para el reparto del tráfico.
- El **gestor**, que establece los pesos que utiliza el ejecutor basándose en:
 - Contadores internos del ejecutor
 - Información recibida de los servidores y proporcionada por los asesores
 - Información recibida de un programa de supervisión del sistema, tal como Metric Server o WLM.

El uso del gestor es opcional. No obstante, si no se utiliza un gestor, el reparto del tráfico se realiza utilizando una planificación rotatoria ponderada basada en los pesos actuales de los servidores, y no podrán utilizarse asesores.

- Los **asesores**, que consultan los servidores y analizan el resultado por protocolo antes de llamar al gestor para que establezca los pesos según convenga. Actualmente existen asesores para los protocolos HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3 y Telnet.

Dispatcher también proporciona asesores que no intercambian información específica del protocolo, tales como el asesor para DB2, que informa sobre el estado de los servidores DB2, y el asesor Ping, que notifica si el servidor responde a un mandato ping. Para obtener una lista completa de los asesores, vea “Lista de asesores” en la página 143.

También tiene la opción de escribir sus propios asesores (consulte “Creación de asesores personalizados (personalizables)” en la página 145).

El uso de asesores es opcional, pero recomendable.

- Para configurar y gestionar el ejecutor, los asesores y el gestor, utilice la línea de mandatos (**ndcontrol**;) o la interfaz gráfica de usuario (**ndadmin**).
- Se proporciona un **archivo de configuración de ejemplo** para configurar y administrar la máquina Dispatcher. Consulte “Apéndice F. Ejemplos de archivos de configuración” en la página 377. Una vez que haya instalado el producto, este archivo se encuentra en el subdirectorio **nd/servers/samples/** del directorio donde reside Network Dispatcher.
- El **subagente SNMP**, que permite a una aplicación de gestión basada en SNMP supervisar el estado de Dispatcher.

Las tres funciones clave de Dispatcher (el ejecutor, los asesores y el gestor) interactúan para repartir y asignar las peticiones entrantes entre los servidores. Además de repartir el tráfico de peticiones, el ejecutor supervisa el número de conexiones nuevas, conexiones activas y conexiones finalizadas. El ejecutor también recoge los datos sobrantes procedentes de conexiones finalizadas y proporciona esta información al gestor.

El gestor recoge información procedente del ejecutor, los asesores y un programa de supervisión del sistema, tal como Metric Server. Basándose en la información recibida, el gestor ajusta los valores de ponderación asignados a los servidores en cada puerto y proporciona al ejecutor la nueva ponderación para que la utilice en el reparto de conexiones nuevas.

Los asesores supervisan cada uno de los servidores del puerto asignado con el fin de determinar cuál es el tiempo de respuesta y la disponibilidad del servidor y, a continuación, facilitan esta información al gestor. También controlan si un servidor está activo o inactivo. Sin el gestor y los asesores, el ejecutor realiza una planificación rotatoria tomando como base el peso actual de los servidores.

Alta disponibilidad

Alta disponibilidad simple

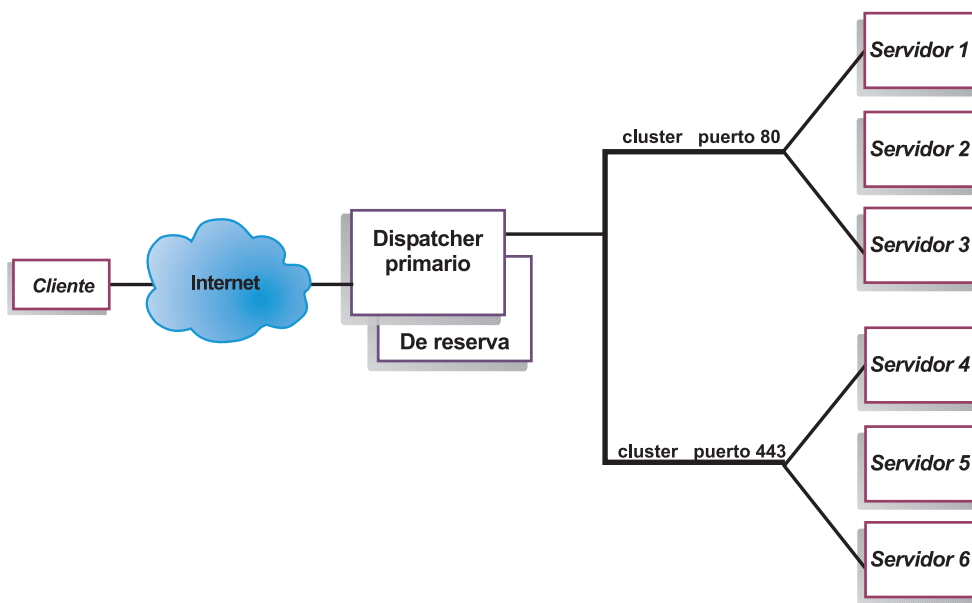


Figura 13. Ejemplo de Dispatcher utilizando la alta disponibilidad simple

La característica de alta disponibilidad conlleva la utilización de una segunda máquina Dispatcher. La primera máquina Dispatcher realiza el reparto del tráfico de clientes del mismo modo que lo haría en una configuración de un único Dispatcher. La segunda máquina Dispatcher supervisa la “salud” de la primera y se ocupa de la tarea de reparto del tráfico si detecta alguna anomalía en la primera máquina Dispatcher.

A cada una de estas dos máquinas se le asigna una función específica: *principal* o *de reserva*. La máquina principal envía datos de conexión a la máquina de reserva constantemente. Mientras la máquina principal está *activa* (reparte el tráfico), la máquina de reserva está en *estado de espera*, actualizándose continuamente y lista para tomar el control si fuera necesario.

Las sesiones de comunicación entre ambas máquinas se denominan *pulsos*. Los pulsos permiten a cada máquina supervisar la "salud" de la otra.

Si la máquina de reserva detecta que la máquina activa ha fallado, asumirá el control y empezará el reparto del tráfico. En ese momento se invierten los *estados* de ambas máquinas: la de reserva pasa a ser la *activa* y la principal pasa a estar en *espera*.

En la configuración de alta disponibilidad, las máquinas principal y de reserva deben estar en la misma subred.

Si desea obtener información sobre la configuración de la característica de alta disponibilidad, consulte el apartado "Alta disponibilidad" en la página 165.

Alta disponibilidad mutua

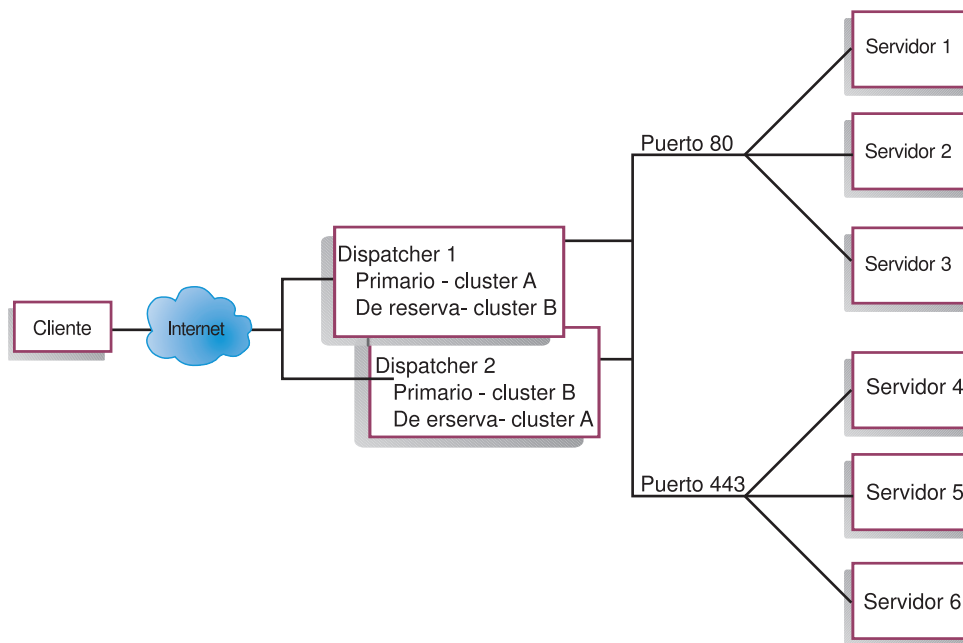


Figura 14. Ejemplo de Dispatcher utilizando la alta disponibilidad mutua

La característica de alta disponibilidad mutua conlleva la utilización de dos máquinas Dispatcher. Ambas máquinas realizan activamente el reparto del tráfico del tráfico de clientes y actúan como máquinas de reserva entre sí. En una configuración de alta disponibilidad simple, sólo una máquina se ocupa del reparto del tráfico. En una configuración de alta disponibilidad mutua, ambas máquinas comparten el reparto del tráfico del tráfico de clientes.

Para la alta disponibilidad mutua, el tráfico de clientes se asigna a cada máquina Dispatcher en base a una dirección de cluster. Cada cluster se puede configurar con la NFA (dirección de no reenvío) del Dispatcher primario. Por lo general, la máquina Dispatcher principal realiza el reparto del tráfico para dicho cluster. En caso de que se produzca una anomalía, la otra máquina se ocupa del reparto del tráfico correspondiente tanto a su cluster como al cluster del Dispatcher anómalo.

En la Figura 14 en la página 48 se muestra una ilustración de una configuración de alta disponibilidad mutua con el “conjunto A de clusters” compartidos y el “conjunto B de clusters” compartidos. Cada Dispatcher puede encaminar activamente paquetes destinados al cluster *principal*. Si cualquiera de los dos Dispatcher fallara y ya no pudiera encaminar paquetes para el cluster principal, el otro Dispatcher podría hacerse cargo del encaminamiento de paquetes para el cluster de *reserva*.

Nota: Ambas máquinas deben configurar sus conjuntos de clusters compartidos del mismo modo.

Para obtener más información sobre la configuración de la alta disponibilidad y de la alta disponibilidad mutua, consulte el apartado “Alta disponibilidad” en la página 165.

Método de reenvío mac del Dispatcher

El reenvío MAC es el método de reenvío por omisión mediante el cual el Dispatcher reparte el tráfico de peticiones entrantes del servidor y el servidor devuelve la respuesta *directamente* al cliente, sin ninguna intervención del Dispatcher. Cuando se utiliza este método de reenvío, Dispatcher sólo necesita observar el tráfico entrante que fluye desde el cliente al servidor. No necesita observar el tráfico saliente que circula desde el servidor al cliente. Esto reduce significativamente el efecto que tiene sobre la aplicación y puede mejorar el funcionamiento de la red.

El método de reenvío se puede seleccionar al añadir un puerto con el mandato **ndcontrol port add cluster:puerto method valor**. El método de reenvío por omisión es **mac**. Puede especificar el parámetro “method”

solamente al añadir el puerto. Después de añadir el puerto, no puede cambiar el valor del método de reenvío. En “*ndcontrol port — configurar puertos*” en la página 287 hallará más información.

Método de reenvío nat del Dispatcher

Cuando se utiliza el recurso NAT (Network Address Translation) o NAPT (Network Address Port Translation) de Dispatcher ya no es necesario que los servidores sujetos a reparto del tráfico estén situados en una red conectada localmente. Si desea tener servidores en ubicaciones remotas, puede utilizar el método de reenvío NAT en lugar de la técnica de encapsulación GRE/WAN. Puede también utilizar la función NAPT para acceder a varios daemons que residen en cada servidor sujeto a reparto del tráfico, en donde cada daemon está a la escucha en un puerto exclusivo.

Existen dos maneras de configurar servidores con varios daemons:

- Con NAT, puede configurar varios daemons de servidor para responder a peticiones dirigidas a diferentes direcciones IP. Esto se denomina vincular un daemon de servidor con una dirección IP.
- Con NAPT, puede configurar varios daemons de servidor (ejecutándose en el mismo servidor físico) para estar a la escucha en números de puerto diferentes.

Esta aplicación es efectiva con protocolos de aplicación de nivel superior, tales como HTTP, SSL, IMAP, POP3, NNTP, SMTP, Telnet, etc.

Limitaciones:

- La implementación de NAT/NAPT utilizada para Dispatcher es una implementación *simple* de esa función. Sólo analiza y trabaja sobre el contenido de las cabeceras de paquetes TCP/IP. No analiza el contenido de la porción de datos de los paquetes. Para Dispatcher, NAT/NAPT no es efectivo con los protocolos de aplicación, tales como FTP, que incluyen las direcciones o números de puerto en la porción de datos de los mensajes. Esta es una limitación bien conocida del NAT/NAPT basado en el uso de cabeceras.
- La función NAT/NAPT de Dispatcher no puede utilizar clusteres comodín ni puertos comodín.

Para implementar NAT/NAPT:

- Defina el parámetro **clientgateway** del mandato **ndcontrol executor set**. Clientgateway es la dirección IP de encaminador a través de la cual se reenvía el tráfico de retorno desde Network Dispatcher a los clientes. Este valor debe ser una dirección IP distinta de 0 para poder utilizar NAT/NAPT. En “*ndcontrol executor — controlar el ejecutor*” en la página 263 hallará más información.

- Añada un puerto utilizando el mandato **ndcontrol port add** *cluster:puerto* **method** *valor*. El valor para el método de reenvío debe ser **nat**. Puede especificar el parámetro "method" solamente al añadir el puerto. Después de añadir el puerto, no puede cambiar el valor del método de reenvío. En "ndcontrol port — configurar puertos" en la página 287 hallará más información.

Nota: Si el valor de clientgateway no es distinto de 0, el método de reenvío sólo podrá ser **mac** (método de reenvío basado en MAC).

- Añada un servidor utilizando los parámetros mapport, returnaddress y router del mandato **ndcontrol**. Por ejemplo:

```
ndcontrol server add cluster:puerto:servidor mapport valor
returnaddress dirección_retorno router dirección_retorno
```

– **mapport**

Correlaciona el número del puerto de destino de la petición del cliente con el número de puerto que Dispatcher utiliza para repartir el tráfico de la petición del cliente.. Mapport permite que Network Dispatcher reciba la petición de un cliente en un puerto y la envíe a un puerto diferente del servidor. Mediante mapport, puede repartir el tráfico de las peticiones de un cliente hacia un servidor donde se pueden estar ejecutando varios daemons de servidor. El valor por omisión para mapport es el número del puerto de destino de la petición del cliente.

– **returnaddress**

La dirección de retorno es una dirección exclusiva o nombre de sistema principal que el usuario configura en la máquina de Dispatcher. Dispatcher utiliza la dirección de retorno como dirección de origen cuando reparte el tráfico de la petición del cliente hacia el servidor. De esta forma se asegura que el servidor devuelva el paquete a Dispatcher, en lugar de enviar el paquete directamente al cliente. ((Seguidamente, Dispatcher reenvía el paquete IP al cliente). Debe especificar la dirección de retorno (returnaddress) cuando añada el servidor. Para cambiar la dirección de retorno debe primero eliminar el servidor y luego añadirlo de nuevo. La dirección de retorno no puede ser la misma que la dirección de cluster, la dirección de servidor ni la dirección NFA.

– **router**

La dirección del encaminador que conduce al servidor remoto.

Para obtener más información sobre el mandato **ndcontrol server** y el uso de los parámetros mapport, returnaddress y router, consulte "ndcontrol server — configurar servidores" en la página 302.

Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)

En versiones anteriores de Network Dispatcher, el encaminamiento por contenido sólo podía utilizarse al usar el componente CBR en combinación con Caching Proxy. Ahora el componente Dispatcher permite realizar encaminamiento por contenido para HTTP (utilizando la norma de tipo "content") y para HTTPS (utilizando la afinidad del ID de sesión de SSL), sin tener que utilizar Caching Proxy. Para el tráfico de HTTP y HTTPS, el componente Dispatcher puede proporcionar un encaminamiento por contenido más rápido que el componente CBR.

Para HTTP: La selección de servidor, para el encaminamiento por contenido del Dispatcher, se basa en el contenido de un URL o una cabecera HTTP. Se configura utilizando la norma de tipo "content". Cuando configure la norma de contenido, especifique la cadena de búsqueda y un conjunto de servidores para la norma. Cuando se procesa una nueva petición entrante, esta norma compara la cadena especificada con el URL del cliente o con la cabecera HTTP especificada en la petición del cliente.

Si Dispatcher encuentra la cadena en la petición del cliente, Dispatcher reenvía la petición a uno de los servidores comprendidos en la norma. Seguidamente, Dispatcher reenvía la respuesta desde el servidor al cliente (método de reenvío "cbr").

Si Dispatcher no encuentra la cadena en la petición del cliente, Dispatcher *no* selecciona un servidor de entre el grupo de servidores comprendidos en la norma.

Nota: La norma de contenido se configura en el componente Dispatcher de la misma manera que en el componente CBR. Dispatcher puede utilizar la norma de contenido para el tráfico HTTP. En cambio, el componente CBR puede utilizar la norma de contenido para el tráfico HTTP y el tráfico HTTPS (SSL).

Para HTTPS (SSL): El direccionamiento basado en contenido de Dispatcher reparte el tráfico basándose en el campo de ID de sesión SSL contenido en la petición del cliente. Cuando se utiliza SSL, la petición de un cliente contiene el ID de sesión SSL de una sesión anterior y los servidores mantienen una antememoria de sus conexiones SSL anteriores. La función de afinidad del Dispatcher para el ID de sesión SSL permite establecer una nueva conexión entre el cliente y el servidor utilizando los parámetros de seguridad de la conexión anterior con el servidor. Debido a que no se tienen que volver a negociar los parámetros de seguridad de SSL, tales como claves compartidas y algoritmos de cifrado, los servidores ahorran ciclos de CPU y el cliente obtiene una respuesta más rápida. Para habilitar la afinidad de ID de sesión

de SSL, puerto **stickytime** debe tener un valor distinto de cero. Una vez transcurrido el tiempo de persistencia, la petición del cliente se puede enviar a un servidor diferente del anterior.

Para implementar el encaminamiento por contenido del Dispatcher (método de reenvío cbr):

- Defina el parámetro **clientgateway** del mandato **ndcontrol executor set**. Clientgateway es la dirección IP de encaminador a través de la cual se reenvía el tráfico de retorno desde Dispatcher a los clientes. El valor por omisión de clientgateway es 0. Este valor debe establecerse en una dirección IP distinta de 0 (cero) para poder añadir un método de reenvío de encaminamiento por contenido. En “ndcontrol executor — controlar el ejecutor” en la página 263 hallará más información.
- Añada un puerto utilizando el parámetro **method** del mandato **ndcontrol port add**. El valor para el método de reenvío debe ser **cbr**. En “ndcontrol port — configurar puertos” en la página 287 hallará más información.

Nota: Si no establece la dirección de clientgateway en un valor distinto de cero, el método de reenvío sólo puede ser el método **mac**.

- Añada un servidor utilizando los parámetros mapport, returnaddress y router

ndcontrol server add *cluster:puerto:servidor* **mapport** *valor* **returnaddress** *dirección_retorno* **router** *dirección_retorno*

Nota: Para obtener información sobre la configuración del servidor mediante los parámetros mapport, returnaddress y router, consulte la página 51.

- **Para HTTP:** Realice la configuración utilizando normas basadas en el contenido de la petición del cliente (tipo de norma **content**). Por ejemplo:
ndcontrol rule 125.22.22.03:80:contentRule1 **type** content **pattern** *patrón*
Donde *patrón* especifica el patrón que debe utilizarse para la norma de tipo content. Para obtener más información sobre el tipo de norma content, vea “Utilización de normas basadas en el contenido de la petición” en la página 181. Para conocer las expresiones válidas para *patrón*, vea “Apéndice C. Sintaxis de la norma de contenido (patrón):” en la página 313.
Para HTTPS (SSL): Para configurar la afinidad del ID de sesión de SSL, establezca el parámetro **stickytime** del puerto en un valor distinto de cero. Para obtener más información sobre **stickytime** en el mandato port, consulte “ndcontrol rule — configurar normas” en la página 294.

Nota: La función de replicación del registro de conexión para la modalidad de alta disponibilidad (que asegura la conservación de la conexión del

cliente cuando el Dispatcher de reserva toma el relevo a la máquina principal) *no* se puede utilizar junto con el encaminamiento por contenido del Dispatcher.

Capítulo 5. Configuración del componente Dispatcher

Antes de seguir los pasos indicados en este capítulo, lea el “Capítulo 4. Planificación del componente Dispatcher” en la página 45. Este capítulo explica cómo crear una configuración básica para el componente Dispatcher de Network Dispatcher.

- Consulte el “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131 para ver configuraciones más complejas de Network Dispatcher.
- Consulte el “Capítulo 15. Utilización y gestión de Network Dispatcher” en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Visión general de las tareas de configuración

Nota: Antes de realizar los pasos de configuración indicados en esta tabla, asegúrese de que las máquinas Dispatcher y todas las máquinas servidor están conectadas a la red, tienen una dirección IP válida y pueden emitir el mandato ping entre sí.

Tabla 3. Tareas de configuración de la función Dispatcher

Tarea	Descripción	Información relacionada
Configurar la máquina Dispatcher.	Instalar la configuración de reparto del tráfico.	“Configurar la máquina Dispatcher” en la página 58
Configurar máquinas para el reparto del tráfico.	Crear un alias para el dispositivo de bucle de retorno, comprobar si existe alguna ruta sobrante y suprimir las rutas sobrantes que existan.	“Configuración de las máquinas servidor para el reparto del tráfico” en la página 65

Métodos de configuración

Existen cuatro métodos básicos para la configuración de Dispatcher:

- Línea de mandatos
- Scripts
- Interfaz gráfica de usuario (GUI)
- Asistente de configuración

Línea de mandatos

Este es el medio más directo para configurar el Dispatcher. Los valores de los parámetros de mandatos se deben escribir en caracteres ingleses. Las únicas excepciones son los nombres de sistema principal (utilizados en los mandatos para clusters y servidores y en la modalidad de alta disponibilidad) y los nombres de archivo (utilizados en los mandatos sobre archivos).

Para iniciar Dispatcher desde la línea de mandatos:

- Emita el mandato **ndserver** desde el indicador de mandatos. En Windows 2000, ndserver se ejecuta como servicio que se inicia automáticamente.

Nota: Para detener el servicio, emita lo siguiente: **ndserver stop**.

- A continuación, emita los mandatos de control de Dispatcher que desee para establecer la configuración. Los procedimientos de este manual presuponen que se utiliza la línea de mandatos. El mandato es **ndcontrol**. Para obtener más información acerca de los mandatos, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.

Puede especificar una versión abreviada de los parámetros de los mandatos ndcontrol. Sólo necesita especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato “file save”, puede entrar **ndcontrol he f** en lugar de **ndcontrol help file**.

Para iniciar la interfaz de línea de mandatos, emita **ndcontrol** para visualizar un indicador de mandatos de ndcontrol.

Para cerrar la interfaz de línea de mandatos, emita **exit** o **quit**.

Scripts

Los mandatos para configurar el Dispatcher se pueden entrar en un archivo script de configuración para que se ejecuten conjuntamente. Consulte “Archivos de configuración de ejemplo para Network Dispatcher” en la página 377.

Nota: Para ejecutar rápidamente el contenido de un archivo de script (por ejemplo, *miscript*), utilice cualquiera de estos dos mandatos:

- Para actualizar la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:
ndcontrol file appendload *miscript*
- Para sustituir totalmente la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:
ndcontrol file newload *miscript*

GUI

Para ver un ejemplo de la interfaz gráfica de usuario (GUI), consulte la Figura 2 en la página 5.

Para iniciar la GUI, siga estos pasos

1. Asegúrese de que ndserver se está ejecutando:
 - Para AIX, Linux o Solaris, ejecute el siguiente mandato como usuario root:
ndserver
 - Para Windows 2000, ndserver se ejecuta como servicio que se inicia automáticamente
2. A continuación, siga uno de estos métodos:
 - Para AIX, Linux o Solaris, especifique **ndadmin**
 - Para Windows 2000, pulse **Inicio, Programas, IBM WebSphere, Edge Server, IBM Network Dispatcher** y finalmente **Network Dispatcher**

Para configurar el componente Dispatcher desde la GUI, debe seleccionar primero **Dispatcher** en la estructura en árbol. Puede arrancar el ejecutor y el gestor cuando esté conectado a un sistema principal. También puede crear clusters que contengan puertos y servidores e iniciar asesores para el gestor.

La GUI se puede utilizar para realizar las mismas acciones que con el mandato **ndcontrol**. Por ejemplo, para definir un cluster desde la línea de mandatos, especifique el mandato **ndcontrol cluster add cluster**. Para definir un cluster desde la GUI, pulse el botón derecho del ratón sobre Ejecutor, y en el menú emergente pulse el botón izquierdo sobre **Añadir cluster**. Escriba la dirección del cluster en la ventana emergente, a continuación pulse **Aceptar**.

Los archivos de configuración preexistentes de Dispatcher se pueden cargar utilizando las opciones **Cargar nueva configuración** (para sustituir totalmente la configuración actual) y **Añadir a configuración actual** (para actualizar la configuración actual); estas opciones aparecen en el menú emergente **Sistema principal**. Debe guardar periódicamente la configuración de Dispatcher en un archivo, mediante la opción **Guardar archivo de configuración como** también del menú emergente **Sistema principal**. El menú **Archivo**, situado en la parte superior de la GUI, le permitirá guardar las conexiones actuales del sistema principal en un archivo o restaurar las conexiones de los archivos existentes en todos los componentes Network Dispatcher.

Los mandatos de configuración también se pueden ejecutar remotamente. Para obtener más información, consulte “Administración autenticada remota” en la página 205.

Puede acceder a la **Ayuda** pulsando el icono de signo de interrogación, situado en la esquina superior derecha de la ventana de Network Dispatcher.

- **Ayuda para los campos** — describe cada campo y sus valores por omisión
- **Cómo puedo** — lista tareas que pueden efectuarse desde esa pantalla
- **Contenido** — es una tabla de contenido de toda la información de la Ayuda
- **Índice** — es un índice alfabético de temas de la Ayuda

Para obtener más información acerca de la utilización de la GUI, consulte “Instrucciones generales para la utilización de la GUI” en la página 6.

Asistente de configuración

Para obtener más información acerca de la utilización del asistente de configuración, consulte “Configuración mediante el asistente para configuración” en la página 4.

Configurar la máquina Dispatcher

Para configurar la máquina Dispatcher, debe ser el usuario root (en AIX, Linux o Solaris) o el administrador en Windows 2000.

En AIX, Linux y Solaris, Network Dispatcher puede tener un servidor con **ubicación compartida**. Esto simplemente significa que Network Dispatcher puede residir físicamente en una máquina servidor para la que realiza reparto del tráfico.

Necesitará al menos dos direcciones IP válidas para la máquina Dispatcher:

- Una dirección IP específicamente para la máquina Dispatcher
Esta dirección IP es la dirección IP principal de la máquina Dispatcher y se denomina dirección de no reenvío (NFA). Esta dirección es por omisión la misma que devuelve el mandato **hostname**. Utilice esta dirección para conectarse a la máquina con fines administrativos, como por ejemplo efectuar una configuración remota por medio de Telnet o acceder al subagente SNMP. Si la máquina Dispatcher ya puede realizar una operación ping con otras máquinas de la red, no es necesario hacer nada más para configurar la dirección de no reenvío.
- Una dirección IP para cada cluster
Una dirección de cluster es una dirección que está asociada con un nombre de sistema principal (como `www.suempresa.com`). Esta dirección IP la utilizan los clientes para conectarse a los servidores de un cluster. Esta es la dirección cuyo tráfico es repartido por Dispatcher.

Sólo Solaris:

1. Por omisión, Dispatcher se configura para repartir el tráfico en las tarjetas de interfaz de red Ethernet de 100 Mbps. Para cambiar el valor por omisión, debe editar el archivo `/opt/nd/servers/ibmnd.conf` del siguiente modo:

- El adaptador predefinido Ethernet de 100 Mbps se especifica en `ibmnd.conf` como `hme`.
- Para utilizar un adaptador Ethernet de 10 Mbps, sustituya `hme` por `le`.
- Para utilizar un adaptador Ethernet de 1 Gbps, sustituya `hme` por `ge`.
- Para utilizar un adaptador multipuerto, sustituya `hme` por `qfe`.
- Para poder utilizar varios tipos de adaptador, copie la línea en el archivo `ibmnd.conf` y modifique cada línea de acuerdo con el tipo de dispositivo.

Por ejemplo, si planea utilizar adaptadores Ethernet de 100 Mbps, el archivo `ibmnd.conf` debe contener una sola línea que especifique el dispositivo `hme`. Si prevé utilizar un adaptador Ethernet de 10 Mbps y un adaptador Ethernet de 100 Mbps, el archivo `ibmnd.conf` contendrá dos líneas: una que especificará el dispositivo `le` y otra que especificará el dispositivo `hme`.

El archivo **`ibmnd.conf`** proporciona datos de entrada para el mandato **`autopush`** de Solaris y debe ser compatible con este mandato.

2. Iniciar o detener el ejecutor de Dispatcher desconfigurará todos los alias de los adaptadores listados en el archivo `ibmnd.conf`. Para volver a configurar automáticamente los alias de esos adaptadores (excepto los que utilice el componente Dispatcher de Network Dispatcher), sírvase del archivo de script **`goAliases`**. Encontrará un script de ejemplo en el directorio `...nd/servers/samples` y *se tiene* que mover a `...nd/servers/bin` para que funcione. El script `goAliases` se ejecuta automáticamente cuando el ejecutor de Dispatcher se inicia o se detiene.

Por ejemplo, si los clusters X e Y están configurados para que los utilice el componente Mailbox Locator en cualquiera de los adaptadores que se muestran en `ibmnd.conf`, los clusters X e Y están desconfigurados cuando se emiten los mandatos **`ndcontrol executor start`** o **`ndcontrol executor stop`**. Puede que éste no sea el resultado que desea. Cuando los clusters X e Y se configuren en el script `goAliases`, los clusters volverán a configurarse automáticamente después de que el ejecutor de Dispatcher se inicie o se detenga.

Sólo para Windows 2000: Asegúrese de que el reenvío de IP no está habilitado para el protocolo TCP/IP. (Consulte la configuración de TCP/IP para Windows 2000).

La Figura 15 muestra un ejemplo de Dispatcher configurado con un solo cluster, dos puertos y tres servidores.

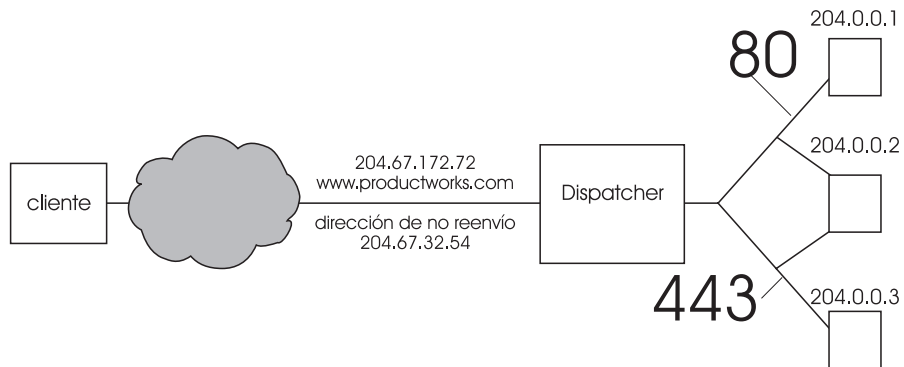


Figura 15. Ejemplo de las direcciones IP que se necesitan para la máquina Dispatcher

Si desea obtener ayuda sobre los mandatos utilizados en este procedimiento, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.

Si desea ver un archivo de configuración de ejemplo, consulte “Archivos de configuración de ejemplo para Network Dispatcher” en la página 377.

Paso 1. Iniciar la función de servidor

AIX, Linux y Solaris: Para iniciar la función del servidor, escriba **ndserver**.

Windows 2000: La función del servidor se inicia automáticamente como un servicio.

Nota: Automáticamente se cargará un archivo de configuración por omisión (default.cfg) cuando inicie ndserver. Si el usuario decide guardar la configuración de Dispatcher en default.cfg, entonces todo lo que haya guardado en este archivo se cargará automáticamente la próxima vez que se inicie ndserver.

Paso 2. Iniciar la función de ejecutor

Para iniciar la función del ejecutor, entre el mandato **ndcontrol executor start**. También puede cambiar diversos valores del ejecutor en este momento. Consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.

Paso 3. Definir la dirección de no reenvío (si es diferente del nombre de sistema principal)

La dirección de no reenvío sirve para conectarse a la máquina con fines administrativos, como por ejemplo, utilizar Telnet o SMTP en esta máquina. Por omisión, esta dirección es el nombre del sistema principal.

Para definir la dirección de no reenvío, entre el mandato **ndcontrol executor set nfa dirección_IP** o edite el archivo de configuración de ejemplo. *Dirección_IP* es el nombre simbólico o la dirección decimal con puntos.

Paso 4. Definir un cluster y establecer las opciones de cluster

Dispatcher repartirá las peticiones enviadas a la dirección de cluster hacia los servidores correspondientes configurados en los puertos de ese cluster.

El cluster es el nombre simbólico, la dirección decimal con puntos o la dirección 0.0.0.0 especial que define un cluster comodín. Para definir un cluster, emita el mandato **ndcontrol cluster add**. Para establecer opciones de cluster, emita el mandato **ndcontrol cluster set**; también puede utilizar la GUI para emitir mandatos. Se pueden utilizar clusters comodín para que coincidan con varias direcciones IP para paquetes entrantes cuyo tráfico se desea repartir. Consulte “Utilizar el cluster comodín para combinar configuraciones de servidores” en la página 185, “Utilizar el cluster comodín para repartir el tráfico de los cortafuegos” en la página 186 y “Utilización del cluster comodín con Caching Proxy para proxy transparente” en la página 187 para obtener más información.

Paso 5. Crear un alias para la tarjeta de interfaz de red

Una vez definido el cluster, generalmente deberá configurar la dirección del cluster en una de las tarjetas de interfaz de red de la máquina Dispatcher. Para ello, emita el mandato **ndcontrol cluster configure dirección_cluster**. De esta forma se buscará un adaptador con una dirección existente que pertenezca a la misma subred que la dirección de cluster. Luego emitirá el mandato de configuración del adaptador del sistema operativo para la dirección de cluster, utilizando el adaptador encontrado y la máscara de red para la dirección existente que se ha encontrado en el adaptador. Por ejemplo:

```
ndcontrol cluster configure 204.67.172.72
```

No se configurará la dirección de cluster en las siguientes circunstancias: para los clusters añadidos a un servidor en espera en modalidad de alta disponibilidad, y para los clusters añadidos a un dispatcher de área amplia que actúe como un servidor remoto. Tampoco es necesario que ejecute el mandato cluster configure si utiliza el script **goIdle** de ejemplo en modalidad autónoma. Para obtener información sobre el script **goIdle**, consulte “Utilización de scripts” en la página 170.

En raros casos es posible que tenga una dirección de cluster que no coincida con ninguna subred de las direcciones existentes. Si así fuera, utilice el segundo formato del mandato cluster configure y proporcione explícitamente el nombre de interfaz y la máscara de red. Utilice **ndcontrol cluster configure dirección_cluster nombre_interfaz máscara_red**.

A continuación se muestran algunos ejemplos:

```
ndcontrol cluster configure 204.67.172.72 en0 255.255.0.0
(AIX)
ndcontrol cluster configure 204.67.172.72 eth0:1 255.255.0.0
(Linux)
ndcontrol cluster configure 204.67.172.72 le0:1 255.255.0.0
(Solaris 7)
ndcontrol cluster configure 204.67.172.72 le0 255.255.0.0
(Solaris 8)
ndcontrol cluster configure 204.67.172.72 en0 255.255.0.0
(Windows 2000)
```

Windows 2000

Para utilizar el segundo formato del mandato de configuración del cluster en Windows 2000, debe determinar el nombre de interfaz que se debe utilizar.

Si tiene una sola tarjeta Ethernet en la máquina, el nombre de interfaz será en0. De igual forma, si tiene una sola tarjeta de Red en Anillo en la máquina, el nombre de interfaz será tr0. Si tiene varias tarjetas de cualquiera de los dos tipos, tendrá que determinar cuál es la correlación de las tarjetas. Siga estos pasos:

1. Inicie **regedit** en el indicador de mandatos.
2. Pulse **HKEY_LOCAL_MACHINE**, pulse **Software**, pulse **Microsoft**, pulse **Windows NT**, pulse **Current Version**.
3. A continuación, pulse **Network Cards**

Debajo de Network Cards figuran los adaptadores de interfaz de red. Pulse en ellos para determinar si se trata de una interfaz Ethernet o de Red en Anillo. El tipo de interfaz figura en la columna *Description*. Los nombres asignados por **ndconfig** están correlacionados con los tipos de interfaz. Por ejemplo, ndconfig asigna la primera interfaz Ethernet de la lista a en0, la segunda a en1, etcétera; la primera interfaz de Red en Anillo se asigna a tr0, la segunda a tr1, etcétera.

Nota: El registro de Windows 2000 numera los adaptadores comenzando por 1, no por 0.

Una vez obtenida esta información sobre correlaciones, puede crear un alias en la interfaz de red para la dirección de cluster.

Utilización de ifconfig/ndconfig para configurar un alias de cluster

El mandato "cluster configure" meramente ejecuta mandatos ifconfig (o ndconfig en Windows 2000), por lo que el usuario puede seguir usando los mandatos ifconfig (ndconfig) si lo desea.

Windows 2000: El mandato ndconfig se suministra con el componente Dispatcher para configurar los alias de cluster utilizando la línea de mandatos. El mandato ndconfig tiene la misma sintaxis que el mandato ifconfig de UNIX.

```
ndconfig en0 alias 204.67.172.72 netmask 255.255.0.0
```

Nota: El parámetro netmask es obligatorio. Debe tener formato decimal separado por puntos (255.255.0.0) o hexadecimal (0xffff0000).

Para determinar el nombre de interfaz, utilice la misma técnica que para el segundo formato del mandato cluster configure.

Solaris: Cuando utilice aplicaciones de servidores de vinculación específica que se vinculen con una lista de direcciones IP que no contienen el valor IP del servidor, utilice el mandato **arp publish** en lugar de ifconfig para establecer dinámicamente una dirección IP en la máquina Network Dispatcher. Por ejemplo:

```
arp -s <cluster> <dirección MAC>  
Network Dispatcher> pub
```

Paso 6. Definir los puertos y establecer las opciones de puerto

Para definir un puerto, entre el mandato **ndcontrol port add cluster:puerto**, edite el archivo de configuración de ejemplo o utilice la GUI. *Cluster* es el nombre simbólico o la dirección decimal con puntos. *Puerto* es el número del puerto utilizado para el protocolo. También puede cambiar diversos valores de puerto en este momento. Debe definir y configurar todos los servidores de un puerto. Consulte el "Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator" en la página 249.

El número de puerto 0 (cero) se utiliza para especificar un puerto comodín. Este puerto aceptará tráfico para un puerto que no está destinado a ninguno de los puertos definidos en el cluster. El puerto comodín se utilizará para configurar las normas y los servidores para cualquier puerto. Esta función también se podría utilizar si tiene una configuración de servidor/norma idéntica para varios puertos. El tráfico de un puerto afectaría luego a las decisiones de reparto del tráfico para el tráfico de otros puertos. Consulte "Utilización del puerto comodín para dirigir el tráfico de puertos no configurados" en la página 187 para obtener más información acerca de cuándo se utiliza un puerto comodín.

Nota: El puerto comodín no se puede utilizar para gestionar tráfico FTP.

Paso 7. Definir los servidores con reparto del tráfico

Para definir una máquina servidor con reparto del tráfico, escriba el mandato **ndcontrol server add cluster:puerto:servidor**, edite el archivo de configuración de ejemplo o utilice la GUI. *Cluster* y *servidor* son el nombre simbólico o la dirección decimal con puntos. *Puerto* es el número del puerto utilizado para el protocolo. Debe definir más de un servidor para un puerto en un cluster para realizar el reparto del tráfico.

Servidores de vinculación específica: Si el componente Dispatcher va a repartir el tráfico para servidores de vinculación específica, los servidores *deben* estar configurados para vincularse con la dirección de cluster. Puesto que Dispatcher reenvía los paquetes sin cambiar la dirección IP de destino, cuando los paquetes alcancen el servidor, todavía contendrán la dirección de cluster como destino. Si un servidor se ha configurado para vincularse con una dirección IP distinta de la dirección de cluster, el servidor no podrá aceptar paquetes/peticiones destinados al cluster.

Nota: Para Solaris y Linux: no se deben definir servidores de vinculación específica como servidores de ubicación compartida.

Ubicación compartida con diferentes direcciones: En una configuración con ubicación compartida, la dirección del servidor con ubicación compartida *no* es necesario que sea idéntica a la dirección de no reenvío (NFA). Puede utilizar otra dirección si la máquina se ha definido con varias direcciones IP. Para el componente Dispatcher, la máquina servidor con ubicación compartida se debe definir como **collocated** mediante el mandato **ndcontrol server**. Para obtener más información acerca de los servidores con ubicación compartida, consulte “Utilización de servidores de ubicación compartida” en la página 155.

Para obtener más información sobre la sintaxis del mandato **ndcontrol server**, consulte “**ndcontrol server** — configurar servidores” en la página 302.

Paso 8. Arrancar la función gestor (opcional)

La función gestor mejora el reparto del tráfico. Para arrancar el gestor, especifique el mandato **ndcontrol manager start**, edite el archivo de configuración de ejemplo o utilice la GUI.

Paso 9. Arrancar la función asesor (opcional)

Los asesores facilitan al gestor más información sobre la capacidad de las máquinas servidor con reparto del tráfico para responder a las peticiones. Cada asesor es específico de un protocolo. Por ejemplo, para iniciar el asesor HTTP, emita el mandato siguiente:

```
cbrcontrol advisor start http
puerto
```

Para obtener una lista de los asesores junto con sus puertos por omisión, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249. Si desea ver una descripción de cada asesor, consulte la sección “Lista de asesores” en la página 143.

Paso 10. Establecer las proporciones del cluster según sea necesario

Si inicia asesores, puede modificar la proporción de importancia que se asigna a la información del asesor utilizada para las decisiones sobre reparto del tráfico. Para establecer las proporciones del cluster, emita el mandato **ndcontrol cluster set cluster proportions**. Para obtener más información, consulte “Grado de importancia dado a la información de estado” en la página 135.

Configuración de las máquinas servidor para el reparto del tráfico

Si el servidor es de ubicación compartida (Dispatcher reside en la misma máquina para la cual reparte el tráfico) o si utiliza los métodos de reenvío nat o cbr, *no* utilice los procedimientos indicados a continuación.

Si utiliza el método de reenvío mac, Dispatcher sólo es efectivo con los servidores de fondo que permiten configurar el adaptador de bucle de retorno con una dirección IP adicional, para la cual el servidor de fondo no responderá nunca a las peticiones ARP (protocolo de resolución de direcciones). Siga los pasos de esta sección para configurar las máquinas servidor con reparto del tráfico.

Paso 1. Crear un alias para el dispositivo de bucle de retorno

Para que las máquinas servidor con reparto del tráfico funcionen, debe asignar el dispositivo de bucle de retorno (normalmente denominado lo0) a la dirección de cluster (o preferiblemente crear un alias para el dispositivo). Si utiliza el método de reenvío mac, el componente Dispatcher no cambia la dirección IP de destino del paquete TCP/IP antes de reenviar el paquete a una máquina servidor TCP. Si asigna el dispositivo de bucle de retorno a la dirección de cluster o crea un alias para el dispositivo, las máquinas servidor de reparto del tráfico aceptarán los paquetes dirigidos a la dirección de cluster.

Si su sistema operativo permite la creación de un alias para interfaces de red (tal como AIX, Linux, Solaris o Windows 2000), es conveniente que cree un alias del dispositivo de bucle de retorno para la dirección de cluster. La ventaja de utilizar un sistema operativo que dé soporte a los alias es que puede configurar máquinas servidor con reparto del tráfico para atender a varias direcciones de cluster.

Nota: Hay algunas versiones del kernel de **Linux** que requieren un parche a fin de crear un alias para el dispositivo de bucle de retorno. Consulte la

sección “Instalación del parche del kernel de Linux (para suprimir las respuestas a arp en la interfaz de bucle de retorno)” en la página 70 con el fin de determinar si es necesario un parche de kernel de Linux.

Para las versiones 2.2.14 o superiores del kernel de **Linux**, emita los mandatos siguientes antes de ejecutar el mandato **ifconfig**:

```
echo 1 > /proc/sys/net/ipv4/conf/lo/hidden
echo 1 > /proc/sys/net/ipv4/conf/all/hidden
```

Si su servidor tiene un sistema operativo que no admite el uso de alias, como HP-UX y OS/2, debe establecer el dispositivo de bucle de retorno en la dirección de cluster.

Utilice el mandato para su sistema operativo como se muestra en la Tabla 4 para establecer o unir mediante un alias el dispositivo de bucle de retorno.

Tabla 4. Mandatos para unir el dispositivo de bucle de retorno (lo0) por medio de un alias para Dispatcher

AIX	ifconfig lo0 alias dirección_cluster netmask máscara_red
HP-UX	ifconfig lo0 dirección_cluster
Linux	ifconfig lo:1 dirección_cluster netmask 255.255.255.255 up
OS/2	ifconfig lo dirección_cluster
Solaris 7	ifconfig lo0:1 dirección_cluster 127.0.0.1 up
Solaris 8	ifconfig lo0:1 plumb dirección_cluster netmask máscara_red up

Tabla 4. Mandatos para unir el dispositivo de bucle de retorno (lo0) por medio de un alias para Dispatcher (continuación)

Windows 2000	<ol style="list-style-type: none"> 1. Pulse en Inicio, Configuración y Panel de control. 2. Si no lo ha hecho con anterioridad, añada el controlador del adaptador MS Loopback. <ol style="list-style-type: none"> a. Pulse dos veces en Agregar o quitar hardware. Se iniciará el Asistente para agregar o quitar hardware. b. Pulse en Siguiente, seleccione Agregar o resolver problemas de un dispositivo y pulse en Siguiente. c. La pantalla parpadeará y mostrará el panel Seleccionar un dispositivo de hardware. d. Si el adaptador MS Loopback figura en la lista, significa que ya está instalado; pulse en Cancelar para salir. e. Si el adaptador MS Loopback <i>no</i> figura en la lista, seleccione Agregar un nuevo dispositivo y pulse en Siguiente. f. Para seleccionar el hardware en una lista, en el panel Buscar nuevo hardware pulse en No y después en Siguiente. g. Seleccione Adaptadores de red y pulse en Siguiente. h. En el panel Seleccionar adaptador de red, seleccione Microsoft en la lista de fabricantes y después seleccione Adaptador Microsoft Loopback. i. Pulse en Siguiente y, a continuación, pulse en Siguiente de nuevo para instalar la configuración por omisión (o seleccione Utilizar disco, inserte el CD y realice la instalación desde el CD). j. Pulse en Finalizar para completar la instalación. 3. Pulse el botón del ratón en Panel de control y pulse dos veces en Red y conexiones telefónicas. 4. Seleccione la conexión cuyo nombre de dispositivo es "Adaptador Microsoft Loopback" y pulse el botón derecho del ratón en ella. 5. Seleccione Propiedades en el menú. 6. Seleccione Protocolo Internet (TCP/IP) y pulse en Propiedades. 7. Pulse en Utilizar la siguiente dirección IP. Rellene <i>Dirección IP</i> con la dirección de cluster y <i>Máscara de subred</i> con la máscara de subred por omisión (255.0.0.0). Nota: No especifique una dirección de enrutador. Utilice el sistema principal local como servidor DNS por omisión.
--------------	--

Tabla 4. Mandatos para unir el dispositivo de bucle de retorno (lo0) por medio de un alias para Dispatcher (continuación)

OS/390	<p>Configuración de un alias de bucle de retorno en el sistema OS/390</p> <ul style="list-style-type: none"> En el miembro de parámetro de IP (archivo), un administrador deberá crear una entrada en la lista de direcciones Home. Por ejemplo: <pre>HOME ;Address Link 192.168.252.11 tr0 192.168.100.100 1tr1 192.168.252.12 loopback</pre> Se pueden definir varias direcciones para el bucle de retorno. Por omisión se configura la dirección 127.0.0.1.
--------	---

Paso 2. Comprobar si existe una ruta sobrante

En algunos sistemas operativos puede que se cree una ruta por omisión, la cual debe eliminarse.

- En Windows 2000, utilice el mandato siguiente para comprobar si existe una ruta sobrante:

```
route print
```
- En los sistemas UNIX, utilice el mandato siguiente para comprobar si existe una ruta sobrante:

```
netstat -nr
```

Ejemplo para Windows 2000:

- Después de especificar **route print**, se mostrará una tabla parecida a la siguiente. (Este ejemplo ilustra la localización y eliminación de una ruta sobrante al cluster 9.67.133.158 con un máscara de subred por omisión de 255.0.0.0.)

Rutas activas:

Direc. red	Máscara subred	Direc. pasarela	Interfaz	Métrica
0.0.0.0	0.0.0.0	9.67.128.1	9.67.133.67	1
9.0.0.0	255.0.0.0	9.67.133.158	9.67.133.158	1
9.67.128.0	255.255.248.0	9.67.133.67	9.67.133.67	1
9.67.133.67	255.255.255.255	127.0.0.1	127.0.0.1	1
9.67.133.158	255.255.255.255	127.0.0.1	127.0.0.1	1
9.255.255.255	255.255.255.255	9.67.133.67	9.67.133.67	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	224.0.0.0	9.67.133.158	9.67.133.158	1
224.0.0.0	224.0.0.0	9.67.133.67	9.67.133.67	1
255.255.255.255	255.255.255.255	9.67.133.67	9.67.133.67	1

- Localice su dirección de cluster en la columna “Dirección de pasarela”. Si hay una ruta sobrante, la dirección del cluster aparecerá dos veces. En el ejemplo, la dirección del cluster (9.67.133.158) aparece en las filas 2 y 8.

3. Localice la dirección de red de cada fila en la que aparece la dirección del cluster. Necesita una de estas rutas y deberá eliminar la sobrante. La ruta sobrante que se debe eliminar debe ser aquélla cuya dirección de red comienza por el primer dígito de la dirección del cluster, seguido de tres ceros. En el ejemplo, la dirección adicional es la que aparece en la fila 2, cuya dirección de red es **9.0.0.0**:

9.0.0.0 255.0.0.0 9.67.133.158 9.67.133.158 1

Paso 3. Eliminar las rutas sobrantes

Debe eliminar la ruta sobrante. Para eliminarla, utilice el mandato correspondiente a su sistema operativo, que aparece en la Tabla 5.

Ejemplo: para eliminar la ruta sobrante mostrada en la tabla de ejemplo "Rutas activas" para el Paso 2, especifique lo siguiente:

route delete 9.0.0.0 9.67.133.158

Tabla 5. Mandatos para eliminar rutas sobrantes para Dispatcher

HP-UX	route delete <i>dirección_cluster dirección_cluster</i>
Windows 2000	route delete <i>dirección_red dirección_cluster</i> (en un indicador de mandatos de MS-DOS) Nota: Debe eliminar la ruta sobrante cada vez que arranque el servidor.

Si utilizamos el ejemplo de la Figura 15 en la página 60 y se configura una máquina servidor en la que se ejecuta AIX, el mandato sería:

route delete -net 204.0.0.0 204.67.172.72

Paso 4. Comprobar que el servidor está configurado debidamente

Para comprobar si un servidor de fondo está configurado debidamente, realice los pasos siguientes desde una máquina diferente de la misma subred cuando Dispatcher no esté en ejecución y *cluster* no esté configurado:

- 1. Emita el mandato:
arp -d *cluster*
- 2. Emita el mandato:
ping *cluster*

No debería producirse ninguna respuesta. Si existe una respuesta al mandato ping, compruebe que no ejecutó ifconfig para asignar la dirección de cluster a la interfaz. Compruebe que no haya ninguna máquina que tenga una entrada "published arp" para la dirección de cluster.

Nota: Para las versiones 2.2.12 y 2.2.13 del kernel de **Linux**, compruebe que existe un "1" en /proc/sys/net/ipv4/conf/lo/**arp_invisible**.

Para las versiones 2.2.14 o superiores del kernel de **Linux**, compruebe que existe un "1" en
/proc/sys/net/ipv4/conf/lo/**hidden** y
/proc/sys/net/ipv4/conf/all/**hidden**.

3. Ejecute Ping para el servidor de fondo y seguidamente emita este mandato:

```
arp -a
```

La salida del mandato debe mostrar la dirección MAC del servidor. Emita el mandato:

```
arp -s cluster dirección_mac_servidor
```

4. Ejecute Ping para el cluster. Debería obtener una respuesta. Emita una petición http, telnet o de otro tipo dirigida al cluster correspondiente al servidor de fondo. Compruebe que la petición es efectiva.
5. Emita el mandato:

```
arp -d cluster
```
6. Ejecute Ping para el cluster. No debería producirse ninguna respuesta.

Nota: Si obtiene una respuesta, emita una instrucción **arp cluster** para obtener la dirección MAC de la máquina mal configurada. Luego, repita los pasos 1 al 6.

Instalación del parche del kernel de Linux (para suprimir las respuestas a arp en la interfaz de bucle de retorno)

En el caso de los servidores Linux únicamente, para crear un alias para el dispositivo de bucle de retorno es necesario un parche determinado (que depende de la versión del kernel de Linux).

El parche asegura que la respuesta a ARP sólo se enviará desde un puerto de adaptador de red que tenga la dirección IP solicitada en la petición ARP. Sin este parche, Linux emitirá respuestas a ARP en la red para los alias de bucle de retorno. El parche también corrige una condición de actualización de ARP cuando varios puertos de adaptador de red con direcciones IP diferentes se encuentran en la misma red física.

Debe instalar el parche si se dan las condiciones siguientes:

- **Versiones 2.4.x del kernel de Linux**
 - Si desea utilizar el método de reenvío MAC de Dispatcher junto con la modalidad de alta disponibilidad y la ubicación compartida, debe instalar el parche para el sistema de Dispatcher.

Nota: Dispatcher puede considerarse de ubicación compartida aunque tan sólo reparta el tráfico de otro componente de Edge Server (como Caching Proxy, Mailbox Locator, CBR, etc.) de la misma máquina en que reside.

- Si utiliza el kernel 2.4 en un servidor de fondo para el que se reparte el tráfico mediante Dispatcher configurado con el método de reenvío MAC, debe instalar el parche en la máquina servidor de fondo.
 - Si la máquina tiene varios puertos de adaptador de red en la misma red física, hay que instalar el parche en la máquina.
- **Versiones 2.2.12 y 2.2.13 del kernel de Linux**
Si utiliza el kernel 2.2.12 ó 2.2.13 en un servidor de fondo.

Notas:

1. Network Dispatcher no se ejecuta en un kernel 2.2.
2. El parche viene incorporado en el kernel 2.2.14.
3. Este parche del kernel de Linux se ha utilizado para probar el producto de IBM y se ha determinado que era satisfactorio en el entorno de pruebas de IBM. El usuario debe evaluar la eficacia de este código en su propio entorno y decidir si satisface sus necesidades. Este código puede estar o no incluido en futuras versiones del código fuente base de Linux.

Versiones 2.4.x del kernel de Linux

El parche del kernel no es necesario para todas las configuraciones. Debe instalar un parche para las versiones 2.4.x del kernel de Linux en las condiciones siguientes:

- Si desea utilizar el método de reenvío MAC de Dispatcher junto con la modalidad de alta disponibilidad y la ubicación compartida, debe instalar el parche en el sistema de Dispatcher.

Nota: Dispatcher puede considerarse de ubicación compartida aunque tan sólo reparta el tráfico de otro componente de Edge Server (como Caching Proxy, Mailbox Locator, CBR, etc.) de la misma máquina en que reside.

- Si utiliza el kernel 2.4 en un servidor de fondo para el que se reparte el tráfico mediante Dispatcher configurado con el método de reenvío MAC, debe instalar el parche en el servidor de fondo.
- Si la máquina tiene varios puertos de adaptador de red en la misma red física, hay que instalar el parche en la máquina.

Es posible descargar este parche desde el sitio Web siguiente:

<http://oss.software.ibm.com/developerworks/opensource/cvs/naslib>.

Seleccione "CVS Tree" en la lista de descarga.

Para aplicar el parche:

1. Obtenga el parche de bucle de retorno en
<http://oss.software.ibm.com/developerworks/opensource/cvs/naslib>.
 2. Instale los RPM del kernel:
 - a. Copie el archivo de parche **arp.c.2.4.0.patch** en `/usr/src/linux-2.4/net/ipv4/`
 - b. Emita los mandatos siguientes:

```
cd /usr/src/linux-2.4/net/ipv4
patch -p0 -l < arp.c.2.4.0.patch
```
- Nota:** Esto se ha probado para las versiones 2.4.0 y 2.4.2 del kernel de Linux.
3. Cambie al directorio `/usr/src/linux-2.4`.
 4. Edite Makefile y añada **-arppatch** al valor EXTRAVERSION.
 5. Emita el mandato: `make mrproper`
 6. Emita el mandato `make config` y seleccione los valores apropiados para el sistema. Compruebe que configura el soporte para módulos.
 7. Emita los mandatos siguientes:

```
make dep;make clean;make bzImage;make modules;make modules_install
cd arch/i386/boot
cat bzImage > /boot/vmlinuz-2.4.2-2-arppatch
cd /usr/src/linux-2.4
cp System.map /boot/System.map-2.4.2-2-arppatch
cd /etc
```
 8. Edite `lilo.conf` y copie el párrafo **image=**. En la nueva copia, haga estos cambios:
 - sustituya `/boot/vmlinuz-2.4.2-2` por `/boot/vmlinuz-2.4.2-2-arppatch`
 - sustituya `label=linux` por `label=linux-arppatch`
 - sustituya `default=linux` por `default=linux-arppatch`
 9. Ejecute el mandato `/sbin/lilo`.
 10. Arranque la máquina con el nuevo kernel.

Versiones 2.2.12. y 2.2.13 del kernel de Linux

Es necesario instalar un parche para las versiones 2.2.12 y 2.2.13 del kernel de Linux en los servidores donde se utilice el método de reenvío MAC. Puede obtener este parche en este sitio Web: <http://www.ibm.com/developer/linux>.

Para aplicar el parche:

1. Obtenga el parche de bucle de retorno en
<http://www.ibm.com/developer/linux>.
2. Instale el fuente del kernel. Para ver las instrucciones de instalación, consulte el archivo **README.kernel-sources** del directorio `/usr/src/linux`.

3. Aplique el parche utilizando el mandato patch desde el directorio /usr/src. Por ejemplo:

```
patch -p0< archivo_parche
```
4. Compile el kernel. Para obtener instrucciones sobre la compilación, consulte el archivo **README** del directorio /usr/src/linux-2.4.
5. Instale el nuevo kernel y ejecute el mandato **lilo**. Para ver las instrucciones, consulte el archivo **README** del directorio /usr/src/linux.
6. Arranque la máquina con el nuevo kernel.
7. Compruebe si existe el archivo siguiente:
/proc/sys/net/ipv4/conf/lo/**arp_invisible**. Si existe, el parche del kernel se ha instalado correctamente. Si el archivo *no* existe, el parche se ha aplicado de forma incorrecta o se ha arrancado con un kernel sin parche. Consulte el archivo /usr/src/linux/README para asegurarse de que ha seguido correctamente los pasos necesarios para la instalación.
8. Emita el mandato:

```
echo 1 > /proc/sys/net/ipv4/conf/lo/arp_invisible
```

El efecto de este mandato sólo durará hasta que la máquina se apague. Cuando se vuelva a arrancar será necesario seguir de nuevo este paso y los pasos siguientes.

9. Cree un alias para el bucle de retorno con la máscara de red 255.255.255.255; por ejemplo:

```
ifconfig lo:1 cluster netmask 255.255.255.255 up
```
10. Añada el servidor al cluster.

Capítulo 6. Planificación del componente Content Based Routing

Este capítulo describe lo que debe tener en cuenta el planificador de la red antes de instalar y configurar el componente CBR con Caching Proxy.

- Consulte el “Capítulo 7. Configuración del componente Content Based Routing” en la página 81 para obtener información sobre cómo configurar el parámetro load-balancing de CBR.
- Consulte el “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131 para obtener información sobre cómo configurar Network Dispatcher para funciones más avanzadas.
- Consulte el “Capítulo 15. Utilización y gestión de Network Dispatcher” en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Este capítulo incluye las secciones siguientes:

- “Requisitos de hardware y de software”
- “Consideraciones referentes a la planificación”

Requisitos de hardware y de software

Requisitos de plataforma:

- Para AIX, vea “Requisitos para AIX” en la página 12
- Para Linux, vea “Requisitos para Red Hat Linux o SuSe Linux” en la página 16
- Para Solaris, vea “Requisitos para Solaris” en la página 19
- Para Windows 2000, vea “Requisitos para Windows 2000” en la página 22

Consideraciones referentes a la planificación

El componente CBR le permite repartir el tráfico HTTP y SSL utilizando Caching Proxy para encaminar la petición

Nota: Debe instalar la modalidad de proxy invertido de Caching Proxy para poder ejecutar CBR como conector.

CBR es muy similar a Dispatcher en la estructura de sus componentes. CBR consta de las funciones siguientes:

- **cbrserver** gestiona las peticiones procedentes de la línea de mandatos destinadas al ejecutor, el gestor y los asesores.
- El **ejecutor** da soporte al reparto del tráfico de las peticiones del cliente. El ejecutor debe estar iniciado para poder utilizar el componente CBR.
- El **gestor** establece los pesos que utiliza el ejecutor basándose en:
 - Contadores internos del ejecutor
 - Información procedente de los servidores proporcionada por los asesores
 - Información proporcionada por un programa de supervisión del sistema, tal como Metric Server.

El uso del gestor es opcional. No obstante, si no se utiliza un gestor, el reparto del tráfico se realiza utilizando una planificación rotatoria ponderada basada en los pesos actuales de los servidores, y no podrán utilizarse asesores.

- Los **asesores**, que consultan los servidores y analizan el resultado por protocolo antes de llamar al gestor para que establezca los pesos según convenga. Es posible que no tenga sentido utilizar algunos de estos asesores en una configuración típica. También tiene la opción de escribir sus propios asesores. El uso de los asesores es opcional aunque se recomienda. Network Dispatcher proporciona un asesor Caching Proxy (ibmproxy). En “Asesores” en la página 139 hallará más información.
- Para configurar y gestionar el ejecutor, los asesores y el gestor, utilice la línea de mandatos (**cbrcontrol**) o la interfaz gráfica de usuario (**ndadmin**).

Las tres funciones clave de CBR (el ejecutor, los asesores y el gestor) interactúan para repartir las peticiones entrantes entre los servidores. Además de repartir el tráfico de peticiones, el ejecutor supervisa el número de conexiones nuevas y activas y proporciona esta información al gestor.

El componente CBR le permite especificar un conjunto de servidores que manejen una petición basándose en la comparación de expresiones regulares del contenido de la petición. CBR permite hacer una partición del sitio para que diferentes servidores de aplicación o de contenido puedan dar servicio a conjuntos de servidores distintos. Esta partición será transparente para los clientes que accedan a su sitio Web. Puesto que CBR le permite especificar varios servidores para cada tipo de petición, se puede repartir el tráfico de las peticiones para optimizar la respuesta al cliente. Al permitir la asignación de varios servidores a cada tipo de contenido, estará protegido cuando falle una estación de trabajo o un servidor. CBR detectará el error y repartirá el tráfico de peticiones de los clientes hacia los demás servidores del grupo.

Una forma de dividir el sitio Web es asignar algunos servidores para que manejen sólo peticiones cgi y otro conjunto de servidores para manejar todas las demás peticiones. De esta forma los scripts cgi que requieren gran potencia de proceso no reducirán la velocidad de los servidores para el tráfico de html

normal, lo que permitirá a los clientes un tiempo de respuesta global mejor. Al utilizar este esquema, podría asignar estaciones de trabajo más potentes a las peticiones normales. Esto daría a los clientes un tiempo de respuesta mejor sin tener que invertir en la actualización de todos los servidores. También podría asignar estaciones de trabajo más potentes a las peticiones cgi.

Otra posibilidad para realizar una partición en el sitio Web sería dirigir hacia un conjunto de servidores a los clientes que accedan a páginas con necesidad de un registro y todas las demás peticiones hacia un segundo conjunto de servidores. De esta forma los navegadores casuales del sitio Web no bloquearán recursos que podrían utilizar los clientes comprometidos con su registro. También le permitirá utilizar estaciones de trabajo más potentes para dar servicio a los clientes que se han registrado.

Por supuesto, también se pueden combinar los métodos anteriores con el fin de obtener mayor flexibilidad y un servicio mejorado.

Caching Proxy se comunica con CBR mediante su interfaz. Caching Proxy debe estar instalado en la misma máquina. Ahora pueden existir varias instancias de Caching Proxy ejecutándose en la misma máquina que se comuniquen simultáneamente con CBR. En versiones anteriores del producto, sólo podía haber una sola instancia de Caching Proxy en comunicación con CBR.

CBR, junto con Caching Proxy, examina las peticiones HTTP utilizando los tipos de normas especificados. Cuando está en ejecución, Caching Proxy acepta peticiones de clientes y consulta al componente CBR para saber cuál es el servidor más apropiado. Después de esta consulta, CBR compara la petición con un grupo de normas clasificadas por prioridades. Cuando una norma coincide, se elige un servidor adecuado de un conjunto de servidores preconfigurados. Finalmente, CBR informa a Caching Proxy sobre qué servidor se ha elegido y la petición se reenvía hacia allí.

Cuando haya definido un cluster para que tenga reparto del tráfico, debe asegurarse de que todas las peticiones hechas a ese cluster tengan una norma para seleccionar un servidor. Si no se encuentra ninguna norma que coincida con una petición concreta, el cliente recibirá una página de error de Caching de Proxy. La forma más fácil de asegurar que todas las peticiones coincidan con alguna norma es crear una norma "siempre cierta" con un valor de prioridad muy alto. Asegúrese de que todos los servidores utilizados por esta norma puedan atender todas las peticiones no gestionadas explícitamente por las normas que tienen valores de prioridad menores. (Nota: las normas con un valor de prioridad menor se evalúan primero.)

Reparto del tráfico a través de conexiones SSL totalmente seguras

CBR, junto con Caching Proxy, puede recibir transmisión SSL desde el cliente y reenviarla al proxy (extremo cliente-proxy) y también encaminar la transmisión desde el proxy al servidor (extremo proxy-servidor). Puede definir un puerto SSL en un servidor de la configuración CBR para recibir la petición procedente del cliente; esto le permite mantener un sitio Web totalmente seguro y utilizar CBR para repartir el tráfico entre servidores SSL seguros.

Se tiene que añadir una sentencia de configuración al archivo `ibmproxy.conf` correspondiente a IBM Caching Proxy para habilitar el cifrado SSL en el extremo proxy-cliente. El formato debe ser:

```
proxy patrón_uri patrón_url dirección
```

donde *patrón_uri* es un patrón con el que hay que coincidir (por ejemplo: `/secure/*`), *patrón_url* es un URL de sustitución (por ejemplo: `https://clusterA/secure/*`) y *dirección* es la dirección del cluster (por ejemplo: `clusterA`).

Reparto del tráfico entre el cliente y el proxy en CBR y entre el proxy y el servidor en HTTP

CBR, junto con Caching Proxy, puede también recibir la transmisión SSL procedente del cliente y descifrar la petición SSL antes de reenviarla a un servidor HTTP. Para poder utilizar las comunicaciones de cliente a proxy bajo SSL y las comunicaciones de proxy a servidor bajo HTTP, existe la palabra clave opcional **mapport** del mandato `cbrcontrol`. Utilice esta palabra clave cuando necesite indicar que el puerto del servidor es diferente que el puerto de entrada del cliente. El ejemplo siguiente añade un puerto utilizando la palabra clave `mapport`; el puerto del cliente es 443 (SSL) y el puerto del servidor es 80 (HTTP):

```
cbrcontrol server add cluster:443 mapport 80
```

El número de puerto utilizado para `mapport` puede ser un valor entero positivo. El número de puerto por omisión es el puerto de entrada del cliente.

Debido a que CBR debe poder asesorar sobre las peticiones HTTP destinadas a un servidor configurado en el puerto 443 (SSL), se proporciona un asesor especial: `ssl2http`. Este asesor se inicia su ejecución en el puerto 443 (puerto de entrada del cliente) e informa sobre los servidores configurados para ese puerto. Si hay dos clusters configurados y cada cluster tiene configurado el puerto 443 y servidores con un valor diferente de `mapport`, entonces una instancia individual del asesor puede abrir el puerto apropiado según convenga. El ejemplo siguiente muestra dicha clase de configuración:


```
Ejecutor
  Cluster1
    Puerto:443
    Servidor1 mapport 80
    Servidor2 mapport 8080
  Cluster2
    Puerto:443
    Servidor3 mapport 80
    Servidor4 mapport 8080
  Gestor
    Asesor ssl2http 443
```

Capítulo 7. Configuración del componente Content Based Routing

Antes de seguir los pasos indicados en este capítulo, consulte el “Capítulo 6. Planificación del componente Content Based Routing” en la página 75. Este capítulo explica cómo crear una configuración básica para el componente CBR de Network Dispatcher.

- Consulte el “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131 para ver configuraciones más complejas de Network Dispatcher.
- Consulte el “Capítulo 15. Utilización y gestión de Network Dispatcher” en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Visión general de las tareas de configuración

Nota: Antes de empezar a realizar los pasos de configuración indicados en esta tabla, asegúrese de que la máquina CBR y todas las máquinas servidor están conectadas a la red, tienen una dirección IP válida y pueden emitir el mandato ping entre sí.

Tabla 6. Tareas de configuración para el componente CBR

Tarea	Descripción	Información relacionada
Configurar la máquina CBR.	Determinar los requisitos.	“Configuración de la máquina CBR” en la página 86
Configurar máquinas para el reparto del tráfico.	Preparar la configuración del reparto del tráfico.	“Paso 7. Definir las máquinas servidor sujetas a reparto del tráfico” en la página 90

Métodos de configuración

Para crear una configuración básica para el componente CBR de Network Dispatcher, existen cuatro métodos básicos:

- Línea de mandatos
- Scripts
- Interfaz gráfica de usuario (GUI)

- Asistente de configuración

Para poder utilizar CBR, debe estar instalado Caching Proxy.

Nota: Caching Proxy es un servicio que se inicia automáticamente por omisión después de la instalación. Debe detener Caching Proxy antes de iniciar la función del servidor CBR (`cbrserver`). Es recomendable modificar el servicio Caching Proxy de forma que se inicie manualmente y no automáticamente.

- Para AIX, Linux y Solaris: Detenga Caching Proxy buscando su identificador de proceso mediante el mandato `ps -ef|grep ibmproxy` y finalizando el proceso con el mandato `kill id_proceso`.
- Para Windows: Detenga Caching Proxy desde el panel Servicios.

Línea de mandatos

Este es el medio más directo para configurar CBR. Los valores de los parámetros de mandatos se deben escribir en caracteres ingleses. Las únicas excepciones son los nombres de sistema principal (utilizados, por ejemplo, en los mandatos para clusters y servidores) y los nombres de archivos.

Para iniciar CBR desde la línea de mandatos:

- Como usuario root, emita el mandato **cbrserver** desde el indicador de mandatos.

Nota: Para detener el servicio, emita lo siguiente: **cbrserver stop**.

- A continuación, emita los mandatos de control de CBR que desee para establecer la configuración. Los procedimientos de este manual presuponen que se utiliza la línea de mandatos. El mandato es **cbrcontrol**. Para obtener más información acerca de los mandatos, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.
- Inicie Caching Proxy. Emita el mandato **ibmproxy** desde el indicador de mandatos. (Debe iniciar el ejecutor antes de iniciar Caching Proxy.)

Nota: Para Windows 2000: Inicie Caching Proxy desde el panel Servicios:
Inicio-> Configuración-> Panel de control -> Herramientas administrativas -> Servicios.

Puede entrar los parámetros del mandato `cbrcontrol` en su forma abreviada. Sólo necesita especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato “file save”, puede entrar **cbrcontrol he f** en lugar de **cbrcontrol help file**.

Para iniciar la interfaz de línea de mandatos, emita el mandato **cbrcontrol** para visualizar un indicador de mandatos de `cbrcontrol`.

Para cerrar la interfaz de línea de mandatos, emita **exit** o **quit**.

Notas:

1. En Windows 2000, el ndserver del componente Dispatcher se inicia automáticamente. Si sólo desea utilizar CBR y no el componente Dispatcher, puede evitar que ndserver se inicie automáticamente realizando estos pasos:
 - a. En la ventana Servicios de Windows 2000, pulse con el botón derecho del ratón sobre IBM Dispatcher.
 - b. Seleccione Propiedades.
 - c. En el campo **Tipo de arranque**, seleccione Manual.
 - d. Pulse Aceptar y cierre la ventana Servicios.
2. Cuando configure Content Based Routing (CBR) desde el indicador de mandatos del sistema operativo, no desde el indicador cbrcontrol>>, tenga cuidado con el uso de estos caracteres:
 - (), paréntesis derecho e izquierdo
 - &, ampersand
 - |, barra vertical
 - ! signo de exclamación
 - *, asterisco

El shell del sistema operativo puede interpretar estos signos como caracteres especiales y convertirlos en texto alternativo antes de que cbrcontrol los evalúe.

Los caracteres especiales de la lista anterior son caracteres opcionales en el mandato **cbrcontrol rule add** y se utilizan cuando se especifica un patrón para una norma de contenido. Por ejemplo, el mandato siguiente puede ser válido solamente cuando se utiliza el indicador cbrcontrol>>.

```
rule add 10.1.203.4:80:cbr_prod_rule_ek type content
pattern client=181.0.153.222&uri=http://10.1.203.4/nipoek/*
```

Para que este mismo mandato funcione en el indicador del sistema operativo, el patrón debe encerrarse entre comillas dobles (""), de la forma siguiente:

```
cbrcontrol rule add 10.1.203.4:80:cbr_prod_rule_ek type content
pattern "client=181.0.153.222&uri=http://10.1.203.4/nipoek/*"
```

Si no se utilizan las comillas, puede truncarse parte del patrón cuando se guarde la norma en CBR. Tenga en cuenta que las comillas no están soportadas cuando se utiliza el indicador de mandatos cbrcontrol>>.

Scripts

Los mandatos para configurar CBR se pueden entrar en un archivo de script de configuración y ejecutarlos juntos.

Nota: Para ejecutar rápidamente el contenido de un archivo de script (por ejemplo, *miscript*), utilice cualquiera de estos dos mandatos:

- Para actualizar la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:

cbrcontrol file appendload *miscript*

- Para sustituir totalmente la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:

cbrcontrol file newload *miscript*

GUI

Para ver un ejemplo de la interfaz gráfica de usuario (GUI), consulte la Figura 2 en la página 5.

Para iniciar la GUI, siga estos pasos

1. Asegúrese de que *cbrserver* está en ejecución. Como usuario root o administrador, emita lo siguiente desde un indicador de mandatos:
cbrserver
2. A continuación, lleve a cabo una de las acciones siguientes:
 - Para AIX, Linux o Solaris, especifique **ndadmin**
 - Para Windows 2000, pulse **Inicio, Programas, IBM WebSphere, Edge Server, IBM Network Dispatcher** y finalmente **Network Dispatcher**
3. Inicie Caching Proxy. (Desde la GUI, debe conectarse primero al sistema principal e iniciar el ejecutor del componente CBR antes de iniciar Caching Proxy.) Lleve a cabo una de las siguientes acciones:
 - Para AIX, Linux o Solaris: Para iniciar Caching Proxy, especifique **ibmproxy**
 - Para Windows 2000: Para iniciar Caching Proxy, vaya al panel Servicios: **Inicio-> Configuración-> Panel de control -> Herramientas administrativas -> Servicios**

Para configurar el componente CBR desde la GUI, debe seleccionar primero **Content Based Routing** en la estructura en árbol. Puede arrancar el gestor una vez que esté conectado a un sistema principal. También puede crear clusters que contengan puertos y servidores e iniciar asesores para el gestor.

La GUI se puede utilizar para realizar cualquier acción que se desee llevar a cabo con el mandato **cbrcontrol**. Por ejemplo, para definir un cluster desde la línea de mandatos, escriba el mandato **cbrcontrol cluster add cluster**. Para definir un cluster desde la GUI, pulse el botón derecho del ratón sobre

Ejecutor, y en el menú emergente pulse el botón izquierdo sobre **Añadir cluster**. Escriba la dirección del cluster en la ventana emergente, a continuación pulse en **Aceptar**.

Los archivos de configuración CBR preexistentes se pueden cargar utilizando las opciones **Cargar nueva configuración** (para sustituir totalmente la configuración actual) y **Añadir a configuración actual** (para actualizar la configuración actual); estas opciones aparecen en el menú emergente **Sistema principal**. Debe guardar periódicamente la configuración CBR en un archivo, mediante la utilización de la opción **Guardar archivo de configuración como** mostrada también en el menú emergente **Sistema principal**. El menú **Archivo**, situado en la parte superior de la GUI, le permitirá guardar las conexiones actuales del sistema principal en un archivo, o restaurar las conexiones de archivos existentes a través de los componentes de Network Dispatcher.

Puede acceder a la **Ayuda** pulsando el icono de signo de interrogación, situado en la esquina superior derecha de la ventana de Network Dispatcher.

- **Ayuda para los campos** — describe cada campo y sus valores por omisión
- **Cómo puedo** — lista tareas que pueden efectuarse desde esa pantalla
- **Contenido** — es una tabla de contenido de toda la información de la Ayuda
- **Índice** — es un índice alfabético de temas de ayuda

Para obtener más información acerca de la utilización de la GUI, consulte “Instrucciones generales para la utilización de la GUI” en la página 6.

Asistente de configuración

Si está utilizando el asistente para configuración, siga estos pasos:

1. Inicie cbrserver: emita **cbrserver** en el indicador de mandatos como usuario root o como administrador.
2. Inicie la función del asistente de CBR:
Puede iniciar el asistente desde el indicador de mandatos emitiendo **cbrwizard**. O, si lo prefiere, seleccione Asistente de configuración desde el menú del componente CBR que aparece en la GUI.
3. Inicie Caching Proxy para repartir el tráfico de HTTP o HTTPS (SSL).
Para AIX, Linux o Solaris: Para iniciar Caching Proxy, especifique **ibmproxy**
Para Windows 2000: Para iniciar Caching Proxy, vaya al panel Servicios: **Inicio-> Configuración-> Panel de control -> Herramientas administrativas -> Servicios**

El asistente CBR le guía paso a paso a través del proceso de creación de una configuración básica para el componente CBR. Le mostrará preguntas acerca

de la red y le guiará durante la configuración de un cluster que permite que CBR lleve a cabo el reparto del tráfico del tráfico entre un grupo de servidores.

Con el asistente para la configuración de CBR, verá los siguientes paneles:

- Introducción al asistente
- Expectativas
- Antes de empezar
- Selección de un sistema principal para configurar (si es necesario)
- Definición de un cluster
- Adición de un puerto
- Adición de un servidor
- Adición de una norma
- Inicio de un asesor

Configuración de la máquina CBR

Antes de configurar la máquina CBR, debe ser el usuario root (para AIX, Linux o Solaris) o el administrador en Windows 2000.

Necesitará una dirección IP para cada cluster de servidores que se van a configurar. Una dirección de cluster es una dirección que está asociada con un nombre de sistema principal (como www.company.com). Esta dirección IP la utilizan los clientes para conectarse a los servidores de un cluster. De forma específica, esta dirección se encuentra en la petición URL del cliente. CBR reparte el tráfico de todas las peticiones realizadas a la misma dirección de cluster.

Sólo para Solaris: Antes de utilizar el componente CBR, deben modificarse los valores por omisión del sistema de IPC (Inter-process Communication). Es necesario aumentar el tamaño máximo de un segmento de memoria compartida y el número de identificadores de semáforo. A fin de ajustar el sistema de forma que dé soporte a CBR, edite el archivo `/etc/system` del sistema para añadir las sentencias siguientes y luego rearranque:

```
set shmsys:shminfo_shmmax=0x02000000
set semsys:seminfo_semmap=750
set semsys:seminfo_semmni=30
set semsys:seminfo_semmns=750
set semsys:seminfo_semmnu=30
set semsys:seminfo_semume=30
```

Si no aumenta el segmento de memoria compartida a los valores mostrados anteriormente, el mandato **cbrcontrol executor start** no será efectivo.

Paso 1. Configurar Caching Proxy para utilizar CBR

Para poder utilizar CBR, debe estar instalado Caching Proxy.

Nota: Caching Proxy es un servicio que se inicia automáticamente por omisión después de la instalación. Debe detener Caching Proxy antes de iniciar la función del servidor CBR. Es recomendable modificar el servicio Caching Proxy de forma que se inicie manualmente y no automáticamente.

- Para AIX, Linux y Solaris: Detenga Caching Proxy buscando su identificador de proceso mediante el mandato `ps -ef|grep ibmproxy` y finalizando el proceso con el mandato `kill id_proceso`.
- Para Windows: Detenga Caching Proxy desde el panel Servicios.

Debe realizar las siguiente modificaciones en el archivo de configuración de Caching Proxy (`ibmproxy.conf`):

Cambie la directiva de URL entrante **CacheByIncomingUrl** para especificar "on".

Hay cuatro entradas que deben editarse para el Plug-in de CBR:

- ServerInit
- PreExit
- PostExit
- ServerTerm

Cada entrada debe estar en una sola línea. Existen varias instancias de "ServerInit" en el archivo `ibmproxy.conf`, una por cada plug-in. Deben editarse las entradas correspondientes al "Plug-in de CBR" y deben eliminarse los comentarios en las mismas.

A continuación se muestran las adiciones específicas que deben hacerse al archivo de configuración para AIX, Linux, Solaris y Windows 2000.

Figura 16. Archivo de configuración CBR para AIX

```
ServerInit  /usr/lpp/nd/servers/lib/libndcbr.so:ndServerInit
PreExit    /usr/lpp/nd/servers/lib/libndcbr.so:ndPreExit
PostExit   /usr/lpp/nd/servers/lib/libndcbr.so:ndPostExit
ServerTerm /usr/lpp/nd/servers/lib/libndcbr.so:ndServerTerm
```

Figura 17. Archivo de configuración de CBR para Linux

```
ServerInit /opt/nd/servers/lib/libndcbr.so:ndServerInit
PreExit /opt/nd/servers/lib/libndcbr.so:ndPreExit
PostExit /opt/nd/servers/lib/libndcbr.so:ndPostExit
ServerTerm /opt/nd/servers/lib/libndcbr.so:ndServerTerm
```

Figura 18. Archivo de configuración de CBR para Solaris

```
ServerInit /opt/nd/servers/lib/libndcbr.so:ndServerInit
PreExit /opt/nd/servers/lib/libndcbr.so:ndPreExit
PostExit /opt/nd/servers/lib/libndcbr.so:ndPostExit
ServerTerm /opt/nd/servers/lib/libndcbr.so:ndServerTerm
```

Figura 19. Archivo de configuración de CBR para Windows 2000

Vía de acceso común de directorio de instalación:

```
ServerInit c:\Progra~1\IBM\edge\nd\servers\lib\libndcbr.dll:ndServerInit
PreExit c:\Progra~1\IBM\edge\nd\servers\lib\libndcbr.dll:ndPreExit
PostExit c:\Progra~1\IBM\edge\nd\servers\lib\libndcbr.dll:ndPostExit
ServerTerm c:\Progra~1\IBM\edge\nd\servers\lib\libndcbr.dll:ndServerTerm
```

Vía de acceso nativa de directorio de instalación:

```
ServerInit c:\Progra~1\IBM\nd\servers\lib\libndcbr.dll:ndServerInit
PreExit c:\Progra~1\IBM\nd\servers\lib\libndcbr.dll:ndPreExit
PostExit c:\Progra~1\IBM\nd\servers\lib\libndcbr.dll:ndPostExit
ServerTerm c:\Progra~1\IBM\nd\servers\lib\libndcbr.dll:ndServerTerm
```

Paso 2. Iniciar la función del servidor

Nota: Caching Proxy es un servicio que se inicia automáticamente por omisión después de la instalación. Debe detener Caching Proxy antes de iniciar la función del servidor CBR. Es recomendable modificar el servicio Caching Proxy de forma que se inicie manualmente y no automáticamente.

- Para AIX, Linux y Solaris: Detenga Caching Proxy buscando su identificador de proceso mediante el mandato `ps -ef|grep ibmproxy` y finalizando el proceso con el mandato `kill id_proceso`.
- Para Windows: Detenga Caching Proxy desde el panel Servicios.

Para iniciar la función del servidor CBR, escriba **cbrserver** en la línea de mandatos.

Automáticamente se cargará un archivo de configuración por omisión (default.cfg) cuando inicie cbrserver. Si el usuario decide guardar la configuración de CBR en default.cfg, todo lo que esté guardado en este archivo se cargará automáticamente la próxima vez que se inicie cbrserver.

Paso 3. Iniciar la función del ejecutor

Para iniciar la función del ejecutor, escriba el mandato **cbrcontrol executor start**. También puede cambiar diversos valores del ejecutor en este momento. Consulte “ndcontrol executor — controlar el ejecutor” en la página 263.

Paso 4. Definir un cluster y establecer las opciones de cluster

CBR repartirá las peticiones enviadas a la dirección de cluster entre los servidores correspondientes configurados en los puertos de ese cluster.

La dirección del cluster es un nombre simbólico o una dirección decimal con puntos. Esta dirección se encuentra en la porción del URL correspondiente al sistema principal.

Para definir un cluster, emita el mandato siguiente:

```
cbrcontrol cluster add cluster
```

Para establecer las opciones de cluster, emita el mandato siguiente:

```
cbrcontrol cluster set cluster opción valor
```

Para obtener más información, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.

Paso 5. Crear un alias para la tarjeta de interfaz de red (opcional)

Si desea ejecutar Caching Proxy configurado como proxy inverso, a la hora de repartir el tráfico para varios sitios Web, deberá añadir la dirección de cluster de cada sitio Web a, como mínimo, una de las tarjetas de interfaz de red del sistema de Network Dispatcher. En caso contrario, este paso puede omitirse.

Para AIX, Linux o Solaris: Para añadir la dirección del cluster a la interfaz de red, utilice el mandato `ifconfig`. Utilice el mandato del sistema operativo tal como se muestra en la Tabla 7 en la página 90.

Tabla 7. Mandatos para unir el NIC por medio de un alias

AIX	ifconfig <i>nombre_interfaz</i> alias <i>dirección_cluster</i> netmask <i>máscara_red</i>
Linux	ifconfig <i>nombre_interfaz</i> <i>dirección_cluster</i> netmask <i>máscara_red</i> up
Solaris 7	ifconfig <i>nombre_interfaz</i> <i>dirección_cluster</i> netmask <i>máscara_red</i> up
Solaris 8	ifconfig addif <i>nombre_interfaz</i> <i>dirección_cluster</i> netmask <i>máscara_red</i> up

Nota: En Linux y Solaris, *nombre_interfaz* debe tener un número exclusivo para cada dirección de cluster que se añada; por ejemplo: eth0:1, eth0:2, etc.

Para **Windows**: Para añadir la dirección del cluster a la interfaz de red, haga lo siguiente:

1. Pulse en **Inicio, Configuración y Panel de control**.
2. Pulse dos veces en **Red y conexiones telefónicas**.
3. Pulse con el botón derecho del ratón en **Conexión de área local**.
4. Seleccione **Propiedades**.
5. Seleccione **Protocolo Internet (TCP/IP)** y pulse en **Propiedades**.
6. Seleccione **Utilizar la dirección IP siguiente** y pulse en **Avanzado**.
7. Pulse **Agregar** y escriba la **dirección IP** y la **máscara de subred** correspondientes al cluster.

Paso 6. Definir los puertos y establecer las opciones de puerto

El número de puerto es el puerto donde las aplicaciones de servidor están a la escucha. Para CBR con Caching Proxy y tráfico HTTP, suele ser el puerto 80.

Para definir un puerto para el cluster que definió en el paso anterior, emita lo siguiente:

```
cbrcontrol port add
cluster:puerto
```

Para establecer las opciones de puerto, emita el mandato siguiente:

```
cbrcontrol port set cluster:puerto opción valor
```

Para obtener más información, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.

Paso 7. Definir las máquinas servidor sujetas a reparto del tráfico

Las máquinas servidor son las máquinas donde se ejecutan las aplicaciones cuyo tráfico desea repartir. El *servidor* es el nombre simbólico o dirección decimal con puntos de la máquina servidor. Para definir un servidor en el cluster y puerto, emita el siguiente mandato:

```
cbrcontrol server add cluster:puerto:servidor
```

Para realizar el reparto del tráfico debe definir más de un servidor por puerto en un cluster.

Paso 8. Añadir normas a la configuración

Este es el paso clave al configurar CBR con Caching Proxy. Una norma define cómo se identificará una petición URL y se enviará hacia uno de los conjuntos de servidores adecuados. El tipo de norma especial utilizado por CBR se denomina norma de contenido. Para definir una norma de contenido, emita el mandato siguiente:

```
cbrcontrol rule add cluster:puerto:norma type content pattern=patrón
```

El valor de *patrón* es la expresión regular que se comparará con el URL de cada petición del cliente. Para obtener más información sobre cómo configurar el patrón, consulte “Apéndice C. Sintaxis de la norma de contenido (patrón):” en la página 313.

Algunos de los demás tipos de norma definidos en Dispatcher también se pueden utilizar en CBR. Para obtener más información, consulte “Configurar el reparto del tráfico basado en normas” en la página 173.

Paso 9. Añadir servidores a las normas

Cuando una norma concuerda con la petición de un cliente, se consulta el conjunto de servidores de la norma para averiguar qué servidor es mejor. El conjunto de servidores de la norma es un subconjunto de los servidores definidos en el puerto. Para añadir servidores al conjunto de servidores de una norma, emita el mandato siguiente:

```
cbrcontrol rule useserver cluster:puerto:norma servidor
```

Paso 10. Iniciar la función del gestor (opcional)

La función del gestor mejora el reparto del tráfico. Para iniciar el gestor, emita el mandato siguiente:

```
cbrcontrol manager start
```

Paso 11. Iniciar la función del asesor (opcional)

Los asesores proporcionan al gestor más información acerca de la capacidad de los servidores sujetos a reparto del tráfico para responder a las peticiones. Cada asesor es específico de cada protocolo. Por ejemplo, para iniciar el asesor HTTP, emita el mandato siguiente:

```
cbrcontrol advisor start http  
puerto
```

Paso 12. Establecer las proporciones del gestor según sea necesario

Si inicia asesores, puede modificar la proporción de importancia que se asigna a la información del asesor utilizada para las decisiones sobre reparto del tráfico. Para establecer las proporciones para el cluster, emita el mandato

cbrcontrol cluster set *cluster* proportions. Para obtener más información, consulte “Grado de importancia dado a la información de estado” en la página 135.

Paso 13. Iniciar Caching Proxy

- Plataforma AIX: añada lo siguiente a la variable de entorno LIBPATH:
/usr/lpp/nd/servers/lib
- Plataforma Linux o Solaris: Añada lo siguiente a la variable de entorno LD_LIBRARY_PATH:
/opt/nd/servers/lib

- Plataforma Windows 2000: Añada lo siguiente a la variable de entorno PATH:

Vía de acceso común de directorio de instalación:

c:\Archivos de programa\IBM\edge\nd\servers\lib

Vía de acceso nativa de directorio de instalación:

c:\Archivos de programa\IBM\nd\servers\lib

En el nuevo entorno, inicie Caching Proxy: desde el indicador de mandatos, emita **ibmproxy**

Nota: Para Windows 2000: Inicie Caching Proxy desde el panel Servicios:
Inicio-> Configuración-> Panel de control -> Herramientas administrativas -> Servicios.

Ejemplo de configuración de CBR

Para configurar CBR, siga estos pasos:

1. Inicie CBR: emita el mandato **cbrserver**.
2. Inicie la interfaz de línea de mandatos: emita el mandato **cbrcontrol**.
3. Aparecerá el indicador de solicitud **cbrcontrol**. Emita los siguientes mandatos. (*cluster(c),port(p),rule(r),server(s)*)
 - **executor start**
 - **cluster add c**
 - **port add c:p**
 - **server add c:p:s**
 - **rule add c:p:r type content pattern uri=***
 - **rule use server c:p:r s**
4. Inicie Caching Proxy: Emita el mandato **ibmproxy**. (Para Windows 2000, inicie Caching Proxy desde el panel Servicios.)
5. Elimine todas las configuraciones proxy del navegador.

6. Cargue `http://c/` en el navegador, donde "c" es el cluster que configuró anteriormente.
 - Se invoca el servidor "s"
 - Se visualiza la página Web siguiente: `http://s/`

Capítulo 8. Planificación para el componente Mailbox Locator

En este capítulo se describen los aspectos que debe tener en cuenta la persona encargada de planificar la red antes de proceder a la instalación y configuración del componente Mailbox Locator.

Nota: Antes, el componente Mailbox Locator era una función dentro del componente CBR que repartía el tráfico entre servidores de correo IMAP y POP3 basándose en el ID de usuario y la contraseña. El separar CBR en dos componentes *elimina* la limitación de que "CBR para IMAP/POP3" (Mailbox Locator) y "CBR para HTTP/HTTPS" (CBR con Caching Proxy) no se pueden ejecutar en la misma máquina.

- Consulte el "Capítulo 9. Configuración del componente Mailbox Locator" en la página 99 para obtener información sobre cómo configurar los parámetros de distribución de tráfico de Mailbox Locator.
- Consulte el "Capítulo 14. Funciones avanzadas de Network Dispatcher" en la página 131 para obtener información sobre cómo configurar Network Dispatcher para funciones más avanzadas.
- Consulte el "Capítulo 15. Utilización y gestión de Network Dispatcher" en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Este capítulo incluye las siguientes secciones:

- "Requisitos de hardware y de software"
- "Consideraciones referentes a la planificación"

Requisitos de hardware y de software

- Para AIX, vea "Requisitos para AIX" en la página 12
- Para Linux, vea "Requisitos para Red Hat Linux o SuSe Linux" en la página 16
- Para Solaris, vea "Requisitos para Solaris" en la página 19
- Para Windows 2000, vea "Requisitos para Windows 2000" en la página 22

Consideraciones referentes a la planificación

El componente Mailbox Locator le permite reenviar el tráfico de IMAP y POP3 basándose en el ID de usuario y la contraseña de la petición del cliente.

Mailbox Locator es muy similar a Dispatcher en su estructura de componentes. Mailbox Locator consta de las siguientes funciones:

- **mlserver** gestiona las peticiones procedentes de la línea de mandatos destinadas al ejecutor, el gestor y los asesores.
- El **ejecutor** da soporte al reparto del tráfico de las peticiones del cliente. El ejecutor se ejecuta siempre que se utiliza el componente Mailbox Locator.
- El **gestor** establece los pesos que utiliza el ejecutor tomando como base:
 - Los contadores internos del ejecutor
 - La información de retorno procedente de los servidores facilitada por los asesores
 - Información proporcionada por un programa de supervisión del sistema, tal como Metric Server.

El uso del gestor es opcional. No obstante, si no se utiliza un gestor, el reparto del tráfico se realiza utilizando una planificación rotatoria ponderada basada en los pesos actuales de los servidores, y no podrán utilizarse asesores.

- Los **asesores**, que consultan los servidores y analizan el resultado por protocolo antes de llamar al gestor para que establezca los pesos según convenga. Es posible que no tenga sentido utilizar algunos de estos asesores en una configuración típica. También tiene la opción de escribir sus propios asesores. El uso de los asesores es opcional aunque se recomienda. En “Asesores” en la página 139 hallará más información.
- Para configurar y gestionar el ejecutor, los asesores y el gestor, utilice la línea de mandatos (**mlcontrol**) o la interfaz gráfica de usuario (**ndadmin**).

Las tres funciones clave de Mailbox Locator (el ejecutor, los asesores y el gestor) interactúan para repartir el tráfico y distribuir entre los servidores las peticiones entrantes. Además de repartir el tráfico de peticiones, el ejecutor supervisa el número de conexiones nuevas y activas y proporciona esta información al gestor.

Para iniciar Mailbox Locator, emita el mandato **mlserver** desde el indicador de mandatos.

Mailbox Locator puede proporcionar un único punto de presencia para varios servidores IMAP o POP3. Cada servidor puede tener un subconjunto de todos los servicios de correo para los que ofrece servicio el punto de presencia. Para IMAP y POP3, Mailbox Locator es un proxy que elige un servidor adecuado basándose en el ID de usuario y la contraseña proporcionados por el cliente.

Nota: Mailbox Locator *no* permite realizar el reparto del tráfico basado en **normas**.

El siguiente método de ejemplo distribuye peticiones basándose en el ID de usuario de los clientes. Si tiene dos (o más) servidores POP3, puede dividir los buzones de correo alfabéticamente según el ID de usuario. Las peticiones de los clientes cuyos ID de usuario empiecen por las letras de la A a la I se pueden repartir hacia el servidor 1. Las peticiones de los clientes cuyos ID de usuario empiecen por las letras de la J a la R se pueden repartir hacia el servidor 2 y así sucesivamente.

También puede elegir que cada buzón se represente en más de un servidor. En este caso, el contenido de cada buzón debe estar disponible para todos los servidores de dicho buzón. En caso de que se produzca una anomalía en el servidor, habrá otro servidor que podrá acceder al buzón.

Para tener una sola dirección que represente varios servidores de correo POP3, puede configurar Mailbox Locator con una sola dirección de cluster que se convierta en la dirección de servidor de correo POP3 para todos los clientes. Los mandatos para configurarlo son los siguientes:

```
mlcontrol cluster add servidorCorreoPop3
mlcontrol port add servidorCorreoPop3:110 protocol pop3
mlcontrol server add
servidorCorreoPop3:110:servidor1Pop3+servidor2Pop3+servidor3Pop3
```

En este ejemplo, *ServidorCorreoPop3* representa la dirección de cluster. El Puerto 110 con el protocolo proxy POP3 se añade a *ServidorCorreoPop3*. *Servidor1Pop3*, *Servidor2Pop3* y *Servidor3Pop3* representan los servidores de correo de POP3 que se añaden al puerto. Con esta configuración, puede configurar las peticiones POP3 de entrada de los clientes de correo con la dirección de cluster *ServidorCorreoPop3*.

Uso de la función de afinidad

Cuando la petición de POP3 o IMAP llega al proxy, éste intenta contactar con todos los servidores configurados para el puerto utilizando la contraseña y el ID de usuario del cliente. La petición del cliente se dirige al primer servidor que responde. Debe utilizar la función de afinidad/persistencia junto con Mailbox Locator para los servidores IMAP o POP3. La función de afinidad permite que las peticiones subsiguientes procedentes del mismo ID de usuario del cliente se envíen al mismo servidor. Establezca el tiempo de persistencia (**stickytime**) del puerto en un valor mayor que cero para habilitar la función de afinidad. Para obtener más información sobre la función de afinidad, consulte “La función de afinidad de Network Dispatcher” en la página 188.

Alteración del temporizador de inactividad de POP3/IMAP

El temporizador de desconexión automática por inactividad para los protocolos POP3 e IMAP es, como mínimo, de 10 minutos y 30 minutos respectivamente. Este tiempo de espera es el número de segundos durante los cuales puede haber ausencia de actividad en una conexión antes de que dicha conexión se elimine. Para optimizar el rendimiento, Mailbox Locator altera el

valor del tiempo de espera de inactividad para que sea de 60 segundos. Para cambiar el tiempo de espera de inactividad, cambie el valor **staletimeout** (tiempo de inactividad) en el mandato **mlcontrol cbrcontrol port**. Para obtener más información sobre la configuración de este mandato, consulte el apartado “ndcontrol port — configurar puertos” en la página 287.

Capítulo 9. Configuración del componente Mailbox Locator

Antes de seguir los pasos indicados en este capítulo, consulte el “Capítulo 8. Planificación para el componente Mailbox Locator” en la página 95. Este capítulo explica cómo crear una configuración básica para el componente Mailbox Locator de Network Dispatcher.

Nota: Antes, el componente Mailbox Locator era una función dentro del componente CBR que repartía el tráfico entre servidores de correo IMAP y POP3 basándose en el ID de usuario y la contraseña. Al separar CBR en dos componentes, se *elimina* la limitación de que “CBR para IMAP/POP3” (Mailbox Locator) y “CBR para HTTP/HTTPS” (CBR con Caching Proxy) no se puedan ejecutar en la misma máquina.

- Consulte el “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131 para ver configuraciones más complejas de Network Dispatcher.
- Consulte el “Capítulo 15. Utilización y gestión de Network Dispatcher” en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Visión general de las tareas de configuración

Nota: Antes de realizar los pasos de configuración indicados en esta tabla, asegúrese de que las máquinas Mailbox Locator y todas las máquinas servidor están conectadas a la red, tienen una dirección IP válida y pueden emitir el mandato ping entre sí.

Tabla 8. Tareas de configuración para el componente Mailbox Locator

Tarea	Descripción	Información relacionada
Configurar la máquina Mailbox Locator.	Determinar los requisitos.	“Configuración de la máquina Mailbox Locator” en la página 103
Configurar máquinas para el reparto del tráfico.	Preparar la configuración del reparto del tráfico.	“Paso 4. Definir servidores de reparto del tráfico” en la página 104

Métodos de configuración

Para crear una configuración básica para el componente Mailbox Locator de Network Dispatcher, existen cuatro métodos básicos:

- Línea de mandatos
- Scripts
- Interfaz gráfica de usuario (GUI)
- Asistente de configuración

Línea de mandatos

Este es el medio más directo para configurar Mailbox Locator. Los valores de los parámetros de mandatos se deben escribir en caracteres ingleses. Las únicas excepciones son los nombres de sistema principal (utilizados, por ejemplo, en los mandatos para clusters y servidores) y los nombres de archivos.

Para iniciar Mailbox Locator desde la línea de mandatos:

- Emita el mandato **mlserver** desde el indicador de mandatos.

Nota: Para detener el servicio, emita lo siguiente: **mlserver stop**.

- A continuación, emita los mandatos de control de Mailbox Locator que desee para establecer la configuración. Los procedimientos de este manual presuponen que se utiliza la línea de mandatos. El mandato es **mlcontrol**. Para obtener más información acerca de los mandatos, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.

Puede especificar una versión abreviada de los parámetros de los mandatos **mlcontrol**. Sólo necesita especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato “file save”, puede entrar **mlcontrol he f** en lugar de **mlcontrol help file**.

Para iniciar la interfaz de línea de mandatos, emita el mandato **mlcontrol** para visualizar un indicador de mandatos de **mlcontrol**.

Para cerrar la interfaz de línea de mandatos, emita **exit** o **quit**.

Nota: En Windows 2000, el **ndserver** del componente Dispatcher se inicia automáticamente. Si sólo desea utilizar Mailbox Locator y no el componente Dispatcher, puede evitar que **ndserver** se inicie automáticamente realizando estos pasos:

1. En la ventana Servicios de Windows 2000, pulse con el botón derecho del ratón sobre IBM Dispatcher.
2. Seleccione Propiedades.

3. En el campo **Tipo de arranque**, seleccione Manual.
4. Pulse Aceptar y cierre la ventana Servicios.

Scripts

Los mandatos para configurar Mailbox Locator se pueden entrar en un archivo de script de configuración y ejecutarlos juntos.

Nota: Para ejecutar rápidamente el contenido de un archivo de script (por ejemplo, *miscript*), utilice cualquiera de estos dos mandatos:

- Para actualizar la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:

```
mlcontrol file appendload miscript
```

- Para sustituir totalmente la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:

```
mlcontrol file newload miscript
```

GUI

Para ver un ejemplo de la GUI, consulte la Figura 2 en la página 5.

Para iniciar la GUI, siga estos pasos

1. Asegúrese de que **mlserver** está en ejecución. Como usuario root o administrador, emita lo siguiente desde un indicador de mandatos:
mlserver
2. A continuación, lleve a cabo una de las siguientes acciones:
 - Para AIX, Linux o Solaris, especifique **ndadmin**
 - Para Windows 2000, pulse **Inicio, Programas, IBM WebSphere, Edge Server, IBM Network Dispatcher** y finalmente **Network Dispatcher**

Para poder configurar el componente Mailbox Locator desde la GUI, antes debe seleccionar **Mailbox Locator** en la estructura en árbol. Puede arrancar el gestor una vez que esté conectado a un sistema principal. También puede crear clusters que contengan puertos y servidores e iniciar asesores para el gestor.

La GUI se puede utilizar para realizar las mismas acciones que pueden efectuarse con el mandato **mlcontrol**. Por ejemplo, para definir un cluster desde la línea de mandatos, escriba el mandato **mlcontrol cluster add cluster**. Para definir un cluster desde la GUI, pulse el botón derecho del ratón sobre Ejecutor, y en el menú emergente pulse el botón izquierdo sobre **Añadir cluster**. Escriba la dirección del cluster en la ventana emergente, a continuación pulse en **Aceptar**.

Los archivos de configuración preexistentes de Mailbox Locator se pueden cargar utilizando las opciones **Cargar nueva configuración** (para sustituir

totalmente la configuración actual) y **Añadir a configuración actual** (para actualizar la configuración actual); estas opciones aparecen en el menú emergente **Sistema principal**. Debe guardar periódicamente la configuración de Mailbox Locator en un archivo, mediante la opción **Guardar archivo de configuración como** del menú emergente **Sistema principal**. El menú **Archivo**, situado en la parte superior de la GUI, le permitirá guardar las conexiones actuales del sistema principal en un archivo o restaurar las conexiones de archivos existentes a través de los componentes de Network Dispatcher.

Puede acceder a la **Ayuda** pulsando el icono de signo de interrogación, situado en la esquina superior derecha de la ventana de Network Dispatcher.

- **Ayuda para los campos** — describe cada campo y sus valores por omisión
- **Cómo puedo** — lista tareas que pueden efectuarse desde esa pantalla
- **Contenido** — es una tabla de contenido de toda la información de la Ayuda
- **Índice** — es un índice alfabético de temas de la Ayuda

Para obtener más información acerca de la utilización de la GUI, consulte el apartado “Instrucciones generales para la utilización de la GUI” en la página 6.

Asistente de configuración

Si está utilizando el asistente para configuración, siga estos pasos:

1. Como usuario root o administrador, emita el mandato **mlserver** desde un indicador de mandatos.
2. Inicie la función del asistente de Mailbox Locator, **mlwizard**.

Puede iniciar este asistente desde el indicador de mandatos emitiendo **mlwizard**. O bien, seleccione Asistente de configuración en el menú del componente Mailbox Locator que aparece en la GUI.

El asistente de Mailbox Locator le guía paso a paso en el proceso de creación de una configuración básica para el componente Mailbox Locator. El asistente le hará preguntas acerca de la red y le guiará mientras configura un cluster que permite que Mailbox Locator reparta el tráfico entre un grupo de servidores.

Cuando se utiliza el asistente de configuración de Mailbox Locator se muestran estos paneles:

- Introducción al asistente
- Expectativas
- Antes de empezar
- Selección de un sistema principal para configurar (si es necesario)
- Definición de un cluster

- Adición de un puerto
- Adición de un servidor
- Inicio de un asesor

Configuración de la máquina Mailbox Locator

Para configurar la máquina Mailbox Locator, debe ser el usuario root (en AIX, Linux o Solaris) o el administrador en Windows 2000.

Necesitará una dirección IP para cada cluster de servidores que se van a configurar. Una dirección de cluster es una dirección que está asociada con un nombre de sistema principal (como `www.suempresa.com`). Esta dirección IP la utilizan los clientes para conectarse a los servidores de un cluster. Mailbox Locator reparte el tráfico de todas las peticiones realizadas a la misma dirección de cluster.

Paso 1. Iniciar la función de servidor

Para iniciar la función del servidor, escriba **mlserver** en la línea de mandatos.

Nota: Automáticamente se cargará un archivo de configuración por omisión (`default.cfg`) cuando inicie `mlserver`. Si el usuario decide guardar la configuración en `default.cfg`, todo lo que haya guardado en este archivo se cargará automáticamente la próxima vez que se inicie `mlserver`.

Paso 2. Definir un cluster y establecer las opciones de cluster

Mailbox Locator repartirá las peticiones enviadas a la dirección de cluster entre los servidores correspondientes configurados en los puertos de ese cluster.

La dirección del cluster es un nombre simbólico o una dirección decimal con puntos.

Para definir un cluster, emita el siguiente mandato:

```
mlcontrol cluster add cluster
```

Para establecer las opciones de cluster, emita el siguiente mandato:

```
mlcontrol cluster set cluster opción valor
```

Para obtener más información, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.

Paso 3. Definir los puertos y establecer las opciones de puerto

El número de puerto es el puerto donde las aplicaciones de servidor están a la escucha. Para el tráfico de IMAP, suele ser el puerto 143. Y para el tráfico de POP3, suele ser el puerto 110.

Para definir un puerto para el cluster que definió en el paso anterior, emita lo siguiente:

```
mlcontrol port add  
cluster:puerto protocolo [pop3|imap]
```

Para establecer las opciones de puerto, emita el siguiente mandato:

```
mlcontrol port set cluster:puerto opción valor
```

Nota: Cuando añada un puerto, debe especificar el protocolo proxy (pop3 o imap). Después de añadir el puerto, no puede cambiar (definir) el valor de protocolo existente para ese puerto.

Para obtener más información, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.

Paso 4. Definir servidores de reparto del tráfico

Los servidores de correo son las máquinas donde se ejecutan las aplicaciones cuyo tráfico se desea repartir. El *servidor* es el nombre simbólico o dirección decimal con puntos de la máquina servidor. Para definir un servidor en el cluster y puerto del paso 3, emita el siguiente mandato:

```
mlcontrol server add cluster:puerto:servidor
```

Para realizar el reparto del tráfico debe definir más de un servidor por puerto en un cluster.

Paso 5. Iniciar la función del gestor (opcional)

La función del gestor mejora el reparto del tráfico. Para iniciar el gestor, emita el siguiente mandato:

```
mlcontrol manager start
```

Paso 6. Iniciar la función del asesor (opcional)

Los asesores proporcionan al gestor más información acerca de la capacidad de los servidores de reparto del tráfico para responder a las peticiones. Cada asesor es específico de un protocolo. Network Dispatcher proporciona asesores para IMAP y POP3. Por ejemplo, para iniciar el asesor de IMAP, emita el mandato siguiente:

```
mlcontrol advisor start imap puerto
```

Para obtener una lista de los asesores junto con sus puertos por omisión, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249. Si desea ver una descripción de cada asesor, consulte la sección “Lista de asesores” en la página 143.

Paso 7. Establecer las proporciones del cluster según sea necesario

Si inicia asesores, puede modificar la proporción de importancia que se asigna a la información del asesor utilizada para las decisiones sobre reparto del

tráfico. Para establecer las proporciones del cluster, emita el mandato **mlcontrol cluster set *cluster* proportions**. Para obtener más información, consulte “Grado de importancia dado a la información de estado” en la página 135.

Capítulo 10. Planificación para el componente Site Selector

En este capítulo se describen los aspectos que debe tener en cuenta la persona encargada de planificar la red antes de proceder a la instalación y configuración del componente Site Selector.

- Consulte el “Capítulo 11. Configuración del componente Site Selector” en la página 113 para obtener información sobre cómo configurar los parámetros de distribución de tráfico de Site Selector.
- Consulte el “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131 para obtener información sobre cómo configurar Network Dispatcher para funciones más avanzadas.
- Consulte el “Capítulo 15. Utilización y gestión de Network Dispatcher” en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Este capítulo incluye las siguientes secciones:

- “Requisitos de hardware y de software”
- “Consideraciones referentes a la planificación”

Requisitos de hardware y de software

- Para AIX, vea “Requisitos para AIX” en la página 12
- Para Linux, vea “Requisitos para Red Hat Linux o SuSe Linux” en la página 16
- Para Solaris, vea “Requisitos para Solaris” en la página 19
- Para Windows 2000, vea “Requisitos para Windows 2000” en la página 22

Consideraciones referentes a la planificación

Site Selector actúa conjuntamente con un servidor de nombres de dominio para repartir el tráfico entre un grupo de servidores, utilizando medidas y valores de ponderación (pesos) recogidos. Puede crear una configuración de sitio Web para poder repartir el tráfico entre un grupo de servidores basándose en el nombre de dominio utilizado para la petición de un cliente.

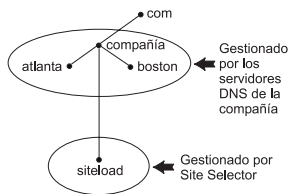


Figura 20. Ejemplo de un entorno DNS

Cuando se configura un subdominio para Site Selector dentro del entorno DNS, Site Selector debe tener autorización sobre su propio subdominio. Por ejemplo, (consulte la Figura 20), se ha asignado a su empresa autorización sobre el dominio **company.com**. Dentro de la empresa, hay varios subdominios. Site Selector tendría autorización para **siteload.company.com**, mientras que el servidor o servidores DNS mantendrían autorización para **atlanta.company.com** y **boston.company.com**.

Para que el servidor de nombres de la empresa pueda reconocer que Site Selector tiene autorización para el subdominio siteload, se tiene que añadir una entrada del servidor de nombres en su archivo de datos con nombre. Por ejemplo, en AIX, una entrada del servidor de nombres sería parecida a la siguiente:

siteload.company.com. IN NS siteselector.company.com.

Donde **siteselector.company.com** es el nombre de sistema principal de la máquina Site Selector. En otros archivos de bases de datos con nombre se tendrían que añadir entradas equivalentes para que las utilizaran los servidores DNS.

Un cliente envía una petición para resolver un nombre de dominio en un nombre de servidor dentro de su red. El servidor de nombres reenvía la petición a la máquina de Site Selector. A continuación, Site Selector resuelve el nombre de dominio y obtiene la dirección IP de uno de los servidores que se ha configurado en el nombre de sitio. Site Selector devuelve la dirección IP del servidor seleccionado al servidor de nombres. El servidor de nombres devuelve la dirección IP al cliente. (Site Selector actúa como servidor de nombres no recursivo (nodo terminal) y devuelve un error si no resuelve la petición de nombre de dominio).

Consulte la Figura 11 en la página 40, que muestra un sitio Web en el que se utiliza Site Selector junto con un sistema DNS para repartir el tráfico entre servidores locales y remotos.

Site Selector consta de las siguientes funciones:

- **ssserver**, que gestiona las peticiones procedentes de la línea de mandatos destinadas al servidor de nombres, el gestor y los asesores.

- El **servidor de nombres**, que permite el reparto de las peticiones entrantes del servidor de nombres. Debe iniciar el servidor de nombres para que Site Selector pueda proporcionar resolución de nombres DNS. Site Selector está a la escucha en el puerto 53 para recibir las peticiones DNS entrantes. Si el nombre de sitio solicitante está configurado, Site Selector devuelve una dirección individual de servidor (de entre un grupo de direcciones de servidor) correspondiente al nombre de sitio.
- El **gestor**, que establece los pesos utilizados por el servidor de nombres basándose en:
 - Información recibida de los servidores y proporcionada por los asesores
 - Información proporcionada por un programa de supervisión del sistema, tal como Metric Server.

El uso del gestor es opcional. No obstante, si no se utiliza un gestor, el reparto del tráfico se realiza utilizando una planificación rotatoria ponderada basada en los pesos actuales de los servidores, y no podrán utilizarse asesores.

- **Metric Server** es un componente de Network Dispatcher, para la supervisión del sistema, que se instala en el servidor de fondo. (Si Network Dispatcher se instala en el mismo servidor para el cual se realiza el reparto del tráfico, entonces Metric Server se instalaría en la máquina de Network Dispatcher).

Mediante Metric Server, Site Selector puede supervisar el nivel de actividad de un servidor, detectar el servidor con menos tráfico y los servidores anómalos. El tráfico es una medida de la intensidad con que trabaja el servidor. El administrador de Site Selector del sistema controla el tipo de medida utilizada para medir el tráfico. Se puede configurar Site Selector para adaptarlo al entorno, tomando en cuenta factores como la frecuencia de acceso, el número total de usuarios y los tipos de acceso (por ejemplo, consultas breves, consultas de larga duración o cargas de datos que exigen un alto consumo de CPU).

El reparto del tráfico está basado en pesos (valores de ponderación) de los servidores. Para Site Selector, existen cuatro proporciones que el gestor utiliza para determinar los pesos:

- CPU
- memoria
- puerto
- sistema

Metric Server suministra los valores de CPU y memoria. Por tanto, es *recomendable* utilizar Metric Server cuando se utiliza el componente Site Selector.

En “Metric Server” en la página 150 hallará más información.

- Los **asesores** obtienen información de los servidores y analizan los resultados para cada protocolo antes de invocar al gestor para establecer los pesos según convenga. Puede que no sea necesario utilizar algunos de estos asesores en una configuración estándar. El usuario tiene también la opción de escribir sus propios asesores. El uso de asesores es opcional, pero recomendable. En “Asesores” en la página 139 hallará más información.
- Para configurar y utilizar el servidor de nombres, los asesores, Metric Server y el gestor, utilice la línea de mandatos (**sscontrol**;) o la interfaz gráfica de usuario (**ndadmin**).

Las cuatro funciones clave de Site Selector (servidor de nombres, gestor, Metric Server y asesores) interactúan para repartir las peticiones entrantes entre los servidores.

Consideraciones sobre TTL

Para utilizar la distribución de tráfico basada en DNS la colocación en antememoria de resoluciones de nombres tiene que estar inhabilitada. El valor TTL (tiempo de vida) determina la eficacia de la distribución de tráfico basada en DNS. TTL determina cuánto tiempo otro servidor de nombres mantendrá en antememoria la respuesta resuelta. Valores de TTL pequeños permiten llevar a cabo pequeños cambios en el servidor o en el tráfico de la red con mayor rapidez. Sin embargo, para inhabilitar la colocación en antememoria los clientes tienen que ponerse en contacto con el servidor de nombres con autorización para cada petición de resolución de nombre, lo que potencialmente aumenta el tiempo de latencia del cliente. Cuando se elige un valor de TTL, hay que tener en cuenta el efecto que tiene sobre un entorno la inhabilitación de la colocación en antememoria. También hay que tener en cuenta que la distribución de tráfico basada en DNS está potencialmente limitada por la colocación en antememoria en el extremo del cliente de las resoluciones de nombres.

TTL se puede configurar utilizando el mandato **sscontrol sitename [add | set]**. Consulte “sscontrol sitename — configurar un nombre de sitio” en la página 341 para obtener más información.

Utilización de la función de Proximidad en la Red

La proximidad en la red es el cálculo del grado de cercanía de cada servidor respecto al cliente solicitante. Para determinar la proximidad en la red, el agente de Metric Server (el cual debe residir en cada servidor sujeto a reparto del tráfico) envía un mandato ping a la dirección IP del cliente y devuelve el tiempo de respuesta a Site Selector. Site Selector utiliza la respuesta de proximidad en las decisiones sobre reparto del tráfico. Site Selector combina el valor de la respuesta de proximidad en la red con el peso obtenido del gestor para crear un valor de ponderación final para el servidor.

La utilización de la función de proximidad en la red junto con Site Selector es opcional.

Site Selector proporciona las opciones siguientes de proximidad en la red que se pueden definir para cada nombre de sitio:

- Permanencia en antememoria: es la cantidad de tiempo que una respuesta de proximidad será válida y se mantendrá en la antememoria.
- Porcentaje de proximidad: es la importancia de la respuesta de proximidad respecto al estado del servidor (como valor derivado del peso del gestor).
- Esperar todas las respuestas: determina si se deben esperar todas las respuestas de proximidad (a ping) procedentes de los servidores antes de responder a la petición del cliente.

Si este parámetro se establece en **sí**, Metric Server emite un mandato ping al cliente para obtener el tiempo de respuesta de proximidad. El servidor de nombres espera a que respondan todos los Metric Servers o hasta que se sobrepase el tiempo de espera. Luego, para cada servidor, el servidor de nombres combina el tiempo de respuesta de proximidad con el peso calculado por el gestor y crea un valor de "peso combinado" para cada servidor. Site Selector proporcionará al cliente la dirección IP del servidor que tenga el mejor peso combinado. (Se espera que la mayoría de los servidores de nombres de cliente tengan un tiempo de espera de 5 segundos. Site Selector intenta responder antes de que se sobrepase ese tiempo de espera.)

Si este parámetro se establece en **no**, se proporcionará una resolución de nombres al cliente basada en los pesos actuales calculados por el gestor. A continuación, Metric Server emite un mandato ping al cliente para obtener el tiempo de respuesta de proximidad. El servidor de nombres coloca en antememoria el tiempo de respuesta que recibe de Metric Server. Cuando el cliente emite una segunda petición, el servidor de nombres combina, para cada servidor, el peso actual (calculado por el gestor) con el tiempo de respuesta (guardado en antememoria) y obtiene el servidor con el mejor "peso combinado". Site Selector devuelve la dirección IP de ese servidor al cliente para la segunda petición de este último.

Las opciones de proximidad en la red pueden establecerse en el mandato **sscontrol sitename [add | set]**. En el "Apéndice D. Consulta de mandatos de Site Selector" en la página 317 hallará más información.

Capítulo 11. Configuración del componente Site Selector

Antes de seguir los pasos indicados en este capítulo, consulte el “Capítulo 10. Planificación para el componente Site Selector” en la página 107. Este capítulo explica cómo crear una configuración básica para el componente Site Selector de Network Dispatcher.

- Consulte el “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131 para ver configuraciones más complejas de Network Dispatcher.
- Consulte el “Capítulo 15. Utilización y gestión de Network Dispatcher” en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Visión general de las tareas de configuración

Nota: Antes de realizar los pasos de configuración indicados en esta tabla, asegúrese de que las máquinas Site Selector y todas las máquinas servidor están conectadas a la red, tienen una dirección IP válida y pueden emitir el mandato ping entre sí.

Tabla 9. Tareas de configuración para el componente Site Selector

Tarea	Descripción	Información relacionada
Configurar la máquina Site Selector.	Determinar los requisitos.	“Configuración de la máquina Site Selector” en la página 116
Configurar máquinas para el reparto del tráfico.	Preparar la configuración del reparto del tráfico.	“Paso 4. Definir servidores de reparto del tráfico” en la página 117

Métodos de configuración

A fin de crear una configuración básica del componente Site Selector de Network Dispatcher, existen cuatro métodos básicos de configuración para este componente:

- Línea de mandatos
- Scripts
- Interfaz gráfica de usuario (GUI)
- Asistente de configuración

Línea de mandatos

Este es el medio más directo para configurar Site Selector. Los valores de los parámetros de mandatos se deben escribir en caracteres ingleses. Las únicas excepciones son los nombres de sistema principal (utilizados, por ejemplo, en los mandatos para nombres de sitio y servidores) y los nombres de archivos.

Para iniciar Site Selector desde la línea de mandatos:

- Emita el mandato **ssserver** desde el indicador de mandatos.

Nota: Para detener el servicio, emita lo siguiente: **ssserver stop**.

- A continuación, emita los mandatos de control de Site Selector que desee para establecer la configuración. Los procedimientos de este manual presuponen que se utiliza la línea de mandatos. El mandato es **sscontrol**. Para obtener más información acerca de los mandatos, consulte el “Apéndice D. Consulta de mandatos de Site Selector” en la página 317.

Puede especificar una versión abreviada de los parámetros de los mandatos **sscontrol**. Sólo necesita especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato “file save”, puede entrar **sscontrol he f** en lugar de **sscontrol help file**.

Para iniciar la interfaz de línea de mandatos, emita **sscontrol** para visualizar un indicador de mandatos de **sscontrol**.

Para cerrar la interfaz de línea de mandatos, emita **exit** o **quit**.

Nota: En Windows 2000, el **ndserver** del componente Dispatcher se inicia automáticamente. Si sólo desea utilizar Site Selector y no el componente Dispatcher, puede evitar que **ndserver** se inicie automáticamente realizando estos pasos:

1. En la ventana Servicios de Windows 2000, pulse con el botón derecho del ratón sobre IBM Dispatcher.
2. Seleccione Propiedades.
3. En el campo **Tipo de arranque**, seleccione Manual.
4. Pulse Aceptar y cierre la ventana Servicios.

Scripts

Los mandatos para configurar Site Selector se pueden entrar en un archivo de script de configuración y ejecutarlos juntos.

Nota: Para ejecutar rápidamente el contenido de un archivo de script (por ejemplo, **miscscript**), utilice cualquiera de estos dos mandatos:

- Para actualizar la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:

```
sscontrol file appendload myscript
```

- Para sustituir totalmente la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:

```
sscontrol file newload myscript
```

GUI

Para ver un ejemplo de la GUI, consulte la Figura 2 en la página 5.

Para iniciar la GUI, siga estos pasos

1. Asegúrese de que ssserver está en ejecución. Como usuario root o administrador, emita lo siguiente desde un indicador de mandatos:
ssserver
2. A continuación, lleve a cabo una de las siguientes acciones:
 - Para AIX, Linux o Solaris, especifique **ndadmin**
 - Para Windows 2000, pulse **Inicio, Programas, IBM WebSphere, Edge Server, IBM Network Dispatcher** y finalmente **Network Dispatcher**

Para poder configurar el componente Site Selector desde la GUI, antes debe seleccionar **Site Selector** en la estructura en árbol. Puede arrancar el gestor una vez que esté conectado a un sistema principal. También puede crear nombres de sitio que contengan puertos y servidores e iniciar asesores para el gestor.

La GUI se puede utilizar para realizar las mismas acciones que con el mandato **sscontrol**. Por ejemplo, para definir un nombre de sitio desde la línea de mandatos, entre el mandato **sscontrol sitename add nombresitio**. Para definir un nombre de sitio de la GUI, pulse el botón derecho del ratón sobre Nombre de servidor, y en el menú emergente pulse el botón izquierdo sobre **Añadir nombre de sitio**. Indique el nombre de sitio en la ventana emergente y pulse **Aceptar**.

Los archivos de configuración preexistentes de Site Selector se pueden cargar utilizando las opciones **Cargar nueva configuración** (para sustituir totalmente la configuración actual) y **Añadir a configuración actual** (para actualizar la configuración actual); estas opciones aparecen en el menú emergente **Sistema principal**. Debe guardar periódicamente la configuración de Site Selector en un archivo, mediante la opción **Guardar archivo de configuración como** del menú emergente **Sistema principal**. El menú **Archivo**, situado en la parte superior de la GUI, le permitirá guardar las conexiones actuales del sistema principal en un archivo o restaurar las conexiones de archivos existentes a través de los componentes de Network Dispatcher.

Puede acceder a la **Ayuda** pulsando el icono de signo de interrogación, situado en la esquina superior derecha de la ventana de Network Dispatcher.

- **Ayuda para los campos** — describe cada campo y sus valores por omisión

- **Cómo puedo** — lista tareas que pueden efectuarse desde esa pantalla
- **Contenido** — es una tabla de contenido de toda la información de la Ayuda
- **Índice** — es un índice alfabético de temas de la Ayuda

Para obtener más información acerca de la utilización de la GUI, consulte el apartado “Instrucciones generales para la utilización de la GUI” en la página 6.

Asistente de configuración

Si está utilizando el asistente para configuración, siga estos pasos:

1. Inicie **ssserver** en Site Selector como usuario root o administrador: emita **ssserver** en el indicador de mandatos.
2. Inicie la función del asistente de Site Selector, **sswizard**.

Puede iniciar este asistente desde el indicador de mandatos emitiendo **sswizard**. O bien, seleccione Asistente de configuración en el menú del componente Site Selector que aparece en la GUI.

El asistente de Site Selector le guía paso a paso en el proceso de creación de una configuración básica para el componente Site Selector. El asistente le hará preguntas acerca de la red y le guiará mientras configura un nombre de sitio que permitirá que Site Selector reparta el tráfico entre un grupo de servidores.

Cuando se utiliza el asistente de configuración de Site Selector se muestran estos paneles:

- Introducción al asistente
- Expectativas
- Antes de empezar
- Selección de un sistema principal para configurar (si es necesario)
- Definición de un nombre de sitio
- Adición de un servidor
- Inicio de un asesor
- Establecimiento de la proximidad en la red

Configuración de la máquina Site Selector

Para configurar la máquina Site Selector, debe ser el usuario root (en AIX, Linux o Solaris) o el administrador en Windows 2000.

Necesitará un nombre de sistema principal DNS que no se pueda resolver, para utilizarlo como nombre de sitio para el grupo de servidores que defina. El nombre de sitio es el nombre que los clientes utilizan para acceder al sitio Web (por ejemplo, www.empresa.com). Site Selector utilizará DNS para repartir el tráfico de ese nombre de sitio entre el grupo de servidores.

Paso 1. Iniciar la función de servidor

AIX, Linux y Solaris: Para iniciar la función del servidor, escriba `sssserver`.

Nota: Automáticamente se cargará un archivo de configuración por omisión (`default.cfg`) cuando inicie `sssserver`. Si el usuario decide guardar la configuración en `default.cfg`, todo lo que haya guardado en este archivo se cargará automáticamente la próxima vez que se inicie `sssserver`.

Paso 2. Iniciar el servidor de nombres

Para iniciar el servidor de nombres, emita el mandato `sscontrol nameserver start`.

Opcionalmente, inicie el servidor de nombres utilizando la palabra clave `bindaddress` para crear una vinculación únicamente con la dirección especificada.

Paso 3. Definir un nombre de sitio y establecer las opciones de nombre de sitio

Site Selector repartirá las peticiones enviadas al nombre de sitio entre los servidores correspondientes configurados para el nombre de sitio.

El nombre de sitio es un nombre de sistema principal que no se puede resolver y que el cliente solicitará. El nombre de sitio debe ser un nombre de dominio totalmente calificado (por ejemplo, `www.dnsdownload.com`). Cuando un cliente solicita este nombre de sitio, se devuelve una de las direcciones IP de servidor asociadas al nombre de sitio.

Para definir un nombre de sitio, emita el mandato siguiente:

```
sscontrol sitename add nombresitio
```

Para establecer las opciones de nombre de sitio, emita el mandato siguiente:

```
sscontrol sitename set valor opción nombresitio
```

Para obtener más información, consulte “Apéndice D. Consulta de mandatos de Site Selector” en la página 317.

Paso 4. Definir servidores de reparto del tráfico

Las máquinas servidor son las máquinas donde se ejecutan las aplicaciones cuyo tráfico desea repartir. El *servidor* es el nombre simbólico o dirección decimal con puntos de la máquina servidor. Para definir un servidor en el nombre de sitio del paso 3, emita el mandato siguiente:

```
sscontrol server add nombresitio:servidor
```

Para repartir el tráfico debe definir más de un servidor para un nombre de sitio.

Paso 5. Iniciar la función del gestor (opcional)

La función del gestor mejora el reparto del tráfico. Antes de iniciar la función del gestor, asegúrese de que el servidor de métricas esté instalado en todas las máquinas de reparto de tráfico.

Para iniciar el gestor, emita el siguiente mandato:

```
sscontrol manager start
```

Paso 6. Iniciar la función del asesor (opcional)

Los asesores facilitan al gestor más información acerca de la capacidad de las máquinas servidor del reparto del tráfico para responder a las peticiones. Cada asesor es específico de cada protocolo. Network Dispatcher proporciona diversos asesores. Por ejemplo, para iniciar el asesor HTTP correspondiente a un nombre de sitio específico, emita el siguiente mandato:

```
sscontrol advisor start http nombresitio:puerto
```

Paso 7. Definir la métrica del sistema (opcional)

Consulte “Metric Server” en la página 150 para obtener información sobre el uso de métricas del sistema y Metric Server.

Paso 8. Establecer las proporciones del nombre de sitio según sea necesario

Si inicia asesores, puede modificar la proporción de importancia que se asigna a la información del asesor (puerto) utilizada para las decisiones sobre reparto del tráfico. Para establecer las proporciones del nombre de sitio, emita el mandato **sscontrol sitename set *nombresitio* proportions**. Para obtener más información, consulte “Grado de importancia dado a la información de estado” en la página 135.

Configuración de las máquinas servidor para el reparto del tráfico

Es recomendable utilizar Metric Server con el componente Site Selector. Consulte “Metric Server” en la página 150 para conocer cómo configurar Metric Server en todos los servidores para los que Site Selector reparte el tráfico.

Capítulo 12. Planificación para el componente Consultant para Cisco CSS Switches

En este capítulo se describen los aspectos que debe tener en cuenta la persona encargada de planificar la red antes de proceder a la instalación y configuración del componente Consultant para Cisco CSS Switches.

- Consulte el “Capítulo 13. Configuración del componente Consultant para Cisco CSS Switches” en la página 125 para obtener información sobre cómo configurar los parámetros de distribución de tráfico en el componente Consultant para Cisco CSS Switches.
- Consulte el “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131 para obtener información sobre cómo configurar Network Dispatcher para funciones más avanzadas.
- Consulte el “Capítulo 15. Utilización y gestión de Network Dispatcher” en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Este capítulo incluye estos temas:

- “Requisitos de hardware y de software”
- “Consideraciones referentes a la planificación”

Requisitos de hardware y de software

- Para AIX, vea “Requisitos para AIX” en la página 12
- Para Linux, vea “Requisitos para Red Hat Linux o SuSe Linux” en la página 16
- Para Solaris, vea “Requisitos para Solaris” en la página 19
- Para Windows 2000, vea “Requisitos para Windows 2000” en la página 22

Consideraciones referentes a la planificación

La configuración de Cisco Consultant depende de la configuración de Cisco CSS Switch (vea Tabla 10 en la página 121). Después de realizar la planificación y configuración de Cisco CSS Switch, puede configurar y utilizar Cisco Consultant. Consulte la documentación de Cisco CSS Switch para obtener instrucciones sobre la planificación y configuración.

El componente Consultant consta de lo siguiente:

- **lbcserver** contiene la información de configuración e interacciona con Cisco CSS Switch. El prefijo "lbc" significa "load-balancing consultant" (asesor de reparto del tráfico). lbcserver consta de:
 - El **ejecutor**, que contiene información de configuración y la información necesaria para conectar con Cisco CSS Switch.
 - El **gestor**, que genera valores de ponderación ("pesos") a partir de la información recogida y los envía a Cisco CSS Switch. El gestor obtiene información a partir de:
 - El Cisco CSS Switch
 - Servidores (utilizando los asesores)

Los asesores obtienen información sobre los servidores y analizan los resultados para cada protocolo antes de invocar al gestor para que defina los pesos apropiados. Actualmente, Cisco Consultant proporciona asesores tales como HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3 (y otros). También tiene la opción de escribir sus propios asesores (consulte "Creación de asesores personalizados (personalizables)" en la página 145). La utilización de asesores es opcional, pero recomendable.
 - Servidores (utilizando Metric Server)

Metric Server proporciona información a Consultant sobre el tráfico existente en los servidores, en forma de métricas específicas del sistema, y notifica el estado de los servidores. El gestor consulta al Metric Server que reside en cada servidor y asigna pesos para el reparto del tráfico utilizando las métricas recogidas por los agentes. Los resultados se colocan en el informe del gestor.
- Para configurar el ejecutor, los asesores y el gestor se proporciona una interfaz de línea de mandatos y una interfaz gráfica de usuario.
 - **lbccontrol** es la interfaz de línea de mandatos para Consultant.
 - **ndadmin** es la interfaz gráfica de usuario utilizada para configurar Consultant y supervisar su estado.

El gestor recoge información a partir del Cisco CSS Switch, los asesores y Metric Server. De acuerdo con la información que el gestor recibe, el gestor ajusta el valor de ponderación para los servidores de cada puerto y proporciona a Cisco CSS Switch la nueva ponderación para que la utilice en el reparto de conexiones nuevas. Cuando el gestor detecta que un servidor está inactivo, le asigna un peso 0 y el servidor se detiene. A partir de este momento, Cisco CSS Switch deja de reenviar tráfico hacia ese servidor.

Los asesores supervisan cada servidor del puerto asignado para determinar el tiempo de respuesta y la disponibilidad del servidor y luego proporcionan esta información al gestor. También controlan si un servidor está activo o inactivo.

Para configurar Consultant debidamente, la configuración debe corresponderse con la configuración de Cisco CSS Switch. Primero, consulte el manual *Cisco Services Switch Getting Started Guide* para configurar Cisco CSS Switch. Compruebe que Cisco Switch funciona correctamente y luego configure Consultant.

La configuración de Cisco CSS Switch consta de propietarios, normas de contenido y servicios que están en correspondencia con una configuración de Consultant, de esta manera:

Tabla 10. Términos de configuración de Consultant y Cisco CSS Switch

Cisco CSS Switch	Consultant
dirección IP virtual (VIP) de una o más de las normas de contenido del propietario	cluster
puerto contenido en la norma de contenido	puerto
servicio	servidor

El árbol de configuración de Consultant consta de:

- *Cluster*, que es un nombre que se puede resolver o una dirección decimal con puntos.
- *Puerto*, que es el número del puerto utilizado para el protocolo.
- *Servidores*.

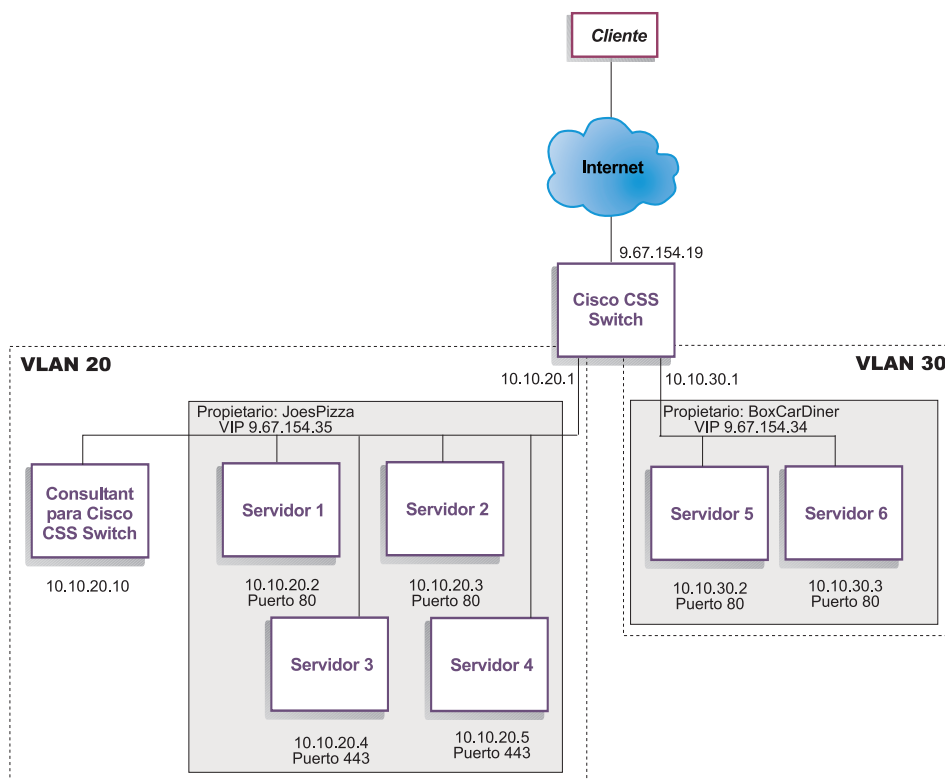


Figura 21. Ejemplo de Consultant configurado con 2 clusters, cada uno con 3 puertos

En la Figura 21:

- 9.67.154.19 es la conexión de red con Internet.
- Existen dos redes LAN virtuales configuradas (20 y 30)

Cuando configure el ejecutor, la dirección del ejecutor y el nombre de comunidad SNMP deben concordar con los atributos correspondientes de Cisco CSS Switch. Vea “lbcontrol ejecutor — controlar el ejecutor” en la página 355 para obtener información sobre cómo configurar el ejecutor.

Tabla 11. Ejemplo de configuración de Cisco CSS Switch y la correspondiente configuración de Consultant

Configuración de Cisco CSS Switch	Configuración de Consultant
username admin superuser snmp community <i>comunidad</i> private read-write	lbcontrol executor set address 10.10.20.1 lbcontrol executor set communityname <i>comunidad</i>
content rule1 port <i>80</i> balance weightedrr add service <i>servidor1</i> add service <i>servidor2</i> vip address <i>9.67.154.35</i> active	lbcontrol cluster add <i>9.67.154.35</i> lbcontrol port add 9.67.154.35: <i>80</i>
content rule 2 protocol tcp port <i>443</i> balance weightedrr add service servidor3 add service servidor4 vip address 9.67.154.35 active	lbcontrol port add 9.67.154.35: <i>443</i>
service servidor1 ip address <i>10.10.20.2</i> port <i>80</i> weight 4 active	lbcontrol server add 9.67.154.35: <i>80</i> :servidor1 address <i>10.10.20.2</i>
service servidor3 ip address <i>10.10.20.4</i> port <i>443</i> weight 4 active	lbcontrol server add 9.67.154.35: <i>443</i> :servidor3 address <i>10.10.20.4</i>

Capítulo 13. Configuración del componente Consultant para Cisco CSS Switches

Antes de seguir los pasos indicados en este capítulo, consulte el “Capítulo 12. Planificación para el componente Consultant para Cisco CSS Switches” en la página 119. Este capítulo explica cómo crear una configuración básica para el componente Consultant para Cisco CSS Switches de Network Dispatcher.

- Consulte el “Capítulo 14. Funciones avanzadas de Network Dispatcher” en la página 131 para ver configuraciones más complejas de Network Dispatcher.
- Consulte el “Capítulo 15. Utilización y gestión de Network Dispatcher” en la página 205 para conseguir información sobre la administración autenticada remota, los archivos de anotaciones de Network Dispatcher y la utilización de los componentes de Network Dispatcher.

Visión general de las tareas de configuración

Antes de comenzar cualquiera de las tareas de configuración de este capítulo:

1. Compruebe que Cisco CSS Switch y todos los servidores están configurados correctamente.
2. Configure Cisco Consultant; la dirección del ejecutor y el nombre de comunidad SNMP deben concordar con los atributos correspondientes de Cisco CSS Switch. Vea “Ibcontrol ejecutor — controlar el ejecutor” en la página 355 para obtener información sobre cómo configurar el ejecutor.

Tabla 12. Tareas de configuración para el componente Consultant para Cisco CSS Switches

Tarea	Descripción	Información relacionada
Configurar la máquina Consultant para Cisco CSS Switches.	Determinar los requisitos	“Configuración de la máquina Consultant para Cisco CSS Switches” en la página 128
Probar la configuración	Comprobar que la configuración es funcional	“Comprobación de la configuración” en la página 130

Métodos de configuración

Dispone de tres métodos para crear una configuración básica para el componente Consultant para Cisco CSS Switches de Network Dispatcher:

- Línea de mandatos
- Scripts
- Interfaz gráfica de usuario (GUI)

Línea de mandatos

Este es el medio más directo para configurar Cisco Consultant. Los procedimientos de este manual presuponen que se utiliza la línea de mandatos. Los valores de los parámetros de mandatos se deben escribir en caracteres ingleses. Las únicas excepciones son los nombres de sistema principal (utilizados, por ejemplo, en los mandatos para clusters y servidores) y los nombres de archivos.

Para iniciar Cisco Consultant desde la línea de mandatos:

- Emita el mandato **lbserver** desde el indicador de mandatos.

Nota: Para detener el servicio, emita lo siguiente: **lbserver stop**.

- A continuación, emita los mandatos de control de Cisco Consultant que desee para establecer la configuración. El mandato es **lbcontrol**. Para obtener más información acerca de los mandatos, consulte el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249.

Puede entrar los parámetros del mandato **lbcontrol** en su forma abreviada. Sólo necesita especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato “file save”, puede escribir **lbcontrol hf** en lugar de **lbcontrol help file**.

Para arrancar la interfaz de línea de mandatos, emita **lbcontrol** con el fin de recibir un indicador de mandatos de **lbcontrol**.

Para cerrar la interfaz de línea de mandatos, emita **exit** o **quit**.

Nota: En Windows 2000, el **ndserver** del componente Dispatcher se inicia automáticamente. Si sólo utiliza Cisco Consultant y no utiliza el componente Dispatcher, puede impedir que **ndserver** arranque automáticamente, de esta manera:

1. En la ventana Servicios de Windows 2000, pulse con el botón derecho del ratón sobre IBM Dispatcher.
2. Seleccione Propiedades.
3. En el campo **Tipo de arranque**, seleccione Manual.

4. Pulse Aceptar y cierre la ventana Servicios.

Scripts

Los mandatos para configurar Consultant para Cisco CSS Switches se pueden entrar en un archivo de script de configuración y ejecutarse juntos.

Nota: Para ejecutar rápidamente el contenido de un archivo de script (por ejemplo, *miscript*), utilice cualquiera de estos dos mandatos:

- Para actualizar la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:

```
lbccontrol file appendload miscript
```

- Para sustituir totalmente la configuración actual, ejecute los mandatos ejecutables del archivo de script utilizando:

```
lbccontrol file newload miscript
```

GUI

Para ver un ejemplo de la interfaz gráfica de usuario (GUI), consulte la Figura 2 en la página 5.

Para iniciar la GUI, siga estos pasos

1. Si *lbserver* no está ya en ejecución, inícielo ahora ejecutando el mandato siguiente como usuario root:

```
lbserver.
```

2. A continuación, siga uno de estos métodos:

- Para AIX, Linux o Solaris, especifique **ndadmin**
- Para Windows 2000, pulse **Inicio, Programas, IBM WebSphere, Edge Server, IBM Network Dispatcher** y finalmente **Network Dispatcher**

Para configurar el componente Cisco Consultant desde la GUI:

1. Pulse con el botón derecho del ratón sobre Cisco Consultant, en la estructura en árbol.
2. Conecte con un sistema principal
3. Cree clusters que contengan puertos y servidores
4. Inicie el gestor
5. Inicie asesores para el gestor

Puede utilizar la GUI para realizar cualquier acción que podría efectuar con el mandato **lbccontrol**. Por ejemplo, para definir un cluster desde la línea de mandatos, escriba el mandato **lbccontrol cluster add cluster**. Para definir un cluster desde la GUI, pulse el botón derecho del ratón sobre Ejecutor y luego seleccione **Añadir cluster**. Escriba la dirección del cluster en la ventana emergente, a continuación pulse en **Aceptar**.

Los archivos de configuración de Cisco Consultant preexistentes se pueden cargar utilizando las opciones **Cargar nueva configuración** (para sustituir totalmente la configuración actual) y **Añadir a configuración actual** (para actualizar la configuración actual); estas opciones aparecen en el menú emergente **Sistema principal**. Seleccione la opción **Guardar archivo de configuración como** para salvar periódicamente la configuración de Cisco Consultant en un archivo. Pulse **Archivo**, en la barra de menús, para guardar las conexiones actuales de sistema principal en un archivo, o para restaurar las conexiones de archivos existentes en todos componentes de Network Dispatcher.

Para acceder a la **Ayuda**, pulse el icono de signo de interrogación, situado en la esquina superior derecha de la ventana de Network Dispatcher.

- **Ayuda para campos** — describe cada campo y sus valores por omisión
- **Cómo puedo** — lista tareas que pueden efectuarse desde esa pantalla
- **Contenido** — es una tabla de contenido de toda la información de la Ayuda
- **Índice** — es un índice alfabético de temas de la Ayuda

Para obtener más información acerca de la utilización de la GUI, consulte “Instrucciones generales para la utilización de la GUI” en la página 6.

Configuración de la máquina Consultant para Cisco CSS Switches

Para configurar la máquina Consultant para Cisco CSS Switches, debe ser el usuario root (en AIX, Linux o Solaris) o el administrador en Windows 2000.

Consultant debe poder conectar con Cisco CSS Switch como administrador de Cisco CSS Switch.

Cuando configure el ejecutor, la dirección del ejecutor y el nombre de comunidad SNMP deben concordar con los atributos correspondientes de Cisco CSS Switch.

Si desea obtener ayuda sobre los mandatos utilizados en este procedimiento, consulte el “Apéndice E. Consulta de mandatos de Consultant para Cisco CSS Switches” en la página 347.

Paso 1. Iniciar la función de servidor

Si lbcserv no está ya en ejecución, inícielo ahora ejecutando el mandato siguiente como usuario root:

lbcserv

Paso 2. Configurar la función del ejecutor

Debe configurar una dirección para el ejecutor y un nombre de comunidad SNMP. Estos valores deben concordar con los atributos correspondientes de Cisco CSS Switch.

Paso 3. Definir un cluster y establecer las opciones de cluster

Cluster es un nombre que se puede resolver o una dirección decimal con puntos. El cluster corresponde a la dirección IP virtual de Cisco CSS Switch contenida en una norma de contenido para un propietario.

Para definir un cluster, escriba **lbcontrol cluster add *cluster***. Para establecer opciones para el cluster, escriba **lbcontrol cluster set**.

Paso 4. Definir los puertos y establecer las opciones de puerto

Para definir un puerto, escriba **lbcontrol port add *cluster:puerto***. El puerto corresponde al puerto configurado en la norma de contenido de Cisco CSS Switch para el propietario.

Puerto es el número del puerto utilizado para el protocolo, tal como especifica la norma de contenido de Cisco CSS Switch para el propietario. En “lbcontrol port — configurar puertos” en la página 370 hallará más información.

Paso 5. Definir servidores con reparto del tráfico

Puede configurar varias instancias del mismo servidor dentro de cualquier cluster y puerto. (Recuerde que la dirección y el nombre de comunidad SNMP deben concordar con los atributos correspondientes de Cisco CSS Switch). Si configura varias instancias del mismo servidor, podrá definir servidores de aplicaciones diferentes que residen en la misma máquina física y tienen la misma dirección IP en el mismo puerto.

Para definir un servidor con reparto del tráfico, escriba:

```
lbcontrol server add cluster:puerto:servidor address x.x.x.x |  
nombre_sistema_principal
```

El *servidor* corresponde al nombre del servicio de Cisco CSS Switch.

Debe definir más de un servidor para un puerto de un cluster para realizar el reparto del tráfico, de lo contrario el tráfico se dirigirá a un solo servidor. Consulte “Particionamiento del servidor: servidores lógicos configurados para un solo servidor físico (dirección IP)” en la página 152.

Para obtener más información sobre la sintaxis del mandato “lbcontrol server”, consulte “lbcontrol server — configurar servidores” en la página 372.

Paso 6. Iniciar la función del gestor

Para iniciar el gestor, escriba el mandato **lbcontrol manager start**. En “lbcontrol manager — controlar el gestor” en la página 362 hallará más información.

Paso 7. Iniciar la función del asesor (opcional)

Los asesores facilitan al gestor más información sobre la capacidad de las máquinas servidor con reparto del tráfico para responder a las peticiones. Cada asesor es específico de un protocolo. Por ejemplo, para iniciar el asesor HTTP, emita el mandato siguiente:

```
lbcontrol advisor start http puerto
```

Si desea obtener una lista de los asesores junto con sus puertos por omisión, consulte el “lbcontrol advisor — controlar el asesor” en la página 348. Si desea ver una descripción de cada asesor, consulte la sección “Lista de asesores” en la página 143.

Paso 8. Establecer las proporciones del cluster según sea necesario

Si inicia cualquier asesor, debe cambiar las proporciones del cluster para que la información procedente del asesor se utilice en la toma de decisiones sobre reparto del tráfico. Para ello utilice el mandato **lbcontrol cluster proportions**. Consulte “Grado de importancia dado a la información de estado” en la página 135.

Nota: Si inicia un asesor y la **Proporción dada a la métrica del sistema** es 0, este valor se incrementa a 1. Debido a que la suma de proporciones del cluster debe ser 100, en este caso, la proporción con el valor más alto se reduce en 1.

Paso 9. Iniciar Metric Server (opcional)

En “Metric Server” en la página 150 hallará información sobre el uso de Metric Server.

Comprobación de la configuración

Efectúe unas pruebas para comprobar que la configuración funciona.

1. Establezca en 4 el nivel de registro de anotaciones (loglevel) del gestor.
2. Desconecte un servidor de Cisco CSS Switch durante un minuto *o bien* cierre el servidor de aplicaciones durante un minuto.
3. Vuelva a conectar el servidor o reinicie el servidor de aplicaciones.
4. Vuelva a establecer el valor loglevel del servidor en el nivel deseado (1).
5. Visualice el archivo manager.log del directorio .../nd/servers/logs/lbc, y busque **setServerWeights setting service**.

Capítulo 14. Funciones avanzadas de Network Dispatcher

Este capítulo describe cómo configurar los parámetros de reparto del tráfico de Network Dispatcher y cómo configurar Network Dispatcher para funciones avanzadas.

Nota: Si *no* está utilizando el componente Dispatcher, las referencias en este capítulo referentes a "ndcontrol" se deben sustituir por lo siguiente:

- Para CBR, utilice **cbrcontrol**
- Para Mailbox Locator, utilice **mlcontrol**
- Para Site Selector, utilice **sscontrol** (consulte el "Apéndice D. Consulta de mandatos de Site Selector" en la página 317)
- Para Cisco Consultant, utilice **lbcontrol** (consulte el "Apéndice E. Consulta de mandatos de Consultant para Cisco CSS Switches" en la página 347)

Tabla 13. Tareas avanzadas de configuración para Network Dispatcher

Tarea	Descripción	Información asociada
Opcionalmente, cambiar los valores de reparto del tráfico	<p>Puede cambiar los valores de reparto del tráfico siguientes:</p> <ul style="list-style-type: none">• Grado de importancia dado a la información de estado <p>Las proporciones por omisión son 50-50-0-0. Si utiliza el valor por omisión, no se utiliza la información procedente de los asesores ni de Metric Server.</p> <ul style="list-style-type: none">• Pesos• Pesos fijos del gestor• Intervalos del gestor• Umbral de sensibilidad• Índice de corrección	"Optimización del reparto del tráfico proporcionado por Network Dispatcher" en la página 134
Utilizar scripts para generar una alerta o registrar un error de servidor cuando el gestor marca un servidor como inactivo/activo	Network Dispatcher proporciona salidas de usuario que provocan la ejecución de scripts personalizables cuando el gestor marca un servidor como inactivo/activo	"Utilización de scripts para generar una alerta o registrar un error de servidor" en la página 139

Tabla 13. Tareas avanzadas de configuración para Network Dispatcher (continuación)

Tarea	Descripción	Información asociada
Utilizar asesores y crear asesores personalizados	Describe los asesores y cómo escribir sus propios asesores personalizados para informar sobre estados determinados de los servidores	“Asesores” en la página 139 “Creación de asesores personalizados (personalizables)” en la página 145
Utilizar el asesor de Workload Manager (WLM)	El asesor de WLM proporciona información sobre el tráfico del sistema a Network Dispatcher	“Asesor de Workload Manager” en la página 149
Utilizar el agente de Metric Server	Metric Server proporciona información sobre el tráfico del sistema a Network Dispatcher	“Metric Server” en la página 150
Utilizar el particionamiento del servidor	Defina servidores lógicos para repartir el tráfico basándose en los servicios proporcionados	“Particionamiento del servidor: servidores lógicos configurados para un solo servidor físico (dirección IP)” en la página 152
Utilizar la opción de petición/respuesta del asesor (URL)	Defina un URL exclusivo para un cliente HTTP, que sea específico del servicio que desea consultar en la máquina.	“Opción de petición/respuesta del asesor HTTP (URL)” en la página 154
Instalar Network Dispatcher en la máquina donde realiza reparto del tráfico	Configure un máquina de Network Dispatcher de ubicación compartida.	“Utilización de servidores de ubicación compartida” en la página 155
Configurar el soporte de Dispatcher para una zona geográfica amplia	Configure un Dispatcher remoto para repartir el tráfico en una red de área amplia. O bien, reparta el tráfico en una red de área amplia (sin un Dispatcher remoto) utilizando una plataforma de servidor que dé soporte a GRE.	“Configurar el soporte de Dispatcher para área amplia” en la página 157
Configurar la modalidad de alta disponibilidad o de alta disponibilidad mutua	Configure una segunda máquina Dispatcher para proporcionar una unidad de reserva.	“Alta disponibilidad” en la página 165
Configurar el reparto del tráfico basado en normas	Defina las condiciones para las que se utilizará un subconjunto de los servidores.	“Configurar el reparto del tráfico basado en normas” en la página 173
Utilizar enlaces explícitos	Evite eludir el Dispatcher en los enlaces.	“Utilización de enlaces explícitos” en la página 183
Utilizar una red privada	Configure el Dispatcher para repartir el tráfico de los servidores en una red privada.	“Utilización de una configuración de red privada” en la página 184

Tabla 13. Tareas avanzadas de configuración para Network Dispatcher (continuación)

Tarea	Descripción	Información asociada
Utilizar un cluster comodín para combinar configuraciones de servidores habituales	Las direcciones que no están configuradas explícitamente utilizarán el cluster comodín como medio para repartir el tráfico.	“Utilizar el cluster comodín para combinar configuraciones de servidores” en la página 185
Utilizar el cluster comodín para repartir el tráfico de los cortafuegos	Todo el tráfico se repartirá hacia los cortafuegos.	“Utilizar el cluster comodín para repartir el tráfico de los cortafuegos” en la página 186
Utilizar el cluster comodín con Caching Proxy para el proxy transparente	Permite utilizar Dispatcher para habilitar un proxy transparente.	“Utilización del cluster comodín con Caching Proxy para proxy transparente” en la página 187
Utilizar el puerto comodín para gestionar el tráfico no configurado de los puertos	Gestiona el tráfico que no está configurado para ningún puerto específico.	“Utilización del puerto comodín para dirigir el tráfico de puertos no configurados” en la página 187
Utilizar la función de persistencia para configurar un puerto de cluster que sea persistente	Permite dirigir las peticiones de los clientes hacia el mismo servidor.	“La función de afinidad de Network Dispatcher” en la página 188
Utilizar la API de SDA (Server Directed Affinity)	Proporciona una API que permite a un agente externo influir en el comportamiento de afinidad de Dispatcher	“API de afinidad dirigida por el servidor (SDA) para controlar la afinidad cliente-servidor” en la página 188
Utilizar la afinidad entre puertos para que la función de persistencia (afinidad) abarque varios puertos	Permite dirigir hacia el mismo servidor las peticiones de los clientes procedentes de puertos diferentes.	“Afinidad entre puertos” en la página 189
Utilizar la máscara de dirección de afinidad para designar una dirección de subred IP común	Permite dirigir hacia el mismo servidor las peticiones de los clientes procedentes de la misma subred.	“Máscara de dirección de afinidad” en la página 190
Utilizar la alteración temporal de afinidad de norma para que un servidor pueda alterar temporalmente la función de persistencia del puerto	Permite que un servidor altere temporalmente el valor de persistencia para su puerto.	“Alteración temporal de afinidad de norma” en la página 191
Utilizar la afinidad de cookie activa con el objeto de repartir el tráfico de los servidores para CBR	Es una opción de norma que permite que una sesión mantenga la afinidad para un servidor determinado.	“Afinidad activa de cookie” en la página 193

Tabla 13. Tareas avanzadas de configuración para Network Dispatcher (continuación)

Tarea	Descripción	Información asociada
Utilizar la afinidad de cookie pasiva para repartir el tráfico de servidores para el encaminamiento por contenido de Dispatcher y el componente CBR	Es una opción de norma que permite que una sesión mantenga la afinidad para un servidor determinado basándose en el nombre de cookie/valor de cookie.	“Afinidad pasiva de cookie” en la página 194
Utilizar la afinidad de URI para repartir el tráfico entre servidores Caching Proxy, con contenido exclusivo que se debe almacenar en cada servidor	Es una opción de norma que permite que una sesión mantenga la afinidad para un servidor determinado basándose en el URI.	“Afinidad de URI” en la página 195
Utilizar la detección de “ataques de denegación de servicio” para informar al administrador (mediante una alerta) sobre posibles ataques.	Dispatcher comprueba si las peticiones entrantes contienen una cantidad importante de conexiones TCP semiabiertas en los servidores.	“Detección de ataques de denegación de servicio” en la página 197
Utilizar las anotaciones en binario para analizar datos estadísticos de servidores	Permite almacenar información sobre servidores en archivos binarios y recuperarla de ellos.	“Utilizar las anotaciones en binario para analizar las estadísticas del servidor” en la página 198
Utilizar Cisco Consultant (información adicional)	Cómo Cisco Consultant interactúa con Cisco CSS Switch e información adicional sobre la configuración de pesos.	“Información adicional sobre las funciones avanzadas de Cisco Consultant” en la página 200

Optimización del reparto del tráfico proporcionado por Network Dispatcher

La función de gestor de Network Dispatcher realiza reparto del tráfico basándose en los valores siguientes:

- “Grado de importancia dado a la información de estado” en la página 135
- “Pesos” en la página 136
- “Intervalos de gestor” en la página 137
- “Intervalos de asesor” en la página 141
- “Tiempo de caducidad del informe del asesor” en la página 142
- “Umbral de sensibilidad” en la página 138
- “Índice de corrección” en la página 138

Se pueden cambiar estos valores para optimizar el reparto del tráfico de la red.

Grado de importancia dado a la información de estado

El gestor puede utilizar algunos o todos los factores externos siguientes en sus decisiones ponderadas:

- *Conexiones activas*: número de conexiones activas de cada máquina servidor sujeta a reparto del tráfico (según el seguimiento realizado por el ejecutor). Esta proporción no es aplicable a Site Selector.

O bien

Cpu: porcentaje de CPU en uso en cada máquina servidor sujeta a reparto del tráfico (datos de entrada procedentes del agente de Metric Server). Para Site Selector solamente, esta proporción sustituye a la columna de la proporción de conexiones activas.

- *Conexiones nuevas*: número de conexiones nuevas en cada máquina servidor sujeta a reparto del tráfico (según el seguimiento realizado por el ejecutor). Esta proporción no es aplicable a Site Selector.

O bien

Memoria: porcentaje de memoria ocupada en cada servidor de reparto del tráfico (información procedentes del agente de Metric Server). Para Site Selector solamente, esta proporción aparece en lugar de la columna de proporción para conexiones nuevas.

- *Específico de puerto*: información procedente de asesores que están a la escucha en el puerto.
- *Métrica del sistema*: información procedente de herramientas de supervisión del sistema, tales como Metric Server o WLM.

Junto con el peso actual de cada servidor e información de otro tipo necesaria para realizar cálculos, el gestor obtiene los dos primeros valores (conexiones activas y conexiones nuevas) a partir del ejecutor. Dichos valores están basados en la información que genera y almacena internamente el ejecutor.

Nota: Para Site Selector, el gestor obtiene los dos primeros valores (cpu y memoria) a partir de Metric Server. Para Cisco Consultant, el gestor obtiene los dos primeros valores (conexiones activas y conexiones nuevas) a partir de Cisco CSS Switch.

Puede cambiar la proporción de importancia relativa de los cuatro valores para cada cluster (o nombre de sitio). Considere las proporciones como porcentajes; la suma de las proporciones relativas debe ser igual a 100%. La proporción por omisión es 50/50/0/0, que no tiene en cuenta la información de los asesores ni del sistema. En su entorno, puede ser necesario probar diferentes proporciones para encontrar la que produzca los mejores resultados.

Nota: Cuando se añade un asesor (distinto de WLM), si la **proporción de puerto** es 0, el gestor aumenta este valor a 1. Debido a que la suma de las proporciones relativas debe ser igual a 100, el valor más alto se reduce en 1.

Cuando se añade el asesor WLM, si la **proporción de métrica del sistema** es 0, el gestor aumenta este valor a 1. Debido a que la suma de las proporciones relativas debe ser igual a 100, el valor más alto se reduce en 1.

El número de conexiones activas depende del número de clientes, así como de por cuánto tiempo se necesita utilizar los servicios que ofrecen las máquinas servidor de reparto del tráfico. Si las conexiones de los clientes son rápidas (como por ejemplo, las realizadas a páginas Web pequeñas con HTTP GET), el número de conexiones activas será bastante bajo. Si las conexiones de los clientes son más lentas (como por ejemplo, una consulta de base de datos), el número de conexiones activas será más elevado.

Evite establecer valores demasiado bajos para las proporciones de conexiones activas y conexiones nuevas. Inhabilitará las funciones de reparto del tráfico y corrección de medidas de Dispatcher a menos que estos dos primeros valores sean 20 como mínimo, cada uno.

Para establecer la proporción de valores de importancia, utilice el mandato **ndcontrol cluster set cluster proportions**. En “ndcontrol cluster — configurar clusters” en la página 258 hallará más información.

Pesos

Nota: Si está utilizando el componente Cisco Consultant, vea la información adicional de “Pesos de Cisco Consultant” en la página 202.

El gestor establece pesos basándose en contadores internos del ejecutor, en información recibida de los asesores y en información procedente de un programa de supervisión del sistema, tal como Metric Server. Si desea establecer pesos manualmente mientras ejecuta el gestor, especifique la opción **fixedweight** en el mandato “ndcontrol server”. Para obtener una descripción de la opción **fixedweight**, consulte “Pesos fijos del gestor” en la página 137.

Los pesos se aplican a todos los servidores de un puerto. En un puerto determinado, las peticiones se distribuirán entre los servidores según el peso relativo que tengan entre sí. Por ejemplo, si un servidor tiene establecido 10 como peso y otro tiene 5, el servidor con 10 debe obtener el doble de peticiones que el servidor con 5.

Para especificar el peso máximo que puede tener un servidor, emita el mandato **ndcontrol port set weightbound**. Este mandato afecta a la diferencia que puede existir entre el número de peticiones que recibirá cada servidor. Si establece el peso máximo en 1, todos los servidores pueden tener 1 como peso, 0 si están detenidos o -1 si están marcados como inactivos. Cuanto más alto sea este número, mayor será la diferencia de pesos para los servidores. Con un peso máximo de 2, un servidor podría recibir el doble de peticiones que otro. Con un peso máximo de 10, un servidor podría recibir diez veces más peticiones que otro. El peso máximo por omisión es 20.

Si un asesor detecta que un servidor está fuera de servicio, informa al gestor y éste asigna el peso 0 al servidor. Como resultado, el ejecutor no enviará más conexiones a ese servidor mientras el peso siga siendo 0. Si había alguna conexión activa con el servidor antes de que cambiase el peso, se dejará que finalice con normalidad.

Pesos fijos del gestor

Si no se utiliza el gestor, no se pueden ejecutar asesores y no pueden detectar si un servidor está inactivo. Si decide ejecutar los asesores, pero *no* desea que el gestor actualice el peso que ha definido para un servidor determinado, utilice la opción **fixedweight** en el mandato "ndcontrol server". Por ejemplo:

```
ndcontrol server set cluster:puerto:servidor fixedweight yes
```

Después de establecer **fixedweight** en "yes", utilice el mandato **ndcontrol server set weight** para establecer el peso en el valor que desee. El valor de peso del servidor permanecerá fijo mientras se ejecute el gestor hasta que emita otro mandato "ndcontrol server" con **fixedweight** establecido en "no". Para obtener más información, consulte "ndcontrol server — configurar servidores" en la página 302.

Intervalos de gestor

Para optimizar el rendimiento global, se restringe la frecuencia con que el gestor puede interactuar con el ejecutor. Se pueden realizar cambios en este intervalo entrando los mandatos **ndcontrol manager interval** y **ndcontrol manager refresh**.

El intervalo de gestor especifica con qué frecuencia actualizará el gestor los pesos de los servidores que utiliza el ejecutor para encaminar las conexiones. Si es demasiado bajo, puede producir un bajo rendimiento, como resultado de las constantes interrupciones que sufre el ejecutor por parte del gestor. Si es demasiado alto, puede ser que el encaminamiento de las peticiones que efectúa el ejecutor no esté basado en una información precisa y actualizada.

Por ejemplo, para establecer 1 segundo como intervalo de gestor, entre el mandato siguiente:

```
ndcontrol manager interval 1
```

El ciclo de renovación del gestor especifica con qué frecuencia pedirá el gestor información de estado al ejecutor. El ciclo de renovación está basado en los intervalos.

Por ejemplo, para establecer 3 como ciclo de renovación del gestor, entre el mandato siguiente:

```
ndcontrol manager refresh 3
```

Con ello se consigue que el gestor espere por espacio de 3 intervalos antes de pedir el estado al ejecutor.

Umbral de sensibilidad

Network Dispatcher proporciona otros métodos para que pueda optimizar el reparto del tráfico para los servidores. Para trabajar a pleno rendimiento, los pesos de los servidores sólo se actualizan si han cambiado significativamente. Actualizar de forma constante los pesos si no se produce apenas ningún cambio, o ninguno, en el estado del servidor, aumenta de forma innecesaria el volumen de actividad general. Cuando el porcentaje de cambios en el peso total de todos los servidores de un puerto es superior al umbral de sensibilidad, el gestor actualiza los pesos que el ejecutor utiliza para distribuir las conexiones. Por ejemplo, suponga que el peso total cambia de 100 a 105. El cambio es del 5%. Con el umbral de sensibilidad establecido en 5, el gestor no actualizará los pesos utilizados por el ejecutor, ya que el porcentaje de cambio no es **superior** al umbral. Sin embargo, si el peso total cambia de 100 a 106, el gestor actualizará los pesos. Para establecer el valor del umbral de sensibilidad del gestor en un valor diferente al valor por omisión (por ejemplo 6), entre el siguiente mandato:

```
ndcontrol manager sensitivity 6
```

En la mayoría de casos, no necesitará cambiar este valor.

Índice de corrección

El gestor calcula el peso de los servidores de forma dinámica. Como resultado, un peso actualizado puede diferir bastante del anterior. En la mayoría de los casos, eso no significa ningún problema. Sin embargo, esto puede provocar ocasionalmente un efecto de oscilación en la manera en que se reparte el tráfico de peticiones. Por ejemplo, un servidor puede acabar recibiendo la mayoría de las peticiones debido a un peso alto. El gestor verá que el servidor tiene un número elevado de conexiones activas y que responde con lentitud. Trasladará entonces el peso a los servidores libres y se producirá el mismo efecto en ellos, lo que desemboca en un uso no eficaz de los recursos.

Para aliviar este problema, el gestor utiliza un índice de corrección. El índice de corrección limita cuánto puede cambiar el peso de un servidor, con lo que se corrige de forma efectiva el cambio en la distribución de las peticiones.

Cuanto más alto sea el índice de corrección, menos radicalmente cambiarán los pesos de los servidores. Cuanto más bajo sea el índice de corrección, más radicalmente cambiarán los pesos de los servidores. El valor por omisión del índice de corrección es 1,5. Con 1,5, los pesos de los servidores pueden ser bastante dinámicos. Si el índice es 4 ó 5, los pesos serán más estables. Por ejemplo, para establecer 4 como índice de corrección, entre el mandato siguiente:

```
ndcontrol manager smoothing 4
```

En la mayoría de casos, no necesitará cambiar este valor.

Utilización de scripts para generar una alerta o registrar un error de servidor

Network Dispatcher proporciona salidas de usuario que provocan la ejecución de scripts personalizables. Puede crear estos scripts para realizar acciones automatizadas, tales como avisar al administrador cuando el gestor marque un servidor como inactivo o simplemente registrar el evento del error. El directorio de instalación **...nd/servers/samples** contiene scripts de ejemplo que puede personalizar. Para poder ejecutar los archivos de script, debe trasladarlos al directorio **...nd/servers/bin** y eliminar la extensión de archivo ".sample". Se proporcionan los scripts de ejemplo siguientes:

- **serverDown** — el gestor marca un servidor como inactivo.
- **serverUp** — el gestor marca un servidor como activo.
- **managerAlert** — todos los servidores se marcan como inactivos para un puerto determinado.
- **managerClear** — como mínimo un servidor está ahora activo, después de haberlos marcado todos como inactivos para un puerto determinado.

Asesores

Los asesores son agentes dentro de Network Dispatcher. Su finalidad es evaluar el estado y el tráfico de los servidores. Esto lo llevan a cabo mediante un intercambio de datos proactivo similar al existente entre un servidor y un cliente. Los asesores pueden considerarse clientes ligeros de los servidores de aplicaciones.

El producto proporciona varios asesores de protocolos específicos para los protocolos más comunes. Sin embargo, no es útil utilizar para cada componente de Network Dispatcher todos los asesores proporcionados. (Por ejemplo, no es aconsejable utilizar el asesor Telnet con el componente CBR). Network Dispatcher también da soporte al concepto de "asesor personalizado", que permite al usuario escribir sus propios asesores.

Limitación para las aplicaciones del servidor de vinculación específica en Linux: Para Linux, Network Dispatcher no da soporte al uso de asesores

cuando se distribuye el tráfico de servidores con aplicaciones del servidor de vinculación específica (incluidos otros componentes de Network Dispatcher como Mailbox Locator o Site Selector) que se vinculan a la dirección IP del cluster.

Cómo funcionan los asesores

Los asesores abren periódicamente una conexión TCP con cada servidor y envían un mensaje de petición al servidor. El contenido del mensaje es específico del protocolo que se ejecuta en el servidor. Por ejemplo, el asesor HTTP envía una petición "HEAD" de HTTP al servidor.

Los asesores esperan entonces una respuesta del servidor. Después de obtener la respuesta, el asesor hace una valoración del servidor. Para calcular este valor de "tráfico", la mayoría de asesores miden el tiempo que tarda el servidor en responder, y después utilizan este valor (en milisegundos) como valor de tráfico.

Entonces, los asesores informan del valor de tráfico a la función del gestor, donde aparece en la columna "Puerto" en el informe del gestor. El gestor calcula entonces los valores de peso agregados a partir de todas sus fuentes de datos, según sus proporciones, y establece estos valores de peso en la función del ejecutor. El Ejecutor utilizará entonces estos pesos para el reparto del tráfico de nuevas conexiones entrantes de clientes.

Si el asesor determina que un servidor está activo y en buen estado, se lo notificará al gestor con un número de tráfico positivo sin ceros. Si el asesor determina que un servidor no está activo, devolverá un valor de tráfico especial de uno negativo (-1). El Gestor y el Ejecutor no reenviarán las posibles conexiones a ese servidor.

Inicio y detención de un asesor

Puede iniciar un asesor para un determinado puerto en todos los clusters (asesor de grupo). O puede ejecutar asesores diferentes para el mismo puerto, pero en clusters diferentes (asesor específico de cluster/sitio). Por ejemplo, si ha definido Network Dispatcher con tres clusters (*clusterA*, *clusterB*, *clusterC*), con el puerto 80 en cada uno, puede hacer lo siguiente:

- Asesor específico de cluster/sitio: para iniciar un asesor en el puerto 80 del *clusterA*, especifique el cluster y el puerto:
`ndcontrol advisor start http clusterA:80`

Este mandato inicia el asesor http en el puerto 80 del *clusterA*. El asesor http informará sobre todos los servidores conectados al puerto 80 de *clusterA*.

- Asesor de grupo: para iniciar un asesor personalizado en el puerto 80 para todos los demás clusters, sólo especifique el puerto:

```
ndcontrol  
advisor start ADV_custom 80
```

Este mandato inicia el asesor *ADV_custom* en el puerto 80 de *clusterB* y *clusterC*. Este asesor personalizado informará sobre todos los servidores conectados al puerto 80 de *clusterB* y *clusterC*. (Para obtener más información sobre los asesores personalizados, consulte “Creación de asesores personalizados (personalizables)” en la página 145).

Nota: El asesor de grupo proporciona información para todos los clusters/sitios que no tienen actualmente un asesor específico de cluster/sitio.

En el ejemplo anterior de configuración del asesor de grupo, puede elegir detener el asesor personalizado *ADV_custom* para el puerto 80 de uno solo de los clusters o de ambos (*clusterB* y *clusterC*).

- Para detener el asesor personalizado para el puerto 80 solamente en *clusterB*, especifique el cluster y el puerto:

```
ndcontrol advisor stop ADV_custom clusterB:80
```
- Para detener el asesor personalizado para el puerto 80 en *clusterB* y *clusterC*, especifique sólo el puerto:

```
ndcontrol advisor stop ADV_custom 80
```

Intervalos de asesor

Nota: Los valores por omisión del asesor deben funcionar adecuadamente en la gran mayoría de las situaciones posibles. Tenga cuidado al entrar valores distintos a los valores por omisión.

El intervalo de asesor establece con qué frecuencia pregunta un asesor el estado a los servidores del puerto que está supervisando y, a continuación, notifica los resultados al gestor. Si es demasiado bajo, puede producir un bajo rendimiento, como resultado de las constantes interrupciones que sufren los servidores por parte de los asesores. Si es demasiado alto, puede ser que las decisiones que tome el gestor en lo que respecta a los pesos no estén basadas en una información precisa y actualizada.

Por ejemplo, para establecer 3 segundos como intervalo del asesor HTTP para el puerto 80, entre el mandato siguiente:

```
ndcontrol advisor interval http 80 3
```

No es útil especificar un intervalo de asesor que sea menor que el intervalo de gestor. El intervalo de gestor por omisión es siete segundos.

Tiempo de caducidad del informe del asesor

Para asegurarse de que el gestor no utilice información obsoleta en sus decisiones referentes al reparto del tráfico, el gestor no utiliza información procedente de un asesor cuya indicación horaria exceda la hora de caducidad del informe del asesor. El intervalo de caducidad del informe del asesor debe ser mayor que el intervalo de sondeo del asesor. Si el intervalo es menor, el gestor no tendrá en cuenta los informes que por lógica deberían utilizarse. Por omisión, los informes del asesor no caducan; es decir, su intervalo de caducidad predeterminado es ilimitado.

Por ejemplo, para establecer en 30 segundos el intervalo de caducidad del asesor HTTP para el puerto 80, entre este mandato:

```
ndcontrol advisor timeout http 80 30
```

Para obtener más información sobre cómo definir el intervalo de caducidad del informe del asesor, consulte “ndcontrol advisor — controlar el asesor” en la página 252.

Tiempo de espera de conexión y de recepción del asesor para servidores

En Network Dispatcher, puede definir los tiempos de espera para los que el asesor detecta si un servidor ha fallado. Los tiempos de espera para servidores anómalos (connecttimeout y receivetimeout) determinan cuánto tiempo espera un asesor antes de notificar que ha fallado una operación de conexión o recepción.

Si desea que la detección de servidores anómalos sea lo más rápida posible, establezca los tiempos de espera de conexión y recepción en el valor más bajo (1 segundo), y haga lo mismo para el intervalo de tiempo del asesor y del gestor.

Nota: Si el entorno experimenta un volumen de tráfico mediano o alto y ello provoca un aumento del tiempo de respuesta de los servidores, tenga cuidado de no asignar un valor demasiado bajo para connecttimeout y receivetimeout, de lo contrario el asesor podría marcar prematuramente como anómalo un servidor ocupado.

Por ejemplo, para establecer en 9 segundos los valores connecttimeout y receivetimeout para el asesor HTTP en el puerto 80, escriba este mandato:

```
ndcontrol advisor connecttimeout http 80 9
ndcontrol advisor receivetimeout http 80 9
```

Los tiempos de espera de conexión y recepción predefinidos son 3 veces el valor especificado para el intervalo del asesor.

Lista de asesores

- El asesor **HTTP** abre una conexión, envía una petición HEAD por omisión, espera una conexión de respuesta y devuelve el tiempo transcurrido como valor de tráfico. Consulte “Opción de petición/respuesta del asesor HTTP (URL)” en la página 154 para obtener más información sobre cómo cambiar el tipo de petición que envía el asesor HTTP.
- El asesor **FTP** abre una conexión, envía una petición SYST, espera una respuesta, cierra la conexión y devuelve el tiempo transcurrido como valor de tráfico.
- El asesor **Telnet** abre una conexión, espera un mensaje inicial del servidor, cierra la conexión y devuelve el tiempo transcurrido como valor de tráfico.
- El asesor **NNTP** abre una conexión, espera un mensaje inicial del servidor, envía un mandato para finalizar, cierra la conexión y devuelve el tiempo transcurrido como valor de tráfico.
- El asesor **IMAP** abre una conexión, espera un mensaje inicial del servidor, envía un mandato para finalizar, cierra la conexión y devuelve el tiempo transcurrido como valor de tráfico.
- El asesor **POP3** abre una conexión, espera un mensaje inicial del servidor, envía un mandato para finalizar, cierra la conexión y devuelve el tiempo transcurrido como valor de tráfico.
- El asesor **SMTP** abre una conexión, espera un mensaje inicial del servidor, envía un mandato para finalizar, cierra la conexión y devuelve el tiempo transcurrido como valor de tráfico.
- El asesor **SSL** abre una conexión, envía una petición CLIENT HELLO, espera una respuesta, cierra la conexión y devuelve el tiempo transcurrido como valor de tráfico.

Nota: El asesor SSL no depende de la gestión de claves o certificados.

- El asesor **ssl2http** arranca e informa sobre los servidores listados para el puerto 443, pero el asesor abre un socket con “mapport” para las peticiones HTTP. Sólo utilice el asesor ssl2http para CBR si el protocolo cliente-proxy es SSL y el protocolo proxy-servidor es HTTP. Consulte “Reparto del tráfico entre el cliente y el proxy en CBR y entre el proxy y el servidor en HTTP” en la página 78, para obtener más información.
- El asesor Caching Proxy (**ibmproxy**) abre una conexión, envía una petición GET de HTTP, específica de Caching Proxy, e interpreta la respuesta como tráfico de Caching Proxy.

Nota: Cuando se utiliza el asesor ibmproxy, Caching Proxy debe estar en ejecución en todos los servidores sujetos a reparto del tráfico. No es necesario que Caching Proxy esté instalado en la máquina donde reside Network Dispatcher a menos que éste se encuentre en la máquina que realiza el reparto del tráfico.

- El asesor **DNS** abre una conexión, envía una consulta de puntero para DNS, espera una respuesta, cierra la conexión y devuelve el tiempo transcurrido como valor de tráfico.
- El asesor **connect** no intercambia datos específicos del protocolo con el servidor. Simplemente mide el tiempo que tarda en abrir y cerrar una conexión TCP con el servidor. Este asesor es útil para aplicaciones de servidores que utilizan TCP, pero con un protocolo de nivel mayor para el que el asesor personalizado o proporcionado por IBM no está disponible.
- El asesor **ping** no abre una conexión TCP con los servidores; en lugar de esto notifica si el servidor responde a un mensaje de sondeo (ping). Aunque el asesor ping se puede utilizar en cualquier puerto, se ha diseñado para configuraciones que utilizan el puerto comodín, en el cual puede estar circulando tráfico de diferentes protocolos. También es útil para configuraciones que utilizan protocolos que no son TCP con sus servidores, como UDP.
- El asesor **reach** envía mensajes de sondeo a sus máquinas de destino. Este asesor se ha diseñado para que los componentes de alta disponibilidad de Dispatcher determinen la accesibilidad de sus “destinos de acceso”. Sus resultados pasan al componente de alta disponibilidad y no aparecen en el informe del gestor. A diferencia de los demás asesores, el asesor “reach” es iniciado *automáticamente* por el gestor del componente Dispatcher.
- El asesor **DB2** trabaja en combinación con los servidores DB2. Dispatcher tiene la capacidad interna de comprobar el estado de los servidores DB2 sin que el usuario deba escribir sus propios asesores personalizados. El asesor DB2 se comunica sólo con el puerto de conexión DB2, con el puerto de conexión Java.
- El asesor **WLM** (Workload Manager) está diseñado para trabajar junto con servidores de sistemas OS/390 que ejecutan el componente Workload Manager (WLM) de MVS. Para obtener más información, consulte “Asesor de Workload Manager” en la página 149.
- El asesor **self** recoge información sobre el estado del tráfico en servidores de fondo. Puede utilizar el asesor self cuando utilice Dispatcher en una configuración de dos niveles, en la que Dispatcher pasa información desde el asesor self al Network Dispatcher de nivel superior. El asesor self mide específicamente la tasa de conexiones por segundo en los servidores de fondo del Dispatcher a nivel de ejecutor. En “Utilización del asesor self en una configuración WAND de dos niveles” en la página 164 hallará más información.
- Dispatcher proporciona la capacidad de que un usuario escriba un asesor *personalizado* (personalizable). Esto permite el soporte para protocolos propietarios (por encima de TCP) para los que IBM no ha desarrollado un asesor específico. Para obtener más información, consulte “Creación de asesores personalizados (personalizables)” en la página 145.

- El asesor **WAS** (WebSphere Application Server) funciona junto con los servidores WebSphere Application. En el directorio de instalación hay archivos de ejemplo para este asesor. Para obtener más información, consulte “Asesor WebSphere Application Server” en la página 146.

Creación de asesores personalizados (personalizables)

El asesor personalizado (personalizable) es una pequeña parte de código Java, que se puede proporcionar como un archivo de clases, llamado por el código base. El código base proporciona todos los servicios administrativos, como iniciar y parar una instancia del asesor personalizado, proporcionar el estado e informes y registrar información de historial en un archivo de anotaciones. También informa de los resultados al componente del gestor. El código base realizará periódicamente un ciclo asesor, donde evalúa individualmente todos los servidores y su configuración. Empieza abriendo una conexión con una máquina servidor. Si el socket se abre, el código base llamará al método (función) “getLoad” en el asesor personalizado. El asesor personalizado realiza entonces los pasos necesarios para evaluar la salud del servidor. Generalmente, enviará al servidor un mensaje definido por el usuario y después esperará una respuesta. (El acceso al socket abierto lo proporciona el asesor personalizado). El código base cierra entonces el socket con el servidor y proporciona al Gestor la información de tráfico.

El código base y el asesor personalizado pueden funcionar en modalidad normal o de sustitución. La elección de la modalidad de funcionamiento se especifica en el archivo del asesor personalizado como parámetro en el método del constructor.

En la modalidad normal, el asesor personalizado intercambia datos con el servidor, y el código base del asesor calcula el tiempo del intercambio y el valor del tráfico. El código base informa entonces al gestor de este valor del tráfico. El asesor personalizado sólo tiene que devolver un cero (en caso satisfactorio) o uno negativo (en caso de error). Para especificar la modalidad normal, el distintivo de sustitución del constructor se establece en falso.

En la modalidad de sustitución, el código base no realiza ninguna medición del tiempo. El código del asesor personalizado realiza las operaciones deseadas para sus requisitos, y a continuación devuelve un número de tráfico real. El código base aceptará el número y se lo notificará al gestor. Para obtener mejores resultados, normalice el valor de tráfico entre 10 y 1000, donde 10 representa un servidor rápido y 1000 representa un servidor lento. Para especificar la modalidad de sustitución, el distintivo de sustitución del constructor se establece en verdadero.

Con esta característica, se pueden escribir asesores propios que proporcionarán la información precisa que se necesite acerca de los servidores.

Junto con el producto Network Dispatcher se proporciona con asesor personalizado de ejemplo, **ADV_sample.java**. Después de instalar Network Dispatcher, puede encontrar el código de ejemplo en el directorio de instalación **...nd/servers/samples/CustomAdvisors**.

Los directorios de instalación por omisión son:

- AIX: /usr/lpp/nd
- Linux: /opt/nd
- Sun: /opt/nd
- Windows 2000: c:\Archivos de programa\IBM\nd

Asesor WebSphere Application Server

El directorio de instalación de Network Dispatcher contiene los archivos de ejemplo específicos para el asesor WebSphere Application Server.

- ADV_was.java es el archivo que se debe compilar y ejecutar en la máquina de Network Dispatcher.
- NDAdvisor.java.servlet (al que se le cambiará el nombre por NDAdvisor.java) es el archivo que se ha de compilar y ejecutar en la máquina WebSphere Application Server.

Los archivos de ejemplo del asesor WebSphere Application Server residen en el mismo directorio de ejemplos que el archivo ADV_sample.java.

Convenio de denominación

El nombre del archivo del asesor personalizado debe tener el formato *"ADV_myadvisor.java"*. Debe empezar por el prefijo *"ADV_"* en mayúsculas. Todos los caracteres siguientes deben estar en minúsculas.

Al igual que para convenios Java, el nombre de la clase definida en el archivo debe coincidir con el nombre del archivo. Si copia el código de ejemplo, asegúrese de modificar todas las apariciones de *"ADV_sample"* del interior del archivo por su nuevo nombre de clase.

Compilación

Los asesores personalizados están escritos en lenguaje Java. Debe obtener e instalar un compilador Java 1.3 para su máquina. Durante la compilación se utilizan estos archivos:

- el archivo del asesor personalizado
- el archivo de clase base, **ibmnd.jar**, que reside en el directorio **...nd/servers/lib** donde Network Dispatcher está instalado.

La vía de clases debe apuntar al archivo del asesor personalizado y al archivo de clase base durante la compilación.

Para Windows 2000, el mandato de compilación puede ser similar al siguiente:

```
javac -classpath <install_dir>\nd\servers\lib\ibmnd.jar ADV_fred.java
```

donde:

- El archivo del asesor se denomina ADV_fred.java
- El archivo del asesor reside en el directorio actual

El resultado de la compilación es un archivo de clase, por ejemplo

ADV_fred.class

Antes de iniciar el asesor, copie el archivo de clase en el directorio **...nd/servers/lib/CustomAdvisors** donde Network Dispatcher está instalado.

Nota: Si lo desea, los asesores personalizados se pueden compilar en un sistema operativo y ejecutarse en otro. Por ejemplo, puede compilar su asesor en Windows 2000, copiar el archivo de clase (en binario) en una máquina AIX y ejecutar allí el asesor personalizado.

Para AIX, Linux y Sun, la sintaxis es similar.

Ejecución

Para ejecutar el asesor personalizado, primero debe copiar el archivo de clase en el subdirectorio apropiado de Network Dispatcher:

```
.../nd/servers/lib/CustomAdvisors/ADV_fred.class
```

Configure el componente, inicie su gestor y emita el mandato para iniciar el asesor personalizado:

```
ndcontrol advisor start fred 123
```

donde:

- fred es el nombre de su asesor, como en ADV_fred.java
- 123 es el puerto en el que va a funcionar el asesor

Rutinas necesarias

Al igual que todos los asesores, un asesor personalizado extiende la función del asesor base, llamado ADV_Base. El asesor base es el que ejecuta realmente la mayoría de las funciones del asesor, como informar del tráfico al gestor, para que dicha información se utilice en el algoritmo de ponderación del gestor. El asesor base también realiza las operaciones de conexión y cierre de socket, además de proporcionar los métodos de envío y recepción para que el asesor los utilice. El asesor en sí solamente se utiliza para recibir y enviar datos desde y hacia el puerto del servidor que se asesora. Los métodos TCP incluidos en el asesor base están temporizados para calcular el tráfico. Si se desea, un indicador dentro del constructor en el ADV_base sobrescribe el tráfico existente con el nuevo tráfico devuelto por el asesor.

Nota: Según el valor establecido en el constructor, el asesor base proporciona periódicamente el tráfico al algoritmo de ponderación. Si el asesor real no se ha completado y por lo tanto no puede devolver un valor válido, el asesor base utiliza el tráfico anterior.

Estos son los métodos de clase base:

- Una rutina **constructor**. El constructor llama al constructor de clase base (consulte el archivo de ejemplo de asesor)
- Un método **ADV_AdvisorInitialize**. Este método proporciona un gancho en caso de que se necesiten llevar a cabo pasos adicionales después de que la clase base complete su inicialización.
- Una rutina **getload**. La clase de asesor base ejecuta la apertura del socket, por lo tanto getload solamente necesita enviar las peticiones de envío y recepción pertinentes para completar el ciclo de asesoría.

Orden de búsqueda

Network Dispatcher examina primero la lista de asesores nativos que ese producto proporciona. Si no encuentran un asesor determinado en esa lista, entonces Dispatcher Dispatcher examina la lista de asesores personalizados del usuario.

Nomenclatura y vía de acceso

- El archivo de clase del asesor personalizado debe residir en el subdirectorio **...nd/servers/lib/CustomAdvisors/** del directorio base de Network Dispatcher. Los valores por omisión para este directorio varían de un sistema operativo a otro:

- AIX
/usr/lpp/nd/servers/lib/CustomAdvisors/
- Linux
/opt/nd/servers/lib/CustomAdvisors/
- Solaris
/opt/nd/servers/lib/CustomAdvisors/
- Windows 2000

Vía de acceso común de directorio de instalación:

C:\Archivos de programa\IBM\edge\nd\servers\lib\CustomAdvisors

Vía de acceso nativa de directorio de instalación:

C:\Archivos de programa\IBM\nd\servers\lib\CustomAdvisors

- Sólo se permiten caracteres alfabéticos en minúsculas. Esto elimina la sensibilidad a mayúsculas y minúsculas cuando un operador entra mandatos en la línea de mandatos. El nombre del asesor debe llevar el prefijo **ADV_**.

Asesor de ejemplo

El listado de programa para un asesor de ejemplo se incluye en “Asesor de ejemplo” en la página 384. Después de la instalación, este asesor de ejemplo se encuentra en el directorio `...nd/servers/samples/CustomAdvisors`.

Asesor de Workload Manager

WLM es el código que se ejecuta en sistemas principales MVS. Se puede consultar para preguntar sobre el tráfico en la máquina MVS.

Cuando MVS Workload Management se ha configurado en el sistema OS/390, Dispatcher puede aceptar la información de capacidad de WLM y utilizarla en el proceso de reparto del tráfico. Mediante la utilización del asesor WLM, Dispatcher abrirá periódicamente conexiones a través del puerto WLM, en cada servidor de la tabla de sistemas principales de Dispatcher y aceptará los enteros de capacidad devueltos. Puesto que estos enteros representan el volumen de capacidad que sigue estando disponible y Dispatcher espera valores que representen los tráficos de cada máquina, el asesor invierte los enteros de capacidad y los normaliza a valores de tráfico (es decir, un entero de gran capacidad pero con un valor de tráfico pequeño representa un servidor con un mejor estado). Los tráficos resultantes se colocan en la columna Sistema del informe del gestor.

Hay varias diferencias importantes entre el asesor WLM y los demás asesores de Dispatcher:

1. Otros asesores abren conexiones con los servidores utilizando el mismo puerto en los que fluye un tráfico de clientes normal. El asesor WLM abre las conexiones a los servidores utilizando un puerto diferente del de tráfico normal. El agente WLM de cada máquina servidor debe configurarse para escuchar en el mismo puerto en el que se ha iniciado el Asesor WLM del Dispatcher. El puerto WLM por omisión es 10007.
2. Otros asesores sólo valoran los servidores definidos en la configuración de Dispatcher cluster:puerto:servidor para la que el puerto del servidor coincide con el puerto del asesor. El asesor WLM asesora a cada servidor en la configuración del Dispatcher cluster:puerto:servidor. Por lo tanto, no debe definir servidores que no son WLM cuando utilice el asesor WLM.
3. Otros asesores colocan su información de tráfico en el informe del gestor en su columna “Puerto”. El asesor WLM coloca su información de tráfico en el informe del gestor en su columna Sistema.
4. Es posible utilizar asesores específicos de protocolo junto con el asesor WLM. Los asesores específicos de protocolo sondearán todos los servidores en sus puertos de tráfico normal, y el asesor WLM sondeará el tráfico del sistema utilizando el puerto WLM.

Restricción de Metric Server

Al igual que Metric Server, el agente WLM genera informes sobre sistemas servidores considerados como un todo, en lugar de hacerlo para daemons de servidor individuales específicos del protocolo. Metric Server y WLM colocan sus resultados en la columna Sistema del informe del gestor. Como consecuencia de esto, no se puede ejecutar el asesor WLM y Metric Server al mismo tiempo.

Metric Server

Esta función se puede utilizar para todos los componentes de Network Dispatcher.

Metric Server proporciona información a Network Dispatcher sobre el tráfico de servidores en forma de métricas específicas del sistema y genera informes sobre el estado de los servidores. El gestor de Network Dispatcher consulta al agente de Metric Server que reside en cada servidor y asigna pesos al proceso de reparto del tráfico utilizando las métricas recogidas por los agentes. Los resultados se colocan en el informe del gestor.

Nota: Cuando se recogen dos o más métricas y se normalizan por servidor en un solo valor de carga del sistema, pueden producirse errores de redondeo.

Para ver un ejemplo de configuración, consulte la Figura 11 en la página 40.

Restricción de WLM

Al igual que el asesor WLM, el Metric Server genera informes sobre los sistemas servidores considerados como un todo, en lugar de hacerlo para daemons de servidor individuales específicos del protocolo. Tanto WLM como Metric Server colocan sus resultados en la columna Sistema del informe del gestor. Como consecuencia de esto, no se puede ejecutar el asesor WLM y Metric Server al mismo tiempo.

Requisitos previos

El agente de Metric Server debe estar instalado y en ejecución en los servidores para los que Network Dispatcher realiza el reparto del tráfico.

Cómo utilizar Metric Server

A continuación, se indican los pasos para configurar Metric Server para Dispatcher. Pueden utilizarse pasos similares en la configuración de Metric Server para los otros componentes de Network Dispatcher.

- gestor de Network Dispatcher (extremo de Network Dispatcher)
 1. Inicie **ndserver**.
 2. Emita el mandato: **ndcontrol manager start *manager.log puerto***

puerto es el puerto RMI seleccionado para ejecutar todos los agentes de Metric Server. El puerto RMI por omisión que está establecido en el archivo `metricserver.cmd` es 10004.

3. Emita el mandato: **ndcontrol metric add cluster:systemMetric**
systemMetric es el nombre del script (que reside en el servidor de fondo) que debe ejecutarse en cada servidor de la configuración del cluster (o nombre de sitio) especificado. Se proporcionan dos scripts para el usuario: **cpuload** y **memload**. O bien, el usuario puede crear scripts personalizados de métricas del sistema. El script contiene un mandato que debe devolver un valor numérico comprendido entre 0 y 100. Este valor numérico debe representar una medición de carga, no un valor de disponibilidad.

Nota: Para Site Selector, `cpuload` y `memload` se ejecutan automáticamente.

Limitación: Para Windows 2000, si el nombre del script de métricas del sistema tiene una extensión diferente de ".exe", debe especificar el nombre completo del archivo (por ejemplo, "mysystemscript.bat"). Esto es debido a una limitación de Java.

4. Añada a la configuración sólo los servidores que contengan un agente de Metric Server ejecutándose en el puerto especificado en el archivo `metricserver.cmd`. El puerto debe coincidir con el valor de puerto especificado en el mandato **manager start**.

Nota: Compruebe la seguridad —

- En la máquina Network Dispatcher, cree un archivo de claves para el componente que está ejecutándose (utilizando el mandato **ndkeys create**). Consulte "Administración autenticada remota" en la página 205 para obtener más información sobre `ndkeys`.
 - En la máquina servidor, copie el archivo de claves resultante en el directorio `.../nd/admin/key`. Compruebe que los permisos del archivo de claves permiten al usuario root leer el archivo.
- agente de Metric Server (extremo de la máquina servidor)
 1. Instale el paquete Metric Server desde el directorio de instalación de Network Dispatcher.
 2. Examine el script **metricserver** del directorio `/usr/bin` para comprobar que se utiliza el puerto RMI deseado. (Para Windows 2000, el directorio es `C:\WINNT\SYSTEM32`.) El puerto RMI por omisión es 10004.

Nota: El valor de puerto RMI especificado debe coincidir con el valor de puerto RMI de Metric Server en la máquina de Network Dispatcher.

3. Se proporcionan los dos scripts siguientes para el usuario: **cpuload** (que devuelve el porcentaje de CPU en uso, entre 0 y 100) y **memload** (que devuelve el porcentaje de memoria utilizada, entre 0 y 100). Estos scripts residen en el directorio **...nd/ms/script**.

Opcionalmente, el usuario puede escribir sus propios archivos personalizados de script de métricas para definir el mandato que Metric Server emitirá para las máquinas servidores. Asegúrese de que los scripts personalizados sean ejecutables y estén situados en el directorio **...nd/ms/script**. Los scripts personalizados **deben** devolver un valor de carga numérico en el rango de 0 a 100.

Nota: Un script de métricas personalizado debe ser un programa o script válido, cuya extensión sea ".bat" o ".cmd". Específicamente, para las plataformas basadas en UNIX, los scripts deben comenzar con la declaración del shell, de lo contrario no se pueden ejecutar correctamente.

4. Inicie el agente emitiendo el mandato **metricserver**.
5. Para detener el agente de Metric Server, emita el mandato **metricserver stop**.

Para que Metric Server se ejecute en una dirección que no sea la del sistema principal local, tiene que editar el archivo **metricserver** en la máquina servidor de distribución de tráfico. Detrás de "java" en el archivo **metricserver**, inserte lo siguiente:

```
-Djava.rmi.server.hostname=OTRA_DIRECCIÓN
```

Además, antes de las sentencias "if" del archivo **metricserver** añada la siguiente línea: `hostname OTRA_DIRECCIÓN`.

Para Windows 2000: También tiene unir mediante alias **OTRA_DIRECCIÓN** en la pila de Microsoft. Para unir mediante un alias una dirección en la pila de Microsoft, consulte la página 172.

Particionamiento del servidor: servidores lógicos configurados para un solo servidor físico (dirección IP)

Cuando define un servidor en la configuración de Network Dispatcher, puede distribuir el tráfico basándose en el estado del servidor considerado en conjunto (utilizando el agente de Metric Server) o el estado de cualquier aplicación para un puerto determinado (utilizando la función del asesor).

Gracias al particionamiento del servidor, puede distinguir mejor entre los URL individuales y sus aplicaciones específicas. Por ejemplo, un servidor Web individual puede servir páginas JSP, páginas HTML, atender peticiones de base de datos, etc. Ahora Network Dispatcher proporciona la capacidad de

particionar un servidor de un cluster y un puerto determinado en varios servidores lógicos. Esto le permite informar sobre un determinado servicio de la máquina para detectar si un motor de servlet o petición de base de datos se está ejecutando más rápidamente o no se está ejecutando.

El particionamiento del servidor permite, por ejemplo, que Network Dispatcher detecte que el servicio HTML está sirviendo páginas rápidamente, pero que la conexión con la base de datos se ha desactivado. Esto permite al usuario repartir el tráfico de una forma más precisa, de acuerdo con el servicio, en lugar de hacerlo basándose solamente en el servidor.

Dentro de la configuración de Network Dispatcher, puede representar un servidor físico o un servidor lógico utilizando la jerarquía *cluster:puerto:servidor*. El servidor puede ser una dirección IP exclusiva de la máquina (servidor físico) expresada en forma de nombre simbólico o en el formato decimal con puntos. O bien, si configura el servidor como servidor particionado, debe proporcionar un dirección de servidor que se pueda resolver para el servidor físico en el parámetro **address** del mandato **ndcontrol server add**. En “ndcontrol server — configurar servidores” en la página 302 hallará más información.

El ejemplo siguiente muestra el particionamiento de servidores físicos en servidores lógicos para gestionar diferentes tipos de peticiones.

```
Cluster: 1.1.1.1
  Puerto: 80
    Servidor: A (dirección IP 1.1.1.2)
                servidor html
    Servidor: B (dirección IP 1.1.1.2)
                servidor gif
    Servidor: C (dirección IP 1.1.1.3)
                servidor html
    Servidor: D (dirección IP 1.1.1.3)
                servidor jsp
    Servidor: E (dirección IP 1.1.1.4)
                servidor gif
    Servidor: F (dirección IP 1.1.1.4)
                servidor jsp
  Normal: \*.htm
    Servidor: A
    Servidor: C
  Norma2: \*.jsp
    Servidor: D
    Servidor: F
  Norma3: \*.gif
    Servidor: B
    Servidor: E
```

En este ejemplo, el servidor 1.1.1.2 está particionado según 2 servidores lógicos: A (que gestiona las peticiones html) y B (que gestiona la peticiones

gif) El servidor 1.1.1.3 está particionado según 2 servidores lógicos: C (que gestiona las peticiones html) y D (que gestiona las peticiones jsp). El servidor 1.1.1.4 está particionado según 2 servidores lógicos: E (que gestiona las peticiones gif) y F (que gestiona las peticiones jsp).

Nota: La función Server Directed Affinity tiene una limitación: no es compatible con el particionamiento del servidor, pues necesita que las direcciones de los servidores sean exclusivas en la configuración, a fin de poder utilizar los recursos de búsqueda. En “API de afinidad dirigida por el servidor (SDA) para controlar la afinidad cliente-servidor” en la página 188 hallará más información.

Opción de petición/respuesta del asesor HTTP (URL)

La opción de URL del asesor HTTP puede utilizarse con los componentes Dispatcher y CBR.

Después de iniciar un asesor HTTP, puede definir un URL exclusivo para un cliente HTTP, que sea específico del servicio que desea consultar en el servidor. Esto permite que el asesor evalúe el estado de cada servicio de un servidor. Para ello, defina servidores lógicos que tengan un nombre de servidor exclusivo y la misma dirección física IP. En “Particionamiento del servidor: servidores lógicos configurados para un solo servidor físico (dirección IP)” en la página 152 hallará más información.

Para cada servidor lógico definido del puerto HTTP, puede especificar un URL exclusivo para un cliente HTTP, que sea específico del servicio que desea consultar en el servidor. El asesor HTTP utiliza la serie de caracteres **advisorrequest** para consultar el estado de los servidores. El valor por omisión es HEAD / HTTP/1.0. La cadena de texto **advisorresponse** es la respuesta de asesor que el asesor HTTP busca en la respuesta HTTP. El asesor HTTP utiliza la cadena de texto **advisorresponse** para compararla con la respuesta real recibida del servidor. El valor por omisión es null.

Importante: Si la serie del URL HTTP contiene un blanco:

- Cuando se emite el mandato desde el indicador de shell **ndcontrol>>**, debe encerrar la serie de caracteres entre comillas. Por ejemplo:

```
server set cluster:puerto:servidor advisorrequest "head / http/2.0"
server set cluster:puerto:servidor advisorresponse "HTTP 200 OK"
```
- Cuando emite el mandato **ndcontrol** desde el indicador del sistema operativo, debe preceder el texto de “\” y seguirlo de “\”. Por ejemplo:

```
ndcontrol server set cluster:puerto:servidor advisorrequest "\"head / http/2.0\""
ndcontrol server set cluster:puerto:servidor advisorresponse "\"HTTP 200 OK\""
```

Nota: Después de iniciar un asesor HTTP para un número de puerto HTTP especificado, el valor de petición/respuesta del asesor se habilita para los servidores comprendidos en ese puerto HTTP.

En “ndcontrol server — configurar servidores” en la página 302 hallará más información.

Utilización de servidores de ubicación compartida

Network Dispatcher puede residir en la misma máquina que un servidor para el que está repartiendo el tráfico de peticiones. Esto se denomina *compartimiento de la ubicación* con un servidor. La ubicación compartida es aplicable a los componentes Dispatcher, Site Selector, Mailbox Locator y Cisco Consultant. La ubicación compartida también está soportada para CBR, pero sólo al utilizar servidores Web de vinculación específica y Caching Proxy de vinculación específica.

Nota: Durante los períodos de tráfico intenso, un servidor de ubicación compartida compite por los recursos con Network Dispatcher. Sin embargo, si no hay máquinas sobrecargadas de trabajo, la utilización de un servidor de ubicación compartida reduce el número total de máquinas necesarias para configurar un sitio Web con reparto del tráfico.

Para el componente Dispatcher

Red Hat Linux v7.1 (kernel de Linux versión 2.4.2-2) o SuSE Linux v7.1 (kernel de Linux versión 2.4.0-4 GB): Para poder configurar al mismo tiempo la ubicación compartida y la modalidad de alta disponibilidad, cuando ejecute el componente Dispatcher utilizando el método de reenvío mac, debe instalar un parche de kernel de Linux. Para obtener más información sobre la instalación del parche, consulte “Instalación del parche del kernel de Linux (para suprimir las respuestas a arp en la interfaz de bucle de retorno)” en la página 70. Cuando siga esas instrucciones, debe omitir el paso referente a la creación de un alias para el adaptador de bucle de retorno. Para crear el alias del adaptador de bucle de retorno, debe añadir la instrucción ifconfig al archivo de script para la alta disponibilidad, goStandby, que se ejecuta cuando un Dispatcher pasa al estado de espera.

Solaris: Existe una limitación: no puede configurar asesores WAND cuando el Dispatcher de punto de entrada es de ubicación compartida. Consulte “Utilización de asesores remotos con soporte de área amplia” en la página 159.

En versiones anteriores, la dirección especificada para el servidor de ubicación compartida debía ser igual que la dirección de no reenvío (NFA) de la configuración. Esta restricción se ha eliminado.

Para configurar un servidor de ubicación compartida, el mandato **ndcontrol server** proporciona una opción denominada **collocated** (ubicación compartida) cuyo valor puede ser *sí* o *no*. El valor por omisión es *no*. La dirección del servidor debe ser una dirección IP válida correspondiente a una tarjeta de interfaz de red de la máquina.

Nota: Para **Windows 2000**: Puede utilizar un Dispatcher de ubicación compartida, pero *no* se utiliza la palabra clave "collocated". El compartimiento de ubicación se utiliza con los métodos de reenvío nat y cbr de Dispatcher, pero no puede utilizarse con el método de reenvío mac de Dispatcher. Para obtener más información sobre los métodos de reenvío del Dispatcher, consulte "Método de reenvío nat del Dispatcher" en la página 50, "Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)" en la página 52 y "Método de reenvío mac del Dispatcher" en la página 49.

Puede configurar un servidor de ubicación compartida en una de las maneras siguientes:

- Si utiliza la NFA (dirección de no reenvío) como dirección del servidor de ubicación compartida: Defina la NFA utilizando el mandato **ndcontrol executor set nfa dirección_IP**. Luego, utilice el mandato **ndcontrol server add cluster:puerto:servidor** para añadir el servidor que hace uso de la dirección NFA.
- Si utiliza una dirección que no sea la NFA: Añada el servidor con la dirección IP deseada y el parámetro "collocated" establecido en "sí", de la manera siguiente: **ndcontrol server add cluster:puerto:servidor collocated sí**.

Consulte "ndcontrol server — configurar servidores" en la página 302 para obtener más información sobre la sintaxis del mandato de servidor ndcontrol.

Para el componente CBR

CBR da soporte al compartimiento de ubicación en todas las plataformas sin necesidad de llevar a cabo tareas adicionales de configuración. Sin embargo, los servidores Web y Caching Proxy que utilice deben ser de vinculación específica.

Para el componente Mailbox Locator

Mailbox Locator permite el compartimiento de ubicación en todas las plataformas. Pero el servidor debe estar asociado a una dirección diferente de la de Network Dispatcher para que ello sea efectivo. Para situar un servidor POP3 o IMAP en la misma máquina, debe estar asociado a una dirección IP diferente de la dirección del cluster. Esto se puede conseguir utilizando la dirección de bucle de retorno.

Para el componente Site Selector

Site Selector permite el compartimiento de ubicación en todas las plataformas, sin ser necesarias tareas adicionales de configuración.

Para el componente Cisco Consultant

Cisco Consultant permite el compartimiento de ubicación en todas las plataformas, sin ser necesarias tareas adicionales de configuración.

Configurar el soporte de Dispatcher para área amplia

Esta característica sólo está disponible para el componente Dispatcher.

Si no desea utilizar el soporte de área amplia de Dispatcher ni el método de reenvío nat de Dispatcher, una configuración de Dispatcher requiere que la máquina Dispatcher y sus servidores estén conectados al mismo segmento de LAN (consulte la Figura 22). El paquete de un cliente llega a la máquina Network Dispatcher y se envía al servidor, y luego desde el servidor se devuelve directamente al cliente.

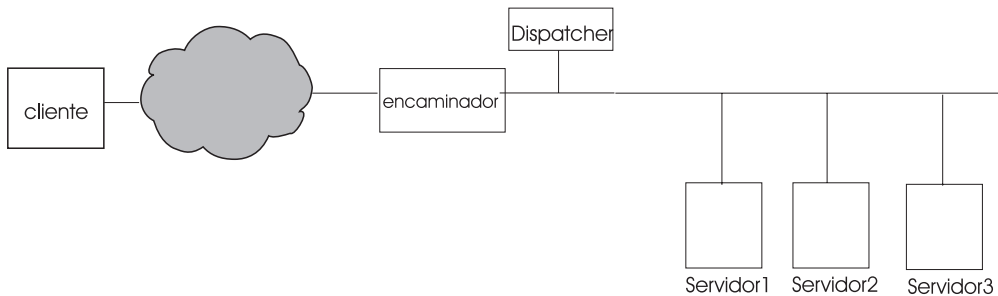


Figura 22. Ejemplo de configuración formada por un sólo segmento de LAN

La mejora de Dispatcher para área amplia añade soporte para servidores situados fuera de las oficinas, conocidos como *servidores remotos* (consulte la Figura 23 en la página 158). Si GRE no recibe soporte en el sitio remoto y no utiliza el método de reenvío nat de Dispatcher, el sitio remoto debe constar de una máquina Dispatcher remota (Dispatcher 2) y sus servidores conectados localmente (ServerG, ServerH y ServerI). Todas las máquinas Dispatcher deben utilizar el mismo sistema operativo. Ahora, el paquete de un cliente puede ir desde Internet a una máquina Dispatcher, desde allí a una máquina Dispatcher geográficamente remota a uno de sus servidores conectados localmente.

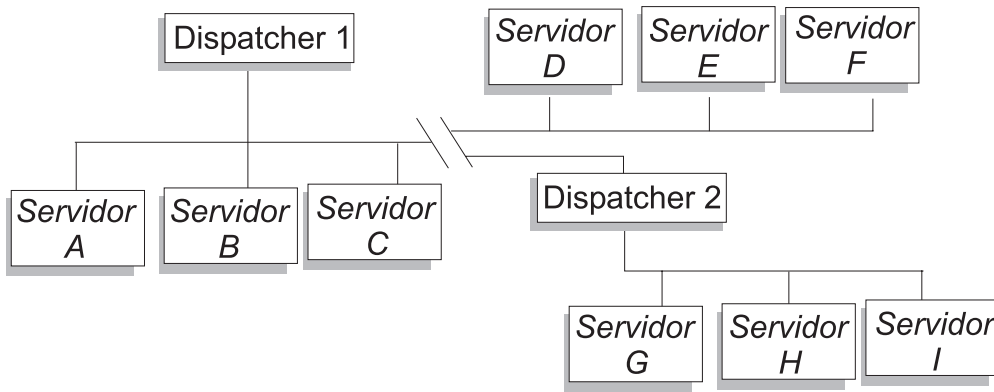


Figura 23. Ejemplo de configuración utilizando servidores locales y remotos

Esto permite que una dirección de cluster dé soporte a todas las peticiones de clientes de cualquier zona geográfica y las distribuya entre servidores repartidos por todo el mundo.

La máquina Dispatcher que recibe inicialmente los paquetes puede seguir teniendo servidores locales conectados a ella y puede distribuir el tráfico entre los servidores locales y los remotos.

Sintaxis de los mandatos

Los mandatos de área amplia no son complicados. Para configurar el soporte de área amplia:

1. Añada los servidores. Cuando añade un servidor a un Dispatcher, debe definir si el servidor es local o remoto (ver más arriba). Para añadir un servidor y definirlo como local, emita el mandato **ndcontrol server add** sin especificar un encaminador. Éste es el método por omisión. Para definir el servidor como remoto, debe especificar el encaminador a través del cual Dispatcher debe enviar los paquetes para que lleguen al servidor remoto. El servidor debe ser otro Dispatcher y la dirección del servidor debe ser la dirección de no reenvío de Dispatcher. Por ejemplo, en la Figura 24 en la página 161, si va a añadir ND 2 como servidor remoto bajo ND 1, deberá definir *encaminador 1* como la dirección del encaminador. Sintaxis general:
`ndcontrol server add cluster:puerto:servidor router dirección`

Para obtener más información sobre la palabra clave "router", consulte "ndcontrol server — configurar servidores" en la página 302.

2. Configure los alias. En la primera máquina Dispatcher (a la que llega la petición del cliente desde Internet), debe asignarse un alias a la dirección de cluster mediante **cluster configure**, **ifconfig** o **ndconfig**, al igual que antes. Sin embargo, en las máquinas Dispatcher remotas, la dirección del cluster **no** es alias de una tarjeta de interfaz de red.

Utilización de asesores remotos con soporte de área amplia

En los Dispatchers de punto de entrada, los asesores funcionarán correctamente sin ninguna configuración especial en la mayoría de plataformas.

Linux: Hay una limitación sobre el uso de asesores remotos con configuraciones con soporte de área amplia. Los asesores específicos del protocolo, como el asesor HTTP, que se ejecutan en la máquina Dispatcher de punto de entrada no asesoran correctamente sobre el estado de las máquinas servidor del sitio remoto. Para solucionar este problema, lleve a cabo una de las siguientes acciones:

- Ejecute el asesor ping independiente del protocolo en la máquina Dispatcher de punto de entrada.
- Ejecute un asesor específico del protocolo en la máquina Dispatcher de punto de entrada junto con un daemon correspondiente de servidor específico de protocolo (como un servidor Web) en la máquina Dispatcher remota.

Cualquiera de estas opciones permitirá que el asesor se ejecute en la máquina Dispatcher de punto de entrada con asesoramiento del estado de la máquina Dispatcher remota.

Solaris: En los Network Dispatchers de punto de entrada, debe utilizar el método de configuración arp (en lugar de los métodos de configuración ifconfig o cluster). Por ejemplo:

```
arp -s <dirección_cluster>  
<dirección_mac> pub
```

Nota: Para Solaris existen algunas limitaciones:

- Los asesores WAND sólo pueden utilizarse con el método arp de configuración de clusters.
- Los asesores correspondientes a los servidores de vinculación específica sólo funcionan con el método arp de configuración de clusters.
- El compartimiento de ubicación sólo puede utilizarse con el método ifconfig de configuración de clusters.

En los Dispatchers remotos, debe seguir los siguientes pasos de configuración para cada dirección de cluster remoto. Para configurar la modalidad de alta disponibilidad en el Network Dispatcher remoto, debe seguir estos pasos en las dos máquinas.

AIX

- Cree un alias para la dirección de cluster del adaptador de bucle de retorno. La máscara de red debe ser 255.255.255.255. Por ejemplo:

ifconfig lo0 alias 9.67.34.123 netmask 255.255.255.255

Nota: Los asesores que se ejecutan en las máquinas Dispatcher locales y remotas son necesarios.

Linux

- Cree un alias para la dirección de cluster del adaptador de bucle de retorno. Por ejemplo:

ifconfig lo:1 9.67.34.123 netmask 255.255.255.255 up

Nota: Los asesores que se ejecutan en las máquinas Dispatcher locales y remotas son necesarios.

Solaris

- No es necesario realizar ningún paso adicional de configuración.

Windows 2000

1. El Dispatcher necesita dos direcciones IP: una dirección para la pila TCP/IP de Microsoft y otra para la pila de Network Dispatcher. Configure la NFA (dirección de no reenvío) utilizando la dirección IP de la pila de Network Dispatcher. Por ejemplo:

ndconfig en0 alias 9.55.30.45 netmask 255.255.240.0

2. Configure el adaptador de bucle de retorno con la dirección del cluster remoto como alias. La máscara de red debe ser 255.255.255.255. Por ejemplo:

ndconfig lo0 alias 9.67.34.123 netmask 255.255.255.255

3. Suprima todas las entradas que haya en la tabla arp correspondientes a la dirección del cluster remoto.

- a. Para visualizar el contenido de la tabla arp, entre:

arp -a

- b. Para suprimir una entrada, si existe alguna, entre:

arp -d 9.67.34.123

Nota: Para determinar la dirección MAC de la interfaz, entre:

1) **ping** *nombre_sistema_principal*

2) **arp -a**

y busque la dirección de la máquina.

4. Añada una ruta que conduzca al cluster remoto (9.67.34.123) utilizando la NFA (dirección IP de la pila de Network Dispatcher). La máscara de red debe ser 255.255.255.255. Por ejemplo:

route add 9.67.34.123 mask 255.255.255.255 9.55.30.45

Ejemplo de configuración

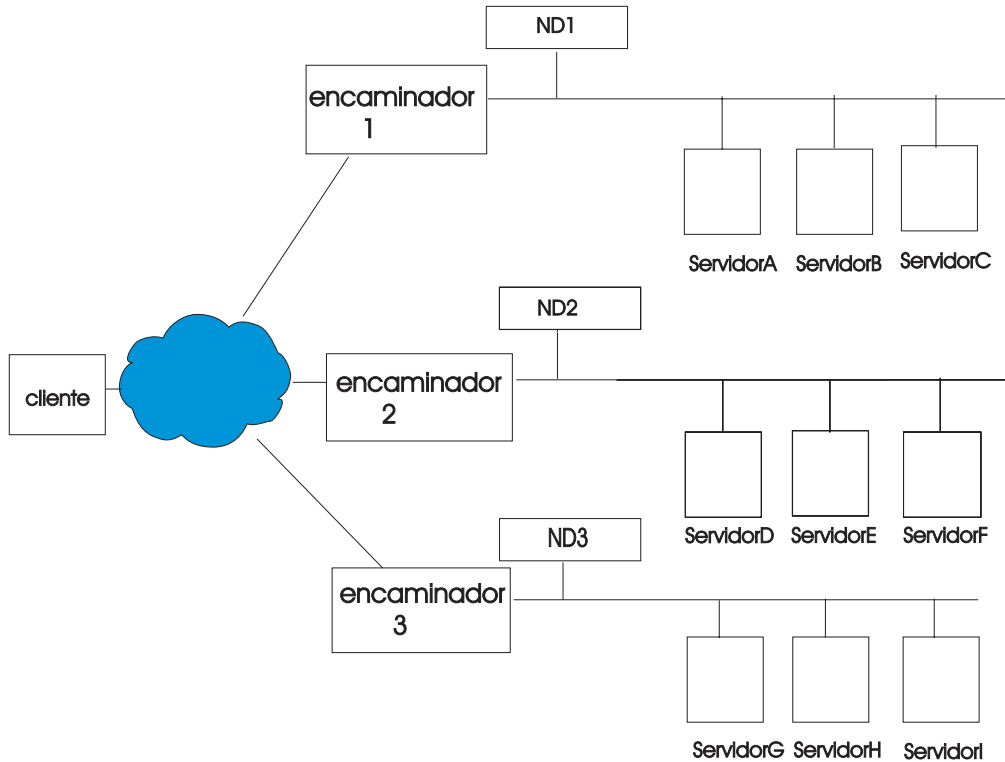


Figura 24. Ejemplo de configuración de área amplia con Network Dispatchers remotos

Este ejemplo es aplicable a la configuración mostrada en la Figura 24.

A continuación se muestra cómo se deben configurar las máquinas Dispatcher para que den soporte a la dirección de cluster xebec en el puerto 80. ND1 se define como “punto de entrada”. Se presupone que se utiliza una conexión Ethernet. Observe que ND1 tiene 5 servidores definidos: 3 locales (ServidorA, ServidorB, ServidorC) y 2 remotos (ND2 y ND3). Los servidores ND2 y ND3 tienen definidos tres servidores locales cada uno de ellos.

En la consola del primer Dispatcher (ND1), haga lo siguiente:

1. Arranca el ejecutor.
ndcontrol executor start
2. Establezca la dirección de no reenvío de la máquina Dispatcher.
ndcontrol executor set nfa ND1
3. Defina el cluster.

ndcontrol cluster add xebec

4. Defina el puerto.

ndcontrol port add xebec:80

5. Defina los servidores.

a. **ndcontrol server add xebec:80:ServidorA**

b. **ndcontrol server add xebec:80:ServidorB**

c. **ndcontrol server add xebec:80:ServidorC**

d. **ndcontrol server add xebec:80:ND2 router Router1**

e. **ndcontrol server add xebec:80:ND3 router Router1**

6. Si utiliza Windows 2000, configure la NFA (dirección de no reenvío) del adaptador de LAN del Dispatcher.

ndcontrol cluster configure ND1 y configure también xebec como la dirección del cluster.

7. Configure la dirección del cluster.

ndcontrol cluster configure xebec

En la consola del segundo Dispatcher (ND2):

1. Arranca el ejecutor.

ndcontrol executor start

2. Establezca la dirección de no reenvío de la máquina Dispatcher.

ndcontrol executor set nfa ND2

3. Defina el cluster.

ndcontrol cluster add xebec

4. Defina el puerto.

ndcontrol port add xebec:80

5. Defina los servidores.

a. **ndcontrol server add xebec:80:ServidorD**

b. **ndcontrol server add xebec:80:ServidorE**

c. **ndcontrol server add xebec:80:ServidorF**

6. Si utiliza Windows 2000, configure la NFA (dirección de no reenvío) del adaptador de LAN del Dispatcher.

ndcontrol cluster configure ND2

En la consola del tercer Dispatcher (ND3):

1. Arranca el ejecutor.

ndcontrol executor start

2. Establezca la dirección de no reenvío de la máquina Dispatcher.

ndcontrol executor set nfa ND3

3. Defina el cluster.
ndcontrol cluster add xebec
4. Defina el puerto.
ndcontrol port add xebec:80
5. Defina los servidores.
 - a. **ndcontrol server add xebec:80:ServidorG**
 - b. **ndcontrol server add xebec:80:ServidorH**
 - c. **ndcontrol server add xebec:80:ServidorI**
6. Si utiliza Windows 2000, configure la NFA (dirección de no reenvío) del adaptador de LAN del Dispatcher.
ndcontrol cluster configure ND3

Notas

1. En todos los servidores (A-I), debe unir la dirección de cluster al bucle de retorno por medio de un alias.
2. Los clusters y los puertos se añaden con **ndcontrol** en todas las máquinas Dispatcher participantes: el Dispatcher de punto de entrada y todos los remotos.
3. Consulte “Utilización de asesores remotos con soporte de área amplia” en la página 159 si precisa información sobre la utilización de asesores remotos con soporte de área amplia.
4. El soporte de área amplia prohíbe los bucles infinitos de encaminamiento. (Si una máquina Dispatcher recibe un paquete de otra máquina Dispatcher, no lo reenviará a una tercera). El área amplia solamente da soporte a un solo nivel de máquinas remotas.
5. El área amplia da soporte a UDP y TCP.
6. El área amplia opera junto con la alta disponibilidad: Cada máquina Dispatcher puede estar respaldada por otra máquina adyacente de reserva (en el mismo segmento de la LAN).
7. El Gestor y los Asesores trabajan con el área amplia y, si se utilizan, deben arrancarse en todas las máquinas Dispatcher participantes.
8. Network Dispatcher da soporte a WAND únicamente en sistemas operativos similares.

Soporte de GRE (Generic Routing Encapsulation)

Generic Routing Encapsulation (GRE) es un protocolo de interred cuyas especificaciones están contenidas en los documentos RFC 1701 y RFC 1702. Mediante GRE, el Network Dispatcher puede encapsular paquetes IP de los clientes dentro de paquetes IP/GRE y reenviarlos a plataformas de servidor, tales como OS/390, que dan soporte a GRE. El soporte de GRE permite que el componente Dispatcher reparta el tráfico de paquetes hacia varias direcciones de servidor asociadas a una sola dirección MAC.

Network Dispatcher utiliza GRE como parte de su función WAND (Network Dispatcher de área amplia). Esto permite que Network Dispatcher reparta el tráfico de una área amplia directamente hacia cualquier servidor que pueda desencapsular los paquetes GRE. No es necesario instalar Network Dispatcher en la ubicación remota si los servidores remotos dan soporte a los paquetes GRE encapsulados. Network Dispatcher encapsula los paquetes WAND utilizando el valor decimal 3735928559 para el campo de clave de GRE.

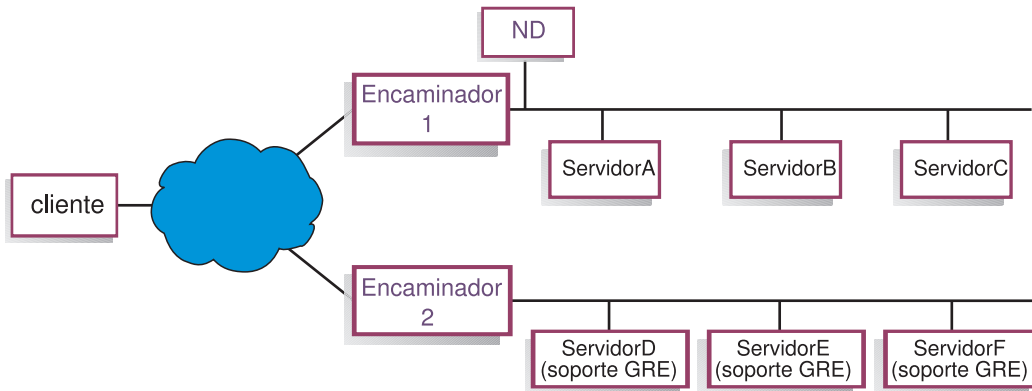


Figura 25. Ejemplo de configuración de área amplia con plataforma de servidor que da soporte a GRE

A los efectos de este ejemplo (Figura 25), para añadir el servidor remoto ServidorD, que da soporte a GRE, defínalo dentro de la configuración de Network Dispatcher como si estuviera definiendo un servidor WAND en la jerarquía `cluster:puerto:servidor`:

```
ndcontrol server add cluster:puerto:ServidorD router Router1
```

Utilización del asesor self en una configuración WAND de dos niveles

El asesor self se puede utilizar en el componente Dispatcher.

En una configuración WAND de dos niveles, Network Dispatcher proporciona un asesor *self* que recoge información sobre el estado del tráfico en los servidores de fondo.

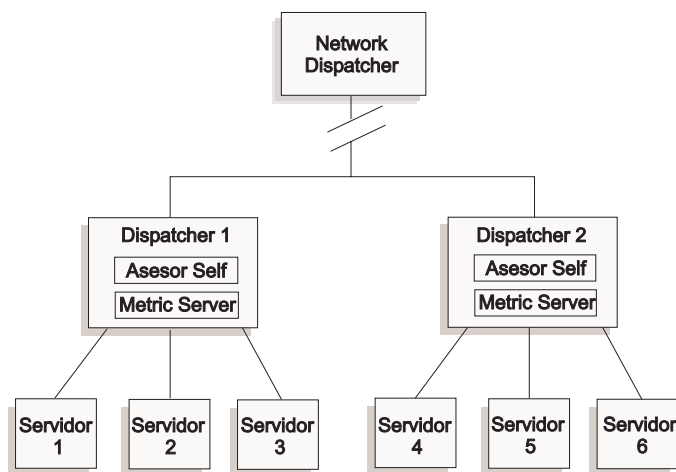


Figura 26. Ejemplo de configuración WAND de dos niveles con utilización del asesor self

En este ejemplo, el asesor self y Metric Server residen en dos máquinas Dispatcher cuyo tráfico se reparte mediante el nivel superior de Network Dispatcher. El asesor self mide específicamente la tasa de conexiones por segundo en los servidores de fondo del Dispatcher a nivel de ejecutor.

El asesor self escribe los resultados en el archivo `ndloadstat`. Network Dispatcher también proporciona una métrica externa llamada `ndload`, la cual es invocada por el agente de Metric Server de cada máquina Dispatcher. El script `ndload` extrae una cadena de texto del archivo `ndloadstat` y la devuelve al agente de Metric Server. Después, cada agente de Metric Server (de cada Dispatcher) devuelve el valor de estado del tráfico al Network Dispatcher de dos niveles, que lo utiliza para determinar a qué Dispatcher debe reenviar las peticiones de los clientes.

El ejecutable `ndload` reside en el directorio `.../nd/ms/script` de Network Dispatcher.

Alta disponibilidad

La característica de alta disponibilidad sólo puede utilizarse con el componente Dispatcher.

Para mejorar la disponibilidad de Dispatcher, la función de alta disponibilidad de Dispatcher utiliza los mecanismos siguientes:

- Dos Dispatchers con conectividad para los mismos clientes y el mismo cluster de servidores, así como conectividad entre los Dispatchers. Ambos Dispatchers deben utilizar el mismo sistema operativo.

- Un mecanismo de “pulsos” (señales de prueba) entre los dos Dispatchers para detectar cualquier anomalía en un Dispatcher. Como mínimo debe haber un par de pulsos cuyas direcciones de no reenvío sean la dirección origen y de destino.

Si es posible, se recomienda que, como mínimo, uno de los pares de pulsos esté en una subred separada del tráfico regular del cluster. Mantener diferenciado el tráfico de pulsos ayudará a impedir falsas tomas de control durante las cargas de red de gran intensidad y también mejorará los tiempos de recuperación completa después de una anomalía.

- Una lista de direcciones y destinos de alcance que ambas máquinas Dispatcher deben poder contactar para que el reparto del tráfico del tráfico sea normal. Para obtener más información, consulte el apartado “Posibilidad de detección de anomalías mediante pulsos y el destino de acceso” en la página 169.
- Sincronización de la información del Dispatcher (es decir, las tablas de conexión, tablas de accesibilidad y otra información).
- Lógica para elegir el Dispatcher activo, encargado de un cluster determinado de servidores, y el Dispatcher de reserva, que se sincroniza de forma continua para ese cluster de servidores.
- Un mecanismo para tomar el control de IP cuando la lógica o un operador decide que la máquina de reserva debe relevar a la máquina activa.

Nota: Para consultar una ilustración y una descripción de una configuración de *alta disponibilidad mutua* en la que dos máquinas Dispatcher que comparten dos conjuntos de cluster son máquinas de reserva entre sí, consulte el apartado “Alta disponibilidad mutua” en la página 48. La alta disponibilidad mutua es similar a la alta disponibilidad pero está basada específicamente en la dirección del cluster en lugar de en una máquina Dispatcher en sí. Ambas máquinas deben configurarse de modo que sus conjuntos de cluster compartidos sean los mismos.

Configurar la característica de alta disponibilidad

La sintaxis completa de **ndcontrol highavailability** se encuentra en “ndcontrol highavailability — controlar la alta disponibilidad” en la página 272.

Si desea obtener una explicación más completa de la mayoría de las tareas indicadas a continuación, consulte “Configurar la máquina Dispatcher” en la página 58.

1. Inicie el servidor en ambas máquinas servidor de Dispatcher.
2. Inicie el ejecutor en ambas máquinas.
3. Asegúrese de que la dirección de no reenvío (NFA) de cada máquina Dispatcher está configurada, y es una dirección IP válida para la subred de las máquinas Dispatcher.

Sólo para Windows 2000: Configure también todas las direcciones de no reenvío con el mandato **ndconfig**. Por ejemplo:

```
ndconfig en0 dirección_nfa netmask máscara_red
```

4. Configure la información referente al cluster, los puertos y los servidores en ambas máquinas.

Nota: Por ejemplo, para una configuración de alta disponibilidad mutua (Figura 14 en la página 48), puede configurar los conjuntos de clusters compartidos entre las dos máquinas Dispatcher del modo siguiente:

- Para la máquina Dispatcher 1, especifique:

```
ndcontrol cluster set clusterA primaryhost dispatcherNFA1  
ndcontrol cluster set clusterB primaryhost dispatcherNFA2
```

- Para la máquina Dispatcher 2, especifique:

```
ndcontrol cluster set clusterB primaryhost dispatcherNFA2  
ndcontrol cluster set clusterA primaryhost dispatcherNFA1
```

5. Arranque el gestor y los asesores en ambas máquinas. El asesor "reach" arranca automáticamente mediante la función del gestor.
6. Cree los archivos de script de alias para cada una de las 2 máquinas Dispatcher. Consulte "Utilización de scripts" en la página 170.
7. Añada la información de pulso en ambas máquinas:

```
ndcontrol highavailability heartbeat add dirección_origen dirección_destino
```

Nota: *Dirección_origen* y *dirección_destino* son las direcciones IP (nombres DNS o direcciones decimales con puntos) de las máquinas Dispatcher. Los valores estarán invertidos en cada máquina. Ejemplo:

```
Principal - highavailability heartbeat add  
9.67.111.3 9.67.186.8  
Reserva - highavailability heartbeat add 9.67.186.8 9.67.111.3
```

Como mínimo debe haber un par de pulsos cuyas direcciones de no reenvío sean la dirección origen y de destino.

Si es posible, se recomienda que, como mínimo, uno de los pares de pulsos esté en una subred separada del tráfico regular del cluster. Mantener diferenciado el tráfico de pulsos ayudará a impedir falsas tomas de control durante las cargas de red de gran intensidad y también mejorará los tiempos de recuperación completa después de una anomalía.

8. Configure en ambas máquinas la lista de direcciones IP a las que Dispatcher debe acceder con el fin de garantizar un servicio completo, utilizando el mandato **reach add** . Ejemplo:

```
ndcontrol highavailability reach add 9.67.125.18
```

Se recomienda utilizar destinos de acceso aunque éstos no son necesarios. Consulte el apartado “Posibilidad de detección de anomalías mediante pulsos y el destino de acceso” en la página 169 para obtener más información.

9. Añada la información sobre la máquina de reserva a cada máquina:

- Para la máquina **principal**:

```
ndcontrol highavailability backup add primary [auto | manual] puerto
```

- Para la máquina de **reserva**:

```
ndcontrol highavailability backup add backup [auto | manual] puerto
```

- En la característica de alta disponibilidad mutua cada máquina Dispatcher tiene **ambas** funciones, esto es, máquina principal y máquina de reserva:

```
ndcontrol highavailability backup add both [auto | manual] puerto
```

Nota: Seleccione un número de puerto no utilizado en las máquinas como *puerto*. Las dos máquinas se comunicarán a través de este puerto.

10. Compruebe el estado de la característica de alta disponibilidad en cada máquina:

```
ndcontrol highavailability status
```

Cada una de las máquinas debe tener la función correcta (máquina de reserva, máquina principal o ambas) y los estados y subestados correctos. La principal debe estar activa y sincronizada; la de reserva debe estar en modalidad de espera y debe quedar sincronizada en un corto plazo de tiempo. Las estrategias deben ser idénticas.

Notas:

1. Para configurar una sola máquina Dispatcher para que encamine los paquetes sin ninguna máquina de reserva, no emita ninguno de los mandatos de alta disponibilidad en el arranque.
2. Para convertir dos máquinas Dispatcher configuradas para alta disponibilidad en una sola que funcione de forma autónoma, detenga el ejecutor en una de las máquinas y, a continuación, suprima las características de alta disponibilidad (pulsos, accesibilidad y función de reserva) en la otra.
3. En los dos casos anteriores, debe unir la tarjeta de interfaz de red con las direcciones de cluster por medio de un alias, según convenga.
4. Cuando las dos máquinas Dispatcher se ejecutan con la configuración de alta disponibilidad y están sincronizadas, se recomienda entrar primero todos los mandatos ndcontrol (para actualizar la configuración) en la máquina de reserva y después en la máquina activa.

5. Cuando hay dos máquinas Dispatcher ejecutándose en una configuración de alta disponibilidad, pueden producirse resultados imprevistos si establece valores diferentes en cada máquina para los parámetros del ejecutor, cluster, puerto o servidor (por ejemplo, `port stickytime`).
6. En la modalidad de alta disponibilidad mutua, tenga en cuenta el caso en el que una de las dos máquinas Dispatcher debe encaminar activamente paquetes para su cluster principal y al mismo tiempo debe encaminar paquetes para el cluster de reserva. Es necesario asegurarse de que esto no superará la capacidad de rendimiento de esta máquina.
7. Para Linux, cuando se configura la modalidad de alta disponibilidad y la ubicación compartida al mismo tiempo que se utiliza el método de reenvío MAC para puertos del componente Dispatcher, se debe instalar un parche de kernel de Linux. Para obtener más información sobre la instalación del parche, consulte la sección “Instalación del parche del kernel de Linux (para suprimir las respuestas a arp en la interfaz de bucle de retorno)” en la página 70.

Posibilidad de detección de anomalías mediante pulsos y el destino de acceso

Además del criterio básico de detección de errores (pérdida de conectividad entre los Dispatchers activo y de reserva, detectada a través de los mensajes de pulsos), existe otro mecanismo de detección de errores denominado *criterio de accesibilidad*. Cuando configure el Dispatcher, puede proporcionar una lista de sistemas principales a los que cada Dispatcher debe poder acceder para funcionar correctamente.

Debe elegir al menos un sistema principal para cada subred que utilice la máquina Dispatcher. Los sistemas principales pueden ser encaminadores, servidores IP u otros tipos de sistemas principales. El asesor de acceso averigua la accesibilidad del sistema principal enviándole mensajes de prueba. El relevo tiene lugar si los mensajes de prueba no pueden establecer conexión, o si los criterios de accesibilidad los cumple en mayor grado el Dispatcher de reserva que el Dispatcher principal. Para tomar la decisión basándose en toda la información disponible, el Dispatcher activo envía con regularidad al Dispatcher de reserva sus capacidades de acceso. El Dispatcher de reserva compara entonces estas capacidades con la suya propia y decide si ha de tomar el relevo.

Nota: Cuando configure el destino de reach, debe también iniciar el *asesor reach*. El asesor reach arranca automáticamente mediante la función del gestor. Para conseguir más información sobre el asesor reach, vea la página 144.

Estrategia de recuperación

Se configuran dos máquinas Dispatcher: la máquina principal y una segunda máquina llamada *de reserva*. Al arrancar, la máquina principal envía todos los

datos de conexión a la máquina de reserva, hasta que ésta queda sincronizada. La máquina principal pasa a estar *activa*, es decir, comienza a repartir el tráfico. Mientras tanto, la máquina de reserva supervisa el estado de la máquina principal y se dice que está en *estado de espera*.

Si la máquina de reserva detecta en cualquier momento que la máquina principal ha fallado, *toma el control* de las funciones de reparto del tráfico de la máquina principal y se convierte en la máquina activa. Cuando la máquina principal vuelve a ser funcional, el comportamiento de las máquinas depende de cómo haya configurado el usuario la *estrategia* de recuperación. Existen dos tipos de estrategia:

Automática

La máquina principal reanuda el encaminamiento de paquetes en cuanto vuelve a ser funcional.

Manual

La máquina de reserva sigue encaminando paquetes incluso después de que la máquina principal vuelva a ser funcional. Es necesaria una intervención manual para devolver la máquina principal al estado activo y la máquina de reserva al estado de espera.

El parámetro de estrategia debe ser el mismo para ambas máquinas.

La estrategia de recuperación manual permite forzar el encaminamiento de paquetes a una máquina en concreto, utilizando el mandato de relevo. La recuperación manual resulta útil cuando se realiza el mantenimiento en la otra máquina. La estrategia de recuperación automática está pensada para el funcionamiento normal desatendido.

En una configuración de alta disponibilidad mutua, no puede haber una anomalía para un solo cluster. Si se produce un problema en una de las máquinas, incluso si solo afecta a uno de los clusters, la otra máquina tomará el control de ambos clusters.

Nota: Durante situaciones de toma de control, puede que se pierdan algunas actualizaciones de conexión. Esto puede hacer que se pierdan conexiones existentes de larga duración (como telnet) a las que se accede en el momento de la toma de control.

Utilización de scripts

Para que Dispatcher encamine paquetes, cada dirección de cluster debe estar unida a un dispositivo de interfaz de red por medio de un alias.

- En una configuración de Dispatcher autónoma, cada dirección de cluster debe estar unida a una tarjeta de interfaz de red por medio de un alias (por ejemplo, en0, tr0).
- En una configuración de alta disponibilidad:

- En la máquina activa, cada dirección de cluster debe estar unida a una tarjeta de interfaz de red (por ejemplo, en0, tr0) por medio de un alias.
- En la máquina de reserva, cada dirección de red debe estar asociada a un dispositivo de bucle de retorno (por ejemplo, lo0) por medio de un alias.
- En cualquier máquina en la que se haya detenido el ejecutor, deben eliminarse los alias para evitar conflictos con otra máquina que pueda iniciarse.

Puesto que las máquinas Dispatcher cambian de estado cuando se detecta una anomalía, los mandatos anteriores deben emitirse de forma automática. Dispatcher ejecutará scripts creados por el usuario para hacerlo. Puede encontrar scripts de ejemplo en el directorio **...nd/servers/samples** y *debe* trasladarlos al directorio **...nd/servers/bin** para ejecutarlos.

Nota: En una configuración de alta disponibilidad mutua, la máquina Dispatcher llamará a cada script “go” con un parámetro que identifica la dirección de la máquina Dispatcher principal. El script debe consultar este parámetro y ejecutar los mandatos **ifconfig** (o los mandatos **ndconfig** si se utiliza Windows 2000) para las direcciones de cluster que estén asociadas a la máquina Dispatcher principal.

Se pueden utilizar los scripts de ejemplo siguientes:

goActive

El script goActive se ejecuta cuando un Dispatcher pasa al estado activo y empieza a encaminar paquetes.

- Si ejecuta Dispatcher en una configuración de alta disponibilidad, debe crear este script. Este script suprime los alias de bucle de retorno y añade alias de dispositivo.
- Si ejecuta Dispatcher en una configuración autónoma, no es necesario que cree este script.

goStandby

El script goStandby se ejecuta cuando un Dispatcher pasa al estado de espera y supervisa el estado de la máquina activa, pero no encamina ningún paquete.

- Si ejecuta Dispatcher en una configuración de alta disponibilidad, debe crear este script. Este script debe suprimir los alias de dispositivo y añadir alias de bucle de retorno.
- Si ejecuta Dispatcher en una configuración autónoma, no es necesario que cree este script.

goInOp

El script goInOp se ejecuta cuando se detiene el ejecutor de un Dispatcher y antes de iniciarlo por primera vez.

- Si normalmente ejecuta Dispatcher en una configuración de alta disponibilidad mutua, debe crear este script. Este script suprime todos los alias de bucle de retorno y dispositivo.
- Si normalmente ejecuta Dispatcher en una configuración autónoma, este script es opcional. Puede crearlo y hacer que suprima los alias de dispositivo o puede optar por suprimirlos manualmente.

goIdle El script goIdle se ejecuta cuando un Dispatcher entra en el estado de inactividad y empieza a encaminar paquetes. Esto sucede cuando no se han añadido las características de alta disponibilidad, como por ejemplo en una configuración autónoma. También sucede en una configuración de alta disponibilidad, antes de añadir las características de alta disponibilidad o después de eliminarlas.

- Si normalmente ejecuta Dispatcher en una configuración de alta disponibilidad, **no** debe crear este script.
- Si normalmente ejecuta Dispatcher en una configuración autónoma, este script es opcional. Puede crearlo y hacer que añada los alias de dispositivo o puede optar por añadirlos manualmente. Si no crea este script para la configuración autónoma, deberá utilizar el mandato de configuración de cluster **ndcontrol** o configurar manualmente los alias cada vez que arranque el ejecutor.

highavailChange

El script highavailChange se ejecuta cada vez que cambia el estado de alta disponibilidad dentro del Dispatcher y se invoca un script "go". El único parámetro que se pasa a este script es el nombre del script "go" que acaba de ser ejecutado por Dispatcher. Puede crear este script para utilizar información sobre cambios de estado, por ejemplo, para avisar a un administrador o simplemente para registrar el evento.

Nota: Para Windows 2000: En la configuración, si Site Selector distribuye el tráfico de dos máquinas Dispatcher que funcionan en un entorno de alta disponibilidad, tendrá que añadir un alias en la pila de Microsoft para los servidores de métrica. Este alias se debe añadir al script goActive. Por ejemplo:

```
call netsh interface ip add address "Local Area Connection"
    addr=9.37.51.28 mask=255.255.240.0
```

En goStandby y en GoInOp, el alias se tiene que eliminar. Por ejemplo:

```
call netsh interface ip delete address "Local Area Connection"
    addr=9.37.51.28
```

Si hay varios NIC en la máquina, primero compruebe qué interfaz debe utilizar emitiendo en siguiente mandato en el indicador de mandatos: netsh interface ip show address. Este mandato devolverá una lista de

las interfaces actualmente configuradas y numerará "Local Area Connection" (por ejemplo, "Local Area Connection 2") de modo que pueda determinar cuál debe utilizar.

Configurar el reparto del tráfico basado en normas

Se puede utilizar el reparto del tráfico basado en normas para ajustar cuándo y cómo se envían los paquetes y a qué servidores. Network Dispatcher revisa las normas añadidas por el usuario desde la prioridad más alta hasta la más baja, deteniéndose en la primera norma que encuentre que sea cierta y, después, reparte el contenido entre los servidores asociados a la norma. El tráfico ya se ha repartido según el destino y el puerto, pero la utilización de normas amplía la capacidad para distribuir conexiones.

En la mayoría de los casos, al configurar normas, es conveniente definir una norma por omisión **always true** para recoger las peticiones no atendidas por las demás normas de mayor prioridad. Esto puede adoptar la forma de una respuesta del tipo "El sitio Web está actualmente fuera de servicio; pruebe más tarde", cuando todos los demás servidores no atienden la petición del cliente.

Debe utilizar el reparto del tráfico basado en normas junto con Dispatcher y Site Selector cuando desee utilizar un subconjunto de servidores por alguna razón. *Debe* siempre utilizar normas para el componente CBR.

Nota: La configuración que utiliza normas *no* es aplicable a Mailbox Locator (que dirige peticiones IMAP o POP3 hacia determinados servidores basándose en el ID de usuario y la contraseña) ni tampoco a Cisco Consultant (que hace uso del gestor y los asesores para repartir el tráfico hacia el Cisco CSS Switch) .

Puede utilizar los siguientes tipos de normas:

- Para Dispatcher:
 - Dirección IP del cliente
 - Hora del día
 - Conexiones por segundo de un puerto
 - Conexiones totales activas de un puerto
 - Puerto cliente
 - Tipo de servicio (TOS)
 - Ancho de banda reservado
 - Ancho de banda compartido
 - Siempre verdadero
 - Contenido de una petición

- Para CBR:
 - Dirección IP del cliente
 - Hora del día
 - Conexiones por segundo de un puerto
 - Conexiones totales activas de un puerto
 - Siempre verdadero
 - Contenido de una petición
- Para Site Selector:
 - Dirección IP del cliente
 - Hora del día
 - Métrica total
 - Métrica promedio
 - Siempre verdadero

Antes de empezar a añadir normas a la configuración, se recomienda planificar la lógica que desea que sigan las normas.

¿Cómo se evalúan las normas?

Todas las normas tienen un nombre, tipo, prioridad, y pueden tener un inicio de rango y un final de rango, junto con un grupo de servidores. Además, la norma de tipo de contenido del componente CBR tiene asociada una expresión regular. (Para conocer ejemplos y casos prácticos de cómo utilizar la norma de contenido y la sintaxis válida de la expresión regular para dicha norma, consulte “Apéndice C. Sintaxis de la norma de contenido (patrón):” en la página 313.)

Las normas se evalúan por orden de prioridad. Es decir, una norma con prioridad 1 se evaluará antes que una norma con prioridad 2. Se utilizará la primera norma que se cumpla. Una vez que se satisface una norma, las normas posteriores no se evalúan.

Para que se satisfaga una norma, debe cumplir dos condiciones:

1. El predicado de la norma debe ser verdadero. Esto es, el valor que se está evaluando debe estar comprendido entre el inicio y el final de rango, o el contenido debe coincidir con la expresión regular especificada en el patrón de la norma de contenido. Para las normas de tipo “verdadero”, el predicado siempre se cumple, sin tener en cuenta los inicios y finales de rango.
2. Si se encuentran servidores asociados a la norma, al menos uno de ellos debe estar disponible para que se le envíen paquetes.

Si una norma no tiene servidores asociados, la norma sólo necesita cumplir la primera condición para que sea cierta. En este caso, Dispatcher eliminará la

petición de conexión, Site Selector devolverá la petición del servidor de nombres junto con un error y CBR hará que Caching Proxy devuelva una página de error.

Si no se cumple ninguna norma, Dispatcher seleccionará un servidor del conjunto total de servidores disponibles en el puerto, Site Selector seleccionará un servidor de entre los disponibles en el nombre de sitio y CBR hará que Caching Proxy devuelva una página de error.

Utilización de normas basadas en la dirección IP del cliente

Este tipo de norma se puede utilizar en el componente Dispatcher, CBR o Site Selector.

Puede que desee utilizar las normas basadas en la dirección IP del cliente si desea examinar los clientes y asignar recursos según su procedencia.

Por ejemplo, puede detectar que la red recibe gran cantidad de tráfico no deseado que procede de un determinado conjunto de direcciones IP, asignadas a diversos clientes morosos. Puede crear una norma por medio del mandato **ndcontrol rule**, por ejemplo:

```
ndcontrol rule add 9.67.131.153:80:ni type ip  
    beginrange 9.0.0.0 endrange 9.255.255.255
```

Esta norma "ni" rechazaría cualquier conexión procedente de clientes IBM. A continuación podría añadir a la norma los servidores accesibles por los clientes de IBM; si no añade ningún servidor a la norma, las peticiones procedentes de las direcciones 9.x.x.x no las atenderá ningún servidor.

Utilización de normas basadas en la hora del día

Este tipo de norma se puede utilizar en el componente Dispatcher, CBR o Site Selector.

Puede que desee utilizar normas basadas en la hora del día por motivos de planificación de los recursos. Por ejemplo, si su sitio Web recibe más visitas a las mismas horas del día, puede que desee dedicar cinco servidores a HTTP durante todo el día y añadir cinco más en las horas punta.

Otra razón por la que podría utilizar una norma basada en la hora del día es que desee desactivar varios servidores todos los días a medianoche para mantenimiento, en cuyo caso podría establecer una norma que excluyese estos servidores durante el período de mantenimiento necesario.

Utilización de normas basadas en las conexiones por segundo de un puerto

Este tipo de norma se puede utilizar en el componente Dispatcher y CBR.

Nota: Para que las siguientes acciones resulten efectivas, el gestor debe estar ejecutándose.

Puede que desee utilizar normas basadas en las conexiones por segundo de un puerto si necesita compartir algunos servidores con otras aplicaciones. Por ejemplo, puede establecer dos normas:

1. Si las conexiones por segundo del puerto 80 > 100 utilizar estos 2 servidores
2. Si las conexiones por segundo del puerto 80 > 2000 utilizar estos 10 servidores

O puede que esté utilizando Telnet y desee reservar dos de los cinco servidores para Telnet, excepto cuando las conexiones por segundo se incrementen por encima de cierto nivel. De esta manera, el Dispatcher podría repartir el tráfico entre los cinco servidores en las horas punta.

Utilización de normas basadas en el total de conexiones activas en un puerto

Este tipo de norma se puede utilizar en el componente Dispatcher y CBR.

Nota: Para que las siguientes acciones resulten efectivas, el gestor debe estar ejecutándose.

Puede que desee utilizar normas basadas en el total de conexiones activas de un puerto si los servidores están sobrecargados y comienzan a descartar paquetes. Ciertos servidores Web continuarán aceptando conexiones, aunque no tengan subprocesos suficientes para responder a la petición. Como resultado, las peticiones de los clientes agotan el tiempo de espera y el cliente que accede al sitio Web no resulta atendido. Para repartir el tráfico entre una agrupación de servidores, se pueden utilizar normas basadas en las conexiones activas.

Por ejemplo, usted sabe por experiencia que sus servidores dejarán de atender a los clientes después de haber aceptado 250 conexiones. Puede crear una norma utilizando el mandato **ndcontrol rule** o el mandato **cbrcontrol rule**, por ejemplo:

```
ndcontrol rule add 130.40.52.153:80:pool2 type active  
beginrange 250 endrange 500
```

o bien

```
cbrcontrol rule add 130.40.52.153:80:pool2 type active  
beginrange 250 endrange 500
```

A continuación podría añadir a la norma los servidores actuales, además de algunos servidores adicionales que de otra manera se utilizarían para otros procesos.

Utilización de normas basadas en el puerto del cliente

Este tipo de norma sólo está disponible en el componente Dispatcher.

Puede que desee utilizar normas basadas en el puerto del cliente si los clientes están utilizando algún tipo de software que solicita un puerto TCP/IP determinado cuando realiza las peticiones.

Por ejemplo, podría crear una norma que especifique que cualquier petición con el puerto cliente 10002 utilizará un conjunto especial de servidores rápidos, ya que las peticiones que llegan por ese puerto proceden de clientes preferentes.

Utilización de normas basadas en el tipo de servicio (TOS)

Este tipo de norma sólo está disponible en el componente Dispatcher.

Es posible que desee utilizar normas basadas en el contenido del campo “tipo de servicio” (TOS) de la cabecera IP. Por ejemplo, si se recibe una petición de cliente con un valor de TOS que indica que se trata de un servicio normal, la petición se puede encaminar hacia un grupo de servidores. Si se recibe una petición de cliente diferente con un valor de TOS diferente que indica que se trata de un servicio de prioridad más alta, la petición se puede encaminar hacia un grupo de servidores diferente.

La norma TOS le permite configurar completamente cada uno de los bits del byte TOS utilizando el mandato **ndcontrol rule**. Para los bits significativos que desea que coincidan con el byte TOS, utilice 0 ó 1. De lo contrario, se utiliza el valor x. El siguiente es un ejemplo de cómo añadir una norma TOS:

```
ndcontrol rule add 9.67.131.153:80:tsr type service tos 0xx1010x
```

Utilización de normas basadas en el ancho de banda reservado y en el ancho de banda compartido

La utilización de capacidad y las normas de ancho de banda sólo se pueden utilizar en el componente Dispatcher.

Mediante la utilización de capacidad, Dispatcher mide el volumen de datos entregados por cada servidor. Dispatcher hace un seguimiento de la capacidad a nivel de servidor, norma, puerto, cluster y ejecutor. Para cada uno de estos niveles existe un nuevo valor contador de bytes: los kilobytes transferidos por segundo. Esta tasa (kilobytes transferidos por segundo) se calcula para un intervalo de 60 segundos. Puede visualizar estos valores de capacidad desde la GUI o en la salida de un informe de línea de mandatos.

Dispatcher le permite asignar un ancho de banda especificado a grupos de servidores de la configuración utilizando la norma de *ancho de banda reservado*. Cuando el tráfico excede el valor umbral de ancho de banda reservado, el usuario tiene opciones:

- Enviar el tráfico hacia otro servidor, utilizando una norma "siempre verdadero", que responde con un mensaje del tipo "sitio ocupado".
- O compartir una cantidad especificada de ancho de banda a nivel de cluster o de ejecutor utilizando la norma de *ancho de banda compartido*. Y, cuando está próximo el valor umbral de ancho de banda compartido, puede enviar el tráfico hacia otro servidor, utilizando una norma "siempre verdadero", que responde con un mensaje del tipo "sitio ocupado".

El uso combinado de las normas de ancho de banda reservado y ancho de banda compartido, tal como se describieron anteriormente, le permite ofrecer a clientes determinados un mejor acceso al servidor y por tanto optimizar el rendimiento de las transacciones. Por ejemplo, mediante el uso del ancho de banda compartido para adquirir ancho de banda no utilizado, puede permitir que los clientes que realizan transacciones comerciales en clusters de servidores reciban un mayor acceso que los clientes que utilizan otros clusters de servidores para el análisis de inversiones.

Tenga en cuenta lo siguiente para determinar si las normas de ancho de banda pueden ayudarle a gestionar el volumen del tráfico de respuesta que circula desde los servidores a los clientes:

- Las normas de ancho de banda pueden ayudar a gestionar el volumen del tráfico de respuesta procedente de máquinas servidor, basándose en las peticiones de los clientes, que circulan por Network Dispatcher. Si parte del tráfico procedente de los clientes va directamente al servidor y no es detectado por Network Dispatcher, los resultados pueden ser imprevisibles.
- Las normas de ancho de banda pueden ayudar a gestionar el volumen del tráfico de respuesta que circula por un enlace desde un grupo de máquinas servidor hacia la red, cuando todos los servidores utilizan el mismo enlace con la red. Si los servidores utilizan enlaces diferentes o varios enlaces para acceder a la red, los resultados para cada enlace individual pueden ser imprevisibles.
- Las normas de ancho de banda sólo son útiles cuando todos los servidores residen en la misma red local que la máquina de Network Dispatcher. Si algunos servidores son remotos, con rutas diferentes para acceder a la red, los resultados pueden ser imprevisibles.

Norma del ancho de banda reservado

Este tipo de norma sólo está disponible en el componente Dispatcher.

La norma del ancho de banda reservado le permite repartir el tráfico basándose en el número de kilobytes por segundo entregados por un grupo de servidores. Puede definir un valor umbral (asignando un rango de ancho de banda especificado) para cada grupo de servidores de la configuración, y de esta forma controlar y asegurar el ancho de banda utilizado por cada

combinación cluster-puerto. Lo siguiente es un ejemplo de cómo añadir una norma de ancho de banda reservado (`reservedbandwidth`):

```
ndcontrol rule add 9.67.131.153:80:rbw type reservedbandwidth  
beginrange 0 endrange 300
```

El inicio de rango y el final de rango se especifican en kilobytes por segundo.

Norma del ancho de banda compartido

Este tipo de norma sólo está disponible en el componente Dispatcher.

Si el volumen de datos transferidos supera el límite definido por la norma del ancho de banda reservado, la norma del ancho de banda compartido le permite adquirir ancho de banda no utilizado que esté disponible en el sitio Web. Puede configurar esta norma para compartir ancho de banda a nivel de cluster o de ejecutor. El ancho de banda compartido a nivel de cluster permite el uso compartido de un ancho de banda máximo por varios puertos (aplicaciones/protocolos) dentro del mismo cluster. El ancho de banda compartido a nivel de ejecutor permite el uso compartido de un ancho de banda máximo por varios clusters dentro de la configuración completa de Dispatcher.

Antes de configurar la norma del ancho de banda compartido, debe especificar el ancho de banda máximo (kilobytes por segundo) que se puede compartir a nivel de ejecutor o de cluster, utilizando el mandato **ndcontrol ejecutor** o **ndcontrol cluster** con la opción `sharedbandwidth`. A continuación se muestran ejemplos de la sintaxis de los mandatos:

```
ndcontrol executor set sharedbandwidth tamaño  
ndcontrol cluster [add | set] 9.12.32.9 sharedbandwidth tamaño
```

El valor *tamaño* para ancho de banda compartido (`sharedbandwidth`) es un valor entero (kilobytes por segundo). El valor por omisión es 0. Si el valor es 0, no se puede compartir el ancho de banda. Debe especificar un ancho de banda compartido máximo que no exceda el ancho de banda total disponible (capacidad total del servidor).

Los ejemplos siguientes muestran cómo añadir o definir una norma de ancho de banda compartido (`sharedbandwidth`):

```
ndcontrol rule add 9.20.30.4:80:shbw type sharedbandwidth sharelevel valor  
ndcontrol rule set 9.20.34.11:80:shrul sharelevel valor
```

El *valor* para el nivel de compartimiento (`sharelevel`) es `executor` o `cluster`. `Sharelevel` es un parámetro obligatorio de la norma de ancho de banda compartido.

Norma de la métrica total

Este tipo de norma sólo puede utilizarse en el componente Site Selector.

Para la norma de la métrica total, el usuario selecciona una métrica del sistema (cpuload, memload o un script personalizado de métricas del sistema) y Site Selector compara el valor de métrica del sistema (devuelto por el agente de Metric Server que reside en cada servidor con reparto del tráfico) con el inicio y final de rango especificados en la norma. El valor actual de la métrica del sistema para todos los servidores del grupo debe estar dentro del rango para que se aplique la norma.

Nota: El script de métricas del sistema que seleccione debe residir en cada uno de los servidores donde se realiza reparto del tráfico.

El ejemplo siguiente muestra cómo añadir una norma de métrica total a la configuración:

```
sscontrol rule add dnsload.com:allrule1 type metricall  
metricname cpuload beginrange 0 endrange 100
```

Norma de la métrica promedio

Este tipo de norma sólo puede utilizarse en el componente Site Selector.

Para la norma de la métrica promedio, el usuario selecciona una métrica del sistema (cpuload, memload o un script personalizado de métricas del sistema) y Site Selector compara el valor de métrica del sistema (devuelto por el agente de Metric Server que reside en cada servidor con reparto del tráfico) con el inicio y final de rango especificados en la norma. El *promedio* de los valores actuales de métricas del sistema para todos los servidores del grupo debe estar dentro del rango para que se aplique la norma.

Nota: El script de métricas del sistema que seleccione debe residir en cada uno de los servidores donde se realiza reparto del tráfico.

El ejemplo siguiente muestra cómo añadir una norma de métrica promedio a la configuración:

```
sscontrol rule add dnsload.com:avgrule1 type metricavg  
metricname cpuload beginrange 0 endrange 100
```

Utilización de normas que son siempre ciertas

Este tipo de norma se puede utilizar en el componente Dispatcher, CBR o Site Selector.

Se puede crear una norma que sea “siempre cierta”. Dicha norma se seleccionará siempre, a no ser que todos los servidores asociados a ella se encuentren desactivados. Por esta razón, debe tener generalmente una prioridad más baja que las demás normas.

Incluso se pueden tener varias normas “siempre ciertas”, cada una de ellas asociada a un conjunto de servidores. Se selecciona la primera norma con un servidor disponible. Por ejemplo, supongamos que usted tiene seis servidores.

Desea que dos de ellos manejen el tráfico en todas las circunstancias, a no ser que ambos estén desactivados. Si los dos servidores están desactivados, desea que un segundo conjunto de dos servidores se encargue de manejar el tráfico. Si estos cuatro servidores están desactivados, se utilizarán los dos servidores restantes para manejar el tráfico. Podría establecer tres normas “siempre ciertas”. De esta manera se seleccionará el primer par de servidores, siempre que al menos uno de ellos esté activado. Si ambos están desactivados, se seleccionará uno de los servidores del segundo par, y así sucesivamente.

Otro ejemplo: puede que desee una norma “siempre cierta” para garantizar que no se atienda a los clientes entrantes si no cumplen ninguna de las normas establecidas. Se podría crear una norma por medio del mandato **ndcontrol rule** de una manera semejante a esta:

```
ndcontrol rule add 130.40.52.153:80:jamais type true priority 100
```

A continuación, podría no añadir ningún servidor a la norma, lo que ocasionaría que los paquetes de los clientes se desechasen sin respuesta.

Nota: Cuando se crea una norma siempre cierta, no es necesario establecer un inicio o final de rango.

Puede definir más de una norma “siempre cierta” y designar posteriormente cuál de ellas se ejecutará por medio de la modificación de sus respectivos niveles de prioridad.

Utilización de normas basadas en el contenido de la petición

Este tipo de norma se puede utilizar en el componente Dispatcher y CBR.

Es aconsejable utilizar normas de tipo de contenido para enviar peticiones a conjuntos de servidores configurados específicamente para manejar una parte determinada del tráfico de su sitio Web. Por ejemplo, si desea utilizar un conjunto de servidores para manejar todas las peticiones *cgi-bin*, otro conjunto para manejar todas las peticiones de sonido continuo y un tercer conjunto para manejar todas las demás peticiones, añadiría una norma con un patrón que coincidiese con la vía del directorio *cgi-bin*, otra que coincidiese con el tipo de archivo de los archivos de sonido continuo y una tercera norma siempre cierta para manejar el resto del tráfico. Después, añadiría los servidores adecuados para cada una de las normas.

Importante: Para conocer ejemplos y casos prácticos de cómo utilizar la norma de contenido y la sintaxis válida de la expresión regular para dicha norma, consulte “Apéndice C. Sintaxis de la norma de contenido (patrón):” en la página 313.

Adición de normas a la configuración

Puede añadir normas utilizando el mandato **ndcontrol rule add**, editando el archivo de configuración de ejemplo o mediante la interfaz gráfica de usuario (GUI). Se pueden añadir una o varias normas a cada uno de los puertos definidos.

Se trata de un proceso en dos etapas: se añade la norma y posteriormente se define a qué servidores atender si la norma es verdadera. Por ejemplo, nuestro administrador del sistema desea efectuar un seguimiento de la utilización de los servidores proxy por parte de cada división del sitio Web. El administrador conoce las direcciones IP asignadas a cada una de las divisiones. Se podría crear el primer conjunto de normas basado en la dirección IP del cliente para separar el tráfico de cada división:

```
ndcontrol rule add 130.40.52.153:80:div1 type ip b 9.1.0.0 e 9.1.255.255
ndcontrol rule add 130.40.52.153:80:div2 type ip b 9.2.0.0 e 9.2.255.255
ndcontrol rule add 130.40.52.153:80:div3 type ip b 9.3.0.0 e 9.3.255.255
```

A continuación, se podría añadir un servidor diferente a cada norma y medir el tráfico en cada uno de los servidores para facturar a cada división por los servicios que utilizan. Por ejemplo:

```
ndcontrol rule useserver 130.40.52.153:80:div1 207.72.33.45
ndcontrol rule useserver 130.40.52.153:80:div2 207.72.33.63
ndcontrol rule use server 130.40.52.153:80:div3 207.72.33.47
```

Opción de evaluación de servidor para normas

La opción de evaluación de servidor sólo puede utilizarse en el componente Dispatcher.

El mandato **ndcontrol rule** tiene una opción de evaluación de servidor para normas. Utilice la opción *evaluate* para evaluar la condición de una norma en todos los servidores del puerto o para evaluar la condición sólo en los servidores comprendidos en la norma. (En versiones anteriores de Network Dispatcher, sólo se podía evaluar la condición de cada norma en todos los servidores del puerto).

Nota: La opción de evaluación de servidor sólo es válida para las normas basadas en características de los servidores: norma de conexiones totales (por segundo), norma de conexiones activas y norma de ancho de banda reservado.

Los ejemplos siguientes muestran cómo añadir o definir una opción de evaluación en una norma de ancho de banda reservado:

```
ndcontrol rule
add 9.22.21.3:80:rbweval type reservedbandwidth evaluate nivel
ndcontrol rule set 9.22.21.3:80:rbweval evaluate nivel
```


El *nivel* de evaluación puede ser "port" (puerto) o "rule" (norma). El valor por omisión es "port".

Evaluación de servidores comprendidos en una norma

La opción para evaluar la condición de una norma en los servidores comprendidos en la norma le permite configurar dos normas con estas características:

- La primera norma que se evalúa contiene todos los servidores que realizan el mantenimiento del contenido del sitio Web, y la opción de evaluación se establece en *rule* (evaluar la condición de la norma en los servidores comprendidos en la norma).
- La segunda norma es una norma siempre verdadera que contiene un servidor individual que responde con una respuesta del tipo "sitio ocupado".

El resultado es que cuando el tráfico excede el valor umbral de los servidores comprendidos en la primera norma, el tráfico se envía al servidor de "sitio ocupado" comprendido en la segunda norma. Cuando el tráfico disminuye por debajo del valor umbral de los servidores comprendidos en la primera norma, el tráfico subsiguiente se envía de nuevo a los servidores de la primera norma.

Evaluación de servidores del puerto

Mediante las dos normas descritas en el ejemplo anterior, si establece la opción de evaluación en *port* para la primera norma (evaluar la condición de la norma en todos los servidores del puerto), cuando el tráfico excede el valor umbral de esa norma, el tráfico se envía al servidor de "sitio ocupado" comprendido en la segunda norma.

La primera norma mide el tráfico de todos los servidores del puerto (incluido el servidor de "sitio ocupado") para determinar si el tráfico excede el valor umbral. Cuando el tráfico disminuye para los servidores de la primera norma, se puede producir un resultado imprevisto cuando el tráfico sigue enviándose hacia el servidor de "sitio ocupado" debido a que el tráfico del puerto todavía excede el umbral de la primera norma.

Utilización de enlaces explícitos

En general, las funciones de reparto del tráfico del Dispatcher funcionan independientemente del contenido de los sitios Web en los que se utiliza el producto. Existe una cuestión, sin embargo, en la que el contenido de los sitios Web puede tener importancia y en la que, además, las decisiones tomadas con respecto a dicho contenido pueden afectar de forma significativa al grado de eficacia del Dispatcher. Se trata de la cuestión de las direcciones de los enlaces.

Si las páginas especifican enlaces que apuntan a servidores individuales del sitio Web, de hecho se obliga al cliente a ir a una máquina específica, con lo que se elude la función de reparto de tráfico que en otro caso podría estar en vigor. Por este motivo, se recomienda utilizar siempre la dirección de Dispatcher en los enlaces que las páginas contengan. Tenga presente que el tipo de direcciones utilizado no siempre resultará evidente si el sitio Web utiliza una programación automatizada que crea HTML dinámicamente. Con el fin de repartir al máximo el tráfico, debe tener en cuenta el encaminamiento explícito que pueda existir y evitarlo en la medida de lo posible.

Utilización de una configuración de red privada

Puede configurar Dispatcher y las máquinas servidor TCP con una red privada. Esta configuración puede reducir el grado de contención en la red pública o externa que puede afectar al rendimiento.

Para AIX, esta configuración también puede beneficiarse de la alta velocidad de SP High Performance Switch si está ejecutando las máquinas Dispatcher y servidor TCP en nodos de un bastidor SP.

Para crear una red privada, cada máquina debe tener al menos dos tarjetas de LAN y una de ellas debe estar conectada a la red privada. Además, la segunda tarjeta de LAN debe configurarse en una subred diferente. La máquina Dispatcher enviará entonces las peticiones de los clientes a las máquinas servidor TCP a través de la red privada.

Windows 2000: Ejecute el mandato siguiente:

```
ndconfig en1 10.0.0.x netmask 255.255.255.0
```

Donde en1 es el nombre de la segunda tarjeta de interfaz en la máquina Dispatcher, 10.0.0.x es la dirección de red de la segunda tarjeta de interfaz y 255.255.255.0 es la máscara de la red privada.

Los servidores que se añadan con el mandato **ndcontrol server add** deben añadirse con las direcciones de red privada; por ejemplo, siguiendo el ejemplo del servidor Apple de la Figura 27 en la página 185, el mandato sería:

```
ndcontrol server add dirección_cluster:80:10.0.0.1
```

y no

```
ndcontrol server add dirección_de_cluster :80:9.67.131.18
```

Si está utilizando Site Selector para proporcionar información sobre el tráfico al Dispatcher, debe configurar Site Selector para que notifique los tráficos de las direcciones privadas.

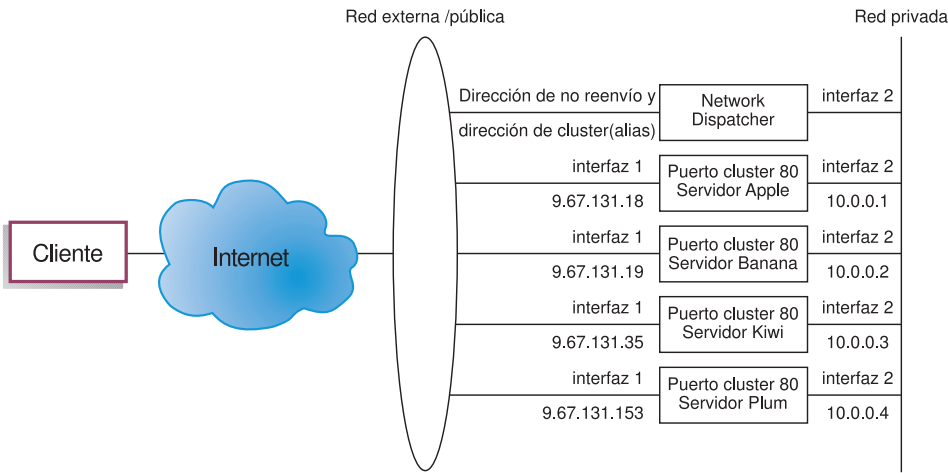


Figura 27. Ejemplo de una red privada mediante Dispatcher

La utilización de una configuración de red privada sólo se aplica al componente Dispatcher.

Utilizar el cluster comodín para combinar configuraciones de servidores

“Comodín” hace referencia a la capacidad del cluster de encontrar coincidencias con varias direcciones IP (es decir, actúa como comodín). La dirección de cluster 0.0.0.0 se utiliza para especificar un cluster comodín.

Si tiene numerosas direcciones de cluster para el reparto del tráfico y las configuraciones puerto/servidor son idénticas para todos los clusters, puede combinar todos los clusters en una configuración en estrella.

Debe seguir configurando explícitamente cada dirección de cluster en uno de los adaptadores de red de la estación de trabajo de Dispatcher. Sin embargo, no debe añadir ninguna de las direcciones de cluster a la configuración del Dispatcher mediante el mandato `ndcontrol cluster add`.

Añada solamente el cluster comodín (dirección 0.0.0.0) y configure los puertos y servidores según sea necesario para el reparto del tráfico. Se repartirá todo el tráfico dirigido a cualquiera de las direcciones configuradas en los adaptadores utilizando la configuración del cluster comodín.

Una ventaja de este método es que se tiene en cuenta el tráfico dirigido a todas las direcciones del cluster cuando se determina el mejor servidor al que se puede acudir. Si un cluster está recibiendo mucho tráfico y ha creado muchas conexiones activas en uno de los servidores, se repartirá el tráfico hacia otras direcciones del cluster utilizando esta información.

Puede combinar el cluster comodín con los clusters reales si tiene algunas direcciones de cluster con configuraciones puerto/servidor exclusivas, y algunas con configuraciones comunes. Se debe asignar a cada una de las configuraciones exclusivas una dirección de cluster real. Se puede asignar un cluster comodín a todas las configuraciones comunes.

La utilización de un cluster comodín para combinar configuraciones sólo se aplica al componente Dispatcher.

Utilizar el cluster comodín para repartir el tráfico de los cortafuegos

La utilización del cluster comodín para repartir el tráfico de los cortafuegos sólo es aplicable al componente Dispatcher. La dirección de cluster 0.0.0.0 se utiliza para especificar un cluster comodín.

El cluster comodín se puede utilizar para repartir el tráfico hacia direcciones que no están configuradas explícitamente en ningún adaptador de red de la estación de trabajo Dispatcher. Para que esto funcione, el Dispatcher debe, como mínimo, ser capaz de ver todo el tráfico que se va a repartir. La estación de trabajo Dispatcher no verá el tráfico hacia las direcciones que no se han configurado de forma explícita en uno de sus adaptadores de red, a menos que esté configurado como la ruta por omisión para parte del tráfico.

Una vez que se ha configurado Dispatcher como ruta por omisión, se repartirá todo el tráfico UDP o TCP a través de la máquina Dispatcher utilizando la configuración del cluster comodín.

Una aplicación de esto es repartir el tráfico de los cortafuegos. Puesto que los cortafuegos pueden procesar paquetes para cualquier dirección de destino y cualquier puerto de destino, es necesario poder repartir el tráfico, independientemente de la dirección y el puerto de destino.

Los cortafuegos se utilizan para gestionar el tráfico desde clientes no seguros a servidores seguros, y las respuestas de los servidores seguros, así como el tráfico de clientes del lado seguro a los servidores del lado no seguro, y las respuestas.

Debe configurar dos máquinas Dispatcher, una para repartir el tráfico no seguro hacia las direcciones de cortafuegos no seguras y otra para repartir el tráfico seguro hacia las direcciones de cortafuegos seguras. Puesto que ambas

máquinas Dispatcher deben utilizar el cluster y puerto comodín con diferentes conjuntos de direcciones de servidores, los dos Dispatchers deben encontrarse en dos estaciones de trabajo distintas.

Utilización del cluster comodín con Caching Proxy para proxy transparente

La utilización del cluster comodín con Caching Proxy para proxy transparente sólo es aplicable al componente Dispatcher. La dirección de cluster 0.0.0.0 se utiliza para especificar un cluster comodín.

La función del cluster comodín también permite utilizar Dispatcher para habilitar una función proxy transparente para un servidor Caching Proxy que reside en la misma máquina que Dispatcher. Esta es una característica de AIX únicamente, ya que debe haber comunicación entre el componente Dispatcher y el componente TCP del sistema operativo.

Para habilitar esta función, debe iniciar la recepción de peticiones de clientes por Caching Proxy en el puerto 80. A continuación debe configurar un cluster comodín. En el cluster comodín, debe configurar el puerto 80. En el puerto 80, debe configurar la dirección de no reenvío (NFA) de la máquina Dispatcher como el único servidor. Ahora todo el tráfico de cliente destinado a cualquier dirección del puerto 80 se entregará al servidor Caching Proxy que se ejecuta en la estación de trabajo de Dispatcher. La petición del cliente se encaminará de la forma habitual y la respuesta se devolverá desde Caching Proxy al cliente. En esta modalidad, el componente Dispatcher no realiza el reparto del tráfico.

Utilización del puerto comodín para dirigir el tráfico de puertos no configurados

El puerto comodín se puede utilizar para manejar el tráfico que no está destinado a ningún puerto configurado explícitamente. Se puede aplicar al reparto del tráfico del cortafuegos. También se puede utilizar para garantizar que el tráfico hacia un puerto no configurado se maneja correctamente. Al definir un puerto comodín sin servidores, garantizará que cualquier petición para un puerto que no se ha configurado se descarte en lugar de volver a entregarse al sistema operativo. Para especificar un puerto comodín, se utiliza el puerto número 0 (cero), por ejemplo:

```
ndcontrol port add cluster:0
```

Nota: El puerto comodín no se puede utilizar para gestionar tráfico FTP.

La función de afinidad de Network Dispatcher

La función de afinidad se habilita al configurar como persistente un puerto de un cluster. El configurar el puerto de un cluster como persistente permite que las peticiones subsiguientes del cliente se envíen al mismo servidor. Esto se realiza estableciendo el “tiempo de persistencia del puerto” en una cierta cantidad de segundos. Esta función se inhabilita estableciendo el tiempo de persistencia en cero.

Interacción con la afinidad entre puertos: Si habilita la afinidad entre puertos, los valores de tiempo de persistencia de los puertos compartidos deben tener el mismo valor (distinto de cero). Consulte “Afinidad entre puertos” en la página 189 para obtener más información.

Comportamiento con la afinidad inhabilitada

Cuando la función de afinidad está inhabilitada, cada vez que se recibe una nueva conexión TCP procedente de un cliente, Dispatcher selecciona el servidor apropiado en ese momento y reenvía paquetes hacia él. Si llega una conexión posterior del mismo cliente, Dispatcher la trata como una conexión nueva independiente y selecciona de nuevo el servidor apropiado en ese momento.

Comportamiento con la afinidad habilitada

Cuando la función de afinidad está habilitada, si se recibe una petición posterior del mismo cliente, la petición se envía al mismo servidor.

Con el paso del tiempo, el cliente dejará de enviar transacciones y el registro de afinidad desaparecerá. De aquí surge el concepto de “persistencia”. Cada registro de afinidad tiene una duración que es igual al “tiempo de persistencia” expresado en segundos. Cuando se reciben varias conexiones posteriores dentro del tiempo de persistencia, el registro de afinidad continúa siendo válido y, por lo tanto, la petición se dirigirá al mismo servidor. Si no se recibe una conexión posterior dentro del intervalo de tiempo de persistencia, el registro se elimina y se seleccionará un nuevo servidor para las conexiones recibidas tras ese tiempo.

API de afinidad dirigida por el servidor (SDA) para controlar la afinidad cliente-servidor

La API de afinidad dirigida por el servidor sólo se aplica al componente Dispatcher.

La función SDA proporciona una API que permite a un agente externo influir en el comportamiento de afinidad de Dispatcher.

Nota: La función SDA (Server Directed Affinity) tiene una limitación: no es compatible con el particionamiento del servidor, pues necesita que las direcciones de los servidores sean exclusivas en la configuración, a fin

de poder utilizar los recursos de búsqueda. SDA tampoco es efectivo con la función de Afinidad de ID de SSL, pues cuando se utiliza SDA los servidores controlan la tabla de afinidades.

Funciones de SDA

La aplicación puede haber indicado que sus sistemas servidor saben mejor que Dispatcher cómo dirigir las peticiones de clientes a determinados sistemas servidor. En lugar de "dirigir" un cliente al mismo servidor elegido por la selección de reparto del tráfico de Dispatcher, quizás desee "dirigir" el cliente al servidor de su elección. La función SDA proporciona esta API. Ahora puede escribir su propio software para implementar un agente SDA, que se comunica con un oyente en Dispatcher. A continuación, puede manipular las tablas de afinidad de Dispatcher para:

- Consultar el contenido
- Insertar nuevos registros
- Eliminar registros

Los registros insertados en una tabla de afinidad por un agente SDA permanecen en la tabla indefinidamente. No tienen un tiempo de espera. Sólo se eliminan cuando el agente SDA los elimina o si un asesor Dispatcher detecta que el servidor no responde.

Componentes SDA de Dispatcher

Dispatcher implementa un nuevo oyente de socket para aceptar y manejar peticiones de un agente SDA. Cuando un agente SDA abre una conexión con Dispatcher, el oyente la aceptará y dejará la conexión abierta. Por esta conexión persistente pueden fluir varias peticiones y respuestas. El socket se cerrará cuando lo cierre el agente SDA o si Dispatcher detecta un error irrecuperable. En el interior de Dispatcher, el oyente toma cada petición del agente SDA, se comunica con la tabla de afinidad adecuada en el kernel ejecutor de Dispatcher y prepara una respuesta para dicho agente SDA.

Para obtener más información, consulte los archivos contenidos en el directorio de instalación de Network Dispatcher:

- API: `...nd/servers/samples/SDA/SDA_API.htm`
- código de ejemplo de un agente SDA:
`...nd/servers/samples/SDA/SDA_SampleAgent.java`

Afinidad entre puertos

La afinidad entre puertos sólo es aplicable al componente Dispatcher.

La afinidad entre puertos es la función de persistencia que se ha ampliado para abarcar varios puertos. Por ejemplo, si primero se recibe una petición del

cliente en un puerto y la petición siguiente se recibe en otro puerto, la afinidad entre puertos permite que la máquina de Dispatcher envíe la petición del cliente al mismo servidor. Para poder utilizar esta característica, los puertos deben:

- compartir la misma dirección de cluster
- compartir los mismos servidores
- tener el mismo valor (distinto de cero) de tiempo de persistencia (**stickytime**)
- tener el mismo valor de **stickymask**

Se puede asociar más de un puerto al mismo puerto (**crossport**). Cuando se reciban conexiones posteriores procedentes del mismo cliente en el mismo puerto o en un puerto compartido, se accederá al mismo servidor. El ejemplo siguiente muestra una configuración de varios puertos con afinidad entre puertos para el puerto 10:

```
ndcontrol port set cluster:20 crossport 10
ndcontrol port set cluster:30 crossport 10
ndcontrol port set cluster:40 crossport 10
```

Una vez establecida la afinidad entre puertos, podrá modificar el valor de tiempo de persistencia (**stickytime**) del puerto. Sin embargo, se le recomienda que modifique los valores de persistencia de todos los puertos compartidos con el mismo valor, de lo contrario pueden producirse resultados imprevisibles.

Para suprimir la afinidad entre puertos, vuelva a establecer el valor de **crossport** ensu propio número de puerto. Consulte el apartado “**ndcontrol port** — configurar puertos” en la página 287 para obtener información detallada sobre la sintaxis del mandato para la opción **crossport**.

Máscara de dirección de afinidad

La máscara de dirección de afinidad sólo es aplicable al componente Dispatcher.

La máscara de dirección de afinidad es una mejora de la función de persistencia para agrupar clientes según la dirección de subred común. Si especifica **stickymask** en el mandato **ndcontrol port** puede enmascarar los bits comunes de orden superior de la dirección IP de 32 bits. Si está habilitada esta característica, la primera vez que una petición de cliente efectúa una conexión con el puerto, todas las peticiones siguientes procedentes de los clientes con la misma dirección de subred (que se representa mediante la parte de la dirección que se va a enmascarar) se dirigirán al mismo servidor.

Por ejemplo, si desea que todas las peticiones de cliente de entrada que tengan la misma dirección de red de clase A se dirijan al mismo servidor,

deberá establecer el valor de stickymask en 8 (bits) para el puerto. Para agrupar las peticiones de cliente que tengan la misma dirección de red de clase B, establezca el valor de stickymask en 16 (bits). Para agrupar las peticiones de cliente que tengan la misma dirección de red de clase C, establezca el valor de stickymask en 24 (bits).

Para obtener los mejores resultados, establezca el valor de stickymask cuando inicie por primera vez Network Dispatcher. Si cambia el valor de stickymask de forma dinámica, los resultados pueden ser imprevisibles.

Interacción con la afinidad entre puertos: Si va a habilitar la afinidad entre puertos, los valores de stickymask de los puertos compartidos deben ser iguales. Consulte el apartado “Afinidad entre puertos” en la página 189 para obtener más información.

Para habilitar la máscara de dirección de afinidad, emita un mandato `ndcontrol port` similar al siguiente:

```
ndcontrol port set cluster:puerto stickymask 8
```

Los valores posibles de stickymask son 8, 16, 24 y 32. El valor 8 especifica que se enmascararán los primeros 8 bits de orden superior de la dirección IP (la dirección de red de clase A). El valor 16 especifica que se enmascararán los primeros 16 bits de orden superior de la dirección IP (la dirección de red de clase B). El valor 24 especifica que se enmascararán los primeros 24 bits de orden superior de la dirección IP (la dirección de red de clase C). Si especifica 32, se enmascarará toda la dirección IP, con lo cual inhabilitará la función que permite enmascarar la dirección de afinidad. El valor por omisión de stickymask es 32.

Consulte el apartado “`ndcontrol port` — configurar puertos” en la página 287 para obtener información detallada sobre la sintaxis del mandato para stickymask (característica para enmascarar la dirección de afinidad).

Alteración temporal de afinidad de norma

Con esta alteración temporal de afinidad de norma, puede alterar temporalmente la persistencia de un puerto para un servidor específico. Por ejemplo, puede utilizar una norma para limitar el número de conexiones a cada servidor de aplicaciones y tener un servidor de desbordamiento con una norma siempre cierta que indica “vuélvalo a intentar más tarde” para dicha aplicación. El puerto tiene un valor de tiempo de persistencia de 25 minutos, por lo tanto no desea que el cliente utilice siempre este servidor. Con la alteración temporal de afinidad de norma, puede cambiar el servidor de desbordamiento de modo que se altere temporalmente la afinidad que normalmente está asociada a dicho puerto. La próxima vez que el cliente hace peticiones al cluster, el tráfico se dirige hacia el servidor de aplicaciones disponible más adecuado, no hacia el servidor de desbordamiento.

Consulte el apartado “`ndcontrol server` — configurar servidores” en la página 302 para obtener información detallada sobre la sintaxis del mandato para la alteración temporal de afinidad de norma, utilizando la opción **sticky** del servidor.

Desactivación de conexiones persistentes

La desactivación de conexiones persistentes es aplicable a los componentes Dispatcher y CBR.

Para eliminar un servidor en la configuración de Network Dispatcher por la razón que sea (actualizaciones, ampliaciones, tareas de mantenimiento, etc.), puede utilizar el mandato **`ndcontrol manager quiesce`**. El submandato `quiesce` permite que las conexiones existentes finalicen (sin ser interrumpidas) y sólo reenvía las nuevas conexiones subsiguientes desde el cliente al servidor desactivado si la conexión está definida como persistente y no ha transcurrido el tiempo de persistencia. El submandato `quiesce` rechaza cualquier otra nueva conexión con el servidor.

Utilice el mandato `quiesce “now”` (desactivar ahora) si tiene establecido un tiempo de persistencia y desea que las nuevas conexiones se envíen a otro servidor (en lugar del servidor desactivado) antes de que finalice el tiempo de persistencia. El ejemplo siguiente muestra cómo utilizar la opción “now” (ahora) para desactivar el servidor 9.40.25.67:

```
ndcontrol manager quiesce 9.40.25.67 now
```

La opción “now” determina la forma en que se manejan las conexiones persistentes, de esta manera:

- Si *no* especifica “now”, podrán finalizar las conexiones existentes y se reenviarán las nuevas conexiones subsiguientes al servidor desactivado para los clientes con conexiones definidas como persistentes, a condición de que el servidor desactivado reciba la nueva petición antes de caducar el tiempo de persistencia. (Sin embargo, si no tiene habilitada la función de persistencia (afinidad), el servidor desactivado no puede recibir ninguna nueva conexión).

Esta es la forma más ordenada, menos abrupta, para detener servidores. Por ejemplo, puede detener ordenadamente un servidor y luego esperar a que haya el menor volumen de tráfico en la red (probablemente a primera hora de la mañana) para eliminar completamente el servidor de la configuración.

- Si especifica “now”, el servidor se detiene y finalizan las conexiones existentes, pero no se permite ninguna nueva conexión, incluidas conexiones las procedentes de clientes con conexiones definidas como persistentes. Esta es la forma más abrupta de detener servidores, que era la única existente en versiones anteriores de Network Dispatcher.

Opción de afinidad en la norma

Puede especificar los siguientes tipos de afinidad en el mandato **ndcontrol rule**:

- **Active cookie** — permite distribuir el tráfico de la Web con afinidad con el mismo servidor según los cookies generados por Network Dispatcher.
- **Passive cookie** — permite distribuir el tráfico de la Web con afinidad con el mismo servidor según los cookies autodefinidos generados por los servidores. Junto con la afinidad pasiva de cookie, debe también especificar el parámetro **cookieName** en el mandato **rule**.
- **URI** — permite distribuir el tráfico de la Web a servidores caching-proxy de modo que se aumente de forma eficiente el tamaño de la antememoria.

El valor por omisión de la opción de afinidad es "none". La opción **stickytime** del mandato **port** debe ser cero (no habilitado) para poder definir para la opción **affinity** en el mandato **rule** el valor **active cookie**, **passive cookie** o **URI**. Cuando la afinidad está definida en la norma, no puede habilitar **stickytime** en el puerto.

La afinidad activa de cookie sólo se aplica al componente CBR. La afinidad pasiva de cookie y URI se aplican al componente CBR y al método de reenvío **cbr** del componente Dispatcher.

Afinidad activa de cookie

La función de afinidad activa de cookie sólo se aplica al componente CBR. Proporciona una forma de hacer que los clientes tengan "persistencia" en un servidor determinado. Esta función se habilita al establecer el tiempo de persistencia (**stickytime**) de una norma en un número positivo y al establecer la afinidad en "activecookie". Esto es posible cuando se añade la norma o mediante el mandato **rule set**. Consulte "ndcontrol rule — configurar normas" en la página 294 para ver información detallada sobre la sintaxis del mandato.

Una vez habilitada una norma para la afinidad activa de cookie, se repartirá el tráfico de las peticiones nuevas de cliente utilizando los algoritmos estándares de CBR, mientras que las peticiones sucesivas del mismo cliente se enviarán al servidor elegido inicialmente. El servidor elegido se almacena como cookie en la respuesta al cliente. Mientras las futuras peticiones del cliente contengan el cookie y cada petición llegue dentro del intervalo de tiempo de persistencia, el cliente mantendrá la afinidad con el servidor inicial.

La afinidad activa de cookie sirve para asegurar que el tráfico de un cliente se continúa distribuyendo al mismo servidor durante un periodo de tiempo. Esto se efectúa enviando un cookie para que lo almacene el navegador del cliente. El cookie contiene el **cluster:puerto** que se utilizó para tomar la decisión, el servidor al que se distribuyó el tráfico y la indicación horaria de tiempo de espera en que la afinidad deja de ser válida. Siempre que una norma aplica la

activación de la afinidad de cookie, se examina el cookie enviado por el cliente. Si se encuentra un cookie en que se incluye el identificador de cluster:puerto que se ha aplicado, se extraen del cookie el servidor del reparto del tráfico y la indicación de la hora de caducidad. Si el servidor todavía está en el conjunto utilizado por la norma y su peso es mayor que cero y la indicación de la hora de caducidad es mayor que ahora, se elige el servidor del cookie para realizar el reparto del tráfico. Si alguna de las tres condiciones anteriores no se cumple, se elige un servidor utilizando el algoritmo normal. Después de la elección de un servidor (mediante cualquiera de los dos métodos), se crea un nuevo cookie que contiene IBM CBR, información cluster:puerto:servidor_elegido y una indicación horaria. La indicación horaria será la hora en que caduca la afinidad. La información “cluster:puerto:servidor_elegido” está codificada para que no se revele información sobre la configuración de CBR. También está insertado en el cookie un parámetro de “caducidad”. Este parámetro tiene un formato inteligible para el navegador y hace que el cookie se vuelva no válido dos horas después de la indicación de la hora de caducidad. Ésta es la razón de que no haya una acumulación excesiva en la base de datos de cookies del cliente.

Este nuevo cookie se inserta en las cabeceras que se devuelven al cliente y, si el navegador del cliente está configurado para aceptar cookies, volverá a enviar peticiones subsiguientes.

La opción de afinidad activa de cookie, para el mandato rule, sólo puede establecerse en activecookie si el tiempo de persistencia (stickytime) de puerto es cero (no habilitado). Cuando la afinidad activa de cookie está activa para una norma, no se puede habilitar el tiempo de persistencia en el puerto.

Cómo habilitar la afinidad activa de cookie

Para activar la afinidad activa de cookie para una determinada norma, utilice el siguiente mandato rule set:

```
rule set cluster:puerto:norma stickytime 60
rule set cluster:puerto:norma affinity activecookie
```

Por qué se utiliza la afinidad activa de cookie

La creación de una norma con persistencia se suele utilizar para CGI o servlets que almacenan el estado del cliente en el servidor. El estado se identifica mediante un ID de cookie (éstos son los cookies de servidor). El estado del cliente sólo se encuentra en el servidor seleccionado, por lo cual el cliente necesita el cookie de ese servidor para mantener ese estado entre las peticiones.

Afinidad pasiva de cookie

La afinidad pasiva de cookie puede utilizarse con el encaminamiento basado en contenido (CBR) del componente Dispatcher y con el componente CBR. Consulte la sección “Encaminamiento por contenido mediante Dispatcher

(método de reenvío cbr)” en la página 52, donde obtendrá información sobre cómo configurar el método de reenvío cbr de Dispatcher.

La afinidad pasiva de cookie proporciona una forma de hacer que los clientes tengan afinidad por un servidor determinado. La afinidad pasiva de cookie le permite repartir el tráfico Web con afinidad por un mismo servidor basándose en los cookies autodefinidos generados por los servidores. La afinidad pasiva de cookie se configura a nivel de norma. Cuando se aplica una norma, si la afinidad pasiva de cookie está habilitada, Network Dispatcher selecciona el servidor basándose en el nombre de cookie contenido en la cabecera HTTP de la petición del cliente. Network Dispatcher enviará las nuevas peticiones entrantes hacia los servidores basándose en los cookies generados por los servidores durante conexiones anteriores. Si el valor de cookie contenido en la petición del cliente no se encuentra o no coincide con ninguno de los valores de cookie de los servidores, el servidor se selecciona utilizando la técnica ponderada rotatoria.

Para configurar la **afinidad pasiva de cookie**:

- Para Dispatcher, configure primero el método de reenvío cbr de Dispatcher. (Consulte la sección “Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)” en la página 52.) Este paso se omite para el componente CBR.
- Establezca el parámetro **affinity** como “passivecookie” en el mandato **ndcontrol rule [add | set]**. Además, el parámetro **cookieName** debe ser el nombre del cookie que Network Dispatcher debe buscar en la cabecera HTTP de la petición del cliente.
- Establezca el parámetro **cookievalue**, para cada servidor del conjunto de servidores de la norma, en el mandato **ndcontrol server [add | set]**.

La opción de afinidad pasiva de cookie, para el mandato rule, sólo puede establecerse en passivecookie si el tiempo de persistencia de puerto es cero (no habilitado). Cuando la afinidad pasiva de cookie está activa para una norma, no se puede habilitar el tiempo de persistencia en el puerto.

Afinidad de URI

La afinidad de URI se puede utilizar con el método de reenvío CBR de Dispatcher y con el componente CBR. Consulte “Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)” en la página 52 para obtener información sobre cómo configurar el método de reenvío CBR.

La afinidad de URI le permite repartir el tráfico Web hacia servidores Caching Proxy, lo que permite poner en antememoria contenido exclusivo en cada servidor individual. Como consecuencia, aumenta de forma efectiva el tamaño de la antememoria del sitio Web al eliminar el almacenamiento redundante de contenido en varias máquinas. La afinidad de URI se configura a nivel de norma. Cuando se aplica una norma, si la afinidad de URI está habilitada y el

mismo grupo de servidores está activo y respondiendo, Network Dispatcher reenvía hacia el mismo servidor las nuevas peticiones de los clientes que tengan el mismo URI.

Habitualmente, Network Dispatcher puede distribuir peticiones hacia varios servidores que abastecen el mismo contenido. Si utiliza Network Dispatcher con un grupo de servidores de antememoria, el contenido de acceso frecuente finalmente pasa a estar en la antememoria de todos los servidores. Esto permite un tráfico muy alto de peticiones de los clientes al duplicar un mismo contenido de antememoria en varias máquinas. Esto es especialmente útil para sitios Web de gran volumen.

Sin embargo, si el sitio Web tiene un tráfico moderado o alto de peticiones de clientes y prefiere tener una antememoria mayor repartida entre varios servidores, el rendimiento del sitio Web será mejor si el contenido de cada servidor es exclusivo y Network Dispatcher sólo distribuye la petición hacia el servidor con ese contenido.

Con la afinidad de URI, Network Dispatcher le permite distribuir el contenido de la antememoria hacia servidores individuales, eliminando el almacenamiento redundante de contenido en varias máquinas. Con esta mejora, los sitios Web con servidores de contenido diverso que utilicen servidores Caching Proxy tendrán un mayor rendimiento. Las peticiones iguales se enviarán hacia el mismo servidor, por lo que sólo se almacenará contenido en servidores individuales. Además, el tamaño efectivo de la antememoria será mayor con cada nueva máquina añadida a la agrupación.

Para configurar la **afinidad de URI**:

- Para Dispatcher, primero configure el método de reenvío CBR del Dispatcher. (Consulte la sección “Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)” en la página 52.) Este paso se omite para el componente CBR.
- Establezca el parámetro **afinidad** en “uri” en el mandato **ndcontrol rule [add | set]** o **cbrcontrol rule [add | set]**.

La opción de afinidad de URI, para el mandato rule, sólo puede establecerse en “URI” si el tiempo de persistencia de puerto es cero (no habilitado). Cuando la afinidad de URI está activa para una norma, no se puede habilitar el tiempo de persistencia en el puerto.

Detección de ataques de denegación de servicio

Esta característica sólo está disponible para el componente Dispatcher.

Dispatcher permite detectar posibles ataques de "denegación de servicio" y avisar al administrador mediante una alerta. Para ello, Dispatcher comprueba si las peticiones entrantes contienen un volumen importante de conexiones TCP semiabiertas en los servidores, lo cual es una característica habitual de los ataques simples de denegación de servicio. En un ataque de denegación de servicio, un sitio Web recibe una gran cantidad de paquetes SYN ficticios procedentes de numerosas direcciones IP y números de puerto, pero el sitio Web no recibe subsiguientes paquetes para esas conexiones TCP. Esto produce un gran número de conexiones TCP semiabiertas en los servidores, los cuales pueden llegar finalmente a ser muy lentos y no aceptar nuevas peticiones entrantes.

Network Dispatcher proporciona salidas de usuario que provocan la ejecución de scripts personalizables que avisan al administrador sobre un posible ataque de denegación de servicio. Dispatcher proporciona los siguientes archivos de script de ejemplo en el directorio **...nd/servers/samples**:

- **halfOpenAlert** — se ha detectado un posible ataque de denegación de servicio
- **halfOpenAlertDone** — el ataque de denegación de servicio ha finalizado

Para poder ejecutar los archivos de script, debe trasladarlos al directorio **...nd/servers/bin** y eliminar la extensión de archivo ".sample".

Para utilizar la detección de ataques de denegación de servicio, establezca el parámetro **maxhalfopen** del mandato **ndcontrol port** de esta manera:

```
ndcontrol port set 127.40.56.1:80 maxhalfopen 1000
```

En el ejemplo anterior, Dispatcher compara el número total actual de conexiones semiabiertas (para todos los servidores que residen en el cluster 127.40.56.1 del puerto 80) con el valor umbral 1000 (especificado por el parámetro **maxhalfopen**). Si el número actual de conexiones semiabiertas excede el valor umbral, se invoca un script de alerta (**halfOpenAlert**). Cuando el número de conexiones semiabiertas desciende por debajo del valor umbral, se invoca otro script de alerta (**halfOpenAlertDone**) para indicar que el ataque ha finalizado.

Para determinar cómo definir el valor maxhalfopen: Periódicamente (por ejemplo, cada 10 minutos) ejecute un mandato de informe de conexiones semiabiertas (**ndcontrol port halfopenaddressreport cluster:puerto**) cuando su sitio Web tenga un volumen de tráfico moderado o alto. El informe de conexiones semiabiertas mostrará el número total actual de conexiones

semiabiertas recibidas. Debe establecer `maxhalfopen` en un valor que sea entre un 50% y un 200% mayor que el número más alto de conexiones semiabiertas que se producen en el sitio Web.

Además de los datos estadísticos presentados, `halfopenaddressreport` también crea entradas en el archivo de anotaciones (`..nd/servers/logs/dispatcher/halfOpen.log`) para todas las direcciones de clientes (hasta aproximadamente 8000 pares de direcciones) que han accedido a servidores y han originado conexiones semiabiertas.

Nota: Existe la correspondiente captura SNMP ("trap") para los scripts `halfOpenAlert` y `halfOpenAlertDone`. Si el subagente SNMP está configurado y en ejecución, las capturas correspondientes se enviarán en las mismas condiciones en que se desencadenan los scripts. Para obtener más información sobre el subagente SNMP, consulte la sección "Utilización de SNMP (Simple Network Management Protocol) con el componente Dispatcher" en la página 211.

Si desea proporcionar una protección adicional contra los ataques de denegación de servicio para los servidores de fondo, puede configurar clusters y puertos comodín. Específicamente, añada un puerto comodín sin servidores bajo cada cluster configurado. Añada, además, un cluster comodín con un puerto comodín y sin servidores. Esto tendrá el efecto de eliminar todos los paquetes que no vayan dirigidos a un cluster y un puerto no comodín. Para obtener información sobre los clusters y puertos comodín, consulte la sección "Utilizar el cluster comodín para combinar configuraciones de servidores" en la página 185 y la sección "Utilización del puerto comodín para dirigir el tráfico de puertos no configurados" en la página 187.

Utilizar las anotaciones en binario para analizar las estadísticas del servidor

Nota: La función de anotaciones en binario no se puede utilizar con el componente Site Selector.

La función de anotaciones en binario permite que la información del servidor se almacene en archivos binarios. Estos archivos pueden procesarse para analizar la información del servidor recopilada a lo largo del tiempo.

Las anotaciones en binario de cada servidor definido en la configuración almacenan la información siguiente:

- Dirección de cluster
- Número de puerto
- ID del servidor
- Dirección del servidor

- Peso del servidor
- Conexiones totales del servidor
- Conexiones activas del servidor
- Tráfico del puerto en el servidor
- Tráfico del sistema en el servidor

Parte de esta información se obtiene del ejecutor como parte del ciclo del gestor. Por lo tanto el gestor debe estar en ejecución para poder anotar información en las anotaciones en binario.

Utilice el conjunto de mandatos **ndcontrol log** para configurar las anotaciones en binario.

- log start
- log stop
- log set interval <segundos>
- log set retention <horas>
- log status

La opción start inicia el registro de información sobre servidores en archivos de anotaciones en binario, en el directorio logs. Cada hora se crea un archivo de anotaciones con la fecha y la hora como nombre del archivo.

La opción stop detiene la anotación de información del servidor en las anotaciones en binario. Por omisión, el servicio de anotaciones está detenido.

La opción set interval controla la frecuencia con la que la información se graba en las anotaciones. El gestor enviará información al servidor de anotaciones en cada intervalo de gestor. La información se grabará en las anotaciones solamente si han transcurrido los segundos especificados como intervalo de anotaciones desde que se grabó el último registro en las anotaciones. Por omisión, el intervalo de anotaciones está definido en 60 segundos. Existe una cierta interacción entre los valores del intervalo del gestor y el intervalo de anotaciones. Debido a que el servidor de anotaciones no recibirá la información en menos tiempo que los segundos del intervalo del gestor, al establecer un intervalo de anotaciones inferior al intervalo del gestor en realidad se establece en el mismo valor que el intervalo del gestor. Este método de anotaciones permite captar información del servidor con cualquier nivel de detalle (granularidad). Puede capturar todos los cambios realizados en la información del servidor detectados por el gestor para calcular los pesos de los servidores. Sin embargo, no es necesaria tanta cantidad de información para analizar la utilización del servidor y la tendencia. La anotación de información del servidor cada 60 segundos le proporciona vistas instantáneas

de la información del servidor a lo largo del tiempo. Si se establece el intervalo de anotaciones en un valor demasiado bajo, se pueden generar grandes cantidades de datos.

La opción `set retention` controla durante cuánto tiempo se conservan los archivos. El servidor de archivos de anotaciones suprimirá los archivos de anotaciones que superen las horas de retención especificadas. Esto sólo se producirá si el gestor llama al servidor de anotaciones, de modo que detener el gestor hará que los archivos de anotaciones antiguos no se supriman.

La opción `status` devuelve los valores actuales del servicio de anotaciones. Estos valores son si el servicio se ha iniciado, cuál es el intervalo y cuáles son las horas de retención.

En el directorio `...nd/servers/samples/BinaryLog` se proporcionan ejemplos de un programa Java y de un archivo de mandatos. Estos ejemplos muestran cómo recuperar toda la información de los archivos de anotaciones y visualizarla en la pantalla. Puede personalizar esos ejemplos para realizar cualquier tipo de análisis que desee con los datos. El siguiente es un ejemplo sobre cómo utilizar el programa y el script proporcionados para Dispatcher:

```
ndlogreport 2001/05/01 8:00 2001/05/01 17:00
```

a fin de obtener un informe sobre el servidor del componente Dispatcher de 8:00 a 17:00 el 1 de mayo de 2001. (Para CBR, utilice **cbrlogreport**. Para Mailbox Locator, utilice **mllogreport**. Para Cisco Consultant, utilice **lbclogreport**.)

Información adicional sobre las funciones avanzadas de Cisco Consultant

En Cisco Consultant, Cisco CSS Switch efectúa las tareas realizadas por el ejecutor en el componente Dispatcher. Además del valor actual de ponderación (peso) de cada servidor e información de otro tipo necesaria para realizar sus cálculos, el gestor obtiene el número de conexiones activas y de conexiones nuevas a partir del Cisco CSS Switch. Estos valores están basados en la información que se genera y almacena internamente en el Cisco CSS Switch.

Cisco Consultant consulta la MIB (base de información de gestión) de Cisco CSS Switch para obtener el número de conexiones activas y nuevas y recibe lo siguiente:

- **Para las conexiones activas**, Cisco Consultant obtiene el valor `apSvcConnections` a partir de `svcExtMIB`. Esta variable está indexada de acuerdo con el nombre de servicio (`serviceName`) y se correlaciona directamente con las conexiones activas tal como están registradas en el gestor. Lo siguiente es la entrada correspondiente a `apSvcConnections` en la MIB:

```

apSvcConnections OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Número total de conexiones TCP con este servicio"
DEFVAL { 0 }
--DEFAULT ap-display-name Service Connections
::= {apSvcEntry 20}

```

El identificador de objeto para apSvcConnections es:

1.3.6.1.4.1.2467.1.15.2.1.20

El número de conexiones activas depende del número de clientes y del período de tiempo necesario para utilizar los servicios proporcionados por los servidores sujetos a reparto del tráfico. Si las conexiones de los clientes son rápidas (por ejemplo, las realizadas para páginas Web pequeñas utilizando GET de HTTP), el número de conexiones activas será bastante bajo. Si las conexiones de los clientes son más lentas (por ejemplo, una consulta de base de datos), el número de conexiones activas será más alto.

- **Para las conexiones nuevas**, Cisco Consultant establece la variable apCntsvcHits de la MIB en cntSvcExtMib de Cisco CSS Switch. Para cada servicio, Cisco Consultant:
 - Calcula la suma de todos los valores apCntsvcHits que tienen ese servicio en el índice
 - Lleva un registro del total del valor apCntsvcHits
 - Calcula el valor diferencial

El índice de esta variable es:

```

INDEX { apCntsvcOwnName, apCntsvcCntName, apCntsvcSvcName }

```

Lo siguiente es la entrada correspondiente en la MIB:

```

apCntsvcHits OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Número total de peticiones del servicio para esta norma de contenido".
DEFVAL { 0 }
--DEFAULT ap-display-name Hits
--DEFAULT apjam-popup-ref apCntSvcInst, Statistics
--DEFAULT apjam-chart-def cntSvcHitsChart, pie, apCntInst, "Número
de accesos a cada servicio:
--DEFAULT apjam-chart-item cntSvcHitsChart, getnext, apCntsvcSvcName
::= {apSvcEntry 20}

```

El identificador de objeto para apCntsvcHits es:

1.3.6.1.4.1.2467.1.18.2.1.4

Pesos de Cisco Consultant

El Cisco CSS Switch se debe configurar para que utilice el método rotatorio ponderado de reparto del tráfico. Consulte "Configuring Weight" en el manual *Content Services Switch Basic Configuration Guide* para conocer cómo hacer esto.

Los pesos (valores de ponderación) son establecidos por el gestor de acuerdo con contadores internos de Cisco CSS Switch e información recibida de los asesores y Metric Server. Si desea definir los pesos manualmente mientras ejecuta el gestor, especifique la opción **fixedweight** en el mandato **lbcontrol server**.

Si todos los servidores están fuera de servicio, todos los pesos son igual a 0. En este caso, cuando no hay ningún servidor procesando peticiones debido a que todos los pesos son 0, los pesos se establecen en un valor igual a la mitad del valor "weightbound" para permitir la misma posibilidad de procesar una petición por parte de cualquier servidor apropiado. El programa monitor muestra el verdadero valor del peso (0), pero Cisco Consultant visualiza un peso igual a la mitad de "weightbound" en todos los demás lugares.

Los pesos se envían al Cisco CSS Switch utilizando SNMP. Cisco Consultant establece apSvcWeight en svcExt.mib. Lo siguiente es la entrada correspondiente a apSvcWeight.

```
apSvcWeight OBJECT-TYPE
SYNTAX Integer32(1..10)
MAX-ACCESS read-create
STATUS current
DESCRIPTION
    "Peso del servicio que se utiliza junto con métricas del tráfico
    para tomar decisiones respecto a su reparto. El peso se puede utilizar
    para desviar el tráfico hacia el servicio especificado".
DEFVAL { 1 }
--DEFAULT ap-display-name Service Weight
--DEFAULT apjam-popup-ref apServicesGroupInst, Properties, Advanced
--DEFAULT apjam-wizard-field 2, normal
 ::= {apSvcEntry 16}
```

El identificador de objeto para apSvcWeight es:

1.3.6.1.4.1.2467.1.15.2.1.12

Los pesos se aplican a todos los servidores de un puerto. Para un puerto determinado cualquiera, las peticiones se reparten entre los servidores según el peso relativo de los servidores. Por ejemplo, si un servidor tiene establecido 10 como peso y otro tiene 5, el servidor con 10 debe obtener el doble de peticiones que el servidor con 5.

Para especificar el peso máximo que puede tener cualquier servidor, emita el mandato **lbcontrol port set weightbound**. Este mandato especifica las

diferencias en el número de peticiones que recibe cada servidor. Si establece el peso máximo en 1, todos los servidores pueden tener 1 como peso, 0 si están desactivados o -1 si están marcados como inactivos. Cuanto más alto sea este número, mayor será la diferencia de pesos entre los servidores. Con un peso máximo de 2, un servidor puede recibir el doble de peticiones que otro.

Cuando un servidor está fuera de línea...

Si un asesor detecta que un servidor está fuera de línea, informa al gestor y éste asigna el peso 0 al servidor. Cuando el peso de un servidor es mayor que 0, el peso se envía al Cisco CSS Switch, y el servidor pasa a estar activo; pero si el peso del servidor es menor o igual que 0, se detiene el servidor. Para activar o detener un servicio se define la variable `apSvcEnable` de la MIB, en `svcExt.mib` de Cisco CSS Switch. Lo siguiente es la entrada correspondiente a `apSvcEnable` en la MIB:

```
apSvcEnable OBJECT-TYPE
SYNTAX  Integer
        disable(0)
        enable(1)
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "Estado del servicio: habilitado o inhabilitado."
DEFVAL { disable }
--DEFAULT ap-display-name Status
--DEFAULT apjam-popup-ref apServicesGroupInst, Properties
--DEFAULT apjam-wizard-field 2, normal
::= {apSvcEntry 12}
```

El identificador de objeto para `apSvcEnable` es:

1.3.6.1.4.1.2467.1.15.2.1.16

Capítulo 15. Utilización y gestión de Network Dispatcher

Nota: Para las secciones generales de este capítulo que no son específicas de un componente individual, si *no* está utilizando el componente Dispatcher, sustituya "ndcontrol" y "ndserver" por lo siguiente:

- Para CBR, utilice **cbrcontrol** y **cbrserver**
- Para Mailbox Locator, utilice **mlcontrol** y **mlserver**
- Para Site Selector, utilice **cbrcontrol** y **ssserver**
- Para Cisco Consultant, utilice **lbcontrol** y **lbserver**

Este capítulo describe cómo utilizar y gestionar Network Dispatcher; incluye las secciones siguientes:

- "Administración autenticada remota"
- "Utilización de los archivos de anotaciones de Network Dispatcher" en la página 207
- "Utilización del componente Dispatcher" en la página 209
 - "Utilización de SNMP (Simple Network Management Protocol) con el componente Dispatcher" en la página 211
- "Utilización del componente Content Based Routing" en la página 217
- "Utilización del componente Mailbox Locator" en la página 217
- "Utilización del componente Site Selector" en la página 218
- "Utilización del componente Cisco Consultant" en la página 219

Administración autenticada remota

Network Dispatcher proporciona una opción para ejecutar sus programas de configuración en una máquina distinta de la que está ejecutando los servidores de Network Dispatcher.

La comunicación entre los programas de configuración (ndcontrol, cbrcontrol, mlcontrol, sscontrol, lbcontrol, ndwizard, cbrwizard, mlwizard, sswizard, ndadmin) se realiza mediante llamadas RMI (Java Remote Method Invocation). El mandato para conectar a una máquina Network Dispatcher para la administración remota es **ndcontrol host:sist_pral_remoto**. Si la llamada RMI procede de una máquina distinta de la máquina local, debe producirse una secuencia de autenticación de clave pública/privada antes de que se acepte el mandato de configuración.

La comunicación entre los programas de control que se ejecutan en la misma máquina que los servidores de componentes no está autenticada.

Utilice el mandato siguiente para generar claves públicas y privadas a fin de utilizarlas en la autenticación remota:

ndkeys [create | delete]

Este mandato sólo se ejecuta en la misma máquina que Network Dispatcher.

Mediante la opción **create** se crea una clave pública en el directorio de claves de servidor (...**nd/servers/key/**) y se crean claves privadas en el directorio de claves de administración (...**nd/admin/keys/**) para cada componente de Network Dispatcher. El nombre de archivo para la clave privada es: *componente-dirección_servidor-puerto_RMI*. Luego, estas claves privadas se deben trasladar a los clientes remotos y situar en el directorio de claves de administración.

Para una máquina de Network Dispatcher cuya dirección de sistema principal es 10.0.0.25 y que utiliza el puerto RMI por omisión para cada componente, el mandato **ndkeys create** crea estos archivos:

- La clave pública: .../nd/servers/key/**authorization.key**
- Las claves privadas:
 - .../nd/admin/keys/**dispatcher-10.0.0.25-10099.key**
 - .../nd/admin/keys/**cbr-10.0.0.25-11099.key**
 - .../nd/admin/keys/**m1-10.0.0.25-13099.key**
 - .../nd/admin/keys/**ss-10.0.0.25-12099.key**
 - .../nd/admin/keys/**lbc-10.0.0.25-14099.key**

El catálogo de archivos de administración se ha instalado en otra máquina. Los archivos de clave privada deben estar situados en el directorio **.../nd/admin/keys** de la máquina cliente remoto.

El cliente remoto ahora estará autorizado para configurar Network Dispatcher en 10.0.0.25.

Estas mismas claves se deben utilizar en todos los clientes remotos a los que desee dar autorización para configurar Network Dispatcher en 10.0.0.25.

Si ejecutase de nuevo el mandato **ndkeys create**, se generaría un nuevo conjunto de claves públicas/privadas. Esto significaría que todos los clientes remotos que han intentado conectarse utilizando las claves anteriores no estarían autorizados. La nueva clave debería colocarse en el directorio correcto en aquellos clientes que desea volver a autorizar.

El mandato **ndkeys delete** suprime las claves privadas y públicas de la máquina servidor. Si estas claves se suprimen, no se autorizará a ningún cliente remoto para conectarse a los servidores.

Tanto para **ndkeys create** como para **ndkeys delete** hay una opción **force**. La opción **force** suprime los indicadores de mandatos que le preguntan si desea sobrescribir o suprimir las claves existentes.

Utilización de los archivos de anotaciones de Network Dispatcher

Network Dispatcher envía entradas a un archivo de anotaciones de servidor, un archivo de anotaciones de gestor, un archivo de anotaciones de supervisor de métrica (anotación de las comunicaciones con los agentes de Metric Server) y un archivo de anotaciones para cada asesor que se utilice.

Nota: Además, para el componente Dispatcher solamente, se pueden anotar entradas en un archivo de anotaciones de subagente (SNMP).

Se puede establecer el nivel de registro para definir el volumen de los mensajes escritos en el archivo de anotaciones. Para el nivel 0, se anotan errores y Network Dispatcher también anota las cabeceras y los registros de eventos que se producen una sola vez (por ejemplo, un mensaje acerca del inicio de un asesor que se escribe en el archivo de anotaciones del gestor). El Nivel 1 incluye información de progreso y el Nivel 5 incluye todos los mensajes generados para ayudar en la depuración de un problema, si es necesario. El valor por omisión para el archivo de anotaciones del servidor es 0. El valor por omisión para los archivos de anotaciones del gestor, los asesores y del subagente es 1.

Se puede establecer también el tamaño máximo de un archivo de anotaciones. Si establece un tamaño máximo del archivo de anotaciones, éste se sobrescribirá; cuando el archivo alcance el tamaño especificado, las entradas siguientes se grabarán al principio del archivo encima de las ya existentes. No se puede establecer como tamaño de archivo de anotaciones un valor inferior al actual. En las entradas de anotaciones figura la indicación de la hora, de forma que puede establecerse el orden en que se han grabado.

Cuanto más alto sea el nivel de anotaciones, más cuidadosamente debe elegirse el tamaño del archivo de anotaciones. En el nivel 0, probablemente lo seguro sea dejar el tamaño del archivo de anotaciones en el valor por omisión de 1 MB; no obstante, si el nivel de anotaciones es 3 o superior, debe limitarse el tamaño sin hacerlo tan pequeño que resulte inútil.

- Para configurar el nivel de registro de anotaciones o el tamaño máximo de un archivo de anotaciones de servidor, utilice el mandato **ndcontrol set**.

- Para configurar el nivel de registro de anotaciones o el tamaño máximo de un archivo de anotaciones de gestor, utilice el mandato **ndcontrol manager**. Este mandato también controla el nivel de anotaciones del archivo de anotaciones de supervisor de métrica, en el cual se registran las comunicaciones con los agentes de Metric Server.
- Para configurar el nivel de registro de anotaciones o el tamaño máximo de un archivo de anotaciones de asesor, utilice el mandato **ndcontrol advisor**.
- Para configurar el nivel de registro de anotaciones o el tamaño máximo de un archivo de anotaciones de subagente, utilice el mandato **ndcontrol subagent**. (El subagente SNMP sólo es utilizado por el componente Dispatcher).

Cambio de la vía de acceso de los archivos de anotaciones

Por omisión, los archivos de anotaciones creados por Network Dispatcher se guardan en el directorio de anotaciones de la instalación de Network Dispatcher. Para cambiar esta vía de acceso, defina la variable *nd_logdir* en el script *ndserver*.

AIX, Linux y Solaris: El script *ndserver* está situado en el directorio */usr/bin*. En este script, la variable *nd_logdir* se establece en el directorio por omisión. Puede modificar esta variable de modo que especifique otro directorio para las anotaciones. Ejemplo:

ND_LOGDIR=/ruta/a/mis/archivos/

Windows 2000: El archivo *ndserver* está situado en el directorio del sistema Windows 2000, generalmente *C:\WINNT\SYSTEM32*. En el archivo *ndserver*, la variable *nd_logdir* tiene asignado el directorio por omisión. Puede modificar esta variable de modo que especifique otro directorio para las anotaciones. Ejemplo:

set ND_LOGDIR=c:\ruta\a\mis\archivos

En todos los sistemas operativos, asegúrese de que no hay espacios en ninguno de los lados del signo igual y de que la vía finaliza con una barra inclinada ("*/*" o "**" según proceda).

Anotaciones en binario

Nota: La función de anotaciones en binario no se puede utilizar para el componente Site Selector.

La función de anotaciones en binario de Network Dispatcher utiliza el mismo directorio que los demás archivos de anotaciones. Consulte "Utilizar las anotaciones en binario para analizar las estadísticas del servidor" en la página 198.

Utilización del componente Dispatcher

Esta sección describe cómo utilizar y gestionar el componente Dispatcher.

Inicio y detención de Dispatcher

- Escriba **ndserver** en una línea de mandatos para iniciar Dispatcher.
- Escriba **ndserver stop** en una línea de mandatos para detener Dispatcher.

Utilización del valor de tiempo de espera de inactividad

Para Network Dispatcher, se considera que una conexión está inactiva cuando no se ha producido actividad en ella durante el número de segundos especificado en el tiempo de espera de inactividad. Una vez transcurridos esos segundos sin que haya habido ninguna actividad, Network Dispatcher elimina el registro de esa conexión en sus tablas y se rechaza el tráfico subsiguiente dirigido a esa conexión.

A nivel de puerto, por ejemplo, puede especificar el valor de tiempo de espera de inactividad en el mandato **ndcontrol port set staletimeout**.

El tiempo de espera de inactividad se puede definir a nivel de ejecutor, cluster y puerto. A nivel de ejecutor y de cluster, el valor por omisión es 300 segundos y se propaga al puerto. A nivel de puerto, el valor por omisión depende del puerto. Algunos puertos bien definidos tienen valores diferentes para el tiempo de espera de inactividad. Por ejemplo, el puerto telnet 23 tiene un valor por omisión de 32.000.000 segundos.

Algunos servicios pueden también tener sus propios valores de tiempo de espera de inactividad. Por ejemplo, LDAP (Lightweight Directory Access Protocol) tiene un parámetro de configuración llamado `idletimeout`. Cuando transcurren los segundos especificados por `idletimeout`, se fuerza el cierre de una conexión de cliente inactiva. El parámetro `idletimeout` puede también tener el valor 0, lo que significa que nunca se hará un cierre forzado de la conexión.

Se pueden producir problemas de conectividad cuando el valor de tiempo de espera de inactividad de Network Dispatcher es menor que el tiempo de espera del servicio. En el caso de LDAP, el valor de tiempo de espera de inactividad de Network Dispatcher (`staletimeout`) se establece por omisión en 300 segundos. Si hay actividad en la conexión durante 300 segundos, Network Dispatcher eliminará el registro de la conexión en sus tablas. Si el valor `idletimeout` es mayor que 300 segundos (o se establece en 0), el cliente puede todavía creer que tiene una conexión con el servidor. Cuando el cliente envía paquetes, éstos son rechazados por Network Dispatcher. Esto hace que LDAP quede bloqueado cuando se efectúa una petición al servidor. Para evitar este

problema, establezca el parámetro `idletimeout` de LDAP en un valor distinto de cero que sea igual o menor que el valor `staletimeout` de Network Dispatcher.

Utilización del número de conexiones finalizadas (FIN) para controlar la recogida de basura

Un cliente envía un paquete FIN una vez que ha enviado todos los paquetes para que, así, el servidor sepa que la transacción ha finalizado. Cuando Dispatcher recibe el paquete FIN, quita a la transacción la marca de estado activo y le pone la marca de estado de finalización. Cuando se ha marcado una transacción con el estado de finalización, el recogedor de basura incluido en el ejecutor puede borrar la memoria reservada para la conexión.

Se puede utilizar el tiempo de espera para estado de finalización y el número de conexiones finalizadas para establecer la frecuencia con la que el ejecutor realizará la recogida de basura y hasta qué punto. El ejecutor comprueba periódicamente la lista de las conexiones que ha asignado. Si el número de conexiones en estado de finalización es mayor o igual que el número de conexiones finalizadas, el ejecutor intentará liberar la memoria utilizada para contener la información sobre las conexiones. Se puede cambiar el número de conexiones finalizadas con el mandato **`ndcontrol executor set fincount`**.

El recogedor de basura libera la memoria de aquellas conexiones que se encuentren en estado de finalización y superen el número de segundos especificado en el tiempo de espera para estado de finalización. Se puede cambiar el tiempo de espera para estado de finalización entrando el mandato **`ndcontrol executor set fintimeout`**.

El valor de tiempo de espera de inactividad (`staletimeout`) es el número de segundos durante los cuales puede haber ausencia de actividad en una conexión antes de que dicha conexión se elimine. Consulte “Utilización del valor de tiempo de espera de inactividad” en la página 209 para obtener más información. El número de conexiones finalizadas también afecta a la frecuencia con que se eliminan las conexiones “sin actividad”. Si tiene poca memoria en la máquina Dispatcher, debe establecer un número de conexiones finalizadas bajo. Si tiene un sitio Web muy ocupado, debe establecer un número de conexiones finalizadas alto.

GUI de notificación — la opción de menú Supervisor

Se pueden mostrar diversos diagramas basándose en la información procedente del ejecutor y transmitida al gestor. La opción de menú Supervisor de GUI necesita que la función del gestor se esté ejecutando):

- Conexiones por segundo para cada servidor (se pueden mostrar varios servidores en el mismo gráfico)
- Valores relativos de peso por servidor en un puerto en particular
- Duración media de la conexión por servidor en un puerto en particular

Utilización de SNMP (Simple Network Management Protocol) con el componente Dispatcher

Nota: En Linux, no se puede utilizar SNMP para Network Dispatcher.

Un sistema de gestión de red es un programa que se ejecuta continuamente y que se utiliza para supervisar, controlar y reflejar el estado de una red. El estándar actual para la gestión de red es el Protocolo simple de gestión de red (SNMP), un popular protocolo para la comunicación con dispositivos en una red. Los dispositivos de red disponen generalmente de un *agente* SNMP y de uno o más subagentes. El agente SNMP se comunica con la *estación de gestión de red* o responde a peticiones SNMP efectuadas desde la línea de mandatos. El *subagente* SNMP recupera y actualiza la información y la entrega al agente SNMP para que la devuelva al peticionario.

Dispatcher proporciona una *Base de información de gestión* (ibmNetDispatcherMIB) SNMP y un subagente SNMP, de manera que para supervisar la salud, la actividad y el rendimiento de Dispatcher, se puede utilizar cualquier sistema de gestión de redes como, por ejemplo, Tivoli NetView, Tivoli Distributed Monitoring o HP OpenView. Los datos MIB describen el Dispatcher que se está gestionando y reflejan al estado actual de Dispatcher. La MIB se instala en el subdirectorio **..nd/admin/MIB**.

Nota: La MIB, ibmNetDispatcherMIB.02, no se puede cargar utilizando el programa xnmloadmib2 de Tivoli NetView. Para corregir este problema, inhabilite la sección NOTIFICATION-GROUP de la MIB. Es decir, añada "--" al comienzo de la línea "indMibNotifications Group NOTIFICATION-GROUP" y de las 6 líneas siguientes.

El sistema de gestión de red utiliza los mandatos GET de SNMP para averiguar los valores MIB de otras máquinas. A continuación le notifica si se han excedido los valores umbral especificados. Posteriormente se puede retocar el rendimiento de Dispatcher modificando los datos de configuración de Dispatcher, para ajustar o solucionar problemas de Dispatcher antes de que se conviertan en cortes de Dispatcher o del servidor Web.

Mandatos y protocolo SNMP

El sistema proporciona generalmente un agente SNMP para cada una de las estaciones de gestión de red. El usuario envía un mandato GET al agente SNMP. En respuesta, el agente SNMP envía un mandato GET para recuperar los valores MIB especificados de un subagente responsable de dichas variables MIB.

Dispatcher proporciona un subagente que actualiza y recupera los datos MIB. Cuando el agente SNMP envía un mandato GET, el subagente responde con los datos MIB apropiados. El agente SNMP comunica los datos a la estación

de gestión de red. La estación de gestión de red le notificará a usted si se superan los valores umbral especificados.

El soporte para SNMP de Dispatcher incluye un subagente SNMP que utiliza las capacidades de la Interfaz de protocolo distribuido (DPI). DPI es una interfaz entre un agente SNMP y sus subagentes.

Habilitación de SNMP en AIX y Solaris

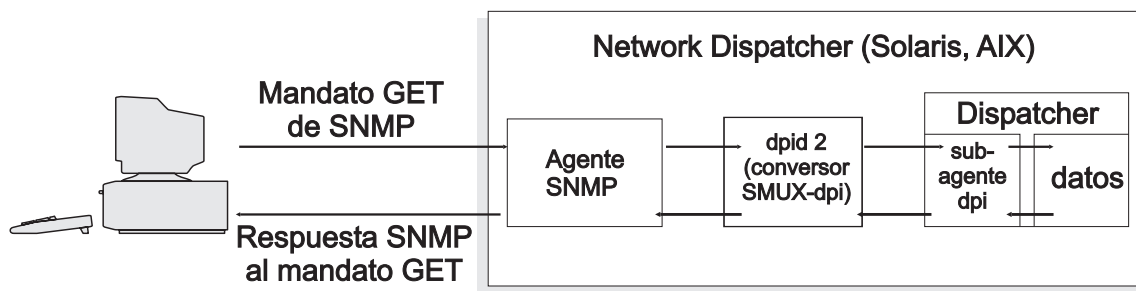


Figura 28. Mandatos SNMP para AIX y Solaris

AIX proporciona un agente SNMP que hace uso del protocolo SMUX (SNMP Multiplexer) y proporciona DPID2, que es un ejecutable adicional que actúa como conversor entre DPI y SMUX.

Para Solaris, debe obtener un agente SNMP que esté habilitado para SMUX, pues Solaris no proporciona uno. Network Dispatcher proporciona DPID2 para Solaris en el directorio `/opt/nd/servers/samples/SNMP`.

El agente DPI debe ejecutarse como usuario root. Antes de ejecutar el daemon DPID2, actualice los archivos `/etc/snmpd.peers` y `/etc/snmpd.conf` de la siguiente manera:

- En el archivo `/etc/snmpd.peers`, añada la entrada siguiente para dpid:
"dpid2" 1.3.6.1.4.1.2.3.1.2.2.1.1.2 "contraseña_dpid"
- En el archivo `/etc/snmpd.conf`, añada la entrada siguiente para dpid:
smux 1.3.6.1.4.1.2.3.1.2.2.1.1.2 contraseña_dpid #dpid

Renueve `snmpd` para que vuelva a leer el archivo `/etc/snmpd.conf`:

```
refresh -s snmpd
```

Inicie el igual DPID SMUX:

```
dpid2
```

Los daemons deben arrancarse en el siguiente orden:

1. Agente SNMP

2. Conversor DPI
3. Subagente de Dispatcher

Habilitación de SNMP en Windows 2000

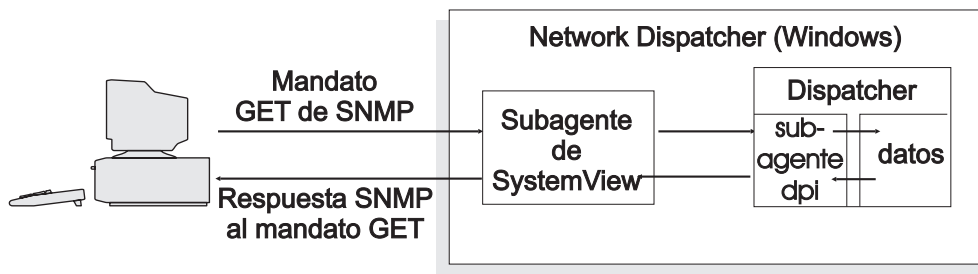


Figura 29. Mandatos de SNMP para Windows 2000

Para obtener un agente de SNMP habilitado para DPI en Windows 2000, instale la versión para Windows NT del kit de utilidades IBM SystemView Agent, contenido en <http://www.tivoli.com/support/sva>.

Antes de iniciar el proceso SNMPD de SystemView, debe inhabilitar el soporte SNMP de Microsoft Windows. El snmpd SystemView da soporte a subagentes DPI y agentes conformes a Microsoft.

Para inhabilitar el soporte de SNMP para Windows:

1. Pulse en Inicio->Programas->Herramientas administrativas->Servicios.
2. Pulse el botón derecho en **SNMP** y, a continuación, seleccione **Propiedades**.
3. Cambie **Tipo de inicio**: a "Inhabilitado"

Nota: Si no inhabilita el soporte de SNMP para Microsoft Windows, el subagente SNMP de Dispatcher no podrá conectar con el agente snmpd.

Para configurar el agente SystemView de SNMP, siga las instrucciones que aparecen en "Provisión de un nombre de comunidad para SNMP".

Provisión de un nombre de comunidad para SNMP

Debe configurar el nombre de comunidad de SNMP. El nombre de comunidad SNMP por omisión es public. En los sistemas UNIX, el nombre de comunidad se define en un archivo llamado /etc/snmpd.conf.

En todos los sistemas, el nombre de comunidad se debe configurar y utilizar de forma coherente. Es decir, si el nombre de comunidad para Network

Dispatcher se define como "NuestraComunidad" en la configuración del agente de SNMP, este nombre también debe ser "NuestraComunidad" en la configuración del subagente.

Para Windows 2000, antes de crear un nombre de comunidad, configure el agente IBM SystemView de SNMP.

1. Desde el escritorio, pulse el icono **Agente IBM SystemView**.
2. Pulse **snmpcfg**.
3. En el cuadro de diálogo Configuración de SNMP, añada el nombre de comunidad. Con fines de prueba, especifique **public** como nombre de comunidad.
Este paso permite que cualquier sistema principal de cualquier red acceda a las variables SNMP de la MIB. Una vez que haya verificado que estos valores funcionan, puede modificarlos de acuerdo a sus necesidades.
4. Examine el archivo `\sva\dm\bin\svastart.bat` y compruebe que está especificada la opción **-dpi**.
5. Inicie el daemon de SNMP ejecutando `svastart.bat` desde el subdirectorio `\sva\dm\bin`.

Con el ejecutor en funcionamiento, utilice el mandato **ndcontrol subagent start [nombrecomunidad]** para definir el nombre de comunidad utilizado entre el subagente DPI y el agente SNMP de Dispatcher. El valor por omisión que corresponde al nombre de comunidad es `public`. Si cambia este valor, debe también añadir el nuevo nombre de comunidad al agente SystemView utilizando `snmpcfg`, como se describió anteriormente.

Detecciones

SNMP se comunica por medio del envío y recepción de *detecciones*, mensajes enviados por los dispositivos gestionados para informar de condiciones excepcionales o de la aparición de sucesos significativos, como que se alcance un umbral.

El subagente utiliza las detecciones siguientes:

- `indHighAvailStatus`
- `indSrvrGoneDown`
- `indDOSAttack`
- `indDOSAttackDone`

La detección **indHighAvailStatus** anuncia que ha cambiado el valor de la variable de estado de alta disponibilidad (`hasState`). Los posibles valores de `hasState` son:

- idle** La máquina está repartiendo el tráfico y no intenta establecer contacto con su Dispatcher asociada.

- listen** Acaba de comenzar la modalidad de alta disponibilidad y Dispatcher está a la espera de recibir mensajes de la máquina asociada.
- active** La máquina está repartiendo el tráfico.
- standby**
La máquina está supervisando a la máquina activa.
- preempt**
Esta máquina está en un estado transitorio durante la conmutación de máquina principal a máquina de reserva.
- elect** Dispatcher está negociando con su asociado respecto a quién será la máquina principal o la máquina de reserva.
- no_exec**
El ejecutor no se está ejecutando.

La detección **indSrvrGoneDown** anuncia que el peso del servidor especificado por la parte csAddr, psNum, ssAddr del Identificador de objeto ha pasado a cero. Se envía a la detección el último número conocido de conexiones activas. Esta detección indica que, por lo que puede determinar Dispatcher, el servidor especificado está desactivado.

La detección **indDOSAttack** indica que numhalfopen, el número de conexiones semiabiertas que sólo constan de paquetes SYN, ha sobrepasado el umbral de maxhalfopen para el puerto especificado por la parte csAddr, psNum del Identificador de objeto. En la detección se envía el número de servidores configurados en el puerto. Esta detección indica que Network Dispatcher puede estar experimentando un ataque de denegación de servicio.

La detección **indDOSAttackDone** indica que numhalfopen, el número de conexiones semiabiertas que sólo constan de paquetes SYN, está por debajo del umbral de maxhalfopen para el puerto especificado por la parte csAddr, psNum del Identificador de objeto. En la detección se envía el número de servidores configurados en el puerto. Cuando Network Dispatcher determine que ha terminado el posible ataque de denegación de servicio, enviará esta detección después de enviar la detección indDOSAttack.

Debido a una limitación de la API SMUX, el identificador de empresa informado en las detecciones del subagente ibmNetDispatcher puede ser el identificador de empresa de dpid2, en lugar del identificador de empresa de ibmNetDispatcher, 1.3.6.1.4.1.2.6.144. No obstante, las utilidades de gestión SNMP podrán determinar el origen de la detección, ya que los datos contendrán un identificador de objeto de la MIB de ibmNetDispatcher.

Activación y desactivación del soporte SNMP por medio del mandato `ndcontrol`

El mandato `ndcontrol subagent start` activa el soporte SNMP. El mandato `ndcontrol subagent stop` desactiva el soporte SNMP.

Para más información acerca del mandato `ndcontrol`, consulte “`ndcontrol subagent` — configurar subagente SNMP” en la página 310.

Utilización de `ipchains` o `iptables` para rechazar todo el tráfico para (reforzar) el recuadro Network Dispatcher (en Linux)

Integrado en el kernel de Linux hay un recurso de cortafuegos denominado `ipchains`. Cuando se ejecutan simultáneamente Network Dispatcher e `ipchains`, Network Dispatcher ve primero paquetes, seguido de `ipchains`. Esto permite utilizar `ipchains` para reforzar un recuadro de Network Dispatcher de Linux, que puede ser, por ejemplo, un recuadro de Network Dispatcher que se utiliza para repartir el tráfico de los cortafuegos.

Cuando `ipchains` o `iptables` se configuran como completamente restringidos (no se permite tráfico de entrada ni de salida), la parte de envío de paquetes de Network Dispatcher continúa funcionando con normalidad.

Tenga en cuenta que `ipchains` e `iptables` *no* se pueden utilizar para filtrar el tráfico de entrada antes de que se reparta el tráfico.

Se debe permitir cierto tráfico adicional para que todo Network Dispatcher funcione correctamente. Algunos ejemplos de esta comunicación son:

- Los asesores establecen comunicación entre el recuadro Network Dispatcher y los servidores de fondo.
- Network Dispatcher realiza ping de servidores de fondo, destinos a alcanzar y recuadros Network Dispatcher de asociados de alta disponibilidad.
- Las interfaces de usuario (interfaz gráfica de usuario, línea de mandatos y asistentes) utilizan RMI.
- Los servidores de fondo deben responder a ping desde el recuadro Network Dispatcher.

En general, una estrategia de `ipchains` adecuada para recuadros Network Dispatcher es no permitir ningún tráfico, excepto el que procede o el que va destinado a los servidores de fondo, Network Dispatcher de alta disponibilidad de asociados, destinos a alcanzar o sistemas principales de configuración.

Utilización del componente Content Based Routing

Esta sección describe cómo utilizar y gestionar el componente CBR de Network Dispatcher.

Inicio y detención de CBR

- Escriba **cbrserver** en una línea de mandatos para iniciar CBR.
- Escriba **cbrserver stop** en una línea de mandatos para detener CBR.

CBR y Caching Proxy trabajan conjuntamente mediante la API de Caching Proxy para gestionar las peticiones HTTP y HTTPS (SSL). Caching Proxy debe estar ejecutándose en la misma máquina para que CBR comience a repartir el tráfico entre servidores. Configure CBR y Caching Proxy tal como se describe en “Ejemplo de configuración de CBR” en la página 92.

Control de CBR

Después de iniciar CBR, puede controlarlo utilizando cualquiera de estos dos métodos:

- Configure CBR mediante el mandato **cbrcontrol**. La sintaxis completa de este mandato se describe en el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249. Aquí se incluyen algunos ejemplos.
- Configure CBR utilizando la interfaz gráfica de usuario (GUI). Escriba **ndadmin** en la línea de mandatos para abrir la GUI. Consulte “GUI” en la página 84 para obtener información sobre cómo configurar CBR utilizando la GUI.

Utilización de archivos de anotaciones de CBR

Los archivos de anotaciones utilizados por CBR son similares a los utilizados en Dispatcher. Para obtener más información, consulte “Utilización de los archivos de anotaciones de Network Dispatcher” en la página 207.

Nota:

En versiones anteriores del producto, el usuario podía cambiar la vía de acceso del directorio de anotaciones de CBR en el archivo de configuración de Caching Proxy. Ahora el usuario puede cambiar la vía de acceso del directorio donde se guarda el archivo de anotaciones, en el archivo **cbrserver**. Consulte “Cambio de la vía de acceso de los archivos de anotaciones” en la página 208.

Utilización del componente Mailbox Locator

Inicio y detención de Mailbox Locator

- Escriba **mlserver** en una línea de mandatos para iniciar Mailbox Locator.
- Escriba **mlserver stop** en una línea de mandatos para detener Mailbox Locator.

Control de Mailbox Locator

Después de iniciar Mailbox Locator, puede controlarlo utilizando cualquiera de estos dos métodos:

- Configure Mailbox Locator mediante el mandato **mlcontrol**. La sintaxis completa de este mandato se describe en el “Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator” en la página 249. Aquí se incluyen algunos ejemplos.
- Configure Mailbox Locator utilizando la interfaz gráfica de usuario (GUI). Escriba **ndadmin** en la línea de mandatos para abrir la GUI. Consulte “GUI” en la página 101 para obtener información sobre cómo configurar Mailbox Locator utilizando la GUI.

Utilización de los archivos de anotaciones de Mailbox Locator

Los archivos de anotaciones utilizados por Mailbox Locator son similares a los utilizados en Dispatcher. Para obtener una descripción más detallada, consulte “Utilización de los archivos de anotaciones de Network Dispatcher” en la página 207.

Utilización del componente Site Selector

Inicio y detención de Site Selector

- Escriba **ssserver** en una línea de mandatos para iniciar Site Selector.
- Escriba **ssserver stop** en una línea de mandatos para detener Site Selector.

Control de Site Selector

Después de iniciar Site Selector, puede controlarlo utilizando cualquiera de estos dos métodos:

- Configure Site Selector mediante el mandato **sscontrol**. El “Apéndice D. Consulta de mandatos de Site Selector” en la página 317 describe la sintaxis completa de este mandato. Aquí se incluyen algunos ejemplos.
- Configure Site Selector utilizando la interfaz gráfica de usuario (GUI). Escriba **ndadmin** en la línea de mandatos para abrir la GUI. Consulte “GUI” en la página 115 para obtener información sobre cómo configurar Site Selector utilizando la GUI.

Utilización de los archivos de anotaciones de Site Selector

Los archivos de anotaciones utilizados por Site Selector son similares a los utilizados en Dispatcher. Para obtener una descripción más detallada, consulte “Utilización de los archivos de anotaciones de Network Dispatcher” en la página 207.

Utilización del componente Cisco Consultant

Inicio y detención de Cisco Consultant

1. Escriba **lbcserver** en una línea de mandatos para iniciar Cisco Consultant.
2. Escriba **lbcserver stop** en una línea de mandatos para detener Cisco Consultant.

Controlar Cisco Consultant

Después de iniciar Cisco Consultant, puede controlarlo utilizando cualquiera de estos dos métodos:

- Configure Cisco Consultant mediante el mandato **lbccontrol**. El “Apéndice E. Consulta de mandatos de Consultant para Cisco CSS Switches” en la página 347 describe la sintaxis completa de este mandato. Aquí se incluyen algunos ejemplos.
- Configure Cisco Consultant utilizando la interfaz gráfica de usuario (GUI). Escriba **ndadmin** en la línea de mandatos para abrir la GUI. Consulte “GUI” en la página 115 para obtener información sobre cómo configurar Cisco Consultant utilizando la GUI.

Utilización de los archivos de anotaciones de Cisco Consultant

Los archivos de anotaciones utilizados por Cisco Consultant son similares a los utilizados en Dispatcher. Para obtener una descripción más detallada, consulte “Utilización de los archivos de anotaciones de Network Dispatcher” en la página 207.

Utilización del componente Metric Server

Inicio y detención de Metric Server

Metric Server proporciona a Network Dispatcher información sobre el tráfico de los servidores. Metric Server reside en cada uno de los servidores para los que se reparte el tráfico.

- En cada máquina servidor donde resida Metric Server, escriba **metricserver start** en una línea de mandatos para iniciar Metric Server.
- En cada máquina servidor donde resida Metric Server, escriba **metricserver stop** en una línea de mandatos para detener Metric Server.

Utilización de los archivos de anotaciones de Metric Server

Cambie el nivel de anotaciones en el script de arranque de Metric Server. Puede especificar un rango de nivel de anotaciones de 0 a 5, similar al rango de nivel de anotaciones de los archivos de anotaciones de Network Dispatcher. Esto generará un archivo de anotaciones de agente en el directorio **...ms/logs**.

Capítulo 16. Resolución de problemas

Este capítulo le ayuda a detectar y a resolver problemas asociados con Network Dispatcher. Busque el síntoma que está experimentando en “Tablas de resolución de problemas”.

Tablas de resolución de problemas

A continuación se proporcionan tablas de resolución de problemas para Dispatcher, CBR, Mailbox Locator, Site Selector y Consultant para Cisco CSS Switches.

Tabla 14. Tabla de resolución de problemas de Dispatcher

Síntoma	Causa posible	Diríjase a...
Dispatcher no se ejecuta correctamente	Números de puerto en conflicto	“Comprobar los números de puerto de Dispatcher” en la página 227
Se ha configurado un servidor con ubicación compartida y no responderá a las peticiones de reparto del tráfico	Dirección errónea o en conflicto	“Problema: Dispatcher y el servidor no responderán” en la página 230
Conexiones de las máquinas cliente no atendidas o se ha agotado el tiempo de espera de las mismas	<ul style="list-style-type: none">• Configuración de encaminamiento incorrecta• NIC no unida a la dirección de cluster por medio de un alias• El servidor no ha unido el dispositivo de bucle de retorno por medio de un alias a la dirección de cluster• Ruta adicional no suprimida• Puerto no definido para cada cluster• Los servidores están desactivados o establecidos para un peso de cero	“Problema: no se realiza el reparto del tráfico para las peticiones de Dispatcher” en la página 231

Tabla 14. Tabla de resolución de problemas de Dispatcher (continuación)

Síntoma	Causa posible	Diríjase a...
Las máquinas cliente no se están atendiendo o están agotando el tiempo de espera	La alta disponibilidad no funciona	“Problema: la modalidad de alta disponibilidad de Dispatcher no funciona” en la página 231
No se puede añadir pulso (Windows 2000)	La dirección origen no está configurada en un adaptador	“Problema: no se puede añadir pulso (Windows 2000)” en la página 231
El servidor no atiende a las peticiones (Windows)	Se ha creado una ruta adicional en la tabla de encaminamiento	“Problema: rutas sobrantes (sólo Windows 2000)” en la página 232
Los asesores no están funcionando correctamente con el área amplia	Los asesores no se están ejecutando en las máquinas remotas	“Problema: los asesores no funcionan correctamente” en la página 232
SNMPD no arranca o no seguirá ejecutándose (Windows 2000)	El nombre de comunidad que se ha pasado en los mandatos SNMP no se corresponde con el nombre de comunidad con el que se ha iniciado el subagente	“Problema: SNMPD no se ejecuta correctamente (Windows 2000)” en la página 232
Dispatcher, Microsoft IIS y SSL no están funcionando o no van a seguir haciéndolo	No se pueden enviar datos cifrados a través de los protocolos	“Problema: Dispatcher, Microsoft IIS y SSL no funcionan (Windows 2000)” en la página 232
Conexión a máquina remota rechazada	Se sigue utilizando una versión más antigua de las claves	“Problema: conexión de Dispatcher a una máquina remota” en la página 232
Un mandato ndcontrol o ndadmin da error con en mensaje ‘El servidor no responde’ o ‘No se puede acceder al servidor RMI’	<ol style="list-style-type: none"> 1. Los mandatos fallan debido a una pila con socks. O los mandatos fallan debido a que ndserver no se ha iniciado 2. Los puertos RMI no están definidos correctamente 	“Problema: el mandato ndcontrol o ndadmin da error” en la página 232
Mensaje de error del tipo “No se puede encontrar el archivo...” cuando se ejecuta Netscape como navegador por omisión para ver la ayuda en línea (Windows 2000)	Valor incorrecto para la asociación de archivo HTML	“Problema: se visualiza el mensaje de error del tipo “No se puede encontrar el archivo...” al intentar visualizar la ayuda en línea (Windows 2000)” en la página 233

Tabla 14. Tabla de resolución de problemas de Dispatcher (continuación)

Síntoma	Causa posible	Diríjase a...
Al iniciar ndserver en Solaris 2.7, aparece el mensaje de error: "stty: No existe tal dispositivo ni dirección".	Puede pasar por alto este mensaje de error. No es indicativo de un problema. Ndserv se ejecutará correctamente	"Problema: mensaje falso de error al iniciar ndserver en Solaris 2.7" en la página 234
La interfaz gráfica de usuario no se inicia correctamente	Espacio de paginación insuficiente	"Problem: la interfaz gráfica de usuario (GUI) no arranca correctamente" en la página 234
Error al ejecutar Dispatcher cuando Caching Proxy está instalado	Dependencia de Caching Proxy respecto a un archivo	"Problema: error al ejecutar Dispatcher cuando Caching Proxy está instalado" en la página 234
La interfaz gráfica de usuario no se visualiza correctamente.	El valor de resolución de pantalla no es correcto.	"Problema: la interfaz gráfica de usuario (GUI) no se visualiza correctamente" en la página 234
Algunas veces los paneles de ayuda quedan ocultos detrás de otras ventanas	Limitación de Java	"Problema: en Windows 2000, las ventanas de ayuda algunas veces quedan ocultas detrás de otras ventanas abiertas" en la página 234
Network Dispatcher no puede procesar y reenviar una trama	Es necesaria una dirección MAC exclusiva para cada adaptador de red	"Problema: Network Dispatcher no puede procesar y reenviar una trama" en la página 235
Aparece una pantalla azul	No hay una tarjeta de red instalada y configurada	"Problema: aparece una pantalla azul al iniciar el ejecutor de Network Dispatcher" en la página 235
La vía de acceso de descubrimiento impide la devolución de tráfico	El cluster tiene un alias en el bucle de retorno	"Problema: la vía de acceso de descubrimiento impide la devolución de tráfico con Network Dispatcher" en la página 235
Los asesores muestran que todos los servidores están inactivos	La suma de comprobación de TCP no se ha calculado correctamente	"Problema: los asesores muestran que todos los servidores están inactivos" en la página 236

Tabla 14. Tabla de resolución de problemas de Dispatcher (continuación)

Síntoma	Causa posible	Diríjase a...
La alta disponibilidad en la modalidad de área amplia de Network Dispatcher no funciona.	Debe definirse un Dispatcher remoto como servidor de un cluster en el Dispatcher local	"Problema: la alta disponibilidad en la modalidad de área amplia de Network Dispatcher no funciona" en la página 237
La GUI se cuelga (o se comporta de forma inesperada) cuando se intenta cargar un archivo de configuración grande.	Java no tiene acceso a la suficiente memoria como para manejar un cambio tan grande en la GUI.	"Problema: la GUI se cuelga (o se comporta de forma inesperada) cuando se intenta cargar un archivo de configuración grande" en la página 237

Tabla 15. Tabla de resolución de problemas de CBR

Síntoma	Causa posible	Ir a...
CBR no se ejecuta correctamente	Números de puerto en conflicto	"Comprobación de los números de puerto de CBR" en la página 228
El mandato cbrcontrol o ndadmin falla y devuelve el mensaje 'El servidor no responde' o 'No se puede acceder al servidor RMI'	Los mandatos fallan debido a una pila con socks. O los mandatos fallan debido a que cbrserver no se ha iniciado	"Problema: el mandato cbrcontrol o ndadmin falla" en la página 238
No se realiza el reparto del tráfico para las peticiones	Se ha iniciado Caching Proxy antes de iniciar el ejecutor	"Problema: no se realiza el reparto del tráfico para las peticiones" en la página 239
En Solaris, el mandato cbrcontrol executor start falla con el mensaje 'Error: No se ha iniciado el ejecutor.'	El mandato falla porque puede que tengan que modificarse los valores por omisión de IPC del sistema	"Problema: en Solaris, el mandato cbrcontrol executor start falla" en la página 239
La norma de URL no funciona	Error sintáctico o de configuración	"Problema: error sintáctico o de configuración" en la página 239

Tabla 16. Tabla de resolución de problemas de Mailbox Locator

Síntoma	Causa posible	Ir a...
Mailbox Locator no se ejecuta correctamente	Números de puerto en conflicto	"Comprobación de los números de puerto de Mailbox Locator" en la página 228

Tabla 16. Tabla de resolución de problemas de Mailbox Locator (continuación)

El mandato mlserver devuelve la excepción "java.rmi.RMI Security Exception: security.fd.read"	El límite de descriptores de archivo del sistema es demasiado pequeño para el número de peticiones a las que intenta atender mlserver	"Problema: el mandato mlserver está detenido" en la página 240
El mandato mlcontrol o ndadmin falla y devuelve el mensaje 'El servidor no responde' o 'No se puede acceder al servidor RMI'	Los mandatos fallan debido a una pila con socks. O bien los mandatos fallan debido a que mlserver no está iniciado.	"Problema: el mandato mlcontrol o ndadmin falla" en la página 240
No se puede añadir un puerto	Otra aplicación ya está a la escucha en ese puerto	"Problema: no se puede añadir un puerto" en la página 240
Se recibe un error de proxy al intentar añadir un puerto	No se ha configurado la dirección de cluster en un adaptador de red antes de iniciar el proxy, O bien otra aplicación está en ejecución en ese puerto.	"Problema: se recibe un error de proxy al intentar añadir un puerto" en la página 241

Tabla 17. Tabla de resolución de problemas de Site Selector

Síntoma	Causa posible	Diríjase a...
Site Selector no se ejecuta correctamente	Número de puerto en conflicto	"Comprobación de los números de puerto de Site Selector" en la página 229
Site Selector no efectúa el reparto rotatorio del tráfico para las peticiones entrantes procedentes de clientes Solaris	Los sistemas Solaris ejecutan una daemon de servicio de nombres en antememoria.	"Problema: Site Selector no efectúa un reparto rotatorio para el tráfico procedente de clientes Solaris" en la página 241
El mandato sscontrol o ndadmin falla y devuelve el mensaje 'El servidor no responde' o 'No se puede acceder al servidor RMI'	Los mandatos fallan debido a una pila con socks. O bien los mandatos fallan debido a que ssserver no está iniciado.	"Problema: el mandato sscontrol o ndadmin falla" en la página 241
ssserver no se inicia en Windows 2000	Windows no necesita que el nombre del sistema principal esté en el DNS.	"Problema: ssserver no se inicia en Windows 2000" en la página 241

Tabla 17. Tabla de resolución de problemas de Site Selector (continuación)

Síntoma	Causa posible	Diríjase a...
La máquina con rutas duplicadas no reparte el tráfico correctamente — la resolución de nombres parece ser anómala	La máquina de Site Selector tiene varios adaptadores de red que están conectados a la misma subred	“Problema: Site Selector no reparte el tráfico correctamente si hay rutas duplicadas” en la página 242

Tabla 18. Tabla de resolución de problemas de Consultant para Cisco CSS Switches

Síntoma	Causa posible	Diríjase a...
lbcserv no arranca	Números de puerto en conflicto	“Comprobación de los números de puerto de Cisco Consultant” en la página 230
El mandato lbcontrol o ndadmin falla y devuelve el mensaje ‘El servidor no responde’ o ‘No se puede acceder al servidor RMI’	Los mandatos fallan debido a una pila con socks. O bien los mandatos fallan debido a que lbcserv no está iniciado.	“Problema: el mandato lbcontrol o ndadmin falla” en la página 242
Error de recepción: No se puede crear registro para el puerto 14099	Licencia de producto caducada	“Problema: No se puede crear el registro para el puerto 14099” en la página 242

Tabla 19. Tabla de resolución de problemas de Metric Server

Síntoma	Causa posible	Diríjase a...
Excepción de E/S de Metric Server en Windows 2000 al ejecutar los archivos de métrica del usuario .bat o .cmd	Es necesario el nombre de métrica completo	“Problema: excepción de E/S de Metric Server en Windows 2000 al ejecutar los archivos de métrica del usuario .bat o .cmd” en la página 243
Metric Server no notifica a la máquina Network Dispatcher información sobre carga	Las posibles causas son: <ul style="list-style-type: none"> no hay archivos de claves en la máquina Metric Server el nombre de sistema principal de la máquina Metric Server no está registrado con el servidor de nombres local 	“Problema: Metric Server no notifica cargas a la máquina Network Dispatcher” en la página 243

Tabla 19. Tabla de resolución de problemas de Metric Server (continuación)

Síntoma	Causa posible	Diríjase a...
Las anotaciones de Metric Server indican que "se necesita una firma para acceder al agente" cuando se transfieren archivos de claves al servidor	El archivo de claves no ofrece autorización porque está dañado.	"Problema: las anotaciones de Metric Server indican que "se necesita una firma para poder acceder al agente"" en la página 244

Comprobar los números de puerto de Dispatcher

Si tiene problemas al ejecutar Dispatcher, es posible que una de las aplicaciones utilice un número de puerto que utiliza normalmente Dispatcher. Tenga presente que el servidor Dispatcher utiliza los números de puerto siguientes:

- 10099 para recibir mandatos de ndcontrol
- 10004 para enviar consultas métricas a Metric Server
- 10005 para recibir información de un agente SDA

Si otra aplicación utiliza uno de los números de puerto de Dispatcher, puede cambiar dicho número para Dispatcher haciendo lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos
 - Modifique la variable ND_RMIPORT, que figura al principio del archivo ndserver, para que sea igual al puerto que Dispatcher debe utilizar para recibir mandatos.
- Para cambiar el puerto utilizado para recibir informes de métrica procedentes de Metric Server
 - Modifique la variable RMI_PORT, en el archivo metricserver, para que sea igual al puerto que Dispatcher debe utilizar para comunicarse con Metric Server.
 - Proporcione el argumento metric_port cuando se inicie el gestor. Vea la descripción de la sintaxis del mandato **ndcontrol manager start** en "ndcontrol manager — controlar el gestor" en la página 279
- Para cambiar el puerto utilizado para recibir la información de SDA, cambie la variable ND_AFFINITY_PORT del archivo ndserver para que sea igual al puerto que Dispatcher debe utilizar para recibir la información de SDA.

Nota: Para Windows 2000, los archivos ndserver y metricserver están situados en el directorio c:\winnt\system32. Para otras plataformas, estos archivos residen en el directorio /usr/bin/.

Comprobación de los números de puerto de CBR

Si tiene problemas al ejecutar CBR, puede que una de las aplicaciones esté utilizando un número de puerto utilizado habitualmente por CBR. Tenga presente que CBR utiliza los siguientes números de puerto:

- 11099 para recibir mandatos de cbrcontrol
- 10004 para enviar consultas métricas a Metric Server

Si otra aplicación utiliza uno de los números de puerto de CBR, puede cambiar el número de puerto de CBR haciendo lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos
 - Modifique la variable ND_RMIPORT, que figura al principio del archivo cbrserver, para que sea igual al puerto que CBR debe utilizar para recibir mandatos.
- Para cambiar el puerto utilizado para recibir informes de métrica procedentes de Metric Server
 - Modifique la variable RMI_PORT, en el archivo metricserver, para que sea igual al puerto que CBR debe utilizar para comunicarse con Metric Server.
 - Proporcione el argumento metric_port cuando se inicie el gestor. Vea la descripción de la sintaxis del mandato **manager start** en “ndcontrol manager — controlar el gestor” en la página 279

Nota: Para Windows 2000, los archivos cbrserver y metricserver están situados en el directorio c:\winnt\system32. Para otras plataformas, estos archivos residen en el directorio /usr/bin/.

Comprobación de los números de puerto de Mailbox Locator

Si tiene problemas al ejecutar Mailbox Locator, puede que una de las aplicaciones esté utilizando un número de puerto utilizado normalmente por Mailbox Locator. Tenga presente que Mailbox Locator utiliza los siguientes números de puerto:

- 13099 para recibir mandatos de mlcontrol
- 10004 para enviar consultas métricas a Metric Server

Si otra aplicación utiliza uno de los números de puerto de Mailbox Locator, puede cambiar el número de puerto de Mailbox Locator haciendo lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos
 - Modifique la variable ND_RMIPORT, que figura al principio del archivo mlserver, para que sea igual al puerto que Mailbox Locator debe utilizar para recibir mandatos.

- Para cambiar el puerto utilizado para recibir informes de métrica procedentes de Metric Server
 - Modifique la variable `RMI_PORT`, en el archivo `metricserver`, para que sea igual al puerto que Mailbox Locator debe utilizar para comunicarse con Metric Server.
 - Proporcione el argumento `metric_port` cuando se inicie el gestor. Vea la descripción de la sintaxis del mandato **manager start** en “ndcontrol manager — controlar el gestor” en la página 279

Nota: Para Windows 2000, los archivos `mlserver` y `metricserver` están situados en el directorio `c:\winnt\system32`. Para otras plataformas, estos archivos residen en el directorio `/usr/bin`.

Comprobación de los números de puerto de Site Selector

Si tiene problemas al ejecutar el componente Site Selector, puede que una de las aplicaciones esté utilizando un número de puerto utilizado normalmente por Site Selector. Tenga presente que Site Selector utiliza los siguientes números de puerto:

- 12099 para recibir mandatos de `sscontrol`
- 10004 para enviar consultas métricas a Metric Server

Si otra aplicación utiliza uno de los números de puerto de Site Selector, puede cambiar el número de puerto de Site Selector haciendo lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos,
 - Modifique la variable `ND_RMIPORT`, que figura al principio del archivo `ssserver`, para que sea igual al puerto que Site Selector debe utilizar para recibir mandatos.
- Para cambiar el puerto utilizado para recibir informes de métrica procedentes de Metric Server
 - Modifique la variable `RMI_PORT`, en el archivo `metricserver`, para que sea igual al puerto que Site Selector debe utilizar para comunicarse con Metric Server.
 - Proporcione el argumento `metric_port` cuando se inicie el gestor. Vea la descripción de la sintaxis del mandato **manager start** en “sscontrol manager — controlar el gestor” en la página 327

Nota: Para Windows 2000, los archivos `ssserver` y `metricserver` están situados en el directorio `c:\winnt\system32`. Para otras plataformas, estos archivos residen en el directorio `/usr/bin/`.

Comprobación de los números de puerto de Cisco Consultant

Si tiene problemas al ejecutar el componente Cisco Consultant, puede que una de las aplicaciones esté utilizando un número de puerto utilizado normalmente por el archivo lbcserver de Cisco Consultant. Tenga presente que Cisco Consultant utiliza los siguientes números de puerto:

14099 para recibir mandatos de lbcontrol

10004 para enviar consultas métricas a Metric Server

Si otra aplicación utiliza uno de los números de puerto de Consultant, puede cambiar los números de puerto de Consultant haciendo lo siguiente:

- Para cambiar el puerto utilizado para recibir mandatos de lbcontrol, modifique la variable ND_RMIPORT en el archivo lbcserver. Cambie el valor 14099 por el número de puerto donde Consultant debe recibir los mandatos de lbcontrol.
- Para cambiar el puerto utilizado para recibir informes de métrica procedentes de Metric Server:
 1. Modifique la variable RMI_PORT en el archivo metricserver. Cambie el valor 10004 por el número de puerto que Consultant debe utilizar para comunicarse con Metric Server.
 2. Proporcione el argumento metric_port cuando se inicie el gestor. Consulte “lbcontrol manager — controlar el gestor” en la página 362 para conocer la sintaxis del mandato lbcontrol manager start.

Nota: Para Windows 2000, los archivos lbcserver y metricserver están situados en el directorio c:\winnt\system32. Para otras plataformas, estos archivos residen en el directorio /usr/bin.

Resolución de problemas habituales—Dispatcher

Problema: Dispatcher no funcionará

Este problema puede suceder cuando otra aplicación utiliza uno de los puertos utilizado por Dispatcher. Para obtener más información, vaya al apartado “Comprobar los números de puerto de Dispatcher” en la página 227.

Problema: Dispatcher y el servidor no responderán

Este problema se produce cuando se está utilizando una dirección diferente a la especificada. Cuando establezca la ubicación compartida del servidor y Dispatcher, asegúrese de que la dirección de servidor utilizada en la configuración es la dirección NFA o que está configurada como ubicación compartida.

Problema: no se realiza el reparto del tráfico para las peticiones de Dispatcher

Los síntomas de este problema son, entre otros, que las conexiones de las máquinas cliente no sean atendidas o que se agote el tiempo de espera de las mismas. Para efectuar un diagnóstico del problema, compruebe lo siguiente:

1. ¿Ha configurado la dirección de no reenvío, los clusters, los puertos y los servidores para encaminamiento? Revise el archivo de configuración.
2. ¿Está unida la tarjeta de interfaz de red a la dirección de cluster por medio de un alias? Utilice `netstat -ni` para comprobarlo.
3. ¿Tiene el dispositivo de bucle de retorno de cada servidor el alias definido como la dirección de cluster? Utilice `netstat -ni` para comprobarlo.
4. ¿Se ha suprimido la ruta adicional? Utilice `netstat -nr` para comprobarlo.
5. Utilice el mandato **ndcontrol cluster status** para consultar la información referente a los clusters que ha definido. Asegúrese de que tiene definido un puerto para cada cluster.
6. Utilice el mandato **ndcontrol server report** para cerciorarse de que los servidores no están inactivos y de que el peso que tienen establecido no es cero.

Problema: la modalidad de alta disponibilidad de Dispatcher no funciona

Este problema se presenta cuando se configura el entorno de alta disponibilidad de Dispatcher y las conexiones de las máquinas cliente no son atendidas o agotan el tiempo de espera. Para corregir o diagnosticar el problema, compruebe lo siguiente:

- Asegúrese de que ha creado los scripts `goActive`, `goStandby` y `goInOp`, y colóquelos en el directorio `bin` en el que está instalado Dispatcher. Para obtener más información sobre estos scripts, consulte “Utilización de scripts” en la página 170.
- Para **AIX**, **Linux** y **Solaris**, asegúrese de que los scripts `goActive`, `goStandby` y `goInOp` tienen establecido el permiso de ejecución (`execute permission`).
- Para **Windows 2000**, asegúrese de configurar la dirección de no reenvío.

Problema: no se puede añadir pulso (Windows 2000)

Este error de Windows 2000 se produce cuando la dirección de origen no está configurada en un adaptador. Para corregir o diagnosticar el problema, compruebe lo siguiente.

- Para **Windows 2000**, debe configurar la dirección de no reenvío mediante la interfaz de red en anillo o Ethernet y emitir los mandatos siguientes:

```
ndconfig tr0 <dirección_IP> netmask <máscara_red> o bien  
ndcontrol cluster configure
```

Problema: rutas sobrantes (sólo Windows 2000)

Después de configurar las máquinas servidor, puede detectar que ha creado accidentalmente una o más rutas sobrantes. Si no se eliminan, estas rutas sobrantes impedirán que Dispatcher funcione. Para comprobar si existen estas rutas y suprimirlas, consulte “Configuración de las máquinas servidor para el reparto del tráfico” en la página 65.

Problema: los asesores no funcionan correctamente

Si está utilizando el soporte de área amplia y los asesores no parecen funcionar correctamente, asegúrese de que se han arrancado tanto en el Dispatcher local como en el remoto. Consulte “Utilización de asesores remotos con soporte de área amplia” en la página 159.

Problema: SNMPD no se ejecuta correctamente (Windows 2000)

Cuando se utilizan subagentes SNMP, si el daemon SNMP SystemViewAgent no se arranca y se mantiene en marcha, asegúrese de que ha configurado la comunidad SNMP por medio del programa snmpcfg. Para acceder a los datos SNMP desde el subagente de Dispatcher, el nombre de comunidad que se pase en los mandatos SNMP debe corresponder con el nombre de comunidad con el que se arrancó el subagente.

Problema: Dispatcher, Microsoft IIS y SSL no funcionan (Windows 2000)

Al utilizar Dispatcher, Microsoft IIS y SSL, si éstos no funcionan conjuntamente, puede existir un problema para habilitar la seguridad de SSL. Para obtener más información sobre cómo generar un par de claves, adquirir un certificado, instalar un certificado con un par de claves y configurar un directorio para que necesite SSL, consulte la publicación *Microsoft Information and Peer Web Services Information and Planning Guide*, que se suministra con Windows 2000. El URL local del documento, que se visualiza mediante un navegador Web, es
archivo:///C:/WINNT/system32/inetsrv/iisadmin/htmldocs/inetdocs.htm.

Problema: conexión de Dispatcher a una máquina remota

Dispatcher utiliza claves para permitirle conectarse a una máquina remota y configurarla. Las claves especifican un puerto RMI para la conexión. Es posible modificar el puerto RMI debido a conflictos o razones de seguridad. Al modificar los puertos RMI, el nombre de archivo de la clave es diferente. Si tiene más de una clave en su directorio de claves para la misma máquina remota, y éstas especifican diferentes puertos RMI, la línea de mandatos sólo probará el primero que encuentre. Si es el incorrecto, la conexión se rechazará. La conexión no se producirá a menos que suprima la clave incorrecta.

Problema: el mandato ndcontrol o ndadmin da error

1. El mandato ndcontrol devuelve: **Error: El servidor no responde.** O el mandato ndadmin devuelve: **Error: no se puede acceder al servidor RMI.**

Estos errores se pueden producir cuando la máquina tiene una pila con socks. Para corregir el problema, edite el archivo socks.cnf e incluya las líneas siguientes:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

2. Las consolas de administración para interfaces de Network Dispatcher (línea de mandatos, interfaz gráfica de usuario y asistentes) se comunican con ndserver mediante la invocación a método remoto (RMI). La comunicación por omisión utiliza dos puertos; un puerto está definido en el script de inicio de ndserver y el otro es aleatorio.

El puerto aleatorio puede ocasionar problemas cuando una de las consolas de administración se ejecuta en la misma máquina que un cortafuegos o a través de un cortafuegos. Por ejemplo, cuando Network Dispatcher se ejecuta en la misma máquina que un cortafuegos y emite mandatos ndcontrol, puede encontrarse con errores del tipo **Error: El servidor no responde**.

Para evitar este problema, edite el archivo de script ndserver (situado en PATH) para definir el puerto aleatorio que utiliza RMI. Incluya -DND_RMI_SERVER_PORT=*suPuerto* en la serie de caracteres END_ACCESS, donde *suPuerto* es el puerto que especifique.

Por ejemplo:

```
END_ACCESS='-DND_CLIENT_KEYS_DIRECTORY=/usr/lpp/nd/admin/keys/dispatcher
-DND_SERVER_KEYS_DIRECTORY=/usr/lpp/nd/dispatcher/key
-DND_RMI_SERVER_PORT=10100'
ND_RMIPORT=10099
```

Una vez completado, vuelva a iniciar ndserver y abra el tráfico para los puertos 10099 y 10100 o para el puerto elegido para la dirección del sistema principal desde el que se ejecutará la consola de administración.

3. Estos errores también se pueden producir si todavía no ha iniciado ndserver.

Problema: se visualiza el mensaje de error del tipo “No se puede encontrar el archivo...” al intentar visualizar la ayuda en línea (Windows 2000)

En Windows 2000, cuando se utiliza Netscape como navegador por omisión, el mensaje de error que se visualiza con este problema es “No se puede encontrar el archivo ‘<nombre_archivo>.html’ (o uno de sus componentes). Asegure de que la vía de acceso y el nombre de archivo son correctos y que están disponibles todas las bibliotecas necesarias”.

El problema se debe a un valor incorrecto para la asociación de archivo HTML. Para corregir el problema:

1. Pulse **Mi PC** --> **Herramientas**, seleccione **Opciones de carpeta** y pulse la pestaña **Tipos de archivo**
2. Seleccione "Netscape Hypertext Document"
3. Pulse el botón **Avanzado**, seleccione **abrir** y pulse el botón **Editar**
4. Especifique *NSShell* en el campo **Aplicación:** (no en el campo Aplicación utilizada para realizar la acción:) y luego pulse **Aceptar**

Problema: mensaje falso de error al iniciar ndserver en Solaris 2.7

Al iniciar ndserver en las plataformas Solaris 2.7, aparece el siguiente mensaje falso de error: "stty: : No existe tal dispositivo ni dirección". Puede pasar por alto este mensaje de error. Ndserver se ejecutará correctamente.

Problem: la interfaz gráfica de usuario (GUI) no arranca correctamente

La interfaz gráfica de usuario (GUI), que es ndadmin, necesita una cantidad suficiente de espacio de paginación para funcionar correctamente. Si la GUI no dispone de espacio de paginación suficiente, puede que no arranque completamente. Si ocurre esto, compruebe el espacio de paginación y aumentelo si es necesario.

Problema: error al ejecutar Dispatcher cuando Caching Proxy está instalado

Si desinstala Network Dispatcher para reinstalar otra versión y obtiene un error al intentar iniciar el componente Dispatcher, compruebe si Caching Proxy está instalado. Caching Proxy depende de uno de los archivos de Dispatcher; este archivo se desinstala sólo al desinstalar Caching Proxy.

Para evitar este problema:

1. Desinstale Caching Proxy.
2. Desinstale Network Dispatcher.
3. Vuelva a instalar Network Dispatcher y Caching Proxy.

Problema: la interfaz gráfica de usuario (GUI) no se visualiza correctamente

Si la GUI de Network Dispatcher tiene un aspecto anómalo, compruebe el valor del sistema operativo correspondiente a la resolución del escritorio. La mejor visualización de la GUI se consigue para una resolución de 1024x768 pixels.

Problema: en Windows 2000, las ventanas de ayuda algunas veces quedan ocultas detrás de otras ventanas abiertas

Cuando abre por primera vez ventanas de ayuda en Windows 2000, algunas veces quedan ocultas detrás de ventanas existentes. Si ocurre esto, pulse sobre la ventana para devolverla al primer plano.

Problema: Network Dispatcher no puede procesar y reenviar una trama

En Solaris, cada adaptador de red tiene la misma dirección MAC por omisión. Esto es apropiado cuando cada adaptador está en una subred IP diferente; sin embargo, en un entorno conmutado, cuando varios adaptadores de red con la misma dirección MAC y la misma dirección de subred IP se comunican con el mismo conmutador, éste envía todo el tráfico destinado a la dirección MAC (y ambos IP) a través del mismo canal. Sólo el adaptador que envió por última vez una trama por la red detecta los paquetes IP destinados a ambos adaptadores. Solaris puede descartar los paquetes destinados a una dirección IP válida que hayan llegado en la interfaz "equivocada".

Si todas las interfaces de red no están diseñadas para Network Dispatcher tal como está configurado en `ibmnd.conf`, y si el adaptador de red que no está definido en `ibmnd.conf` recibe una trama, Network Dispatcher no puede procesar y reenviar la trama.

Para evitar este problema, debe anular el valor por omisión y establecer una dirección MAC exclusiva para cada interfaz. Utilice este mandato:

```
ifconfig interfaz ether  
macAddr
```

Por ejemplo:

```
ifconfig hme0 ether 01:02:03:04:05:06
```

Problema: aparece una pantalla azul al iniciar el ejecutor de Network Dispatcher

En Windows 2000, antes de iniciar el ejecutor debe instalar y configurar una tarjeta de red.

Problema: la vía de acceso de descubrimiento impide la devolución de tráfico con Network Dispatcher

El sistema operativo AIX contiene un parámetro de red denominado "path MTU discovery". Durante una transacción con un cliente, si el sistema operativo determina que debe utilizar una unidad de transmisión máxima (MTU) más pequeña para los paquetes de salida, el parámetro "path MTU discovery" hace que AIX cree una ruta para recordar esos datos. La nueva ruta es para ese cliente IP específico y registra la MTU necesaria para su acceso.

Mientras se crea la ruta, puede producirse un problema relacionado con los servidores como consecuencia de que el cluster tenga un alias en el bucle de retorno. Si la dirección de pasarela de la ruta es la subred del cluster/máscara de red, AIX crea la ruta en el bucle de retorno. Sucede así porque era la última interfaz unida a esa subred por medio de un alias.

Por ejemplo, si el cluster es 9.37.54.69 y se utiliza la máscara de red 255.255.255.0 y la pasarela que se pretende es 9.37.54.1, AIX utiliza el bucle de retorno para la ruta. Esto provoca que las respuestas del servidor nunca salgan del sistema y se sobrepase el tiempo de espera del cliente. Normalmente, el cliente obtiene una respuesta del cluster, entonces se crea la ruta y el cliente ya no recibe más información.

Existen dos soluciones para este problema.

1. Inhabilite el parámetro "path MTU discovery" para que AIX no añada rutas dinámicamente. Utilice los mandatos siguientes.

no -a lista los valores de red de AIX

no -o opción=valor

establece los parámetros de TCP en AIX

2. Cree un alias para el cluster IP en el bucle de retorno con la máscara de red 255.255.255.255. Esto significa que la subred con alias sólo es el cluster IP. Cuando AIX cree las rutas dinámicas, la pasarela IP de destino no coincidirá con esa subred, lo que dará como resultado que la ruta utilice la interfaz de red correcta. Después, suprima la nueva ruta lo0 que se ha creado durante el paso de la unión por medio del alias. Para ello, busque la ruta en el bucle de retorno con el destino de red del cluster IP y suprima esa ruta. Debe hacer esto cada vez que cree un alias para el cluster.

Notas:

1. El parámetro "path MTU discovery" está inhabilitado por omisión en AIX 4.3.2 y en versiones inferiores; no obstante, a partir de AIX 4.3.3, éste incluido, se habilita por omisión.
2. Los mandatos siguientes desactivan el parámetro "path MTU discovery" y deben ejecutarse en cada arranque del sistema. Añada estos mandatos al archivo /etc/rc.net.
 - -o udp_pmtu_discover=0
 - -o tcp_pmtu_discover=0

Problema: los asesores muestran que todos los servidores están inactivos

Windows 2000 tiene una nueva función denominada Descarga de tareas, que permite calcular la suma de comprobación de TCP mediante la tarjeta adaptadora en lugar del sistema operativo. Esto mejora el rendimiento del sistema. Si se habilita la Descarga de tareas, los asesores de Network Dispatcher informan de que los servidores están inactivos cuando no lo están.

El problema es que la suma de comprobación de TCP no se calcula correctamente para los paquetes que proceden de la dirección de cluster, que es lo que sucede con el tráfico de los asesores.

Para evitar este problema, vaya a los valores de tarjeta adaptadora e inhabilite la Descarga de tareas.

Este problema se observó por primera vez con el adaptador de Adaptec ANA62044 QuadPort. Esta tarjeta adaptadora reconoce la función con el nombre de Descarga de la suma de comprobación de transmisiones. Inhabilite la Descarga de la suma de comprobación de transmisiones para evitar el problema.

Problema: la alta disponibilidad en la modalidad de área amplia de Network Dispatcher no funciona

Cuando configure un Network Dispatcher de área amplia, debe definir el Dispatcher remoto como servidor de un cluster en el Dispatcher local. Normalmente, se utiliza la dirección de no reenvío (NFA) del Dispatcher remoto como dirección de destino del servidor remoto. Si hace esto y luego configura la modalidad de alta disponibilidad en el Dispatcher remoto, el resultado no será satisfactorio. Sucede así porque el Dispatcher local siempre apunta al principal de la parte remota cuando se utiliza su NFA para el acceso.

Para solucionar este problema:

1. Defina un cluster adicional en el Dispatcher remoto. No es necesario definir puertos ni servidores para este cluster.
2. Añada esta dirección de cluster a los scripts goActive y goStandby.
3. En el Dispatcher local, defina esta dirección de cluster como servidor en lugar de la NFA del Dispatcher principal remoto.

Cuando el Dispatcher principal remoto se active, creará un alias para esta dirección en su adaptador, lo que le permitirá aceptar el tráfico. Si se produce una anomalía, la dirección pasa a la máquina de reserva y ésta continúa aceptando el tráfico para esa dirección.

Problema: la GUI se cuelga (o se comporta de forma inesperada) cuando se intenta cargar un archivo de configuración grande

Cuando se intenta cargar un archivo de configuración grande (con unos 200 o más mandatos `add`), puede que la GUI se cuelgue o muestre un comportamiento inesperado, como por ejemplo que responda a cambios en la pantalla a una velocidad extremadamente baja.

Esto se debe a que Java no tiene acceso a suficiente memoria como para manejar un cambio tan grande en la GUI.

Se puede especificar una opción en el entorno de ejecución para aumentar la agrupación de asignación de memoria disponible para Java.

Esta opción es `-Xmxn`, donde `n` es el tamaño máximo, en bytes, para la agrupación de asignación de memoria. `n` debe ser múltiplo de 1024 y debe ser mayor que 2 MB. El valor `n` puede ir seguido de `k` o `K` para indicar kilobytes, o de `m` o `M` para indicar megabytes. Por ejemplo, `-Xmx128M` y `-Xmx81920k` son valores válidos. El valor por omisión es 64MB. Las plataformas SPARC de Solaris 7 y Solaris 8 tienen un valor máximo de 4000m; las plataformas Solaris 2.6 y x86 tienen un valor máximo de 2000m.

Para añadir esta opción, modifique el script `ndadmin` del siguiente modo:

- **Windows NT o 2000**

```
START jrew -mx64m %END_ACCESS% %CONFIG_DIR%  
-DEND_INSTALL_PATH=%IBMNDPATH% -cp %NDCLASSPATH%  
com.ibm.internet.nd.framework.FWK_Framework  
com.ibm.internet.nd.gui.GUI_eNDRootNode1
```

- **Solaris**

```
$JREDIR/$JRE -mx64m $END_ACCESS $CONFIG_DIR  
-DEND_INSTALL_PATH=/opt/&BASEDIR -cp $NDCLASSPATH  
com.ibm.internet.nd.framework.FWK_Framework  
com.ibm.internet.nd.gui.GUI_eNDRootNode &1
```

- **Linux**

```
re -mx64m $END_ACCESS $CONFIG_DIR $NDLOCALE  
-DEND_INSTALL_PATH=/opt/nd -classpath $NDCLASSPATH  
com.ibm.internet.nd.framework.FWK_Framework  
com.ibm.internet.nd.gui.GUI_eNDRootNode 1>/dev/null 2>&1 &1
```

- **AIX**

```
ava -mx64m $END_ACCESS $CONFIG_DIR $NDLOCALE  
-DEND_INSTALL_PATH=/usr/lpp/&BASEDIR -classpath $NDCLASSPATH  
com.ibm.internet.nd.framework.FWK_Framework  
com.ibm.internet.nd.gui.GUI_eNDRootNode 1>/dev/null 2>&1 &
```

No hay ningún valor recomendado para `n`, pero debe ser mayor que la opción por omisión. Un buen punto de partido es el doble que el valor por omisión.

Resolución de problemas habituales—CBR

Problema: CBR no funcionará

Este problema puede suceder cuando otra aplicación utiliza uno de los puertos utilizados por CBR. Para obtener más información, vaya al apartado “Comprobación de los números de puerto de CBR” en la página 228.

Problema: el mandato `cbrcontrol` o `ndadmin` falla

El mandato `cbrcontrol` devuelve: “Error: El servidor no responde”. O bien el mandato `ndadmin` devuelve: “Error: no se puede acceder al servidor RMI”. Estos errores se pueden producir cuando la máquina tiene una pila con socks. Para corregir el problema, edite el archivo `socks.cnf` e incluya las líneas siguientes:


```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Estos errores también se pueden producir si todavía no ha iniciado **cbrserver**.

Problema: no se realiza el reparto del tráfico para las peticiones

Caching Proxy y CBR se han iniciado, pero no se realiza el reparto del tráfico para las peticiones. Puede producirse este error si se inicia Caching Proxy antes de iniciar el ejecutor. Si es así, el archivo de anotaciones stderr de Caching Proxy contendrá el siguiente mensaje de error: "ndServerInit: No se ha podido conectar con el ejecutor". Para evitar este problema, inicie el ejecutor antes de iniciar Caching Proxy.

Problema: en Solaris, el mandato cbrcontrol executor start falla

En Solaris, el mandato **cbrcontrol executor start** devuelve: "Error: No se ha iniciado el ejecutor". Este error se produce si no configura IPC (Inter-process Communication) para el sistema de manera que el tamaño máximo de un segmento de memoria compartida y los ID de semáforo superen el valor por omisión del sistema operativo. Para aumentar el tamaño del segmento de memoria compartida y los ID de semáforo, debe editar el archivo **/etc/system**. Para obtener más información sobre cómo configurar este archivo, consulte 86.

Problema: error sintáctico o de configuración

Si la norma de URL no funciona, puede deberse a un error sintáctico o de configuración. Para corregir este problema, compruebe lo siguiente:

- Verifique si la norma está correctamente configurada. Consulte el apartado "Apéndice C. Sintaxis de la norma de contenido (patrón):" en la página 313 para obtener más detalles.
- Emita un mandato **cbrcontrol rule report** para esta norma y compruebe la columna 'Veces disparada' para ver si ha aumentado según el número de peticiones efectuadas. Si ha aumentado correctamente, vuelva a comprobar la configuración del servidor.
- Si la norma no se dispara, añada una norma 'siempre cierta'. Emita un mandato **cbrcontrol rule report** en la norma 'siempre cierta' para verificar si se está disparando.

Resolución de problemas habituales—Mailbox Locator

Problema: Mailbox Locator no funcionará

Este problema puede suceder cuando otra aplicación utiliza uno de los puertos utilizados por Mailbox Locator. Para obtener más información, consulte "Comprobación de los números de puerto de Mailbox Locator" en la página 228.

Problema: el mandato mlserver está detenido

En una plataforma UNIX, este problema se produce cuando se utiliza **mlserver** para repartir un gran número de peticiones de clientes IMAP/POP3 y el límite del sistema para los descriptores de archivo es demasiado pequeño para el número de peticiones que mlserver intenta atender. Mlserver produce la excepción siguiente y luego se detiene:

```
java.rmi.RMISecurityException: security.fd.read
```

El archivo de anotaciones de proxy específico del protocolo informa:

```
SocketException=java.net.SocketException: Socket closed
```

La solución consiste en modificar el límite **nofiles** (AIX, Linux) o modificar el límite **open files** (Solaris) en el shell donde se ha iniciado mlserver. Aumente el valor de nofiles a un valor razonable mayor. Utilice `ulimit -a` para visualizar el valor de nofiles actual y utilice `ulimit -n valor` para aumentar el valor.

Problema: el mandato mlcontrol o ndadmin falla

El mandato mlcontrol devuelve: “Error: El servidor no responde”. O bien el mandato ndadmin devuelve: “Error: no se puede acceder al servidor RMI”. Estos errores se pueden producir cuando la máquina tiene una pila con socks. Para corregir el problema, edite el archivo socks.cnf e incluya las líneas siguientes:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Estos errores también se pueden producir si todavía no ha iniciado **mlserver**.

Problema: no se puede añadir un puerto

Cuando intente añadir un puerto a una configuración, puede recibir este mensaje de error: **Error: No se puede añadir el puerto**. Es posible que otra aplicación ya esté a la escucha en ese puerto. Mailbox Locator intenta iniciar un proxy que se vincula con el cluster IP en el puerto especificado en el mandato. Si otra aplicación se está vinculando con ese IP o está escuchando a todos los IP en ese puerto, el arranque del proxy falla. Para utilizar Mailbox Locator en ese puerto, deberá detener la aplicación que provoca el conflicto.

Tenga en cuenta que, en la plataforma Linux, el daemon xinetd puede iniciar un oyente sin que se ejecute, como, por ejemplo, un programa POP3. Por lo tanto, es importante comprobar **netstat -a** para determinar si alguna aplicación está a la escucha en el puerto deseado.

Problema: se recibe un error de proxy al intentar añadir un puerto

Para Mailbox Locator, el mandato **mlcontrol port add** produce el mensaje de error siguiente: "El proxy del cluster <cluster> , puerto <puerto> no se inició." La solución consiste en configurar la dirección del cluster en una NIC antes de iniciar el proxy. Compruebe también que no haya ninguna otra aplicación activa en ese puerto que esté a la escucha de la dirección del cluster (incluidas las aplicaciones de escucha genérica).

Resolución de problemas habituales—Site Selector

Problema: Site Selector no funcionará

Este problema puede suceder cuando otra aplicación utiliza uno de los puertos utilizados por Site Selector. Para obtener más información, consulte "Comprobación de los números de puerto de Site Selector" en la página 229.

Problema: Site Selector no efectúa un reparto rotatorio para el tráfico procedente de clientes Solaris

Síntoma: el componente Site Selector no efectúa el reparto rotatorio del tráfico para las peticiones entrantes procedentes de los clientes Solaris.

Causa posible: los sistemas Solaris ejecutan una daemon de servicio de nombres en antememoria. Si este daemon está en ejecución, la petición subsiguiente de resolución de direcciones se responderá desde esta antememoria, en lugar de consultar a Site Selector.

Solución: Desactive el daemon del servicio de nombres en antememoria para la máquina Solaris.

Problema: el mandato sscontrol o ndadmin falla

El mandato **sscontrol** devuelve: "Error: El servidor no responde". O bien el mandato **ndadmin** devuelve: "Error: no se puede acceder al servidor RMI". Estos errores se pueden producir cuando la máquina tiene una pila con socks. Para corregir el problema, edite el archivo **socks.cnf** e incluya las líneas siguientes:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Estos errores también se pueden producir si todavía no ha iniciado **ssserver**.

Problema: ssserver no se inicia en Windows 2000

Site Selector debe poder participar en un DNS. Todas las máquinas que intervienen en la configuración deben participar también en este sistema. Windows no siempre necesita que el nombre del sistema principal

configurado esté en el DNS. Site Selector necesita que su nombre de sistema principal esté definido en el DNS para que se inicie correctamente.

Compruebe que este sistema principal esté definido en el DNS. Edite el archivo `ssserver.cmd` y elimine la "w" de "javaw". Esto debería ocasionar más errores.

Problema: Site Selector no reparte el tráfico correctamente si hay rutas duplicadas

El servidor de nombres de Site Selector no establece ninguna asociación con ninguna dirección de la máquina. El servidor responderá a las peticiones destinadas a cualquier IP válido de la máquina. Site Selector depende del sistema operativo para encaminar la respuesta hacia el cliente. Si la máquina de Site Selector tiene varios adaptadores de red y varios de ellos están conectados a la misma subred, puede que el sistema operativo envíe la respuesta a un cliente que tiene una dirección diferente a la dirección desde donde se recibió la petición. Algunas aplicaciones de cliente no aceptan una respuesta recibida desde una dirección diferente a aquélla desde donde se envió. Como consecuencia, la resolución de nombres fallará.

Resolución de problemas habituales — Consultant para Cisco CSS Switches

Problema: lbcserver no arranca

Este problema puede suceder cuando otra aplicación utiliza uno de los puertos utilizado por el archivo `lbcserver` de Consultant. Para obtener más información, consulte "Comprobación de los números de puerto de Cisco Consultant" en la página 230.

Problema: el mandato lbcontrol o ndadmin falla

El mandato `lbcontrol` devuelve: "Error: El servidor no responde". O bien el mandato `ndadmin` devuelve: "Error: no se puede acceder al servidor RMI". Estos errores se pueden producir cuando la máquina tiene una pila con socks. Para corregir el problema, edite el archivo `socks.cnf` e incluya las líneas siguientes:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Estos errores también se pueden producir si todavía no ha iniciado `lbcserver`.

Problema: No se puede crear el registro para el puerto 14099

Este problema se puede producir si falta una licencia válida de producto. Cuando intenta iniciar `lbcserver`, recibe este mensaje:

Su licencia ha caducado. Consulte al representante local de IBM o al distribuidor autorizado de IBM.

Para corregir este problema:

1. Si ya intentado iniciar **lbcserver**, escriba **lbcserver stop**.
2. Copie su licencia válida en el directorio **...nd/servers/conf**.
3. Escriba **lbcserver** para iniciar el servidor.

Resolución de problemas habituales—Metric Server

Problema: excepción de E/S de Metric Server en Windows 2000 al ejecutar los archivos de métrica del usuario **.bat** o **.cmd**

Debe utilizar el nombre de métrica completo para la métrica escrita por el usuario en los Metric Servers de Windows 2000. Por ejemplo, debe especificar **usermetric.bat** en lugar de **usermetric**. El nombre **usermetric** es válido en la línea de mandatos, pero no funciona cuando se ejecuta desde el entorno de unidad ejecutable. Si no utiliza el nombre de métrica completo, recibirá una excepción de E/S (IOException) de Metric Server. Establezca la variable **LOG_LEVEL** en el valor 3 en el archivo de mandatos **metricserver** y luego compruebe la salida del archivo de anotaciones. En este ejemplo, la excepción aparece así:

```
... java.io.IOException: CreateProcess: usermetric error=2
```

Problema: Metric Server no notifica cargas a la máquina **Network Dispatcher**

Puede haber varias razones por las que Metric Server no notifique información sobre cargas a Network Dispatcher. Para determinar la causa, realice las siguientes comprobaciones:

- Asegúrese de que los archivos de claves se han transferido a Metric Server.
- Compruebe que el nombre del sistema principal de la máquina Metric Server está registrada con el servidor de nombres local.
- Vuelva a iniciar con un nivel de anotaciones superiores y mire si hay errores.
- En la máquina Network Dispatcher, aumente el nivel de anotaciones del gestor. Mire si hay errores en las anotaciones de Metric Monitor.

Problema: las anotaciones de Metric Server indican que "se necesita una firma para poder acceder al agente"

Las anotaciones de Metric Server notifican este mensaje de error después de que los archivos de claves se hayan transferido al servidor.

Este error queda anotado cuando el archivo de claves no consigue autorización con la clave emparejada debido a que el par está dañado. Para corregir este problema intente lo siguiente:

- Vuelva a emitir FTP para el archivo de claves utilizando el método de transferencia binaria.
- Cree una nueva clave y distribúyala.

Apéndice A. Cómo leer un diagrama de sintaxis

El diagrama de sintaxis muestra cómo especificar un mandato de forma que el sistema operativo pueda interpretar correctamente lo que se teclea. El diagrama de sintaxis se lee de izquierda a derecha y de arriba a abajo, siguiendo la línea horizontal (línea principal).

Símbolos y puntuación

En los diagramas de sintaxis se utilizan los símbolos siguientes:

Símbolo

Descripción

- ▶▶ Marca el principio de la sintaxis del mandato.
- ◀◀ Marca el final de la sintaxis del mandato.

Deben incluirse todos los signos de puntuación, como por ejemplo dos puntos, comillas y signos menos que aparecen en el diagrama de sintaxis.

Parámetros

En los diagramas de sintaxis se utilizan los siguientes tipos de parámetros.

Parámetro

Descripción

Obligatorio

Los parámetros obligatorios se visualizan en la línea principal.

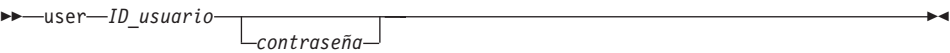
Opcional

Los parámetros opcionales se visualizan debajo de la línea principal.

Los parámetros se clasifican como palabras clave o variables. Las palabras clave se visualizan en letras minúsculas y pueden especificarse en letras minúsculas. Por ejemplo, un nombre de mandato es una palabra clave. Las variables aparecen en cursiva y representan nombres o valores suministrados por el usuario.

Ejemplos de sintaxis

En el ejemplo siguiente, el mandato `user` es una palabra clave. La variable obligatoria es `ID_usuario` y la variable opcional es `contraseña`. Sustituya las variables por los valores que desee.

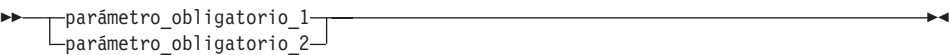


Palabras clave obligatorias: Las palabras clave y las variables obligatorias aparecen en la línea principal.

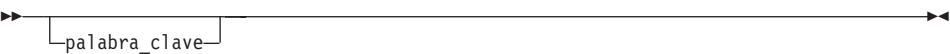


Debe codificar las palabras clave y los valores obligatorios.

Elija un elemento obligatorio de una lista: Si puede elegirse más de una palabra clave o variable obligatoria mutuamente excluyente, se clasifican verticalmente en orden alfanumérico.

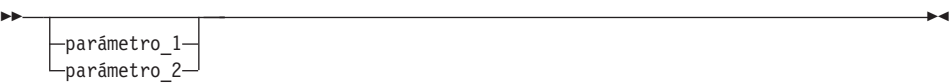


Valores opcionales: Las palabras clave y variables opcionales aparecen debajo de la línea principal.



Puede elegir no codificar las palabras clave y variables opcionales.

Elija una palabra clave opcional de una lista: Si puede elegirse más de una palabra clave o variable opcional mutuamente excluyente, se clasifican verticalmente en orden alfanumérico debajo de la línea principal.



Variables: Una palabra en cursiva es una *variable*. Cuando vea una variable en la sintaxis, debe sustituirla por uno de los nombres o valores permitidos, tal como se define en el texto.

►►—*variable*—◄◄

Caracteres no alfanuméricos: Si un diagrama muestra un carácter que no es alfanumérico (como por ejemplo dos puntos, comillas o signos menos), debe codificar el carácter como parte de la sintaxis. En este ejemplo, debe codificar *cluster:puerto*.

►►—*cluster:puerto*—◄◄

Apéndice B. Consulta de mandatos para Dispatcher, CBR y Mailbox Locator

Este apéndice describe cómo utilizar los mandatos **ndcontrol** de Dispatcher. También es una guía de consulta para los mandatos de CBR y Mailbox Locator. CBR y Mailbox Locator utilizan un subconjunto de los mandatos de Dispatcher. En “Diferencias de configuración entre CBR, Mailbox Locator y Dispatcher” en la página 250 hallará más información.

Nota: Tenga en cuenta lo siguiente al utilizar los diagramas de sintaxis de este apéndice:

- Para CBR, utilice **cbrcontrol** en lugar de **ndcontrol**
- Para Mailbox Locator, utilice **mlcontrol** en lugar de **ndcontrol**

A continuación sigue una lista de los mandatos descritos en este apéndice:

- “**ndcontrol advisor** — controlar el asesor” en la página 252
- “**ndcontrol cluster** — configurar clusters” en la página 258
- “**ndcontrol executor** — controlar el ejecutor” en la página 263
- “**ndcontrol file**— gestionar archivos de configuración” en la página 268
- “**ndcontrol help** — visualizar o imprimir ayuda para este mandato” en la página 270
- “**ndcontrol highavailability** — controlar la alta disponibilidad” en la página 272
- “**ndcontrol host** — configurar una máquina remota” en la página 277
- “**ndcontrol log** — controlar el archivo de anotaciones en binario” en la página 278
- “**ndcontrol manager** — controlar el gestor” en la página 279
- “**ndcontrol metric** — configurar métricas del sistema” en la página 285
- “**ndcontrol port** — configurar puertos” en la página 287
- “**ndcontrol rule** — configurar normas” en la página 294
- “**ndcontrol server** — configurar servidores” en la página 302
- “**ndcontrol set** — configurar anotaciones de servidor” en la página 308
- “**ndcontrol status** — visualizar si el gestor y los asesores están en funcionamiento” en la página 309
- “**ndcontrol subagent** — configurar subagente SNMP” en la página 310

Puede especificar una versión abreviada de los parámetros de los mandatos **ndcontrol**. Sólo necesita especificar las letras exclusivas de los parámetros. Por

ejemplo, para obtener ayuda sobre el mandato "file save", puede entrar **ndcontrol he f** en lugar de **ndcontrol help file**.

Para iniciar la interfaz de línea de mandatos, emita **ndcontrol** para visualizar un indicador de mandatos de ndcontrol.

Para cerrar la interfaz de línea de mandatos, emita **exit** o **quit**.

Nota: Los valores de los parámetros de mandatos se deben escribir en caracteres ingleses. Las únicas excepciones son los nombres de sistema principal (utilizados en los mandatos para clusters y servidores y en la modalidad de alta disponibilidad) y los nombres de archivo (utilizados en los mandatos sobre archivos).

Diferencias de configuración entre CBR, Mailbox Locator y Dispatcher

La interfaz de línea de mandatos de CBR y Mailbox Locator es en su mayor parte un subconjunto de la interfaz de línea de mandatos de Dispatcher. Para configurar el componente, utilice el mandato **cbrcontrol** (para el componente CBR) o utilice el mandato **mlcontrol** (para el componente Mailbox Locator) en lugar de ndcontrol.

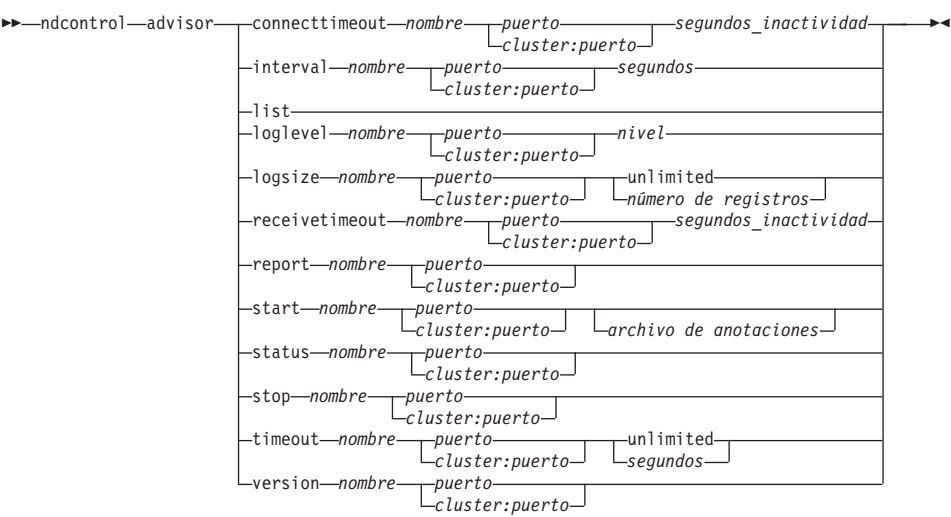
Estos son algunos de los mandatos que están *omitidos* en CBR:

1. highavailability
2. subagent
3. executor
 - report
 - set nfa <valor>
 - set fincount <valor>
 - set fintimeout <valor>
 - set porttype <valor>
4. cluster
 - report {c}
 - set {c} porttype
5. port add {c:p} porttype
6. port set {c:p} porttype
7. rule add {c:p:r} type port
8. server add {c:p:s} router
9. server set {c:p:s} router

Estos son algunos de los mandatos que están *omitidos* en Mailbox Locator:

1. highavailability
2. rule
3. subagent
4. executor
 - start
 - stop
 - report
 - set nfa <valor>
 - set fincount <valor>
 - set fintimeout <valor>
 - set porttype <valor>
5. cluster
 - report {c}
 - set {c} porttype
6. port [add | set] {c:p} porttype
7. server [add | set] {c:p:s} router

ndcontrol advisor — controlar el asesor



connecttimeout

Establece el tiempo durante el cual un asesor espera antes de notificar un error de conexión con un servidor. Para obtener más información, consulte “Tiempo de espera de conexión y de recepción del asesor para servidores” en la página 142.

nombre

Nombre del asesor. Los valores posibles son **connect**, **db2**, **dns**, **ftp**, **http**, **ibmproxy (Caching Proxy)**, **imap**, **nntp**, **ping**, **pop3**, **self**, **smtp**, **ssl**, **ssl2http**, **telnet** y **wlm**.

Los nombres de los asesores personalizados se encuentran en el formato xxxx, donde ADV_xxxx es el nombre de la clase que implementa el asesor personalizado. En “Creación de asesores personalizados (personalizables)” en la página 145 hallará más información.

puerto

Número del puerto que el asesor está supervisando.

cluster:puerto

El valor de cluster es opcional en los mandatos de asesor, pero el valor de puerto es necesario. Si no se especifica el valor de cluster, el asesor comienza a ejecutarse en el puerto para todos los clusters. Si especifica un cluster, el asesor comienza a ejecutarse en el puerto, pero sólo para el cluster especificado. En “Inicio y detención de un asesor” en la página 140 hallará más información.

El cluster es la dirección en formato decimal con puntos o un nombre simbólico. El puerto es el número del puerto que el asesor está supervisando.

segundos_inactividad

Es un valor entero positivo que representa el tiempo, en segundos, que un asesor espera antes de notificar un error de conexión con un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

interval

Establece la frecuencia con la que el asesor solicitará información a los servidores.

segundos

Es un número entero positivo que representa el número de segundos transcurridos entre las peticiones hechas a los servidores acerca de su estado actual. El valor por omisión es 7.

list

Muestra una lista de los asesores que están actualmente suministrando información al gestor.

loglevel

Establece el nivel de anotaciones del archivo de anotaciones de un asesor.

nivel

Número del nivel (0 a 5). El valor por omisión es 1. Cuanto mayor es el número, más información se escribe en el archivo de anotaciones del asesor. Los valores posibles son: 0 para None, 1 para Minimal, 2 para Basic, 3 para Moderate, 4 para Advanced, 5 para Verbose.

logsize

Establece el tamaño máximo del archivo de anotaciones de un asesor. Si establece el tamaño máximo para el archivo de anotaciones, el archivo se sobregrebará cuando esté lleno. Cuando el archivo alcance el tamaño especificado, las entradas subsiguientes se grabarán a partir del comienzo del archivo, sobre las entradas de anotaciones anteriores. El tamaño del archivo de anotaciones no puede ser menor que el tamaño actual del archivo. Las entradas del archivo de anotaciones contienen una indicación horaria para poder determinar el orden en el que se escribieron. Cuanto más alto sea el nivel de las anotaciones, más cuidadosamente debe elegirse el tamaño de las mismas, ya que puede quedarse rápidamente sin espacio si efectúa anotaciones a los niveles más altos.

número de registros

El tamaño máximo en bytes del archivo de anotaciones del asesor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Puede que el archivo de anotaciones no alcance el tamaño máximo exacto

antes de sobrescribirse, ya que las propias entradas de anotaciones varían en tamaño. El valor por omisión es 1 MB.

receivetimeout

Establece el tiempo durante el cual un asesor espera antes de notificar un error de recepción con un servidor. Para obtener más información, consulte “Tiempo de espera de conexión y de recepción del asesor para servidores” en la página 142.

segundos_inactividad

Es un valor entero positivo que representa el tiempo, en segundos, que un asesor espera antes de notificar un error de recepción con un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

report

Muestra un informe sobre el estado del asesor.

start

Arranca el asesor. Hay asesores para cada protocolo. Los puertos por omisión son los siguientes:

Nombre de asesor	Protocolo	Puerto
connect	ICMP	12345
db2	privado	50000
dns	DNS	53
ftp	FTP	21
http	HTTP	80
ibmproxy	HTTP (a través de Caching Proxy)	80
imap	IMAP	143
nnntp	NNTP	119
ping	PING	0
pop3	POP3	110
self	privado	12345
smtp	SMTP	25
ssl	HTTP	443
ssl2http	SSL	443
telnet	Telnet	23
WLM	privado	10.007

Nota: El asesor FTP sólo debe asesorar en el puerto de control FTP (21). No inicie un asesor FTP en el puerto de datos FTP (20).

archivo de anotaciones

Nombre de archivo en el que se anotan los datos de gestión. Cada registro del archivo de anotaciones contendrá una indicación horaria.

El archivo por omisión es *nombreasesor_puerto.log*, por ejemplo, **http_80.log**. Para cambiar el directorio en el que se conservarán los archivos de anotaciones, consulte la sección “Cambio de la vía de acceso de los archivos de anotaciones” en la página 208. Los archivos de anotaciones por omisión para asesores específicos del cluster (o sitio Web) se crean con la dirección de cluster, por ejemplo, **http_127.40.50.1_80.log**.

status

Muestra el estado actual de todos los valores de un asesor que pueden establecerse globalmente y sus valores por omisión.

stop

Detiene el asesor.

tiempo de espera

Establece el número de segundos durante los que el gestor considerará como válida la información del asesor. Si el gestor averigua que la información del asesor es anterior a este período de tiempo de espera, el gestor no utilizará dicha información para determinar los pesos de los servidores en el puerto que el asesor está supervisando. Una excepción a este tiempo de espera se produce cuando el asesor ha informado al gestor de que un servidor específico está fuera de servicio. El gestor utilizará esa información referente al servidor incluso después de que la información del asesor haya agotado el tiempo de espera.

segundos

Número positivo que representa el número de segundos o la palabra **unlimited**. El valor por omisión es “unlimited”.

version

Muestra la versión actual del asesor.

Ejemplos

- Para iniciar el asesor http en el puerto 80 para el cluster 127.40.50.1:
ndcontrol advisor start http 127.40.50.1:80
- Para iniciar el asesor http en el puerto 88 para todos los clusters:
ndcontrol advisor start http 88
- Para detener el asesor http en el puerto 80 para el cluster 127.40.50.1:
ndcontrol advisor stop http 127.40.50.1:80
- Para establecer el tiempo (30 segundos) que un asesor HTTP del puerto 80 espera antes de notificar un error de conexión con un servidor:

```
ndcontrol advisor connecttimeout http 80 30
```

- Para establecer el tiempo (20 segundos) que un asesor HTTP del puerto 80 del cluster 127.40.50.1 espera antes de notificar un error de conexión con un servidor:

```
ndcontrol advisor connecttimeout http 127.40.50.1:80 20
```

- Para establecer el intervalo del asesor FTP (para el puerto 21) en 6 segundos:

```
ndcontrol advisor interval ftp 21 6
```

- Para visualizar la lista de asesores que actualmente suministran información al gestor:

```
ndcontrol advisor list
```

Este mandato produce una salida similar a la siguiente:

ADVISOR	CLUSTER:PORT	TIMEOUT
http	127.40.50.1:80	unlimited
ftp	21	unlimited

- Para cambiar el nivel de las anotaciones del asesor por 0 para mejorar el rendimiento:

```
ndcontrol advisor loglevel http 80 0
```

- Para cambiar a 5000 bytes el tamaño del archivo de anotaciones del asesor ftp para el puerto 21:

```
ndcontrol advisor logsize ftp 21 5000
```

- Para establecer el tiempo (60 segundos) que un asesor HTTP (del puerto 80) espera antes de notificar un error de recepción con un servidor:

```
ndcontrol advisor receivetimeout http 80 60
```

- Para visualizar un informe de estado del asesor ftp (para el puerto 21):

```
ndcontrol advisor report ftp 21
```

Este mandato produce una salida similar a la siguiente:

Advisor Report:

Advisor name Ftp

Port number 21

Cluster address 9.67.131.18

Server address 9.67.129.230

Load 8

Cluster address 9.67.131.18

Server address 9.67.131.215

Load -1

- Para visualizar el estado actual de los valores asociados al asesor http para el puerto 80:

```
ndcontrol advisor status http 80
```

Este mandato produce una salida similar a la siguiente:

```
Advisor Status:
```

```
-----
```

```
Interval (seconds) ..... 7
Timeout (seconds) ..... Unlimited
Connect timeout (seconds).....21
Receive timeout (seconds).....21
Advisor log filename ..... Http_80.log
Log level ..... 1
Maximum log size (bytes) ..... Unlimited
```

- Para establecer el tiempo de caducidad de la información del asesor en 5 segundos para el puerto 21:

```
ndcontrol advisor timeout ftp 21 5
```

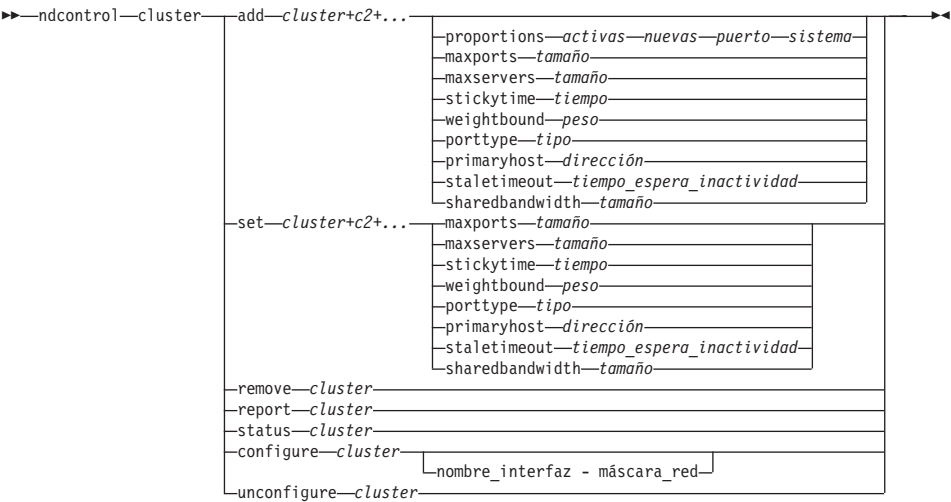
- Para averiguar el número de la versión actual del asesor ssl para el puerto 443:

```
ndcontrol advisor version ssl 443
```

Este mandato produce una salida similar a la siguiente:

```
Version: 04.00.00.00 - 07/12/2001-10:09:56-EDT
```

ndcontrol cluster — configurar clusters



add

Añade este cluster. Debe definir como mínimo un cluster.

cluster

La dirección del cluster expresada como nombre simbólico o en formato decimal con puntos. Puede utilizar la dirección de cluster 0.0.0.0 para especificar un cluster comodín. En “Utilizar el cluster comodín para combinar configuraciones de servidores” en la página 185 hallará más información.

Puede utilizar un signo de dos puntos (:) como comodín, con excepción del mandato `ndcontrol cluster add`. Por ejemplo, el mandato `ndcontrol cluster set : weightbound 80` definirá un peso máximo de 80 para todos los clusters.

Nota: Los clusters adicionales se separan mediante un signo más (+).

proportions

A nivel de cluster, establezca la proporción de importancia para las conexiones activas (*activas*), las conexiones nuevas (*nuevas*), información procedente de asesores (*puerto*), e información procedente de un programa de supervisión del sistema, tal como Metric Server (*sistema*) que son utilizados por el gestor para definir los pesos de los servidores. Cada uno de estos valores, descrito más abajo, se expresa como un porcentaje sobre el total y, por lo tanto, deben sumar siempre 100. Para obtener más información, consulte “Grado de importancia dado a la información de estado” en la página 135.

activas

Un número de 0 a 100 que representa la proporción de peso que debe otorgarse a las conexiones activas. El valor por omisión es 50.

nuevas

Un número de 0 a 100 que representa la proporción de peso que debe otorgarse a las conexiones nuevas. El valor por omisión es 50.

puerto

Un número de 0 a 100 que representa la proporción de peso que debe otorgarse a la información de los asesores. El valor por omisión es 0.

Nota: Cuando se inicia un asesor y si la proporción de puerto es 0, Network Dispatcher establece automáticamente ese valor en 1 para que el gestor utilice la información del asesor para calcular el peso de los servidores.

sistema

Un número del 0 al 100 que representa la proporción de peso que debe otorgarse a la información de métricas del sistema, tal como la procedente de Metric Server. El valor por omisión es 0.

maxports

El número máximo de puertos. El valor de maxports por omisión es 8.

tamaño

El número de puertos permitidos.

maxservers

El número máximo por omisión de servidores por puerto. Este valor puede alterarse temporalmente para puertos individuales por medio de **port maxservers**. El valor por omisión de maxservers es 32.

tamaño

El número de servidores permitidos en un puerto.

stickytime

El valor por omisión de tiempo de persistencia para que se creen los puertos. Este valor puede alterarse temporalmente para puertos individuales por medio de **port stickytime**. El valor por omisión de stickytime es 0.

Nota: Para el método de reenvío cbr de Dispatcher, si el valor de stickytime para los puertos que se van a crear es distinto de cero y se añade un puerto nuevo, la afinidad de ID de SSL estará habilitada para el puerto. Para inhabilitar la afinidad de ID de SSL en el puerto, tendrá que establecer de forma explícita 0 como valor de stickytime del puerto.

tiempo

El valor del tiempo de persistencia (stickytime) expresado en segundos.

weightbound

El peso máximo por omisión del puerto. Este valor puede alterarse temporalmente para puertos individuales por medio de **port weightbound**. El valor por omisión de weightbound es 20.

peso

El valor de weightbound.

porttype

El tipo de puerto por omisión. Este valor puede alterarse temporalmente para puertos individuales por medio de **port porttype**.

Nota: El parámetro porttype es aplicable a Dispatcher.

tipo

Los valores posibles son **tcp**, **udp** y **both**.

primaryhost

Dirección de no reenvío de esta máquina Dispatcher o dirección de no reenvío de la máquina Dispatcher de reserva. En una configuración de alta disponibilidad mutua, un cluster está asociado a una máquina principal o de reserva.

Si se modifica el sistema principal primario de un cluster cuando las máquinas principal y de reserva ya se han iniciado y están ejecutándose con alta disponibilidad mutua, deberá forzar también el nuevo sistema principal primario para que asuma el control. También deberá actualizar los scripts, así como anular la configuración y volver a configurar manualmente el cluster de forma correcta. En “Alta disponibilidad mutua” en la página 48 hallará más información.

dirección

El valor de dirección del sistema principal primario. El valor por omisión es la dirección de no reenvío (NFA) de esta máquina.

staletimeout

El número de segundos durante los cuales puede haber ausencia de actividad en una conexión antes de que dicha conexión se elimine. El valor por omisión para FTP es 900; el valor por omisión para Telnet es 32.000.000. El valor por omisión para todos los demás protocolos es 300. Este valor puede modificarse para puertos individuales por medio de **port staletimeout**. En “Utilización del valor de tiempo de espera de inactividad” en la página 209 hallará más información.

Nota: Para Mailbox Locator, el valor de staletimeout corresponde al temporizador de desconexión automática por inactividad de estos protocolos. Para Mailbox Locator, el valor por omisión de

staletimeout es 60 segundos, el cual prevalece sobre los tiempos de inactividad definidos para POP3 e IMAP. Para obtener más información sobre staletimeout para Mailbox Locator, consulte la sección “Alteración del temporizador de inactividad de POP3/IMAP” en la página 97.

tiempo_espera_inactividad

El valor del tiempo de espera de inactividad.

sharedbandwidth

Es el ancho de banda máximo (kilobytes por segundo) que se puede compartir a nivel de cluster. Para obtener más información sobre el ancho de banda compartido, consulte “Utilización de normas basadas en el ancho de banda reservado y en el ancho de banda compartido” en la página 177 y “Norma del ancho de banda compartido” en la página 179.

Nota: El ancho de banda compartido no es aplicable a CBR ni a Mailbox Locator.

tamaño

Es el tamaño de **sharedbandwidth**, que es un valor entero. El valor por omisión es 0. Si el valor es 0, no se puede compartir el ancho de banda a nivel de cluster.

set

Establece las propiedades del cluster.

remove

Se elimina este cluster.

report

Muestra los campos internos del cluster.

Nota: El parámetro report no es aplicable a CBR ni a Mailbox Locator.

status

Muestra el estado actual de un cluster específico.

configure

Configura un alias de cluster para la tarjeta de interfaz de la red.

Nota: El parámetro configure no es aplicable a CBR ni a Mailbox Locator.

nombre_interfaz máscara_red

Es un parámetro obligatorio si es un alias diferente del que Dispatcher encuentra en primer lugar.

unconfigure

Suprime el alias de cluster de la tarjeta de interfaz de la red.

Nota: El parámetro `unconfigure` no es aplicable a CBR ni a Mailbox Locator.

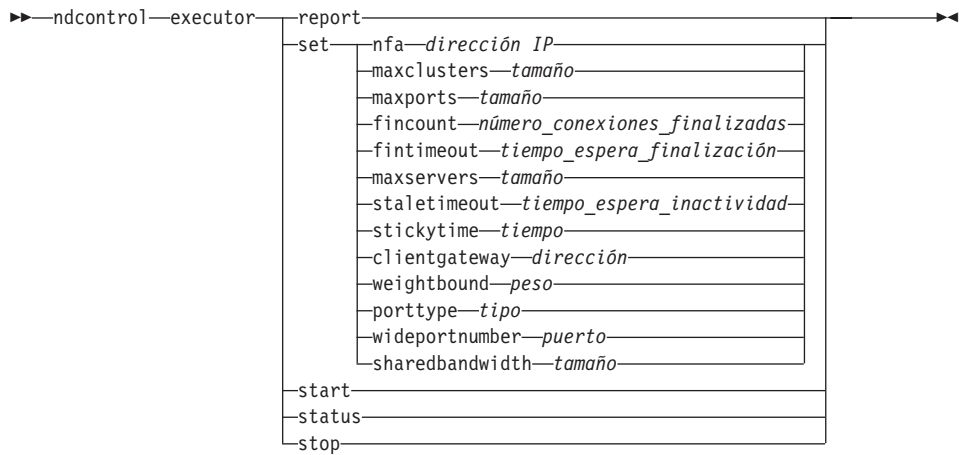
Ejemplos

- Para añadir la dirección de cluster 130.40.52.153:
`ndcontrol cluster add 130.40.52.153`
- Para eliminar la dirección de cluster 130.40.52.153:
`ndcontrol cluster remove 130.40.52.153`
- Para establecer la importancia relativa que se asigna a la información de entrada (conexiones activas, conexiones nuevas, puerto, sistema) recibida por el gestor para los servidores del cluster 9.6.54.12:
`ndcontrol cluster set 9.6.54.12 proportions 60 35 5 0`
- Para añadir un cluster comodín:
`ndcontrol cluster add 0.0.0.0`
- En una configuración de alta disponibilidad mutua, establezca la dirección de cluster 9.6.54.12 con la dirección de no reenvío de la máquina de reserva (9.65.70.19) como sistema principal:
`ndcontrol cluster set 9.6.54.12 primaryhost 9.65.70.19`
- Para mostrar el estado de la dirección de cluster 9.67.131.167:
`ndcontrol cluster status 9.67.131.167`

Este mandato produce una salida similar a la siguiente:

```
Cluster Status:
-----
Address ..... 9.67.131.167
Number of target ports ..... 3
Default sticky time ..... 0
Default stale timeout ..... 30
Default port weight bound ..... 20
Maximum number of ports ..... 8
Default port protocol ..... tcp/udp
Default maximum number of servers ..... 32
Proportion given to active connections... 0.5
Proportion given to new connections..... 0.5
Proportion given specific to the port... 0
Proportion given to system metrics..... 0
Shared bandwidth (KBytes) ..... 0
Primary Host Address ..... 9.67.131.167
```


ndcontrol ejecutor — controlar el ejecutor



report

Visualiza un informe de estadísticas. Por ejemplo: número total de paquetes recibidos, paquetes rechazados, paquetes reenviados con errores, etc.

Nota: El parámetro report no es aplicable a CBR ni a Mailbox Locator.

set

Establece los campos del ejecutor.

nfa

Establece la dirección de no reenvío. Cualquier paquete enviado a esta dirección no se reenviará mediante la máquina Dispatcher.

Nota: El parámetro NFA no es aplicable a CBR ni a Mailbox Locator.

dirección IP

La dirección de Protocolo Internet expresada como nombre simbólico o en formato decimal con puntos.

maxclusters

El número máximo de clusters que se puede configurar. El valor por omisión de maxclusters es 100.

tamaño

El número máximo de clusters que se puede configurar.

maxports

El número máximo de puertos por omisión para que se creen clusters.

Este valor puede modificarse con los mandatos **cluster set** o **cluster add**. El valor de maxports por omisión es 8.

tamaño

El número de puertos.

fincount

El número de conexiones que deben estar en estado de finalización antes de que se inicie la recogida de basura de conexiones. El valor por omisión de fincount es 4000.

número_conexiones_finalizadas

El valor de fincount.

Nota: El parámetro fincount no es aplicable a CBR ni a Mailbox Locator.

fintimeout

El número de segundos para mantener una conexión en la memoria después de que la conexión tome el estado de finalización. El valor de fintimeout por omisión es 60.

tiempo_espera_finalización

El valor del tiempo de espera de finalización.

Nota: El parámetro fintimeout no es aplicable a CBR ni a Mailbox Locator.

maxservers

El número máximo por omisión de servidores por puerto. Este valor puede alterarse temporalmente mediante el mandato **cluster** o el mandato **port**. El valor por omisión de maxservers es 32.

tamaño

El número de servidores.

staletimeout

El número de segundos durante los cuales puede haber ausencia de actividad en una conexión antes de que dicha conexión se elimine. El valor por omisión para FTP es 900; el valor por omisión para Telnet es 32.000.000. El valor por omisión para todos los demás puertos es 300. Este valor puede alterarse temporalmente mediante el mandato **cluster** o el mandato **port**. Consulte "Utilización del valor de tiempo de espera de inactividad" en la página 209 para obtener más información.

Nota: Para Mailbox Locator, el valor de staletimeout corresponde al temporizador de desconexión automática por inactividad de estos protocolos. Para Mailbox Locator, el valor por omisión de staletimeout es 60 segundos, el cual prevalece sobre los tiempos de espera de inactividad definidos para POP3 e IMAP. Para obtener

más información sobre `staletimeout` para Mailbox Locator, consulte la sección “Alteración del temporizador de inactividad de POP3/IMAP” en la página 97.

tiempo_sin_act.

El valor de `staletimeout`.

stickytime

El valor por omisión del tiempo de persistencia de puertos para todos los clusters futuros. Este valor puede modificarse con los mandatos **cluster** o **port**. El valor de `stickytime` por omisión es 0.

tiempo

El valor del tiempo de persistencia (`stickytime`) expresado en segundos.

clientgateway

Clientgateway es una dirección IP utilizada para NAT/NAPT o el encaminamiento por contenido mediante Dispatcher (CBR). Es la dirección de encaminador a través de la cual se reenvía el tráfico de retorno desde Network Dispatcher a los clientes. Clientgateway se debe establecer en un valor distinto de cero antes de añadir un puerto cuyo método de reenvío sea NAT/NAPT o el encaminamiento por contenido mediante Dispatcher (CBR). Consulte “Método de reenvío nat del Dispatcher” en la página 50 y “Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)” en la página 52 para obtener más información.

Nota: El parámetro `clientgateway` sólo es aplicable al componente Dispatcher.

dirección

La dirección `clientgateway` expresada como nombre simbólico o en formato decimal con puntos. El valor por omisión es 0.0.0.0.

weightbound

El valor por omisión del peso máximo para todos los puertos futuros. Este valor puede modificarse con los mandatos **cluster** o **port**. El valor por omisión de `weightbound` es 20.

peso

El valor de `weightbound`.

porttype

El valor de tipo de puerto por omisión para todos los puertos futuros. Este valor puede modificarse con los mandatos **cluster** o **port**.

Nota: El parámetro `porttype` no es aplicable a CBR ni a Mailbox Locator.

tipo

Los valores posibles son **tcp**, **udp** y **both**.

wideportnumber

Un puerto TCP no utilizado en cada máquina Dispatcher. El valor de *wideportnumber* ha de ser el mismo para todas las máquinas Dispatcher. El valor por omisión de *wideportnumber* es 0, lo que indica que el soporte de área amplia no está en uso.

Nota: El parámetro *wideportnumber* no es aplicable a CBR ni a Mailbox Locator.

puerto

El valor de **wideportnumber**.

sharedbandwidth

Es el ancho de banda máximo (kilobytes por segundo) que se puede compartir a nivel de ejecutor. Para obtener más información sobre el ancho de banda compartido, consulte “Utilización de normas basadas en el ancho de banda reservado y en el ancho de banda compartido” en la página 177 y “Norma del ancho de banda compartido” en la página 179.

Nota: El ancho de banda compartido no es aplicable a CBR ni a Mailbox Locator.

tamaño

Es el tamaño de **sharedbandwidth**, que es un valor entero. El valor por omisión es 0. Si el valor es 0, no se puede compartir el ancho de banda a nivel de ejecutor.

start

Arranca el ejecutor.

Nota: El parámetro *start* no es aplicable a Mailbox Locator.

status

Muestra el estado actual de los valores del ejecutor que pueden definirse y sus valores por omisión.

stop

Detiene el ejecutor. Para Dispatcher, *stop no* es un parámetro válido en Windows 2000.

Nota: El parámetro *stop* es aplicable a Dispatcher y CBR.

Ejemplos

- Para visualizar los contadores internos de Dispatcher:

```
ndcontrol executor status
```

```
Executor Status:
```

```
-----
```

```
Nonforwarding address ..... 9.67.131.151
```

```
Client gateway address ..... 0.0.0.0
```

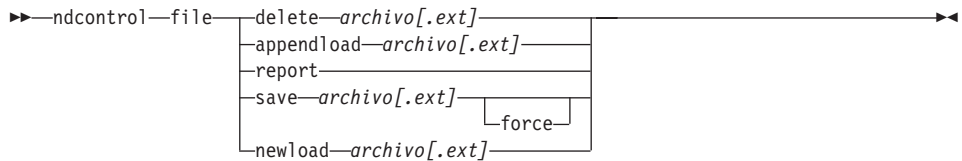
```

Fin count ..... 4,000
Fin timeout ..... 60
Wide area network port number ..... 2,001
Shared bandwidth (Kbytes) ..... 0
Default maximum ports per cluster ... 8
Maximum number of clusters ..... 100
Default maximum servers per port .... 32
Port stale timeout ..... 300
Port sticky time ..... 0
Port weight bound ..... 20
Maximum number of clusters ..... 100

```

- Para establecer la dirección de no reenvío en 130.40.52.167:
ndcontrol executor set nfa 130.40.52.167
- Para establecer el número máximo de cluster:
ndcontrol executor set maxclusters 4096
- Para arrancar el ejecutor:
ndcontrol executor start
- Para detener el ejecutor (**sólo AIX, Linux y Solaris**):
ndcontrol executor stop

ndcontrol file— gestionar archivos de configuración



delete

Elimina el archivo.

archivo[.ext]

Archivo de configuración que consta de mandatos ndcontrol.

La extensión del archivo (.ext) puede ser cualquiera que elija el usuario y se puede omitir.

appendload

Para actualizar la configuración actual, el mandato appendload ejecuta los mandatos ejecutables del archivo de script definido por el usuario.

report

Informe sobre el archivo o archivos disponibles.

save

Guarda la configuración actual de Network Dispatcher en el archivo.

Nota: Los archivos se guardan y cargan desde los directorios siguientes, donde *componente* es dispatcher, cbr o ml (Mailbox Locator):

- AIX: */usr/lpp/nd/servers/configurations/componente*
- Linux: */opt/nd/servers/configurations/componente*
- Solaris: */opt/nd/servers/configurations/componente*
- Windows 2000:

Vía de acceso común de directorio de instalación — **c:\Archivos de programa\ibm\edge\nd\servers\configurations\componente**

Vía de acceso nativa de directorio de instalación — **c:\Archivos de programa\ibm\edge\nd\servers\configurations\componente**

Vía de acceso nativa de directorio de instalación — **c:\Archivos de programa\ibm\nd\servers\configurations\componente**

force

Utilice **force** para guardar su archivo en un archivo existente del mismo nombre, el cual se suprime previamente. Si no utiliza la opción force, el archivo existente no se sobrescribe.

newload

Carga un nuevo archivo de configuración en Network Dispatcher y lo ejecuta. El nuevo archivo de configuración sustituirá a la configuración actual.

Ejemplos

- Para suprimir un archivo:
`ndcontrol file delete archivo3`

Se ha suprimido el archivo (archivo3).
- Para cargar un nuevo archivo de configuración con el que sustituir el archivo de configuración actual:
`ndcontrol archivo newload archivo1.sv`

Se ha cargado el archivo (archivo1.sv) en Dispatcher.
- Para añadir un archivo de configuración a la configuración actual y cargarlo:
`ndcontrol archivo appendload archivo2.sv`

Se ha añadido el archivo (archivo2.sv) a la configuración actual y se ha cargado.
- Para visualizar un informe de los archivos (esto es, aquellos archivos guardados anteriormente):
`ndcontrol file report`

INFORME DE ARCHIVOS:
archivo1.guardar
archivo2.sv
archivo3
- Para guardar la configuración en un archivo llamado archivo3:
`ndcontrol file save archivo3`

La configuración se ha guardado en el archivo (archivo3).

ndcontrol help — visualizar o imprimir ayuda para este mandato

➤➤ndcontrol—help	help	➤➤
	sistema principal	
	executor	
	manager	
	advisor	
	cluster	
	puerto	
	rule	
	server	
	subagent	
	highavailability	
	file	
	set	
	status	
	log	

Ejemplos

- Para obtener ayuda sobre el mandato ndcontrol:
ndcontrol help

Este mandato produce una salida similar a la siguiente:

```
ARGUMENTOS DEL MANDATO HELP:
-----
Uso:  help <opción de ayuda>
Ejemplo: help cluster

help          - imprimir texto completo de la ayuda
advisor       - ayuda para el mandato advisor
cluster       - ayuda para el mandato cluster
executor      - ayuda para el mandato executor
file          - ayuda para el mandato file
host          - ayuda para el mandato host
log           - ayuda para el mandato log
manager       - ayuda para el mandato manager
metric        - ayuda para el mandato metric
port          - ayuda para el mandato port
rule          - ayuda para el mandato rule
server        - ayuda para el mandato server
set           - ayuda para el mandato set
status        - ayuda para el mandato status
subagent      - ayuda para el mandato subagent
highavailability - ayuda para el mandato high availability
```

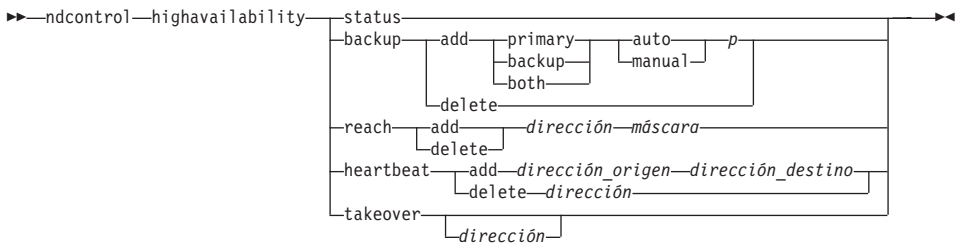
Tenga en cuenta que los parámetros especificados entre <> son variables.

- A veces, la ayuda mostrará opciones para las variables utilizando el signo | para separar las opciones:


```
fintimeout <dirección cluster>|all <tiempo>  
-Cambiar tiempo de espera de finalización  
(Utilice 'all' para cambiar todos los clusters)
```

ndcontrol highavailability — controlar la alta disponibilidad

Nota: El diagrama de sintaxis para ndcontrol high availability no es aplicable a CBR ni a Mailbox Locator.



status

Devolver un informe sobre la alta disponibilidad. Las máquinas se identifican mediante una de estas tres condiciones de estado:

Activo Una máquina determinada (que puede ser la máquina principal, de reserva o ambas cosas) está encaminando paquetes.

En espera

Una máquina determinada (que puede ser la máquina principal, de reserva o ambas cosas) no está encaminando paquetes. Está supervisando el estado de un Dispatcher **activo**.

Desocupado

Una máquina determinada está encaminando paquetes, y no está intentando establecer contacto con su Dispatcher asociado.

Además, la palabra clave **status** devuelve información acerca de diversos subestados:

Sincronizado

Una máquina determinada ha establecido contacto con otro Dispatcher.

Otros subestados

Esta máquina está intentando establecer contacto con su Dispatcher asociado, pero no ha podido hacerlo todavía.

backup

Especifica información para la máquina principal o la de reserva.

add

Define y ejecuta las funciones de alta disponibilidad de esta máquina.

principal

Identifica la máquina Dispatcher cuya función es la de máquina *principal*.

backup

Identifica la máquina Dispatcher cuya función es la de máquina *de reserva*.

both

Identifica la máquina Dispatcher que tiene *ambas* funciones, esto es, la función de máquina principal y máquina de reserva. Esta es la característica de alta disponibilidad mutua en la que las funciones de máquina principal y de reserva están asociadas por conjunto de clusters. En “Alta disponibilidad mutua” en la página 48 hallará más información.

auto

Especifica una estrategia de recuperación *automática*, en la que la máquina principal reanuda el encaminamiento de paquetes tan pronto como entre de nuevo en servicio.

manual

Especifica una estrategia de recuperación *manual*, en la que la máquina principal no reanuda el encaminamiento de paquetes hasta que el administrador emite el mandato **takeover**.

p[uerto]

Un puerto TCP no utilizado en ambas máquinas, que debe utilizar Dispatcher para los mensajes de pulso. El *puerto* debe ser el mismo en la máquina principal y en la de reserva.

delete

Elimina esta máquina de la alta disponibilidad, de forma que ya no podrá utilizarse como máquina de reserva ni como máquina principal.

reach

Añadir o suprimir la dirección de destino para los Dispatchers principal y de reserva; el asesor de accesibilidad envía mandatos *ping* desde los Dispatcher principal y de reserva para determinar la accesibilidad de los destinos.

Nota: Cuando configure el destino de reach, debe también iniciar el asesor reach. El asesor reach arranca automáticamente mediante la función del gestor.

add

Añade una dirección destino al asesor de accesibilidad.

delete

Elimina una dirección destino del asesor de accesibilidad.

dirección

Dirección IP (simbólica o decimal con puntos) del nodo destino.

máscara

Máscara de subred

heartbeat

Define una sesión de comunicación entre las máquinas Dispatcher principal y de reserva.

add

Indica al Dispatcher origen la dirección de su asociado (dirección destino).

dirección_origen

Dirección de origen. La dirección (IP o simbólica) de este Dispatcher.

dirección_destino

Dirección de destino. La dirección (IP o simbólica) de la otra máquina Dispatcher.

Nota: La dirección de origen y la dirección de destino deben ser las direcciones de no reenvío (NFA) de las máquinas como mínimo para un par de pulsos.

delete

Elimina el par de direcciones en la información de pulso. Puede especificar la dirección de destino o la dirección de origen del par de pulsos.

dirección

La dirección (IP o simbólica) del destino o del origen.

takeover

Configuración de alta disponibilidad simple (la función de las máquinas Dispatcher son la de máquina *principal* o máquina *de reserva*):

- Indica a la máquina Dispatcher que está en espera que pase al estado activo e inicie el encaminamiento de paquetes. De este modo, la máquina Dispatcher que está activa en este momento pasará al estado de espera. El mandato takeover se debe emitir en la máquina que está en estado de espera y únicamente funciona cuando la estrategia es **manual**. El subestado de ser *sincronizado*

Configuración de alta disponibilidad mutua (la función de las máquinas Dispatcher es la de *ambas* máquinas).

- La máquina Dispatcher con la característica de alta disponibilidad mutua contiene dos clusters que coinciden los de con su asociada. Uno de los clusters se considera el cluster primario (el cluster de reserva de la asociada) y el otro es el cluster de reserva (el cluster primario de la asociada). El mandato takeover indica a la máquina Dispatcher que inicie el encaminamiento de paquetes para los otros clusters de la máquina. El mandato takeover sólo se puede emitir cuando los clusters de la máquina Dispatcher están en estado *de espera* y su subestado es *sincronizado*. Esto hace que los clusters que están activos actualmente de la máquina asociada pasen a estado de espera. El mandato takeover

sólo funciona cuando la estrategia es **manual**. En “Alta disponibilidad mutua” en la página 48 hallará más información.

Notas:

1. Tenga en cuenta que las *funciones* de las máquinas (*principal*, *de reserva* o *ambas*) no cambian. Sólo cambia su *estado* relativo (*activo* o *en espera*).
2. Existen tres *scripts* posibles de toma de control: `goActive`, `goStandby` y `goInOp`. Consulte “Utilización de scripts” en la página 170.

dirección

El valor de dirección de takeover es opcional. Sólo debe utilizarse cuando la función de la máquina sea la de *ambas* máquinas, esto es, la de máquina principal y máquina de reserva (configuración de alta disponibilidad mutua). La dirección especificada es la dirección de no reenvío de la máquina Dispatcher que generalmente encamina el tráfico de este cluster. Cuando se produzca una toma de control de ambos clusters, especifique la dirección de no reenvío del Dispatcher.

Ejemplos

- Para comprobar el estado de alta disponibilidad de una máquina:
`ndcontrol highavailability status`

Salida:

Estado de alta disponibilidad:

```
-----  
Función ..... primario  
Estrategia de recuperación .. manual  
Estado ..... Activo  
Subestado ..... Sincronizado  
Sis. principal primario 9.67.131.151  
Puerto .....12,345  
Destino preferente .... 9.67.134.223
```

Estado de pulso:

```
-----  
Número ..... 1  
Estado de accesibilidad:  
-----  
Número ..... 1
```

- Para añadir la información de reserva a la máquina principal utilizando la estrategia de recuperación automática y el puerto 80:
`ndcontrol highavailability backup add primary auto 80`
- Para añadir una dirección que el Dispatcher pueda alcanzar:
`ndcontrol highavailability reach add 9.67.125.18`
- Para añadir información de pulso para la máquina principal y la de reserva.
Principal - `highavailability heartbeat add 9.67.111.3 9.67.186.8`
Reserva - `highavailability heartbeat add 9.67.186.8 9.67.111.3`
- Para indicar al Dispatcher en espera que se active, forzando a la máquina activa a colocarse en situación de espera:
`ndcontrol highavailability takeover`

ndcontrol host — configurar una máquina remota

►►—ndcontrol—host:—*sispral_remoto*—◄◄

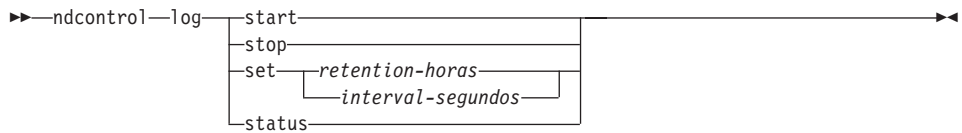
sispral_remoto

El nombre de la máquina Network Dispatcher que se va a configurar. Cuando escriba este mandato, compruebe que no haya espacios entre **host:** y *sispral_remoto*, por ejemplo:

```
ndcontrol  
host: sistema_principal_remoto
```

Una vez emitido este mandato en el indicador de mandatos, escriba cualquier mandato ndcontrol válido que desee emitir en la máquina Network Dispatcher remoto.

ndcontrol log — controlar el archivo de anotaciones en binario



start

Inicia el archivo de anotaciones en binario.

stop

Detiene el archivo de anotaciones en binario.

set

Establece los campos para las anotaciones en binario. Para obtener más información sobre cómo definir campos para las anotaciones en binario, consulte “Utilizar las anotaciones en binario para analizar las estadísticas del servidor” en la página 198.

retention

El número de horas que se conservarán los archivos de anotaciones en binario. El valor por omisión de `retention` es 24.

horas

El número de horas.

intervals

El número de segundos entre entradas de anotaciones. El valor por omisión de `interval` es 60.

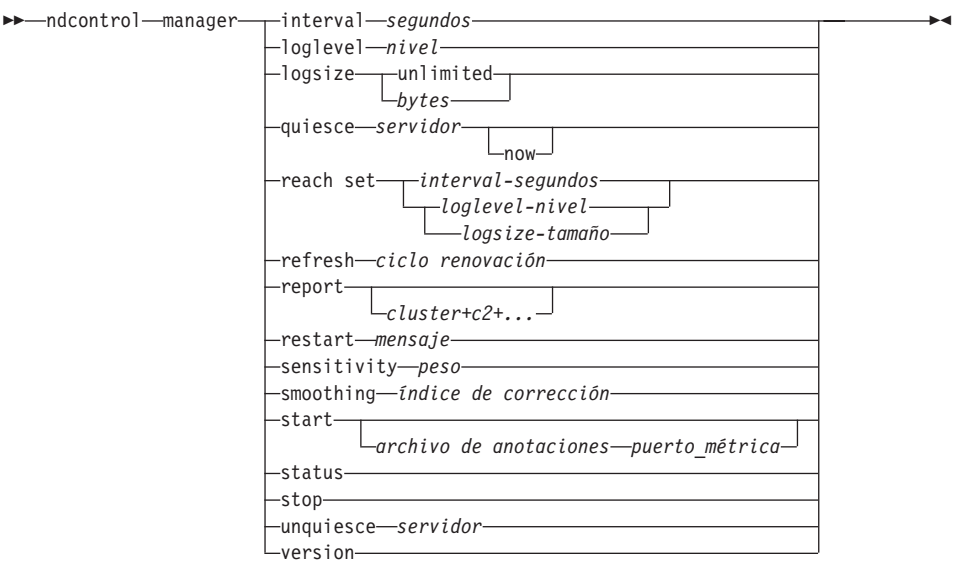
segundos

El número de segundos.

status

Muestra la retención y los intervalos de las anotaciones en binario.

ndcontrol manager — controlar el gestor



interval

Establece la periodicidad con la que el gestor actualizará los pesos de los servidores con respecto al ejecutor, actualizando los criterios utilizados por el ejecutor para encaminar las peticiones de los clientes.

segundos

Un número positivo que representa en segundos la frecuencia con la que el gestor actualizará los pesos con respecto al ejecutor. El valor por omisión es 2.

loglevel

Establece el nivel de anotaciones del archivo de anotaciones de gestor y del archivo de anotaciones de Supervisor de métrica.

nivel

Número del nivel (0 a 5). Cuanto mayor es el número, más información se graba en el archivo de anotaciones del gestor. El valor por omisión es 1. Los valores posibles son: 0 para None, 1 para Minimal, 2 para Basic, 3 para Moderate, 4 para Advanced, 5 para Verbose.

logsize

Establece el tamaño máximo de las anotaciones del gestor. Si establece el tamaño máximo para el archivo de anotaciones, el archivo se sobregrabará cuando esté lleno. Cuando el archivo alcance el tamaño especificado, las entradas subsiguientes se grabarán a partir del comienzo del archivo, sobre las entradas de anotaciones anteriores. El tamaño del archivo de

anotaciones no puede ser menor que el tamaño actual del archivo. Las entradas del archivo de anotaciones contienen una indicación horaria para poder determinar el orden en el que se escribieron. Cuanto más alto sea el nivel de las anotaciones, más cuidadosamente debe elegirse el tamaño de las mismas, ya que puede quedarse rápidamente sin espacio si efectúa anotaciones a los niveles más altos.

bytes

El tamaño máximo en bytes del archivo de anotaciones del gestor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Puede que el archivo de anotaciones no alcance el tamaño máximo exacto antes de sobrescribirse, ya que las propias entradas de anotaciones varían en tamaño. El valor por omisión es 1 MB.

quiesce

Especifica que no se envíen más conexiones al servidor y sólo se envían las nuevas conexiones subsiguientes desde el cliente al servidor desactivado si la conexión está definida como persistente y no ha transcurrido el tiempo de persistencia. El gestor establece en 0 el peso para ese servidor en cada uno de los puertos para los que está definido. Utilice este mandato si desea efectuar un mantenimiento rápido en un servidor y a continuación activarlo. Si suprime un servidor desactivado de la configuración y luego lo añade de nuevo, no conservará el estado que tenía antes de desactivarlo. Para obtener más información, consulte “Desactivación de conexiones persistentes” en la página 192.

servidor

La dirección IP expresada como nombre simbólico o en formato decimal con puntos.

O bien, si ha utilizado el particionamiento de servidores, utilice el nombre exclusivo del servidor lógico. En “Particionamiento del servidor: servidores lógicos configurados para un solo servidor físico (dirección IP)” en la página 152 hallará más información.

now

Utilice el mandato quiesce “now” (desactivar ahora) sólo si tiene establecido un tiempo de persistencia y desea que las nuevas conexiones se envíen a otro servidor (distinto del servidor desactivado) antes de que finalice el tiempo de persistencia. Para obtener más información, consulte “Desactivación de conexiones persistentes” en la página 192.

reach set

Establece el intervalo, nivel de registro y tamaño del archivo de anotaciones para el asesor reach.

refresh

Establece el número de intervalos antes de solicitar al ejecutor una renovación de la información acerca de las conexiones activas y nuevas.

ciclo de renovación

Número positivo que representa el número de intervalos. El valor por omisión es 2.

report

Visualiza un informe instantáneo de estadísticas.

cluster

La dirección del cluster que desea que se muestre en el informe. La dirección puede ser un nombre simbólico o puede tener un formato decimal con puntos. Por omisión, se muestra un informe del gestor para todos los clusters.

Nota: Los clusters adicionales se separan mediante un signo más (+).

restart

Rearranca todos los servidores (que no estén inactivos) con pesos normalizados (1/2 del peso máximo).

mensaje

Un mensaje que desea grabar en el archivo de anotaciones del gestor.

sensitivity

Establece la sensibilidad mínima para que se actualicen los pesos. Este valor define cuándo el gestor debe cambiar la ponderación del servidor en función de la información externa.

peso

Un número de 1 a 100 que se utiliza como porcentaje de peso. El valor por omisión 5 crea una sensibilidad mínima del 5%.

smoothing

Establece un índice que corrige las variaciones de ponderación al repartir el tráfico. Cuanto más alto sea el índice de corrección, menos acusadamente cambiarán los pesos de los servidores cuando se modifiquen las condiciones de la red. Un índice más bajo ocasionará que los pesos de los servidores se modifiquen más acusadamente.

índice

Un número positivo de coma flotante. El valor por omisión es 1,5.

start

Arranca el gestor.

archivo de anotaciones

Nombre de archivo en el que se anotan los datos del gestor. En cada registro de las anotaciones figurará la indicación de la hora.

El archivo por omisión se instalará en el directorio **logs**. Consulte “Apéndice F. Ejemplos de archivos de configuración” en la página 377. Para cambiar el directorio en el que se conservarán los archivos de

anotaciones, consulte la sección “Cambio de la vía de acceso de los archivos de anotaciones” en la página 208.

puerto_métrica

Puerto que Metric Server utilizará para informar de los niveles de tráfico del sistema. Si especifica un puerto de métrica, debe especificar un nombre de archivo de anotaciones. El puerto de métrica por omisión es 10004.

status

Muestra el estado actual de todos los valores del gestor que pueden establecerse globalmente y sus valores por omisión.

stop

Detiene el gestor.

unquiesce

Especifica que el gestor puede empezar a suministrar un peso superior a 0 a un servidor que se ha desactivado anteriormente, en cada puerto en el que está definido.

servidor

La dirección IP expresada como nombre simbólico o en formato decimal con puntos.

version

Muestra la versión actual del gestor.

Ejemplos

- Para establecer el intervalo de actualización del gestor a cada 5 segundos:
`ndcontrol manager interval 5`
- Para establecer el nivel de anotaciones a 0 para mejorar el rendimiento:
`ndcontrol manager loglevel 0`
- Para establecer el tamaño de las anotaciones del gestor a 1.000.000 bytes:
`ndcontrol manager logsize 1000000`
- Para especificar que no se envíen más conexiones al servidor de 130.40.52.153:
`ndcontrol manager quiesce 130.40.52.153`
- Para establecer a 3 el número de intervalos de actualización antes de renovar los pesos:
`ndcontrol manager refresh 3`
- Para obtener una instantánea de las estadísticas del gestor:
`ndcontrol manager report`

Este mandato produce una salida similar a la siguiente:

HOST TABLE LIST	STATUS
9.67.129.221	ACTIVE
9.67.129.213	ACTIVE
9.67.134.223	ACTIVE

9.67.131.18	WEIGHT		ACTIVE % 48	NEW % 48		PORT % 4	SYSTEM % 0	
PORT: 80	NOW		NEW	WT		CONN	WT	
9.67.129.221	8		8	10		0	10	
9.67.134.223	11		11	10		0	10	
PORT TOTALS:	19		19			0		

9.67.131.18	WEIGHT			ACTIVE % 48			NEW % 48			PORT % 4			SYSTEM % 0		
PORT: 23	NOW	NEW	WT	CONN		WT	CONN		WT	LOAD		WT	LOAD		
9.67.129.213	10	10	10	0		10	0		10	71		0	0		
9.67.134.223	0	0	10	0		10	0		-9999	-1		0	0		
PORT TOTALS:	10	10		0			0			70			0		

ADVISOR	PORT	TIMEOUT
reach	0	unlimited
http	80	unlimited
ftp	21	unlimited

- Para reiniciar todos los servidores con pesos normalizados y grabar un mensaje en el archivo de anotaciones del gestor:

ndcontrol manager restart Reiniciando el gestor para actualizar código

Este mandato produce una salida similar a la siguiente:

320-14:04:54 Reiniciando el gestor para actualizar código

- Para establecer la sensibilidad a los cambios de peso a 10:

ndcontrol manager sensitivity 10

- Para establecer el índice de corrección en 2.0:

ndcontrol manager smoothing 2.0

- Para iniciar el gestor y especificar el archivo de anotaciones denominado ndmgr.log (la vía de acceso no puede establecerse)

ndcontrol manager start ndmgr.log

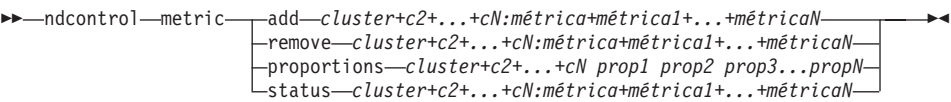
- Para visualizar el estado actual de los valores asociados con el gestor:
`ndcontrol manager status`

Este mandato produce una salida similar al ejemplo siguiente:

```
Manager status:
=====
Metric port..... 10,004
Manager log filename..... manager.log
Manager log level..... 1
Maximum manager log size (bytes)..... unlimited
Sensitivity level..... 0.05
Smoothing index..... 1.5
Update interval (seconds)..... 2
Weights refresh cycle..... 2
Reach log level..... 1
Maximum reach log size (bytes)..... unlimited
Reach update interval (seconds)..... 7
```

- Para detener el gestor:
`ndcontrol manager stop`
- El mandato siguiente especifica que no se envíen más conexiones nuevas al servidor situado en 130.40.52.153. (Nota: utilice el mandato `quiesce "now"` (desactivar ahora) sólo si tiene establecido un tiempo de persistencia y desea que las nuevas conexiones se envíen a otro servidor antes de que finalice el tiempo de persistencia.):
`ndcontrol manager quiesce 130.40.52.153 now`
- El mandato siguiente especifica que no se envíen más conexiones nuevas al servidor situado en 130.40.52.153. (Nota: si tiene definido un tiempo de persistencia, las nuevas conexiones subsiguientes procedentes del cliente se enviarán a este servidor hasta que finalice el tiempo de persistencia.) :
`ndcontrol manager quiesce 130.40.52.153`
- Para especificar que el gestor puede empezar a otorgar un peso mayor que 0 a un servidor situado en 130.40.52.153 que se desactivó anteriormente:
`ndcontrol manager unquiesce 130.40.52.153`
- Para visualizar el número de la versión actual del gestor:
`ndcontrol manager version`

ndcontrol metric — configurar métricas del sistema



add

Añade la métrica especificada.

cluster

La dirección a la que se conectan los clientes. La dirección puede ser el nombre de sistema principal de la máquina o la dirección IP en formato decimal con puntos. Los clusters adicionales se separan mediante un signo más (+).

Nota: para Cisco Consultant, la dirección de cluster corresponde la dirección IP virtual (dirección VIP) de la norma de contenido del propietario en la configuración de Cisco CSS Switch.

métrica

Es el nombre de la métrica del sistema. Debe ser el nombre de un archivo ejecutable o de script contenido en el directorio de scripts de Metric Server.

remove

Elimina la métrica especificada.

proportions

Establece las proporciones para todas las métricas asociada al objeto.

status

Muestra los valores actuales de la métrica.

Ejemplos

- Para añadir una métrica del sistema:
`sscontrol metric add site1:metric1`
- Para establecer las proporciones de las dos métricas del sistema correspondientes a un sitio Web:
`sscontrol metric proportions site1 0 100`
- Para visualizar el estado actual de los valores asociados a la métrica especificada:
`sscontrol metric status site1:metric1`

Este mandato produce una salida similar a la siguiente:

Metric Status:

Cluster 10.10.10.20

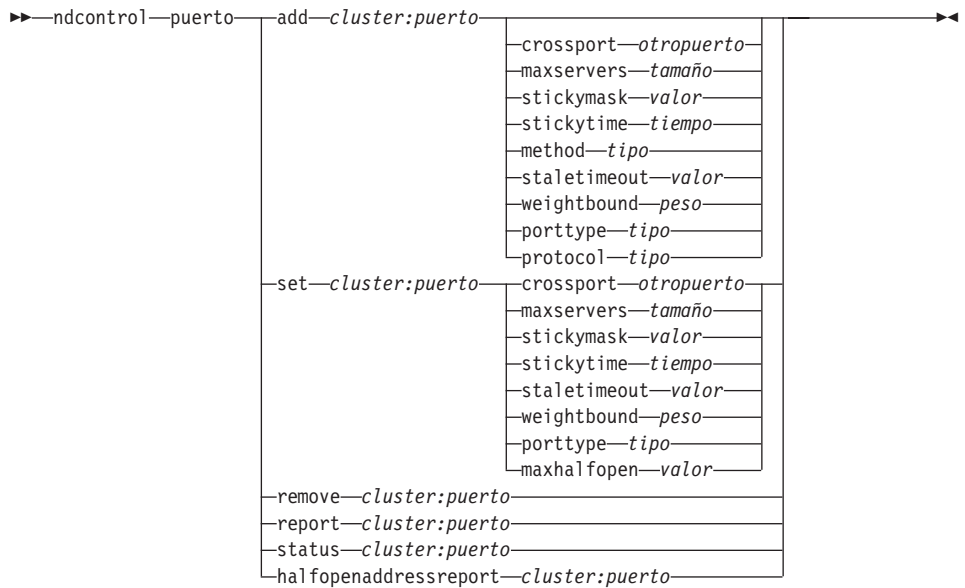
Metric name metric1

Metric proportion 50

Server plm3

Metric data -1

ndcontrol port — configurar puertos



add

Añade un puerto a un cluster. Ha de añadir un puerto a un cluster antes de poder añadir servidores a este puerto. Si no existen puertos para un cluster, todas las peticiones de cliente se procesarán localmente. Puede añadir más de un puerto a la vez utilizando este mandato.

Nota: Para el componente Mailbox Locator de Network Dispatcher, debe crear un alias del cluster IP en la máquina antes de intentar añadir un puerto. El mandato **add port** intenta iniciar un proxy Java que se vincula con el cluster; por lo tanto, debe existir el IP en la pila de IP.

En Windows, esto significa que debe estar en la configuración de red de Windows. No basta con el mandato **cluster configure** porque sólo simula el alias de IP y el proxy no puede vincularse con este IP falso. Para los otros sistemas operativos, el mandato **cluster configure** es adecuado porque utiliza ifconfig para crear el alias del IP.

cluster

La dirección del cluster expresada como nombre simbólico o en formato decimal con puntos. Puede utilizar un signo de dos puntos (:) como comodín. Por ejemplo, el mandato `ndcontrol port add :80` añadirá el puerto 80 a todos los clusters.

Nota: Los clusters adicionales se separan mediante un signo más (+).

puerto

El número del puerto. Se puede utilizar el valor 0 (cero) como número de puerto para especificar un puerto comodín.

Nota: Los puertos adicionales se separan mediante un signo más (+).

crossport

Crossport le permite ampliar la función de persistencia/afinidad para varios puertos, para que las peticiones subsiguientes de los clientes que se reciban en los diferentes puertos se puedan seguir enviando al mismo servidor. Como valor de crossport, especifique el número de *otro puerto* con el que desea compartir la función de afinidad entre puertos. Para poder utilizar esta característica, los puertos deben:

- compartir la misma dirección de cluster
- compartir los mismos servidores
- tener el mismo valor de tiempo de persistencia (stickytime) (distinto de cero)
- tener el mismo valor de máscara de afinidad (stickymask)

Para suprimir la afinidad entre puertos, vuelva a establecer el valor crossport a su propio número de puerto. Para obtener más información sobre la afinidad entre puertos, consulte “Afinidad entre puertos” en la página 189.

Nota: La afinidad entre puertos sólo es aplicable al componente Dispatcher.

otro puerto

El valor de crossport. Por omisión es el mismo que el número de su propio *puerto*.

maxservers

El número máximo de servidores. El valor por omisión de maxservers es 32.

tamaño

El valor de maxservers.

stickymask

La máscara de dirección de afinidad agrupa las peticiones entrantes de los clientes basándose en direcciones de subred comunes. La primera vez que una petición de cliente efectúa una conexión con el puerto, todas las peticiones posteriores procedentes de los clientes con la misma dirección de subred (que se representa mediante la parte de la dirección que se va a enmascarar) se dirigirán al mismo servidor. En “Máscara de dirección de afinidad” en la página 190 hallará más información.

Nota: La palabra clave stickymask sólo es aplicable al componente Dispatcher.

valor

El valor de stickymask es el número de bits de orden superior de la dirección IP de 32 bits que desea enmascarar. Los valores posibles son 8, 16, 24 y 32. El valor por omisión es 32, que inhabilita la característica de máscara de dirección de afinidad.

stickytime

Intervalo que transcurre entre el cierre de una conexión y la apertura de una nueva conexión y durante el cual se envía el cliente al mismo servidor utilizado en la primera conexión. Después del tiempo de persistencia, el cliente se puede enviar a un servidor diferente del primero.

Para el componente Dispatcher:

- Para el método de reenvío cbr de Dispatcher
 - Si establece para stickytime del puerto un valor distinto de cero, el tipo de afinidad de la norma debe ser ninguno (valor por omisión). La afinidad basada en normas (cookie pasiva, URI) no puede coexistir cuando stickytime está establecido en el puerto.
 - Puerto que al definir un valor de stickytime se habilita la afinidad de ID de SSL, no puede añadir una norma de contenido al puerto.
- Para los métodos de reenvío mac y nat de Dispatcher
 - Si establece para stickytime del puerto un valor distinto de cero, no puede definir un tipo de afinidad en la norma. La afinidad basada en normas no puede coexistir cuando stickytime está establecido en el puerto.
 - Al establecer un valor de stickytime se habilita la afinidad de direcciones IP.
- El valor de stickytime debería ser 1 si se utiliza la API del Server Directed Affinity.

Para el componente CBR: Si establece para stickytime del puerto un valor distinto de cero, el tipo de afinidad de la norma debe ser ninguno (valor por omisión). La afinidad basada en normas (cookie pasiva, URI, cookie activa) no puede coexistir cuando stickytime está establecido en el puerto.

tiempo

El tiempo de persistencia del puerto, expresado en segundos. Cero significa que el puerto no permite la persistencia.

method

El método de reenvío. Los métodos de reenvío posibles son: MAC, NAT/NAPT y CBR (Content-Based Routing). No puede añadir el método de reenvío NAT/NAPT ni CBR a menos que primero especifique una

dirección IP distinta de cero en el parámetro `clientgateway` del mandato `"ndcontrol executor"`. Consulte "Método de reenvío nat del Dispatcher" en la página 50 y "Encaminamiento por contenido mediante Dispatcher (método de reenvío cbr)" en la página 52 para obtener más información.

Nota: Si el servidor de fondo está en la misma subred que la dirección de retorno y el usuario desea utilizar el método de reenvío de encaminamiento por contenido o el método de reenvío NAT/NAPT, hay que definir la dirección del encaminador como dirección del servidor de fondo.

tipo

El tipo de método de reenvío. Los valores posibles son: `mac`, `nat` o `cbr`. El valor por omisión es `mac` (reenvío MAC).

staletimeout

El número de segundos durante los cuales puede haber ausencia de actividad en una conexión antes de que dicha conexión se elimine. Para el componente Dispatcher o CBR, el valor por omisión es 900 para el puerto 21 (FTP) y 32.000.000 para el puerto 23 (Telnet). Para los demás puertos, el valor por omisión es 300. El valor de `staletimeout` también se puede definir a nivel de ejecutor o de cluster. En "Utilización del valor de tiempo de espera de inactividad" en la página 209 hallará más información.

Nota: Para Mailbox Locator, el valor de `staletimeout` corresponde al temporizador de desconexión automática por inactividad de estos protocolos. Para Mailbox Locator, el valor por omisión de `staletimeout` es 60 segundos, el cual prevalece sobre los tiempos de espera de inactividad definidos para POP3 e IMAP. Para obtener más información sobre `staletimeout` para Mailbox Locator, consulte la sección "Alteración del temporizador de inactividad de POP3/IMAP" en la página 97.

valor

El valor de **`staletimeout`** en número de segundos.

weightbound

Establece el peso máximo para los servidores en este puerto. Esto afecta a la diferencia que puede haber entre el número de peticiones que el ejecutor suministrará a cada servidor. El valor por omisión es 20.

peso

Un número del 1 al 100 que representa la ponderación máxima.

porttype

El tipo de puerto.

Nota: `Porttype` sólo es aplicable a Dispatcher.

tipo

Los valores posibles son **tcp**, **udp** y **ambos**. El valor por omisión es ambos (tcp/udp).

protocol

El tipo de protocolo del proxy (POP3 o IMAP). El parámetro protocol es necesario al añadir un puerto para Mailbox Locator.

Nota: Este parámetro sólo es aplicable a Mailbox Locator.

tipo

Los valores posibles son **POP3** o **IMAP**.

maxhalfopen

Es el valor umbral para el número máximo de conexiones semiabiertas. Utilice este parámetro para detectar posibles ataques de denegación de servicio, los cuales producen gran número de conexiones TCP semiabiertas en los servidores.

Un valor positivo indica que se comprobará si el número actual de conexiones semiabiertas excede el valor umbral. Si el valor actual es mayor que el umbral, se invoca un script de alerta. En “Detección de ataques de denegación de servicio” en la página 197 hallará más información.

Nota: maxhalfopen sólo es aplicable a Dispatcher.

valor

El valor de maxhalfopen. El valor por omisión es 0 (no se realiza ninguna comprobación).

set

Establece los campos de un puerto.

remove

Se elimina este puerto.

report

Informe de este puerto.

status

Muestra el estado de los servidores de este puerto. Si desea ver el estado de todos los puertos, no especifique un *puerto* en este mandato. No se olvide de los dos puntos.

númSegundos

Período de tiempo en segundos antes de restablecer las conexiones semiabiertas.

halfopenaddressreport

Crea entradas en el archivo de anotaciones (halfOpen.log) para todas las

direcciones de clientes (hasta aproximadamente 8000 pares de direcciones) que han accedido a servidores y han originado conexiones semiabiertas. También muestra datos estadísticos en la línea de mandatos, tales como: número total, mayor y promedio de conexiones semiabiertas y el tiempo promedio de las conexiones semiabiertas (en segundos). En “Detección de ataques de denegación de servicio” en la página 197 hallará más información.

Ejemplos

- Para añadir los puertos 80 y 23 a la dirección del cluster 130.40.52.153:
`ndcontrol port add 130.40.52.153:80+23`
- Para añadir un puerto comodín a la dirección del cluster 130.40.52.153:
`ndcontrol port set 130.40.52.153:0`
- Para Mailbox Locator, para añadir el puerto 20 del protocolo POP3 a la dirección de cluster 9.37.60.91:
`mlcontrol port add 9.37.60.91:20 protocol pop3`
- Para establecer el peso máximo 10 en el puerto 80 de la dirección de cluster 130.40.52.153:
`ndcontrol port set 130.40.52.153:80 weightbound 10`
- Para establecer el valor de stickytime en 60 segundos para el puerto 80 y el puerto 23 en la dirección del cluster 130.40.52.153:
`ndcontrol port set
130.40.52.153:80+23 stickytime 60`
- Para establecer el valor de característica de afinidad entre puertos del puerto 80 en el puerto 23, en la dirección del cluster 130.40.52.153:
`ndcontrol port set 130.40.52.153:80 crossport 23`
- Para eliminar el puerto 23 de la dirección de cluster 130.40.52.153:
`ndcontrol port remove 130.40.52.153:23`
- Para obtener el estado del puerto 80 de la dirección de cluster 9.67.131.153:
`ndcontrol port status 9.67.131.153:80`

Este mandato produce una salida similar a la siguiente:

Port Status:

```
Port number ..... 80
Cluster address ..... 9.67.131.153
Number of servers ..... 2
Stale timeout ..... 30
Weight bound ..... 20
Maximum number of servers ..... 32
Sticky time ..... 0
Port type ..... tcp/udp
```

```
Forwarding method ..... MAC Based Forwarding
Sticky mask bits ..... 32
Cross Port Affinity ..... 80
Max Half Open Connections ..... 0
```

- Para obtener el informe sobre direcciones semiabiertas para el puerto 80 de la dirección de cluster 9.67.127.121:

```
ndcontrol port halfopenaddressreport 9.67.127.121:80
```

Este mandato produce una salida similar a la siguiente:

```
Half open connection report successfully created:
```

```
-----
```

```
Half Open Address Report for cluster:port = 9.67.127.121:80
```

```
Total addresses with half open connections reported ... 0
```

```
Total number of half open connections reported ..... 0
```

```
Largest number of half open connections reported ..... 0
```

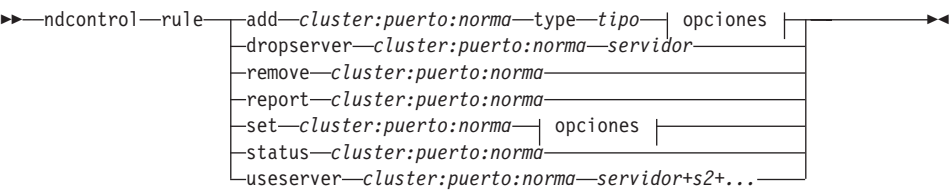
```
Average number of half open connections reported ..... 0
```

```
Average half open connection time (seconds) reported .. 0
```

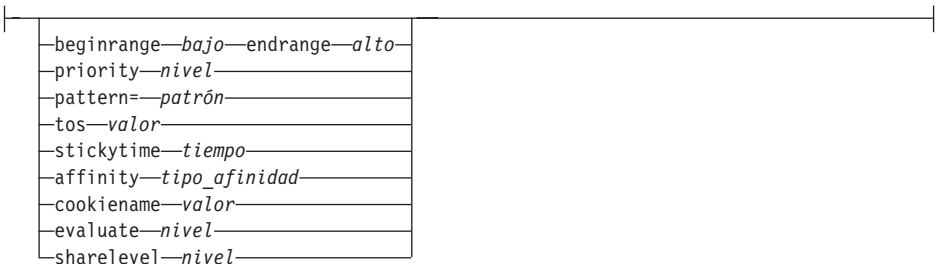
```
Total half open connections received ..... 0
```

ndcontrol rule — configurar normas

Nota: Los diagramas de sintaxis para el mandato rule no son aplicables a Mailbox Locator.



opciones:



add

Añade esta norma a un puerto.

cluster

La dirección del cluster expresada como nombre simbólico o en formato decimal con puntos. Puede utilizar un signo de dos puntos (:) como comodín. Por ejemplo, el mandato `ndcontrol rule add :80:RuleA type tipo` añadirá la norma RuleA al puerto 80 para todos los clusters.

Nota: Los clusters adicionales se separan mediante un signo más (+).

puerto

El número del puerto. Puede utilizar un signo de dos puntos (:) como comodín. Por ejemplo, el mandato `ndcontrol rule add clusterA:RuleA type tipo` añadirá la norma RuleA a todos los puertos del cluster ClusterA.

Nota: Los puertos adicionales se separan mediante un signo más (+).

norma

El nombre que elige para la norma. Este nombre puede contener cualquier

carácter alfanumérico, subrayados, guiones o puntos. Puede tener de 1 a 20 caracteres y no puede contener espacios en blanco.

Nota: Las normas adicionales se separan mediante un signo más (+).

type

El tipo de norma.

tipo

Las opciones para *tipo* son:

ip La norma se basa en la dirección IP del cliente.

time La norma se basa en la hora del día.

connection

La norma se basa en el número de conexiones por segundo del puerto. Esta norma funcionará solamente si el gestor se está ejecutando.

active La norma se basa en el número total de conexiones activas del puerto. Esta norma funcionará solamente si el gestor se está ejecutando.

port La norma se basa en el puerto del cliente.

Nota: Port no se aplica a CBR.

service

Esta norma está basada en el campo de bytes de tipo de servicio (TOS) de la cabecera IP.

Nota: Esta norma sólo se aplica al componente Dispatcher.

reservedbandwidth

Esta norma está basada en el ancho de banda (kilobytes por segundo) proporcionado por un grupo de servidores. Para obtener más información, consulte “Utilización de normas basadas en el ancho de banda reservado y en el ancho de banda compartido” en la página 177 y “Norma del ancho de banda reservado” en la página 178.

Nota: Reservedbandwidth sólo es aplicable al componente Dispatcher.

sharedbandwidth

Esta norma está basada en el ancho de banda (kilobytes por segundo) que se compartirá a nivel de ejecutor o de cluster. Para obtener más información, consulte “Utilización de normas basadas

en el ancho de banda reservado y en el ancho de banda compartido” en la página 177 y “Norma del ancho de banda compartido” en la página 179.

Nota: Sharedbandwidth sólo es aplicable al componente Dispatcher.

true Esta norma es siempre cierta. Considérela como una sentencia else en lógica de programación.

content

Esta norma describe una expresión regular que se comparará con los URL solicitados por el cliente. Esto sólo es válido para Dispatcher y CBR.

beginrange

Valor inferior del rango utilizado para determinar si la norma es verdadera.

bajo

Depende del tipo de norma. El tipo de valor y su valor por omisión se listan a continuación por tipo de norma:

ip La dirección del cliente expresada como nombre simbólico o en formato decimal con puntos. El valor por omisión es 0.0.0.0.

hora Un entero. El valor por omisión es 0, que representa la medianoche.

conexión

Un entero. El valor por omisión es 0.

activas Un entero. El valor por omisión es 0.

puerto Un entero. El valor por omisión es 0.

anchobandareservado

Valor entero (kilobytes por segundo). El valor por omisión es 0.

endrange

Valor superior del rango utilizado para determinar si la norma es verdadera.

alto

Depende del tipo de norma. El tipo de valor y su valor por omisión se listan a continuación por tipo de norma:

ip La dirección del cliente expresada como nombre simbólico o en formato decimal con puntos. El valor por omisión es 255.255.255.254.

hora Un entero. El valor por omisión es 24, que representa la medianoche.

Nota: Cuando defina el valor inferior y superior del rango de intervalos de tiempo, tenga en cuenta que cada valor debe ser un entero representando únicamente la hora; no se especifican las porciones de la hora. Por esta razón, para especificar una sola hora—por ejemplo, la hora entre las 3:00 y las 4:00— especificaría un valor inferior de 3 y un valor superior de 3. Esto significa todos los minutos entre las 3 y las 3:59. Especificar un valor inferior de 3 y un valor superior de 4 cubriría el periodo de dos horas desde las 3:00 a las 4:59.

conexiones

Un entero. El valor por omisión es 2 elevado a la potencia 32 menos 1.

activas Un entero. El valor por omisión es 2 elevado a la potencia 32 menos 1.

puerto Un entero. El valor por omisión es 65535.

anchobanda reservado

Valor entero (kilobytes por segundo). El valor por omisión es 2 elevado a la potencia 32 menos 1.

priority

El orden en el que se comprobarán las normas.

nivel

Un entero. Si no especifica la prioridad de la primera norma que añada, Dispatcher la establecerá por omisión en 1. Cuando se añada una norma nueva, la prioridad por omisión se calcula como 10 + la prioridad más baja actual de todas las normas existentes. Por ejemplo, supongamos que tiene una norma con prioridad 30. Añade una nueva norma y establece la prioridad de la misma en 25 (por tanto, una prioridad *mayor* que 30). A continuación añade una tercera norma sin establecer ninguna prioridad. La prioridad de la tercera norma se calcula como 40 (30 + 10).

pattern

Especifica el patrón que se utilizará para una norma de tipo de contenido.

patrón

El patrón que se utilizará. Para obtener más información sobre los valores válidos, consulte “Apéndice C. Sintaxis de la norma de contenido (patrón):” en la página 313.

tos

Especifica el valor de “tipo de servicio” (TOS) utilizado por la norma de tipo **service**.

Nota: TOS sólo es aplicable al componente Dispatcher.

valor

La serie de 8 caracteres que se utilizará para el valor TOS, siendo los caracteres válidos: 0 (cero binario), 1 (uno binario) y x (no importa). Por ejemplo: 0xx1010x. Para obtener más información, consulte “Utilización de normas basadas en el tipo de servicio (TOS)” en la página 177.

stickytime

Especifica el valor de stickytime que se utilizará para una norma. Si establece el parámetro affinity en “activecookie” en el mandato rule, debe establecer el parámetro stickytime en un valor distinto de cero para habilitar este tipo de afinidad. El valor de stickytime en la norma no se aplica a los tipos de normas de afinidad “passivecookie” ni “uri”.

En “Afinidad activa de cookie” en la página 193 hallará más información.

Nota: El valor stickytime de norma sólo se aplica al componente CBR.

tiempo

El tiempo en segundos.

affinity

Especifica el tipo de afinidad a utilizar para una norma: afinidad activa de cookie, afinidad pasiva de cookie, afinidad de URI o ninguna.

El tipo de afinidad “activecookie” permite repartir el tráfico Web con afinidad por el mismo servidor basándose en los cookies generados por Network Dispatcher.

El tipo de afinidad “passivecookie” permite repartir el tráfico Web con afinidad por el mismo servidor basándose en los cookies autodefinidos generados por los servidores. Debe utilizarse el parámetro cookienam e junto con la afinidad pasiva de cookie.

La afinidad de tipo URI le permite repartir el tráfico Web hacia servidores caching-proxy y aumentar de forma efectiva el tamaño de la antememoria.

Consulte la sección “Afinidad activa de cookie” en la página 193, la sección “Afinidad pasiva de cookie” en la página 194 y la sección “Afinidad de URI” en la página 195 para obtener más información.

Nota: Affinity es aplicable a las normas configuradas con el método de reenvío cbr del componente Dispatcher y al componente CBR.

tipo_afinidad

Los tipos de afinidad posibles son: none (valor por omisión), activecookie, passivecookie o uri.

cookienam e

Es un nombre arbitrario definido por el administrador y que sirve de identificador para Network Dispatcher. Es el nombre que Network Dispatcher debe buscar en la cabecera HTTP de la petición del cliente. El

nombre del cookie, junto con el valor del cookie, sirven de identificador para Network Dispatcher y permiten que éste envíe a la misma máquina servidor las peticiones subsiguientes de un sitio Web. El nombre de cookie sólo es aplicable con la afinidad "pasiva de cookie".

En "Afinidad pasiva de cookie" en la página 194 hallará más información.

Nota: El nombre de cookie es aplicable a las normas configuradas con el método de reenvío cbr del componente Dispatcher y al componente CBR.

valor

Es el valor del nombre de cookie.

evaluate

Esta opción sólo está disponible en el componente Dispatcher. Especifica si la condición de la norma se debe evaluar para todos los servidores del puerto o para los servidores comprendidos en la norma. Esta opción sólo es válida para las normas de toma de decisiones basadas en características de los servidores, tales como las normas de conexiones totales, conexiones activas y de ancho de banda reservado. Para obtener más información, consulte "Opción de evaluación de servidor para normas" en la página 182.

nivel

Los valores posibles son puerto y norma. El valor por omisión es puerto.

sharelevel

Este parámetro sólo puede utilizarse para la norma de ancho de banda compartido. Especifica si se debe compartir ancho de banda a nivel de cluster o de ejecutor. El compartimiento de ancho de banda a nivel de cluster permite el uso compartido de la cantidad máxima de ancho de banda por varios puertos de un mismo cluster. El compartimiento de ancho de banda a nivel de ejecutor permite el uso compartido de la cantidad máxima de ancho de banda por los clusters de la configuración completa de Dispatcher. Para obtener más información, consulte "Norma del ancho de banda compartido" en la página 179.

nivel

Los valores posibles son ejecutor y cluster.

dropserver

Elimina un servidor de un conjunto de normas.

servidor

La dirección IP de la máquina servidor TCP expresada como nombre simbólico o en formato decimal con puntos.

O bien, si ha utilizado el particionamiento de servidores, utilice el nombre exclusivo del servidor lógico. En "Particionamiento del servidor:

servidores lógicos configurados para un solo servidor físico (dirección IP)” en la página 152 hallará más información.

Nota: Los servidores adicionales se separan mediante un signo más (+).

remove

Elimina una o más normas, separadas entre sí con signos más.

report

Visualiza los valores internos de una o más normas.

set

Establece valores para esta norma.

status

Visualiza los valores configurables de una o más normas.

useserver

Inserta servidores en un conjunto de normas.

Ejemplos

- Para añadir una norma que siempre será verdadera, no especifique el inicio ni el final de rango:
`ndcontrol rule add 9.37.67.100:80:trule type true priority 100`
- Para crear una norma que prohíba el acceso a un rango de direcciones IP, en este caso aquellas que comienzan con “9”:
`ndcontrol rule add 9.37.131.153:80:ni type ip b 9.0.0.0 e 9.255.255.255`
- Para crear una norma que especifique la utilización de un servidor dado desde las 11:00 a las 15:00:
`ndcontrol rule add cluster1:80:timerule type time beginrange 11 endrange 14`
`ndcontrol rule useserver cluster1:80:timerule server05`
- Para crear una norma basada en el contenido del campo de bytes TOS en la cabecera IP:
`ndcontrol rule add 9.67.131.153:80:tosrule type service tos 0xx1001x`

- Para crear una norma basada en ancho de banda reservado que asignará un grupo de servidores (evaluados dentro de la norma) para entregar datos a una velocidad de 100 kylobytes por segundo:

```
ndcontrol rule add 9.67.131.153:80:rbwrule type reservedbandwidth
beginrange 0 endrange 100 evaluate rule
```

- El mandato siguiente crea una norma basada en el ancho de banda compartido que ocupará ancho de banda no utilizado a nivel de cluster. (Nota: primero debe especificar el ancho de banda máximo (kilobytes por segundo) que se puede compartir a nivel de cluster, utilizando el mandato `ndcontrol cluster`)

```
ndcontrol cluster set 9.67.131.153 sharedbandwidth 200
```

```
ndcontrol rule add 9.67.131.153:80:shbwrule type sharedbandwidth
sharelevel cluster
```

ndcontrol server — configurar servidores



add

Añade este servidor.

cluster

La dirección del cluster expresada como nombre simbólico o en formato decimal con puntos. Puede utilizar un signo de dos puntos (:) como comodín. Por ejemplo, el mandato `ndcontrol server add :80:ServerA` añade el servidor ServerA al puerto 80 para todos los clusters.

Nota: Los clusters adicionales se separan mediante un signo más (+).

puerto

El número del puerto. Puede utilizar un signo de dos puntos (:) como comodín. Por ejemplo, el mandato `ndcontrol server add ::ServerA` añade el servidor ServerA a todos los puertos para todos los clusters.

Nota: Los puertos adicionales se separan mediante un signo más (+).

servidor

El parámetro **server** es la dirección IP exclusiva del servidor TCP expresada como nombre simbólico o en formato decimal con puntos.

O bien, si utiliza un nombre exclusivo que no da lugar a una dirección IP, debe proporcionar el parámetro **address** en el mandato **ndcontrol server add**. En “Particionamiento del servidor: servidores lógicos configurados para un solo servidor físico (dirección IP)” en la página 152 hallará más información.

Nota: Los servidores adicionales se separan mediante un signo más (+).

address

Es la dirección IP exclusiva del servidor TCP expresada como nombre de sistema principal o en el formato decimal con puntos. Si el nombre del servidor no se puede resolver, debe proporcionar la dirección del servidor físico. En “Particionamiento del servidor: servidores lógicos configurados para un solo servidor físico (dirección IP)” en la página 152 hallará más información.

dirección

Es el valor de la dirección del servidor.

collocated

La opción “collocated” (ubicación compartida) le permite especificar si si Network Dispatcher se instala en una de las máquinas servidor para las que Dispatcher realiza el reparto del tráfico. La opción “collocated” no es aplicable a la plataforma Windows 2000.

Nota: El parámetro “collocated” sólo es válido cuando se utilizan los métodos de reenvío mac o nat de Dispatcher. Mailbox Locator, Site Selector y Cisco Consultant pueden tener ubicación compartida en todas las plataformas, pero no necesitan esta palabra clave. Para obtener más información, consulte “Utilización de servidores de ubicación compartida” en la página 155.

valor

Valor de collocated: sí o no. El valor por omisión es no.

sticky

Permite que un servidor altere temporalmente en su puerto el valor de tiempo de persistencia. Con el valor por omisión, “sí”, el servidor conserva la afinidad normal que se ha definido en el puerto. Con el valor “no”, el cliente *no* regresará a dicho servidor la próxima vez que emita una petición en este puerto, cualquiera que sea el valor del tiempo de persistencia (stickytime) del puerto. Esto es útil en determinadas situaciones en las que se utilizan normas. Para obtener más información, consulte “Alteración temporal de afinidad de norma” en la página 191.

valor

Valor de persistencia: sí o no. El valor por omisión es sí.

weight

Es un número del 0 al 100 que representa el peso asignado al servidor (pero sin exceder el peso máximo especificado para el puerto). Si se establece el peso a cero se impedirá el envío de nuevas peticiones al servidor, pero no finalizará las conexiones actualmente activas para dicho

servidor. El valor por omisión es la mitad del peso máximo especificado para el puerto. Si el gestor está en ejecución, este valor se sobrescribirá rápidamente.

valor

Es el valor del peso asignado al servidor.

fixedweight

La opción `fixedweight` le permite especificar si desea modificar o no el peso del servidor. Si establece el valor de `fixedweight` en sí, cuando el gestor se ejecuta no se le permitirá modificar el peso del servidor. Para obtener más información, consulte el apartado “Pesos fijos del gestor” en la página 137.

valor

Valor de `fixedweight`: sí o no. El valor por omisión es no.

mapport

Correlaciona el número del puerto de destino de la petición del cliente con el número de puerto que Dispatcher utiliza para repartir el tráfico de la petición del cliente. Permite que Network Dispatcher reciba la petición de un cliente en un puerto y la envíe a un puerto diferente del servidor. Mediante `mapport`, puede repartir el tráfico de las peticiones de un cliente hacia un servidor donde se pueden estar ejecutando varios daemons de servidor.

Nota: El parámetro `mapport` es aplicable a Dispatcher (cuando se utilizan los métodos de reenvío `nat` o `cbr`) y a CBR. Para Dispatcher, consulte “Método de reenvío `nat` del Dispatcher” en la página 50 y “Encaminamiento por contenido mediante Dispatcher (método de reenvío `cbr`)” en la página 52. Para CBR, consulte “Reparto del tráfico entre el cliente y el proxy en CBR y entre el proxy y el servidor en HTTP” en la página 78.

valor_puerto

Es el valor del número de puerto de correlación. El valor por omisión es el número del puerto de destino de la petición del cliente.

router

Si está configurando una red de área amplia, es la dirección del encaminador que conduce hacia el servidor remoto. El valor por omisión es 0, que indica un servidor local. Observe que una vez que se ha establecido la dirección del encaminador del servidor en un valor distinto de cero (lo que denota un servidor remoto), no puede restaurar este valor a 0 para hacer que el servidor vuelva a ser local. Para ello, debe eliminar el servidor y añadirlo de nuevo sin especificar una dirección de encaminador. Igualmente, un servidor definido como local (dirección de encaminador = 0) no se puede convertir en remoto cambiando la dirección

del encaminador. Debe eliminar el servidor y añadirlo de nuevo. En “Configurar el soporte de Dispatcher para área amplia” en la página 157 hallará más información.

Nota: El parámetro router sólo es aplicable a Dispatcher. Si desea utilizar los métodos de reenvío nat o cbr, debe especificar la dirección del encaminador cuando añada un servidor a la configuración.

dirección

El valor de la dirección del encaminador.

cookievalue

Cookievalue (valor de cookie) es un valor arbitrario que representa el extremo servidor del par nombre de cookie / valor de cookie. El valor de cookie, junto con el nombre de cookie, sirve de identificador y permite que Network Dispatcher envíe hacia el mismo servidor las peticiones subsiguientes del cliente. En “Afinidad pasiva de cookie” en la página 194 hallará más información.

Nota: El parámetro cookievalue es válido para Dispatcher (cuando se utiliza el método de reenvío cbr) y para CBR.

valor

Es un valor arbitrario. Por omisión no se utiliza ningún valor de cookie.

returnaddress

Es una dirección IP exclusiva o nombre de sistema principal. Es una dirección que se configura en la máquina Dispatcher y que éste utiliza como dirección de origen cuando reparte el tráfico de las peticiones de los clientes hacia el servidor. De esta forma se asegura que el servidor devuelva el paquete a Dispatcher para procesar el contenido de la petición, en lugar de enviar el paquete directamente al cliente. (Seguidamente, Dispatcher reenviará el paquete IP al cliente). Debe especificar la dirección de retorno (returnaddress) cuando añada el servidor. Para cambiar la dirección de retorno debe primero eliminar el servidor y luego añadirlo de nuevo. La dirección de retorno no puede ser la misma que la dirección de cluster, la dirección de servidor ni la dirección NFA.

Nota: El parámetro returnaddress sólo es aplicable a Dispatcher. Si desea utilizar los métodos de reenvío nat o cbr, debe especificar la dirección del devolución.

dirección

Es el valor de la dirección de retorno.

advisorrequest

El asesor HTTP utiliza la cadena de texto de petición para consultar el estado de los servidores. Este parámetro sólo es válido para los servidores

sobre los que se informa mediante el asesor HTTP. Para que este valor sea efectivo debe iniciar el asesor HTTP. En “Opción de petición/respuesta del asesor HTTP (URL)” en la página 154 hallará más información.

Nota: El parámetro `advisorrequest` es aplicable a los componentes Dispatcher y CBR.

cadena_caracteres

Es el valor de la cadena de caracteres utilizada por el asesor HTTP. El valor por omisión es HEAD / HTTP/1.0.

Nota: Si la serie contiene un blanco —

- Cuando se emite el mandato desde el indicador de shell **ndcontrol**>>, debe encerrar la serie de caracteres entre comillas. Por ejemplo: **server set cluster:puerto:servidor advisorrequest "head / http/2.0"**
- Cuando emite el mandato **ndcontrol** desde el indicador del sistema operativo, debe preceder el texto de `"\"` y seguirlo de `\""`. Por ejemplo: **ndcontrol server set cluster:puerto:servidor advisorrequest "\"head / http/2.0\""**

advisorresponse

Es la cadena de texto de respuesta que el asesor HTTP busca en la respuesta HTTP. Este parámetro sólo es válido para los servidores sobre los que se informa mediante el asesor HTTP. Para que este valor sea efectivo debe iniciar el asesor HTTP. En “Opción de petición/respuesta del asesor HTTP (URL)” en la página 154 hallará más información.

Nota: El parámetro `advisorresponse` es aplicable a los componentes Dispatcher y CBR.

cadena_caracteres

Es el valor de la cadena de caracteres utilizada por el asesor HTTP. El valor por omisión es la cadena nula.

Nota: Si la serie contiene un blanco —

- Cuando se emite el mandato desde el indicador de shell **ndcontrol**>>, debe encerrar la serie de caracteres entre comillas.
- Cuando emite el mandato **ndcontrol** desde el indicador del sistema operativo, debe preceder el texto de `"\"` y seguirlo de `\""`.

down

Marca este servidor como inactivo. Este mandato interrumpe todas las conexiones activas con ese servidor e impide el envío de otras conexiones o paquetes al mismo.

remove

Elimina este servidor.

report

Informa sobre este servidor.

set

Establece valores para este servidor.

status

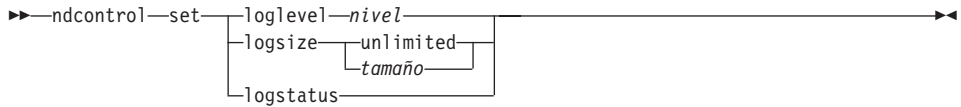
Muestra el estado de los servidores.

up Marca este servidor como activo. Dispatcher enviará ahora conexiones nuevas a ese servidor.

Ejemplos

- Para añadir el servidor con dirección 27.65.89.42 al puerto 80 de la dirección de cluster 130.40.52.153:
`ndcontrol server add 130.40.52.153:80:27.65.89.42`
- Para que el servidor de la dirección 27.65.89.42 sea un servidor sin persistencia (la característica de alteración temporal de afinidad de norma):
`ndcontrol server set 130.40.52.153:80:27.65.89.42 sticky no`
- Para marcar como inactivo el servidor situado en 27.65.89.42:
`ndcontrol server down 130.40.52.153:80:27.65.89.42`
- Para eliminar el servidor situado en 27.65.89.42 para todos los puertos de todos los clusters:
`ndcontrol server remove ::27.65.89.42`
- Para que el servidor de la dirección 27.65.89.42 tenga una ubicación compartida (el servidor reside en la misma máquina que Network Dispatcher):
`ndcontrol server set 130.40.52.153:80:27.65.89.42 collocated yes`
- Para establecer en 10 el peso del servidor 27.65.89.42 en el puerto 80 de la dirección de cluster 130.40.52.153:
`ndcontrol server set 130.40.52.153:80:27.65.89.42 weight 10`
- Para marcar el servidor con dirección 27.65.89.42 como activo:
`ndcontrol server up 130.40.52.153:80:27.65.89.42`
- Para añadir un servidor remoto:
`ndcontrol server add 130.40.52.153:80:130.60.70.1 router 130.140.150.0`
- Para permitir que el asesor HTTP consulte una petición de URL HTTP HEAD / HTTP/2.0 para el servidor 27.65.89.42 en el puerto HTTP 80.:
`ndcontrol server set 130.40.52.153:80:27.65.89.42 advisorrequest "\"HEAD / HTTP/2.0\""`

ndcontrol set — configurar anotaciones de servidor



loglevel

El nivel al que el mandato ndserver anota sus actividades.

nivel

El valor por omisión de **loglevel** es 0. El rango es 0–5. Los valores posibles son: 0 para None, 1 para Minimal, 2 para Basic, 3 para Moderate, 4 para Advanced, 5 para Verbose.

logsize

El número máximo de bytes que deben anotarse en el archivo de anotaciones.

tamaño

El valor por omisión de logsize es 1 MB.

logstatus

Muestra los valores referentes al archivo de anotaciones del servidor (nivel de registro de anotaciones y tamaño del archivo de anotaciones).

ndcontrol status — visualizar si el gestor y los asesores están en funcionamiento

➤—ndcontrol—status—➤

Ejemplos

- Para ver lo que está en funcionamiento:
ndcontrol status

Este mandato produce una salida similar a la siguiente:

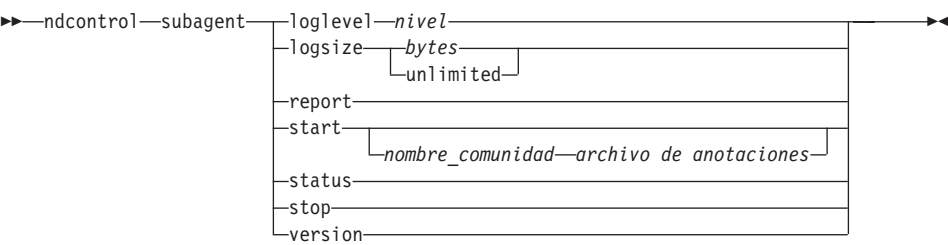
Executor has been
started.
Manager has been started.

ADVISOR	PORT	TIMEOUT

reach	0	unlimited
http	80	unlimited
ftp	21	unlimited

ndcontrol subagent — configurar subagente SNMP

Nota: Los diagramas de sintaxis para el mandato Ndcontrol subagent no son aplicables a CBR ni a Mailbox Locator.



loglevel

El nivel al que el subagente anota sus actividades en un archivo.

nivel

Número del nivel (0 a 5). Cuanto mayor es el número, más información se graba en el archivo de anotaciones del gestor. El valor por omisión es 1. Los valores posibles son: 0 para None, 1 para Minimal, 2 para Basic, 3 para Moderate, 4 para Advanced, 5 para Verbose.

logsize

Defina el tamaño máximo de bytes que se anotarán en el archivo de anotaciones del subagente. El valor por omisión es 1 MB.Si establece el tamaño máximo para el archivo de anotaciones, el archivo se sobregrabará cuando esté lleno. Cuando el archivo alcance el tamaño especificado, las entradas subsiguientes se grabarán a partir del comienzo del archivo, sobre las entradas de anotaciones anteriores. El tamaño del archivo de anotaciones no puede ser menor que el tamaño actual del archivo. En las entradas de anotaciones figura la indicación de la hora, de forma que puede establecerse el orden en que se han grabado. Cuanto más alto sea el nivel de las anotaciones, más cuidadosamente debe elegirse el tamaño de las mismas, ya que puede quedarse rápidamente sin espacio si efectúa anotaciones a los niveles más altos.

bytes

El tamaño máximo en bytes del archivo de anotaciones del subagente. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Puede que el archivo de anotaciones no alcance el tamaño máximo exacto antes de sobrescribirse, ya que las propias entradas de anotaciones varían en tamaño. El valor por omisión es "unlimited".

report

Visualiza un informe instantáneo de estadísticas.

start

Arranca el subagente.

nombre_comunidad

Nombre del valor SNMP del nombre de comunidad que puede utilizar como contraseña de seguridad. El valor por omisión es public.

archivo_de anotaciones

Nombre de archivo en el que se anotan los datos del subagente. En cada registro de las anotaciones figurará la indicación de la hora. El nombre por omisión es subagent.log. El archivo por omisión se instalará en el directorio **logs**. Consulte el “Apéndice F. Ejemplos de archivos de configuración” en la página 377. Para cambiar el directorio en el que se conservarán los archivos de anotaciones, consulte “Cambio de la vía de acceso de los archivos de anotaciones” en la página 208.

status

Muestra el estado actual de todos los valores del subagente SNMP que pueden establecerse globalmente y sus valores por omisión.

version

Muestra la versión actual del subagente.

Ejemplos

- Para arrancar el subagente con un nombre de comunidad de bigguy:
`ndcontrol subagent start bigguy bigguy.log`

Apéndice C. Sintaxis de la norma de contenido (patrón):

Este apéndice describe cómo utilizar la sintaxis de norma de contenido (patrón) para el componente CBR y el método de envío cbr del componente Dispatcher, junto con escenarios y ejemplos de su uso.

Sintaxis de la norma de contenido (patrón):

Sólo es aplicable si ha seleccionado "content" para el tipo de norma.

Entre la sintaxis del patrón que desea utilizar, siguiendo las siguientes restricciones

- no se pueden utilizar espacios en el patrón
- caracteres especiales, a no ser que preceda el carácter con una barra inclinada invertida (\)::
 - * carácter comodín (representa un número cualquiera de caracteres)
 - (paréntesis izquierdo utilizado para la agrupación lógica
 -) paréntesis derecho utilizado para la agrupación lógica
 - & AND lógico
 - | OR lógico
 - ! NOT lógico

Palabras clave reservadas

Las palabras clave reservadas van siempre seguidas por un signo igual ("=").

Method

es el método HTTP utilizado en la petición, por ejemplo, GET, POST, etc.

URI es la ruta de acceso de la petición URL

Version

es la versión específica de la petición, que puede ser HTTP/1.0 o HTTP/1.1

Host valor procedente del sistema principal: cabecera.

Nota: Opcional en los protocolos HTTP/1.0

<clave>

es cualquier nombre válido de cabecera HTTP que pueda ser

examinada por Dispatcher. Son ejemplos de cabeceras HTTP: User-Agent, Connection, Referer, etc.

Un navegador que apunte a `http://www.company.com/path/webpage.htm` puede producir valores tales como:

```
Method=GET
URI=/path/webpage.htm
Version=/HTTP/1.1
Host=www.company.com
Connection=Keep-Alive
Referer=http://www.company.com/path/parentwebpage.htm
```

Nota: El shell del sistema operativo puede interpretar caracteres especiales, como "&", y convertirlos en texto alternativo antes de que **cbrcontrol** los evalúe.

Por ejemplo, el siguiente mandato sólo es válido cuando se utiliza el indicador **cbrcontrol**>>.

```
rule add 10.1.203.4:80:cbr_prod_rule_ek type content
pattern client=181.0.153.222&uri=http://10.1.203.4/nipoek/*
```

Cuando se utilizan caracteres especiales, para que este mismo mandato funcione en el indicador del sistema operativo se debe encerrar el patrón entre dobles comillas (" ") del siguiente modo:

```
cbrcontrol rule add 10.1.203.4:80:cbr_prod_rule_ek type content
pattern "client=181.0.153.222&uri=http://10.1.203.4/nipoek/*"
```

Si no se utilizan las comillas, puede truncarse parte del patrón cuando se guarde la norma en CBR. Tenga en cuenta que las comillas no están soportadas cuando se utiliza el indicador de mandatos **cbrcontrol**>>.

A continuación siguen varios casos prácticos y ejemplos sobre la utilización de sintaxis de patrones

Caso 1:

La instalación para un solo nombre de cluster comprende un grupo de servidores Web para contenido HTML estándar, otro grupo de servidores Web con WebSphere Application Server para peticiones de servlet, otro grupo de servidores Lotus Notes para archivos NSF, etc. Es necesario el acceso a los datos del cliente para diferenciar entre esas páginas solicitadas. También es necesario enviarlas a los servidores apropiados. Las normas para la comparación de patrones de contenido proporcionan la separación necesaria para realizar esas tareas. Se configuran una serie de normas para que se produzca automáticamente la separación necesaria de las peticiones. Por ejemplo, los mandatos siguientes llevan a cabo las tres separaciones mencionadas:

```
>>rule add cluster1:80:servlets type content pattern uri=*/servlet/*priority 1
>>rule uses cluster1:80:servlets server1+server2

>>rule add cluster1:80:notes type content pattern uri=*.nsf* priority 2
>>rule uses cluster1:80:notes server3+server4

>>rule add cluster1:80:regular type true priority 3
>>rule uses cluster1:80:regular server5+server6
```

Si Network Dispatcher recibe una petición para un archivo NSF, se prueba primero la norma para servlets, pero no se produce coincidencia. Luego la petición se prueba con la norma de notes y se obtiene una coincidencia. El tráfico del cliente se reparte entre server3 y server4.

Caso 2

Otro caso habitual es aquél en el que el sitio Web principal controla varios grupos internos diferenciados. Por ejemplo, `www.company.com/software` comprende un grupo de servidores y contenido que son diferentes de la división `www.company.com/hardware`. Debido a que las peticiones están todas basadas en el cluster raíz `www.company.com`, son necesarias normas de contenido para encontrar las diferencias de URI y efectuar el reparto del tráfico. La norma de este caso práctico tiene este aspecto:

```
>>rule add cluster1:80:div1 type content pattern uri=/software/* priority 1
>>rule uses cluster1:80:div1 server1+server2

>>rule add cluster1:80:div2 type content pattern uri=/hardware/* priority 2
>>rule uses cluster1:80:div2 server3+server4
```

Caso 3

Determinadas combinaciones son sensibles al orden en el que se buscan las normas. Por ejemplo, en el Caso 2, los clientes se repartieron de acuerdo con un directorio existente en la ruta de la petición; pero el directorio de destino puede aparecer en varios niveles de la ruta y tener significados diferentes según la ubicación. Por ejemplo, `www.company.com/pcs/fixes/software` representa un destino diferente que `www.company.com/mainframe/fixes/software`. Las normas se deben definir teniendo en cuenta esta posibilidad y no pretender abarcar demasiados casos al mismo tiempo. Por ejemplo, la especificación `"uri=*/software/*"` es una búsqueda general demasiado amplia en este caso. Se podrían estructurar normas alternativas de la manera indicada a continuación:

La siguiente búsqueda de combinación puede limitar el ámbito de la búsqueda:

```
>>rule add cluster1:80:pcs type content pattern (uri=/pcs/*)&(uri=*/software/*)
>>rule uses cluster 1:80:pcs server1
```

Cuando no hay combinaciones para utilizar, el orden se convierte en una cuestión importante:

```
>>rule add cluster1:80:pc1 type content pattern uri=/pcs/*  
>>rule uses cluster1:80:pc1 server2
```

La segunda norma se aplica cuando “pcs” aparece en lugares posteriores de la ruta de directorios en lugar de aparecer en primer lugar.

```
>>rule add cluster1:80:pc2 type content pattern uri=/*/pcs/*  
>>rule uses cluster1:80:pc2 server3
```

En la mayoría de los casos, es conveniente finalizar las normas con una norma **siempre cierto** para abarcar las situaciones no cubiertas por las demás normas. Esto también puede adoptar la forma de una respuesta del tipo “El sitio Web está actualmente fuera de servicio; pruebe más tarde”, cuando todos los demás servidores no atienden la petición del cliente.

```
>>rule add cluster1:80:sorry type true priority 100  
>>rule uses cluster1:80:sorry server5
```

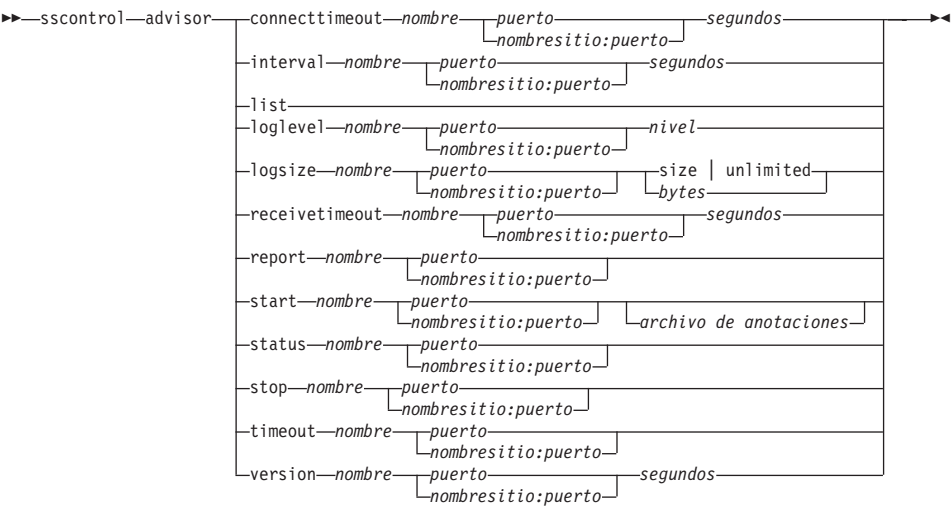
Apéndice D. Consulta de mandatos de Site Selector

Este apéndice describe cómo utilizar los siguientes mandatos **sscontrol** de Site Selector:

- “**sscontrol advisor** — controlar el asesor” en la página 318
- “**sscontrol file** — gestionar archivos de configuración” en la página 324
- “**sscontrol help** — visualizar o imprimir ayuda para el mandato” en la página 326
- “**sscontrol manager** — controlar el gestor” en la página 327
- “**sscontrol metric** — configurar métricas del sistema” en la página 332
- “**sscontrol nameserver** — controlar el servidor de nombres” en la página 333
- “**sscontrol rule** — configurar normas” en la página 334
- “**sscontrol server** — configurar servidores” en la página 338
- “**sscontrol set** — configurar archivo de anotaciones del servidor” en la página 340
- “**sscontrol sitename** — configurar un nombre de sitio” en la página 341
- “**sscontrol status** — visualizar si el gestor y los asesores están en ejecución” en la página 345

Puede especificar una versión abreviada de los parámetros de los mandatos **sscontrol**. Sólo necesita especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato “file save”, puede entrar **sscontrol he f** en lugar de **sscontrol help file**.

Nota: Los valores de los parámetros de mandatos se deben escribir en caracteres ingleses. Las únicas excepciones son los nombres de sistema principal (utilizados en los mandatos para clusters y servidores) y los nombres de archivo (utilizados en los mandatos sobre archivos).



connecttimeout

Establece el tiempo que un asesor espera antes de notificar un error de conexión con un servidor. Para obtener más información, consulte “Tiempo de espera de conexión y de recepción del asesor para servidores” en la página 142.

nombre

Nombre del asesor. Los valores posibles son **http**, **ftp**, **ssl**, **smtp**, **imap**, **pop3**, **nntp**, **telnet**, **connect**, **ping**, **WLM** y **WTE**. Los nombres de los asesores personalizados se encuentran en el formato **xxxx**, donde **ADV_xxxx** es el nombre de la clase que implementa el asesor personalizado.

puerto

Número del puerto que el asesor está supervisando.

segundos

Es un valor entero positivo que representa el tiempo, en segundos, que un asesor espera antes de notificar un error de conexión con un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

interval

Establece la frecuencia con la que el asesor obtiene información sobre los servidores.

segundos

Es un número entero positivo que representa el número de segundos transcurridos entre las peticiones de estado hechas a los servidores. El valor por omisión es 7.

list

Muestra una lista de los asesores que están actualmente suministrando información al gestor.

loglevel

Establece el nivel de anotaciones del archivo de anotaciones de un asesor.

nivel

Número del nivel (0 a 5). El valor por omisión es 1. Cuanto mayor es el número, más información se escribe en el archivo de anotaciones del asesor. Los valores posibles son:

- 0 para None
- 1 para Minimal
- 2 para Basic
- 3 para Moderate
- 4 para Advanced
- 5 para Verbose

.

logsize

Establece el tamaño máximo del archivo de anotaciones de un asesor. Si establece el tamaño máximo para el archivo de anotaciones, el archivo se sobrescribirá cuando esté lleno. Cuando el archivo alcance el tamaño especificado, las entradas subsiguientes se escribirán encima de las entradas de anotaciones anteriores. El tamaño del archivo de anotaciones no puede ser menor que el tamaño actual del archivo. Las entradas del archivo de anotaciones contienen una indicación horaria para poder determinar el orden en el que se escribieron. Cuanto más alto sea el nivel de registro de anotaciones, más cuidadosamente debe elegirse el tamaño del archivo, pues el espacio puede agotarse rápidamente cuando se efectúan anotaciones a los niveles más altos.

tamaño | unlimited

El tamaño máximo en bytes del archivo de anotaciones del asesor. Puede especificar un número positivo mayor que cero o **unlimited**. Es posible que el archivo de anotaciones no alcance el tamaño máximo exacto antes de sobregrabarse, ya que las propias entradas de anotaciones varían en tamaño. El valor por omisión es 1 MB.

receivetimeout

Establece el tiempo que un asesor espera antes de notificar un error de

recepción con un servidor. Para obtener más información, consulte “Tiempo de espera de conexión y de recepción del asesor para servidores” en la página 142.

segundos

Es un valor entero positivo que representa el tiempo, en segundos, que un asesor espera antes de notificar un error de recepción con un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

report

Muestra un informe sobre el estado del asesor.

start

Arranca el asesor. Hay asesores para cada protocolo. Los puertos por omisión son:

Nombre de asesor	Protocolo	Puerto
Connect	n/d	definido por el usuario
db2	privado	50000
ftp	FTP	21
http	HTTP	80
imap	IMAP	143
nntp	NNTP	119
PING	PING	0
pop3	POP3	110
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23

nombre

El nombre del asesor.

nombresitio:puerto

El valor de nombresitio es opcional en los mandatos de asesor, pero el valor de puerto es necesario. Si no se especifica el valor de nombresitio, el asesor empieza a ejecutarse en todos los nombres de sitio configurados disponibles. Si se especifica un nombresitio, el asesor empieza a ejecutarse únicamente para el nombresitio especificado. Los nombres de sitio adicionales se separan mediante el signo más (+).

archivo de anotaciones

Nombre de archivo en el que se anotan los datos de gestión. Cada registro del archivo de anotaciones contiene una indicación horaria.

El archivo por omisión es *nombreasesor_puerto.log*, por ejemplo, **http_80.log**. Para cambiar el directorio donde se guardan los archivos de anotaciones, consulte “Cambio de la vía de acceso de los archivos de anotaciones” en la página 208.

Puede iniciar un solo asesor para cada nombresitio.

status

Muestra el estado actual y los valores por omisión de todos los valores globales de un asesor.

stop

Detiene el asesor.

timeout

Establece el número de segundos durante los cuales el gestor considerará como válida la información procedente del asesor. Si el gestor detecta que la información del asesor es anterior a este tiempo de espera, el gestor no utilizará esa información para determinar los pesos de los servidores para el puerto que el asesor está supervisando. Una excepción a este tiempo de espera se produce cuando el asesor ha informado al gestor de que un servidor específico está fuera de servicio. El gestor utilizará esa información referente al servidor incluso después de que la información del asesor haya caducado.

segundos

Número positivo que representa el número de segundos o **unlimited**. El valor por omisión es "unlimited".

version

Muestra la versión actual del asesor.

Ejemplos

- Para establecer el tiempo (30 segundos) que un asesor HTTP (del puerto 80) espera antes de notificar un error de conexión con un servidor:
`sscontrol advisor connecttimeout http 80 30`
- Para establecer el intervalo del asesor FTP (para el puerto 21) en 6 segundos:
`sscontrol advisor interval ftp 21 6`
- Para visualizar la lista de asesores que actualmente suministran información al gestor:
`sscontrol advisor list`

Este mandato produce una salida similar a la siguiente:

ADVISOR	SITENAME:PORT	TIMEOUT
http	80	unlimited
ftp	21	unlimited

- Si desea cambiar el nivel de anotaciones del archivo de anotaciones del asesor http por 0 para el nombre de sitio "mysite" a fin de mejorar el rendimiento:
sscontrol advisor loglevel http mysite:80 0
- Si desea cambiar el tamaño del archivo de anotaciones del asesor ftp por 5000 bytes para el nombre de sitio "mysite":
sscontrol advisor logsize ftp mysite:21 5000
- Para establecer el tiempo (60 segundos) que un asesor HTTP (del puerto 80) espera antes de notificar un error de recepción con un servidor:
sscontrol advisor receivetimeout http 80 60
- Para visualizar un informe de estado del asesor ftp (para el puerto 21):
sscontrol advisor report ftp 21

Este mandato produce una salida similar a la siguiente:

Advisor Report:

```
-----  
Advisor name ..... http  
Port number ..... 80  
  
sitename ..... mySite  
Server address ..... 9.67.129.230  
Load ..... 8
```

- Para arrancar el asesor con el archivo ftpadv.log:
sscontrol advisor start ftp 21 ftpadv.log
- Para visualizar el estado actual de los valores asociados al asesor http:
sscontrol advisor status http 80

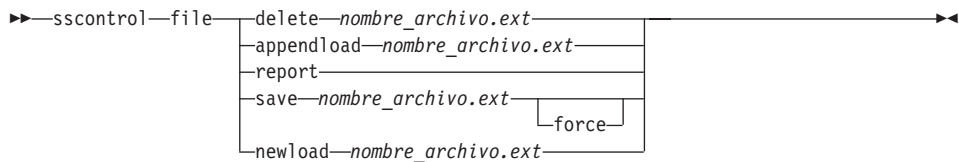
Este mandato produce una salida similar a la siguiente:

Advisor Status:

```
-----  
Interval (seconds) ..... 7  
Timeout (seconds) ..... Unlimited  
Connect timeout (seconds).....21  
Receive timeout (seconds).....21  
Advisor log filename ..... Http_80.log  
Log level ..... 1  
Maximum log size (bytes) ..... Unlimited
```

- Para detener el asesor http en el puerto 80:
`sscontrol advisor stop http 80`
- Para establecer el valor de tiempo de espera de la información del asesor en 5 segundos:
`sscontrol advisor timeout ftp 21 5`
- Para averiguar el número de la versión actual del asesor ssl:
`sscontrol advisor version ssl 443`

sscontrol file — gestionar archivos de configuración



delete

Elimina el archivo.

archivo.ext

Archivo de configuración.

La extensión del archivo (*.ext*) puede ser cualquiera que elija el usuario y es opcional.

appendload

Añade un archivo de configuración a la configuración actual y lo carga en Site Selector.

report

Informar acerca del archivo o archivos disponibles.

save

Guarda la configuración actual de Site Selector en el archivo.

Nota: Los archivos se guardan y cargan desde los directorios siguientes:

- AIX: `/usr/lpp/nd/servers/configurations/ss`
- Linux: `/opt/nd/servers/configurations/ss`
- Solaris: `/opt/nd/servers/configurations/ss`
- Windows 2000:

Vía de acceso común de directorio de instalación — `c:\Archivos de programa\ibm\edge\nd\servers\configurations\componente`

Vía de acceso nativa de directorio de instalación — `c:\Archivos de programa\ibm\nd\servers\configurations\componente`

force

Utilice **force** para guardar su archivo en un archivo existente del mismo nombre, el cual se suprime previamente. Si no utiliza la opción **force**, el archivo existente no se sobrescribe.

newload

Carga un nuevo archivo de configuración en Site Selector. El nuevo archivo de configuración sustituirá a la configuración actual.

Ejemplos

- Para suprimir un archivo:
`sscontrol file delete file3`

Se ha suprimido el archivo (file3).
- Para cargar un nuevo archivo de configuración con el que sustituir el archivo de configuración actual:
`sscontrol file newload file1.sv`

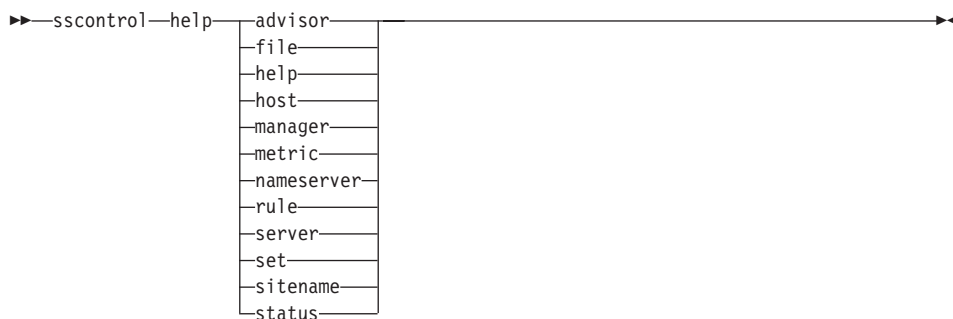
Se ha cargado el archivo (file1.sv) en Dispatcher.
- Para añadir un archivo de configuración a la configuración actual y cargarlo:
`sscontrol file appendload file2.sv`

Se ha añadido el archivo (file2.sv) a la configuración actual y se ha cargado.
- Para visualizar un informe de los archivos (esto es, aquellos archivos guardados anteriormente):
`sscontrol file report`

FILE REPORT:
file1.save
file2.sv
file3
- Para guardar la configuración en un archivo llamado file3:
`sscontrol file save file3`

La configuración se ha guardado en el archivo (file3).

sscontrol help — visualizar o imprimir ayuda para el mandato



Ejemplos

- Para obtener ayuda para el mandato sscontrol:

```
sscontrol help
```

Este mandato produce una salida similar a la siguiente:

```
HELP COMMAND ARGUMENTS:
```

```
-----
```

```
Usage:  help <help option>
```

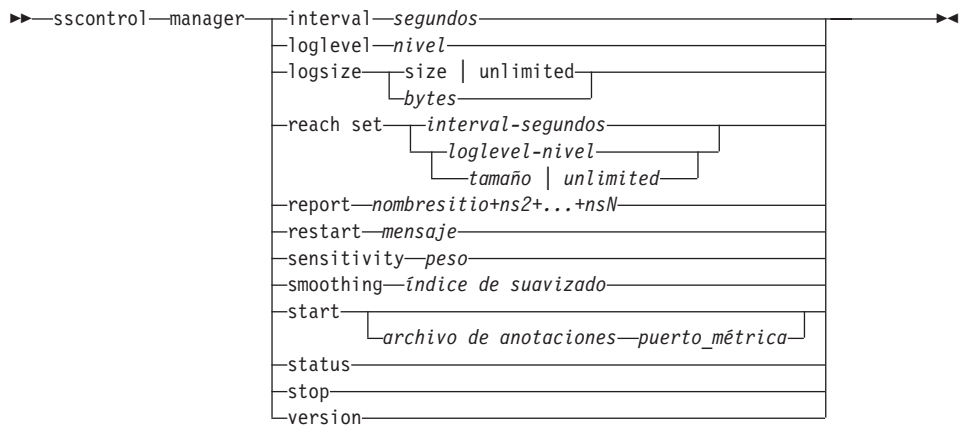
```
Example: help name
```

```
help          - print complete help text
advisor       - help on advisor command
file          - help on file command
host          - help on host command
manager       - help on manager command
metric        - help on metric command
sitename      - help on sitename command
nameserver    - help on nameserver command
rule          - help on rule command
server        - help on server command
set           - help on set command
status        - help on status command
```

Los parámetros especificados dentro de < > son variables.

- A veces, la ayuda mostrará opciones para las variables utilizando el signo | para separar las opciones:
logsize <número de bytes | unlimited>
-Establece el número máximo de bytes que se registrarán en el archivo de anotaciones.

sscontrol manager — controlar el gestor



interval

Establece la frecuencia con la que el gestor actualiza los pesos de los servidores.

segundos

Un número positivo que representa, en segundos, la frecuencia con la que el gestor actualiza los pesos. El valor por omisión es 2.

loglevel

Establece el nivel de anotaciones del archivo de anotaciones de gestor y del archivo de anotaciones de supervisor de métrica.

nivel

Número del nivel (0 a 5). Cuanto mayor es el número, más información se graba en las anotaciones del gestor. El valor por omisión es 1. Los valores posibles son:

- 0 para None
- 1 para Minimal
- 2 para Basic
- 3 para Moderate
- 4 para Advanced
- 5 para Verbose

logsize

Establece el tamaño máximo del archivo de anotaciones del gestor. Si establece el tamaño máximo para el archivo de anotaciones, el archivo se sobrescribirá cuando esté lleno. Cuando el archivo alcance el tamaño especificado, las entradas subsiguientes se escribirán a partir del comienzo del archivo, sobre las entradas de anotaciones anteriores. El tamaño del

archivo de anotaciones no puede ser menor que el tamaño actual del archivo. Las entradas del archivo de anotaciones contienen una indicación horaria para poder determinar el orden en el que se escribieron. Cuanto más alto sea el nivel de registro de anotaciones, más cuidadosamente debe elegirse el tamaño del archivo, pues el espacio puede agotarse rápidamente cuando se efectúan anotaciones a los niveles más altos.

bytes

El tamaño máximo en bytes del archivo de anotaciones del gestor. Puede especificar un número positivo mayor que cero o **unlimited**. Es posible que el archivo de anotaciones no alcance el tamaño máximo exacto antes de sobregrabarse, ya que las propias entradas de anotaciones varían en tamaño. El valor por omisión es 1 MB.

reach set

Establece el intervalo, nivel y tamaño de las anotaciones para el asesor de reach.

report

Visualiza un informe instantáneo de estadísticas.

nombresitio

El nombresitio que desea que se visualice en el informe. Éste es un nombre de sistema principal que no puede resolverse y que el cliente solicitará. El nombresitio debe ser un nombre de dominio totalmente calificado.

Nota: Los nombres de sitio adicionales se separan mediante el signo más (+).

restart

Rearranca todos los servidores (que no están inactivos) con pesos normalizados (1/2 del peso máximo).

mensaje

Un mensaje que desea grabar en el archivo de anotaciones del gestor.

sensitivity

Establece la sensibilidad mínima para que se actualicen los pesos. Este valor define cuándo el gestor debe cambiar la ponderación del servidor en función de la información externa.

peso

Un número del 0 al 100 que se utiliza como porcentaje de peso. El valor por omisión 5 crea una sensibilidad mínima del 5%.

smoothing

Establece un índice que corrige las variaciones de ponderación al repartir el tráfico. Cuanto más alto sea el índice de corrección, menos acusadamente cambiarán los pesos de los servidores cuando se

modifiquen las condiciones de la red. Un índice más bajo ocasionará que los pesos de los servidores se modifiquen más acusadamente.

índice

Un número positivo de coma flotante. El valor por omisión es 1,5.

start

Arranca el gestor.

archivo de anotaciones

Nombre de archivo en el que se anotan los datos del gestor. Cada registro del archivo de anotaciones contiene una indicación horaria.

El archivo por omisión se instala en el directorio **logs**. Consulte “Apéndice F. Ejemplos de archivos de configuración” en la página 377. Para cambiar el directorio donde se guardarán los archivos de anotaciones, consulte “Cambio de la vía de acceso de los archivos de anotaciones” en la página 208.

puerto_métrica

Puerto que Metric Server utiliza para informar de los niveles de tráfico del sistema. Si especifica un puerto de métrica, debe especificar un nombre de archivo de anotaciones. El puerto de métrica por omisión es 10004.

status

Muestra el estado actual y los valores por omisión de todos los valores globales del gestor.

stop

Detiene el gestor.

version

Muestra la versión actual del gestor.

Ejemplos

- Para establecer el intervalo de actualización del gestor a cada 5 segundos:
`sscontrol manager interval 5`
- Para establecer el nivel de anotaciones a 0 para mejorar el rendimiento:
`sscontrol manager loglevel 0`
- Para establecer el tamaño de las anotaciones del gestor a 1.000.000 bytes:
`sscontrol manager logsize 1000000`
- Para obtener una instantánea de las estadísticas del gestor:
`sscontrol manager report`

Este mandato produce una salida similar a la siguiente:

SERVER	STATUS
9.67.129.221	ACTIVE
9.67.129.213	ACTIVE
9.67.134.223	ACTIVE

MANAGER REPORT LEGEND	
CPU	CPU Load
MEM	Memory Load
SYS	System Metric
NOW	Current Weight
NEW	New Weight
WT	Weight

mySite	WEIGHT	CPU	49%	MEM	50%	PORT	1%	SYS	0%	
	NOW	NEW	WT	LOAD	WT	LOAD	WT	LOAD	WT	LOAD
9.37.56.180	10	10	-99	-1	-99	-1	-99	-1	0	0
TOTALS:	10	10		-1		-1		-1		0

ADVISOR	SITENAME:PORT	TIMEOUT
http	80	unlimited

- Para reiniciar todos los servidores con pesos normalizados y escribir un mensaje en el archivo de anotaciones del gestor:
sscontrol manager restart Restarting the manager to update code

Este mandato produce una salida similar a la siguiente:

320-14:04:54 Reiniciando el gestor para actualizar código

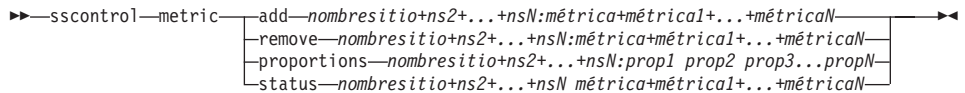
- Para establecer la sensibilidad a los cambios de peso a 10:
sscontrol manager sensitivity 10
- Para establecer el índice de corrección en 2.0:
sscontrol manager smoothing 2.0
- Para iniciar el gestor y especificar el archivo de anotaciones denominado ndmgr.log (la vía de acceso no puede establecerse)
sscontrol manager start ndmgr.log
- Para visualizar el estado actual de los valores asociados con el gestor:
sscontrol manager status

Este mandato produce una salida similar al ejemplo siguiente:

```
Manager
status:
=====
Metric port..... 10004
Manager log filename..... manager.log
Manager log level..... 1
Maximum manager log size (bytes)..... unlimited
Sensitivity level..... 5
Smoothing index..... 1.5
Update interval (seconds)..... 2
Weights refresh cycle..... 2
Reach log level..... 1
Maximum reach log size (bytes)..... unlimited
Reach update interval (seconds)..... 7
```

- Para detener el gestor:
sscontrol manager stop
- Para visualizar el número de la versión actual del gestor:
sscontrol manager version

sscontrol metric — configurar métricas del sistema



add

Añade la métrica especificada.

nombresitio

El nombresitio configurado. Los nombres de sitio adicionales se separan mediante el signo más (+).

métrica

Es el nombre de la métrica del sistema. Debe ser el nombre de un archivo ejecutable o de script contenido en el directorio de scripts de Metric Server.

remove

Elimina la métrica especificada.

proportions

Proportions determina el significado de cada métrica en comparación con las otras cuando se combinan en un solo valor de tráfico del sistema para un servidor.

status

Visualiza los valores actuales del servidor para esta métrica.

Ejemplos

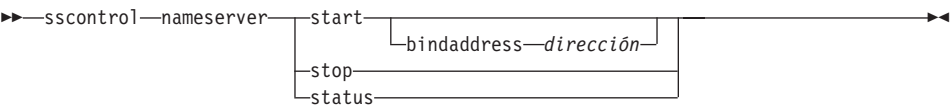
- Para añadir una métrica del sistema:
`sscontrol metric add sitel:metric1`
- Para establecer las proporciones de las dos métricas del sistema correspondientes a un sitio Web:
`sscontrol metric proportions sitel 0 100`
- Para visualizar el estado actual de los valores asociados a la métrica especificada:
`sscontrol metric status sitel:metric1`

Este mandato produce una salida similar a la siguiente:

Metric Status:

```
sitename ..... sitel
Metric name ..... metric1
Metric proportion ..... 50
  Server ..... 9.37.56.100
  Metric data .... -1
```

sscontrol nameserver — controlar el servidor de nombres



start
Inicia el servidor de nombres.

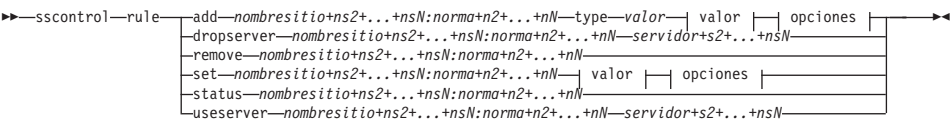
bindaddress
Inicia el servidor de nombres vinculado con la dirección especificada. El servidor de nombres sólo responderá a una petición destinada a esta dirección.

dirección
Una dirección (IP o simbólica) configurada en el sistema de Site Selector.

stop
Detiene el servidor de nombres.

status
Muestra el estado del servidor de nombres.

sscontrol rule — configurar normas



opciones:



add

Añade esta norma a un nombresitio.

nombresitio

Un nombre de sistema principal que no puede resolverse y que el cliente solicitará. El nombresitio debe ser un nombre de dominio totalmente calificado. Los nombres de sitio adicionales se separan mediante el signo más (+).

norma

El nombre que elige para la norma. Este nombre puede contener cualquier carácter alfanumérico, subrayados, guiones o puntos. Puede tener de 1 a 20 caracteres y no puede contener espacios en blanco.

Nota: Las normas adicionales se separan mediante un signo más (+).

type

El tipo de norma.

tipo

Las opciones para *tipo* son:

ip La norma se basa en la dirección IP del cliente.

metricall

La norma se basa en el valor de métrica actual para todos los servidores del grupo de servidores.

metricavg

La norma se basa en el promedio de los valores de métrica actuales para todos los servidores del grupo de servidores.

time La norma se basa en la hora del día.

true Esta norma es siempre cierta. Considérela como una sentencia `else` en lógica de programación.

beginrange

Valor inferior del rango utilizado para determinar si la norma es verdadera.

bajo

Depende del tipo de norma. El tipo de valor y su valor por omisión se listan a continuación por tipo de norma:

ip La dirección del cliente expresada como nombre simbólico o en formato decimal con puntos. El valor por omisión es 0.0.0.0.

hora Un entero. El valor por omisión es 0, que representa la medianoche.

métricatodos

Un entero. El valor por omisión es 100.

prométrica

Un entero. El valor por omisión es 100.

endrange

Valor superior en el rango utilizado para determinar si la norma es verdadera.

alto

Depende del tipo de norma. El tipo de valor y su valor por omisión se listan a continuación por tipo de norma:

ip La dirección del cliente expresada como nombre simbólico o en formato decimal con puntos. El valor por omisión es 255.255.255.254.

hora Un entero. El valor por omisión es 24, que representa la medianoche.

Nota: Cuando defina el valor inferior y superior del rango de intervalos de tiempo, tenga en cuenta que cada valor debe ser un entero representando únicamente la hora; no se especifican las porciones de la hora. Por esta razón, para especificar una sola hora—por ejemplo, la hora entre las 3:00 y las 4:00— especificaría un valor inferior de 3 y un valor superior de 3. Esto significa todos los minutos entre las 3 y las 3:59. Especificar un valor inferior de 3 y un valor superior de 4 cubriría el periodo de dos horas, desde las 3:00 a las 4:59.

métricatodos

Un entero. El valor por omisión es 2 elevado a la potencia 32 menos 1.

prommétrica

Un entero. El valor por omisión es 2 elevado a la potencia 32 menos 1.

priority

El orden en el que se comprobarán las normas.

nivel

Un entero. Si no especifica la prioridad de la primera norma que añade, Site Selector la establecerá por omisión en 1. Cuando se añada una norma nueva, la prioridad por omisión se calcula como 10 + la prioridad más baja actual de todas las normas existentes. Por ejemplo, supongamos que tiene una norma con prioridad 30. Añade una nueva norma y establece su prioridad en 25 (que es una una prioridad *mayor* que 30). A continuación añade una tercera norma sin establecer ninguna prioridad. La prioridad de la tercera norma se calcula como 40 (30 + 10).

metricname

Nombre de la métrica que se mide para una norma.

dropserver

Elimina un servidor de un conjunto de normas.

servidor

La dirección IP de la máquina servidor TCP expresada como nombre simbólico o en formato decimal con puntos.

Nota: Los nombres de sitio adicionales se separan mediante el signo más (+).

remove

Elimina una o más normas, separadas entre sí con signos más.

set

Establece valores para esta norma.

status

Visualiza todos los valores de una o más normas.

useserver

Inserta servidor en un conjunto de normas.

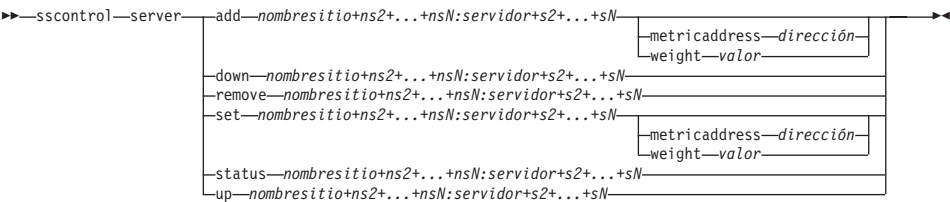
Ejemplos

- Para añadir una norma que siempre será verdadera, no especifique el inicio ni el final de rango:

```
sscontrol rule add nombresitio:nombrenorma type true priority 100
```

- Para crear una norma que prohíba el acceso a un rango de direcciones IP, que en este caso comienzan con "9":
`sscontrol rule add nombresitio:nombrenorma type ip b 9.0.0.0 e 9.255.255.255`
- Para crear una norma que especifique la utilización de un servidor dado desde las 11:00 a las 15:00:
`sscontrol rule add nombresitio:nombrenorma type time beginrange 11 endrange 14`
`sscontrol rule useserver nombresitio:nombrenorma server05`

sscontrol server — configurar servidores



add
Añade este servidor.

nombresitio
Un nombre de sistema principal que no puede resolverse y que el cliente solicita. El nombresitio debe ser un nombre de dominio totalmente calificado. Los nombres de sitio adicionales se separan mediante el signo más (+).

servidor
La dirección IP de la máquina servidor TCP expresada como nombre simbólico o en formato decimal con puntos.

Nota: Los servidores adicionales se separan mediante un signo más (+).

metricaddress
La dirección de Metric Server.

dirección
La dirección del servidor expresada como nombre simbólico o en formato decimal con puntos.

weight
Es un número del 0 al 100 (pero no mayor que el peso máximo del servidor especificado) que representa el peso asignado al servidor. Si establece el peso en cero, impedirá que se envíen nuevas peticiones al servidor. El valor por omisión es la mitad del peso máximo del servidor especificado. Si el gestor está en ejecución, este valor se sobrescribirá rápidamente.

valor
El valor de peso del servidor.

down
Marca este servidor como inactivo. Este mandato impide que se resuelvan otras peticiones para ese servidor.

remove
Elimina este servidor.

set

Establece valores para este servidor.

status

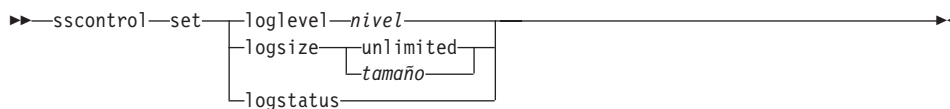
Muestra el estado de los servidores.

up Marca este servidor como activo. Site Selector resolverá ahora nuevas peticiones para ese servidor.

Ejemplos

- Para añadir el servidor situado en 27.65.89.42 al nombre de sitio "site1":
`sscontrol server add site1:27.65.89.42`
- Para marcar el servidor con dirección 27.65.89.42 como inactivo:
`sscontrol server down site1:27.65.89.42`
- Para eliminar el servidor situado en 27.65.89.42 para todos los nombres de sitio:
`sscontrol server remove :27.65.89.42`
- Para marcar como activo el servidor situado en 27.65.89.42:
`sscontrol server up site1:27.65.89.42`

sscontrol set — configurar archivo de anotaciones del servidor



loglevel

El nivel para el cual ssserver registra sus actividades.

nivel

El valor por omisión de **loglevel** es 0. Los valores posibles son:

- 0 para None
- 1 para Minimal
- 2 para Basic
- 3 para Moderate
- 4 para Advanced
- 5 para Verbose

logsize

El número máximo de bytes que deben anotarse en el archivo de anotaciones.

tamaño

El valor por omisión de logsize es 1 MB.

logstatus

Muestra los valores referentes al archivo de anotaciones del servidor (nivel de registro de anotaciones y tamaño del archivo de anotaciones).

sscontrol sitename — configurar un nombre de sitio



add

Añade un nuevo nombre de sitio.

nombresitio

Es un nombre de sistema principal que no se puede resolver y que solicita el cliente. Los nombres de sitio adicionales se separan mediante el signo más (+).

cachelife

Es el período de tiempo para el que una respuesta de proximidad será válida y se guardará en la antememoria. El valor por omisión es 1800. En “Utilización de la función de Proximidad en la Red” en la página 110 hallará más información.

valor

Un número positivo que representa el número de segundos durante los cuales una respuesta de proximidad es válida y se guarda en la antememoria.

networkproximity

Determina la proximidad en la red de cada servidor respecto al cliente solicitante. Utilice esta respuesta de proximidad para determinar el reparto del tráfico. Establezca este parámetro en on (activo) u off (inactivo). En “Utilización de la función de Proximidad en la Red” en la página 110 hallará más información.

valor

Las opciones son sí o no. El valor por omisión es no, que significa que la proximidad en la red está desactivada.

proportions

Establece la proporción de importancia de cpu, memoria, puerto (información de cualquier asesor) y métrica del sistema de Metric Server

que el gestor utiliza para establecer los pesos de servidor. Cada uno de estos valores se expresa como un porcentaje del total y deben sumar siempre 100.

cpu El porcentaje de CPU en uso de cada máquina servidor sujeta a reparto del tráfico (datos de entrada del agente de Metric Server).

memoria

El porcentaje de memoria en uso (datos de entrada del agente de Metric Server) en cada servidor sujeto a reparto del tráfico.

puerto Los datos de entrada de los asesores que están a la escucha en el puerto.

sistema Los datos de entrada de Metric Server.

proximitypercentage

Establece la importancia de la respuesta de proximidad respecto al estado del servidor (peso del gestor). En “Utilización de la función de Proximidad en la Red” en la página 110 hallará más información.

valor

El valor por omisión es 50.

stickytime

El intervalo durante el cual un cliente recibirá el mismo ID de servidor devuelto anteriormente para la primera petición. El valor por omisión de stickytime es 0, que significa que no hay persistencia en el nombre de sitio.

tiempo

Un número positivo distinto de cero que representa el número de segundos durante los cuales el cliente recibe el mismo ID de servidor devuelto anteriormente para la primera petición.

tfl Establece el tiempo de vida. Indica durante cuánto tiempo otro servidor de nombres conservará en la antemoria la respuesta resuelta. El valor por omisión es 5.

valor

Un número positivo que representa el número de segundos durante los cuales el servidor de nombres conservará en la antememoria la respuesta resuelta.

waitforallresponses

Establece si deben esperarse todas las respuestas de proximidad procedentes de los servidores antes de responder a la petición del cliente. En “Utilización de la función de Proximidad en la Red” en la página 110 hallará más información.

valor

Las opciones son sí o no. El valor por omisión es afirmativo.

weightbound

Es un número que representa el peso máximo que se puede establecer para los servidores del nombre de sitio. El peso máximo establecido para el nombre de sitio se puede modificar utilizando el mandato **server weight** para servidores individuales. El peso máximo por omisión del nombre de sitio es 20.

peso

El valor de weightbound.

set

Establece las propiedades del nombre de sitio,

remove

Elimina el nombre de sitio.

status

Muestra el estado actual de un nombre de sitio específico.

Ejemplos

- Para añadir un nombre de sitio:
`sscontrol sitename add 130.40.52.153`
- Para activar la proximidad en la red:
`sscontrol sitename set mySite networkproximity yes`
- Para establecer en 1900000 segundos la permanencia en la antememoria:
`sscontrol sitename set mySite cachelife 1900000`
- Para establecer un porcentaje de proximidad igual a 45:
`sscontrol sitename set mySite proximitypercentage 45`
- Para establecer que un nombre de sitio no espere todas las respuestas antes de responder:
`sscontrol sitename set mySite waitforallresponses no`
- Para establecer un tiempo de vida igual a 7 segundos:
`sscontrol sitename set mySite ttl 7`
- Para establecer las proporciones de importancia para CpuLoad, MemLoad, Port y System Metric, respectivamente:
`sscontrol sitename set mySite proportions 50 48 1 1`
- Para eliminar un nombre de sitio:
`sscontrol sitename remove 130.40.52.153`
- Para mostrar el estado del nombre de sitio mySite:
`sscontrol sitename status mySite`

Este mandato produce una salida similar a la siguiente:

SiteName Status:

SiteName	mySite
WeightBound	20
TTL	5
StickyTime	0
Number of Servers	1
Proportion given to CpuLoad	49
Proportion given to MemLoad	50
Proportion given to Port	1
Proportion given to System metric ..	0
Advisor running on port	80
Using Proximity	N

sscontrol status — visualizar si el gestor y los asesores están en ejecución

```
➤—sscontrol—status—➤
```

Ejemplos

- Para ver lo que está en ejecución, escriba:
sscontrol status

Este mandato produce una salida similar a la siguiente:

```
      NameServer has been started.  
      Manager has been started.  
-----  
| ADVISOR | SITENAME:PORT | TIMEOUT |  
-----  
|   http |           80 | unlimited |  
-----
```

Apéndice E. Consulta de mandatos de Consultant para Cisco CSS Switches

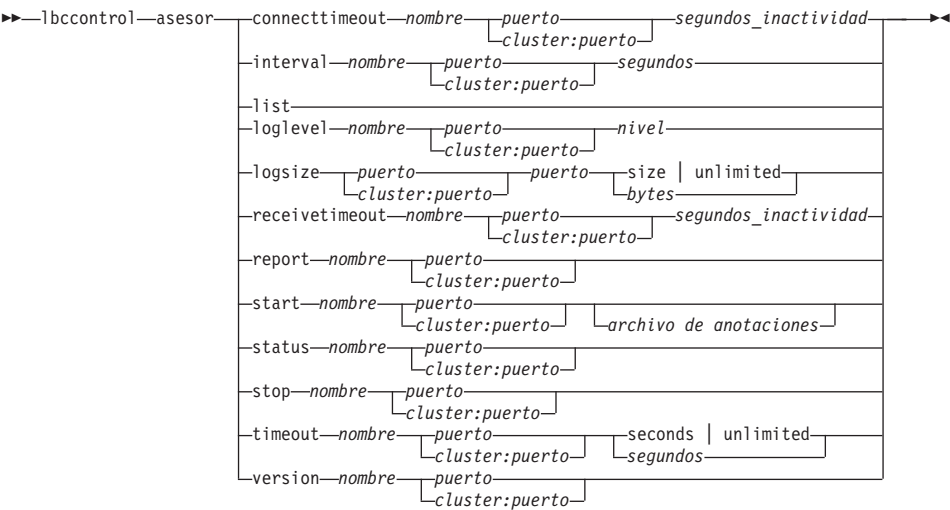
Este apéndice describe cómo utilizar los siguientes mandatos **lbcontrol** para Consultant para Cisco CSS Switches:

- “lbcontrol advisor — controlar el asesor” en la página 348
- “lbcontrol cluster — configurar clusters” en la página 353
- “lbcontrol executor — controlar el ejecutor” en la página 355
- “lbcontrol file — gestionar archivos de configuración” en la página 357
- “lbcontrol help — visualizar o imprimir ayuda para el mandato” en la página 359
- “lbcontrol host — configurar una máquina remota” en la página 360
- “lbcontrol log — controlar el archivo de anotaciones en binario” en la página 361
- “lbcontrol manager — controlar el gestor” en la página 362
- “lbcontrol metric — configurar métricas del sistema” en la página 368
- “lbcontrol port — configurar puertos” en la página 370
- “lbcontrol server — configurar servidores” en la página 372
- “lbcontrol set — configurar archivo de anotaciones del servidor” en la página 374
- “lbcontrol status — visualizar si el gestor y los asesores están en ejecución” en la página 375

Puede especificar una versión abreviada de los parámetros de los mandatos **lbcontrol**. Sólo necesita especificar las letras exclusivas de los parámetros. Por ejemplo, para obtener ayuda sobre el mandato “file save”, puede entrar **lbcontrol he f** en lugar de **lbcontrol help file**.

El prefijo “lbc” significa “load-balancing consultant” (asesor de reparto del tráfico).

Nota: Los valores de los parámetros de mandatos se deben escribir en caracteres ingleses. Las únicas excepciones son los nombres de sistema principal (utilizados en los mandatos para clusters y servidores) y los nombres de archivo (utilizados en los mandatos sobre archivos).



connecttimeout

Establece el tiempo que un asesor espera antes de notificar un error de conexión con un servidor. Para obtener más información, consulte “Tiempo de espera de conexión y de recepción del asesor para servidores” en la página 142.

nombre

Nombre del asesor. Los valores posibles son **http**, **ftp**, **ssl**, **smtp**, **imap**, **pop3**, **nnntp**, **telnet**, **connect**, **ping** y **WTE**. Los nombres de los asesores personalizados se encuentran en el formato `xxxx`, donde `ADV_xxxx` es el nombre de la clase que implementa el asesor personalizado.

puerto

Número del puerto que el asesor está supervisando.

segundos_inactividad

Es un valor entero positivo que representa el tiempo, en segundos, que un asesor espera antes de notificar un error de conexión con un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

interval

Establece la frecuencia con la que el asesor obtiene información sobre los servidores.

segundos

Es un número entero positivo que representa el número de segundos

transcurridos entre las peticiones hechas a los servidores acerca de su estado actual. El valor por omisión es 15.

list

Muestra una lista de los asesores que están actualmente suministrando información al gestor.

loglevel

Establece el nivel de anotaciones del archivo de anotaciones de un asesor.

nivel

Número del nivel (0 a 5). El valor por omisión es 1. Cuanto mayor es el número, más información se escribe en el archivo de anotaciones del asesor. Los valores posibles son: 0 para None, 1 para Minimal, 2 para Basic, 3 para Moderate, 4 para Advanced, 5 para Verbose.

logsize

Establece el tamaño máximo del archivo de anotaciones de un asesor. Si establece el tamaño máximo para el archivo de anotaciones, el archivo se sobrescribirá cuando esté lleno. Cuando el archivo alcance el tamaño especificado, las entradas subsiguientes se escribirán a partir del comienzo del archivo, sobre las entradas de anotaciones anteriores. El tamaño del archivo de anotaciones no puede ser menor que el tamaño actual del archivo. Las entradas del archivo de anotaciones contienen una indicación horaria para poder determinar el orden en el que se escribieron. Cuanto más alto sea el nivel de registro de anotaciones, más cuidadosamente debe elegirse el tamaño del archivo, pues el espacio puede agotarse rápidamente cuando se efectúan anotaciones a los niveles más altos.

número de registros

El tamaño máximo en bytes del archivo de anotaciones del asesor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Puede que el archivo de anotaciones no alcance el tamaño máximo exacto antes de sobrescribirse, ya que las propias entradas de anotaciones varían en tamaño. El valor por omisión es 1 MB.

receivetimeout

Establece el tiempo que un asesor espera antes de notificar un error de recepción con un servidor. Para obtener más información, consulte "Tiempo de espera de conexión y de recepción del asesor para servidores" en la página 142.

segundos_inactividad

Es un valor entero positivo que representa el tiempo, en segundos, que un asesor espera antes de notificar un error de recepción con un servidor. El valor por omisión es 3 veces el valor especificado para el intervalo del asesor.

report

Muestra un informe sobre el estado del asesor.

start

Arranca el asesor. Hay asesores para cada protocolo. Los puertos por omisión son los siguientes:

Nombre de asesor	Protocolo	Puerto
connect	ICMP	12345
db2	privado	50000
ftp	FTP	21
http	HTTP	80
ibmproxy	HTTP (a través de Caching Proxy)	80
imap	IMAP	143
nntp	NNTP	119
ping	PING	0
pop3	POP3	110
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23
WLM	privado	10007

Nota: El asesor FTP sólo debe asesorar en el puerto de control FTP (21). No inicie un asesor FTP en el puerto de datos FTP (20).

archivo de anotaciones

Nombre de archivo en el que se anotan los datos de gestión. En cada registro de las anotaciones figurará la indicación de la hora.

El archivo por omisión es *nombreasesor_puerto.log*, por ejemplo, **http_80.log**. Para cambiar el directorio en el que se conservarán los archivos de anotaciones, consulte “Cambio de la vía de acceso de los archivos de anotaciones” en la página 208.

Establezca las proporciones del gestor de modo que se utilice la información del asesor.

status

Muestra el estado actual de todos los valores globales del asesor y sus valores por omisión.

stop

Detiene el asesor.

timeout

Establece el número de segundos durante los cuales el gestor considerará

como válida la información procedente del asesor. Si el gestor detecta que la información del asesor es anterior a este tiempo de espera, el gestor no utilizará esa información para determinar los pesos de los servidores para el puerto que el asesor está supervisando. Una excepción a este tiempo de caducidad se produce cuando el asesor notifica al gestor que un servidor determinado está inactivo. El gestor utilizará esa información referente al servidor incluso después de que la información del asesor haya caducado.

segundos

Número positivo que representa el número de segundos o la palabra **unlimited**. El valor por omisión es "unlimited".

version

Muestra la versión actual del asesor.

Ejemplos

- Para establecer el tiempo (30 segundos) que un asesor HTTP (del puerto 80) espera antes de notificar un error de conexión con un servidor:
`lbcontrol advisor connecttimeout http 80 30`
- Para establecer el intervalo del asesor FTP (para el puerto 21) en 6 segundos:
`lbcontrol advisor interval ftp 21 6`
- Para visualizar la lista de asesores que actualmente suministran información al gestor:
`lbcontrol advisor list`

Este mandato produce una salida similar a la siguiente:

ADVISOR	PORT	TIMEOUT	

http	80	unlimited	
ftp	21	unlimited	

- Para cambiar a 0 el nivel de registro de anotaciones del asesor a fin de mejorar el rendimiento:
`lbcontrol advisor loglevel http 80 0`
- Para cambiar el tamaño del archivo de anotaciones del asesor a 5000 bytes:
`lbcontrol advisor logsize ftp 21 5000`
- Para establecer el tiempo (60 segundos) que un asesor HTTP (del puerto 80) espera antes de notificar un error de recepción con un servidor:
`lbcontrol advisor receivetimeout http 80 60`
- Para visualizar un informe de estado del asesor ftp (para el puerto 21):
`lbcontrol advisor report ftp 21`

Este mandato produce una salida similar a la siguiente:

Advisor Report:

Advisor name Ftp
Port number 21

Cluster address 9.67.131.18
Server address 9.67.129.230
Load 8

Cluster address 9.67.131.18
Server address 9.67.131.215
Load -1

- Para arrancar el asesor con el archivo ftpadv.log:
lbccontrol advisor start ftp 21 ftpadv.log
- Para visualizar el estado actual de los valores asociados al asesor http:
lbccontrol advisor status http 80

Este mandato produce una salida similar a la siguiente:

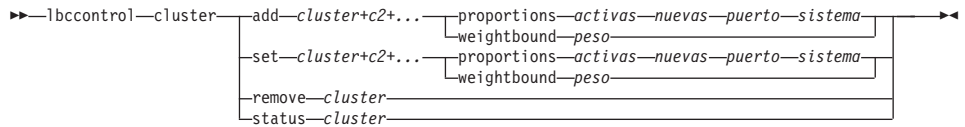
Advisor

Status:

Interval (seconds) 15
Timeout (seconds) Unlimited
Connect timeout (seconds).....21
Receive timeout (seconds).....21
Advisor log filename Http_80.log
Log level 1
Maximum log size (bytes) Unlimited

- Para detener el asesor http en el puerto 80:
lbccontrol advisor stop http 80
- Para establecer el valor de tiempo de espera de la información del asesor en 5 segundos:
lbccontrol advisor timeout ftp 21 5
- Para averiguar el número de la versión actual del asesor ssl:
lbccontrol advisor version ssl 443

lbcontrol cluster — configurar clusters



add

Añade este cluster. Debe definir como mínimo un cluster.

weightbound

Establece el peso máximo para los servidores del puerto. Este valor determina la diferencia que puede haber entre el número de peticiones que el Cisco CSS Switch proporcionará a cada servidor. El valor por omisión es 10.

peso

El valor de weightbound.

set

Establece las propiedades del cluster.

proportions

Establece la proporción de importancia para las conexiones activas (*activas*), las conexiones nuevas (*nuevas*), información procedente de asesores (*puerto*), e información procedente de Metric Server (*sistema*), que es utilizada por el gestor para definir los pesos de los servidores. Cada uno de estos valores, descrito más abajo, se expresa como un porcentaje sobre el total y, por lo tanto, deben sumar siempre 100. Para obtener más información, consulte “Grado de importancia dado a la información de estado” en la página 135.

activas

Un número del 0 al 100 que representa la proporción de peso que se otorga a las conexiones activas. El valor por omisión es 50.

nuevas

Un número del 0 al 100 que representa la proporción de peso que se otorga a las conexiones nuevas. El valor por omisión es 50.

puerto

Un número del 0 al 100 que representa la proporción de peso que se otorga a la información procedente de asesores. El valor por omisión es 0.

sistema

Un número del 0 al 100 que representa la proporción de peso que se otorga a la información procedente de las métricas del sistema. El valor por omisión es 0.

remove

Se elimina este cluster.

status

Muestra el estado actual de un cluster específico.

Ejemplos

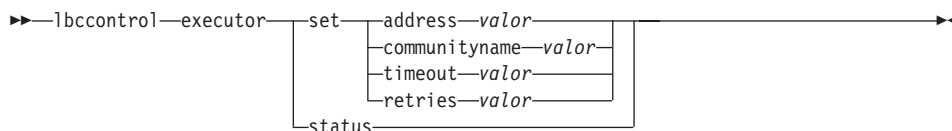
- Para añadir la dirección de cluster 130.40.52.153:
`lbcontrol cluster add 130.40.52.153`
- Para eliminar la dirección de cluster 130.40.52.153:
`lbcontrol cluster remove 130.40.52.153`
- Para establecer la importancia relativa que se da a la entrada recibida por el gestor:
`lbcontrol cluster proportions 60 35 5 0`
- Para mostrar el estado de la dirección de cluster 9.67.131.167:
`lbcontrol cluster status 9.67.131.167`

Este mandato produce una salida similar a la siguiente:

Cluster Status:

```
Address ..... 9.67.131.167
Number of target ports ..... 3
Default port weight bound ..... 10
Proportion given to active connections .. 49
Proportion given to new connections ..... 49
Proportion given specific to the port ... 2
Proportion given to system metrics ..... 0
```

lbcontrol ejecutor — controlar el ejecutor



set

Establece los campos del ejecutor.

address

Es la dirección IP o nombre de sistema principal utilizado para establecer comunicación con el Cisco CSS Switch con fines administrativos. Para obtener más información, consulte el manual *Cisco Content Services Switch Basic Configuration Guide*.

valor

Es una dirección IP o nombre de sistema principal válidos.

communityname

Es el nombre de comunidad SNMP utilizado en las comunicaciones SNMP con el Cisco CSS Switch. Para obtener más información, consulte el manual *Cisco Content Services Switch Basic Configuration Guide*.

valor

El valor por omisión es public, con acceso de lectura-escritura.

timeout

Es el número de segundos después de los cuales las consultas SNMP desde Cisco Consultant al Cisco CSS Switch exceden el tiempo asignado. Cisco Consultant utiliza SNMP para recoger información a partir del Cisco CSS Switch. Si los mensajes de manager.log indican un número elevado de tiempos de espera excedidos, puede ajustar este valor para corregir el problema.

valor

El valor por omisión es 3.

retries

Es el número de veces que Cisco Consultant reintenta una consulta SNMP destinada al Cisco CSS Switch. Si los mensajes de manager.log indican un número elevado de errores en las consultas SNMP, puede ajustar este valor para corregir el problema.

valor

El valor por omisión es 2.

status

Muestra el estado actual de los valores del ejecutor que pueden definirse y sus valores por omisión.

Ejemplos

- Para visualizar los contadores internos de Cisco Consultant:

```
lbcontrol executor status
```

```
Executor Status:
```

```
-----
```

```
address ..... 9.67.131.151
```

```
community name ..... public
```

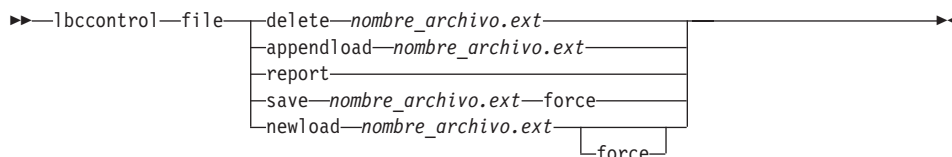
```
timeout value ..... 3
```

```
retires value ..... 2
```

- Para establecer la dirección en 130.40.52.167:

```
lbcontrol executor set address 130.40.52.167
```

lbccontrol file — gestionar archivos de configuración



delete

Elimina el archivo.

nombre_archivo.ext

Archivo de configuración.

La extensión del archivo (*.ext*) puede ser cualquiera que elija el usuario y es opcional.

appendload

Añade un archivo de configuración a la configuración actual y lo carga en Cisco Consultant.

report

Informa acerca del archivo o archivos disponibles.

save

Guarda la configuración actual de Cisco Consultant en el archivo.

Nota: Los archivos se guardan y cargan desde los directorios siguientes:

- AIX: **/usr/lpp/nd/servers/configurations/lbc**
- Linux: **/opt/nd/servers/configurations/lbc**
- Solaris: **/opt/nd/servers/configurations/lbc**
- Windows 2000:

Vía de acceso común de directorio de instalación — **c:\Archivos de**

programa\ibm\edge\nd\servers\configurations\componente

Vía de acceso nativa de directorio de instalación — **c:\Archivos de programa\ibm\nd\servers\configurations\componente**

force

Utilice **force** para guardar su archivo en un archivo existente del mismo nombre, el cual se suprime previamente. Si no utiliza la opción **force**, el archivo existente no se sobrescribe.

newload

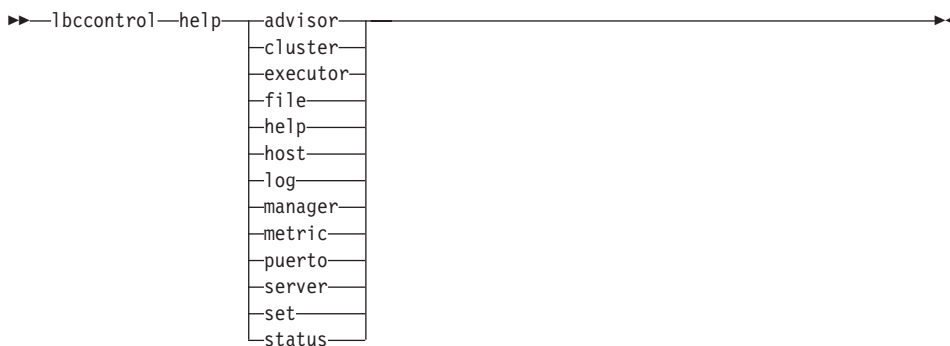
Carga un nuevo archivo de configuración en Cisco Consultant. El nuevo archivo de configuración sustituirá a la configuración actual.

Ejemplos

- Para suprimir un archivo:
`lbccontrol file delete file3`
Se ha suprimido el archivo (file3).
- Para cargar un nuevo archivo de configuración con el que sustituir el archivo de configuración actual:
`lbccontrol file newload file1.sv`
Se ha cargado el archivo (archivo1.sv) en Dispatcher.
- Para añadir un archivo de configuración a la configuración actual y cargarlo:
`lbccontrol file appendload file2.sv`
Se ha añadido el archivo (file2.sv) a la configuración actual y se ha cargado.
- Para visualizar un informe de los archivos (esto es, aquellos archivos guardados anteriormente):
`lbccontrol file report`

FILE REPORT:
file1.save
file2.sv
file3
- Para guardar la configuración en un archivo llamado archivo3:
`lbccontrol file save file3`
La configuración se ha guardado en el archivo (file3).

lbccontrol help — visualizar o imprimir ayuda para el mandato



Ejemplos

- Para obtener ayuda para el mandato lbccontrol:

```
lbccontrol help
```

Este mandato produce una salida similar a la siguiente:

```
HELP COMMAND ARGUMENTS:
```

```
-----
```

```
Usage:  help <help option>
```

```
Example: help cluster
```

```
executor      - help on executor command
cluster       - help on cluster command
port          - help on port command
server        - help on server command
manager       - help on manager command
metric        - help on metric command
advisor       - help on advisor command
file          - help on file command
host          - help on host command
log           - help on log command
set           - help on set command
status        - help on status command
help          - print complete help text
```

Los parámetros especificados dentro de < > son variables.

lbcontrol host — configurar una máquina remota

►►—lbcontrol—host:—*sispral_remoto*—◄◄

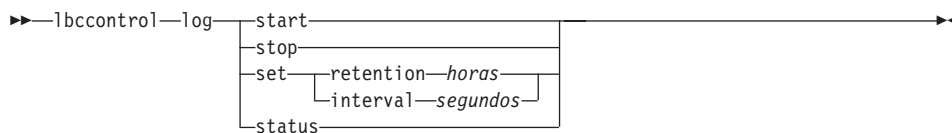
sispral_remoto

El nombre de la máquina Cisco Consultant que se va a configurar.
Cuando escriba este mandato, compruebe que no haya espacios entre
host: y *sispral_remoto*, por ejemplo:

```
lbcontrol  
host:sispral_remoto
```

Emita este mandato desde un indicador de mandatos, y luego escriba cualquier mandato lbcontrol válido que desee emitir para la máquina Cisco Consultant remota.

lbccontrol log — controlar el archivo de anotaciones en binario



start

Inicia el archivo de anotaciones en binario.

stop

Detiene el archivo de anotaciones en binario.

set

Establece los cambios para las anotaciones en binario. Para obtener más información sobre cómo definir campos para las anotaciones en binario, consulte “Utilizar las anotaciones en binario para analizar las estadísticas del servidor” en la página 198.

retention

El número de horas que se conservarán los archivos de anotaciones en binario. El valor por omisión de retention es 24.

horas

El número de horas.

interval

El número de segundos entre entradas del archivo de anotaciones. El valor por omisión de interval es 60.

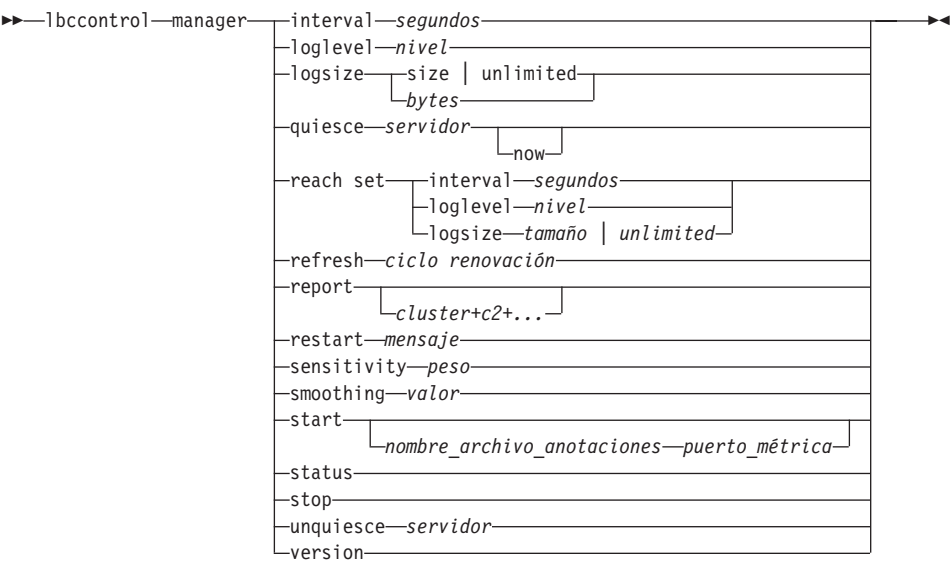
segundos

El número de segundos.

status

Muestra la retención y los intervalos de las anotaciones en binario.

lbcontrol manager — controlar el gestor



interval

Establece la frecuencia con la que el gestor actualiza los pesos de los servidores para el Cisco CSS Switch, actualizando los criterios que el Cisco CSS Switch utiliza para encaminar las peticiones de los clientes.

segundos

Un número positivo que representa, en segundos, la frecuencia con la que el gestor actualiza los pesos para el Cisco CSS Switch. El valor por omisión es 15, y el intervalo mínimo es 10. Si intenta establecer un valor menor que 10 segundos para el intervalo del gestor, el intervalo se establece en 10 segundos. Es recomendable utilizar el intervalo por omisión para el gestor (15 segundos), pues el Cisco CSS Switch no saca provecho de unas actualizaciones más frecuentes.

loglevel

Establece el nivel de anotaciones del archivo de anotaciones del gestor.

nivel

Número del nivel (0 a 5). Cuanto mayor es el número, más información se graba en las anotaciones del gestor. El valor por omisión es 1. Los valores posibles son: 0 para None, 1 para Minimal, 2 para Basic, 3 para Moderate, 4 para Advanced, 5 para Verbose.

logsize

Establece el tamaño máximo del archivo de anotaciones del gestor. Si establece el tamaño máximo para el archivo de anotaciones, el archivo se

sobreescribirá cuando esté lleno. Cuando el archivo alcance el tamaño especificado, las entradas subsiguientes se escribirán a partir del comienzo del archivo, sobre las entradas de anotaciones anteriores. El tamaño del archivo de anotaciones no puede ser menor que el tamaño actual del archivo. Las entradas del archivo de anotaciones contienen una indicación horaria para poder determinar el orden en el que se escribieron. Cuanto más alto sea el nivel de registro de anotaciones, más cuidadosamente debe elegirse el tamaño del archivo, pues el espacio puede agotarse rápidamente cuando se efectúan anotaciones a los niveles más altos.

bytes

El tamaño máximo en bytes del archivo de anotaciones del gestor. Puede especificar un número positivo mayor que cero o la palabra **unlimited**. Puede que el archivo de anotaciones no alcance el tamaño máximo exacto antes de sobrescribirse, ya que las propias entradas de anotaciones varían en tamaño. El valor por omisión es 1 MB.

quiesce

Especifica que no se envíen más conexiones a un servidor. El gestor establece en 0 el peso de ese servidor en cada uno de los puertos para los que está definido; a continuación, envía un mensaje de suspensión al Cisco CSS Switch. Utilice este mandato si desea detener un servidor para realizar tareas rápidas de mantenimiento y luego activarlo de nuevo. Si suprime un servidor desactivado de la configuración y luego lo añade de nuevo, el servidor no conservará el estado que tenía antes de desactivarlo.

servidor

La dirección IP expresada como nombre simbólico o en formato decimal con puntos.

reach

Establece el intervalo, nivel de registro y tamaño de archivo de anotaciones para el asesor reach.

refresh

Establece el número de intervalos antes de solicitar al Cisco CSS Switch una renovación de la información acerca de las conexiones nuevas y las conexiones activas.

ciclo de renovación

Número positivo que representa el número de intervalos. El valor por omisión es 1.

report

Visualiza un informe instantáneo de estadísticas.

cluster

La dirección del cluster que desea que se muestre en el informe. La

dirección puede ser un nombre simbólico o puede tener un formato decimal con puntos. Por omisión, se muestra un informe del gestor para todos los clusters.

Nota: Los clusters adicionales se separan mediante un signo más (+).

restart

Rearranca todos los servidores (que no están inactivos) con pesos normalizados (1/2 del peso máximo).

mensaje

Un mensaje que desea grabar en el archivo de anotaciones del gestor.

sensitivity

Establece la sensibilidad mínima para que se actualicen los pesos. Este valor define cuándo el gestor debe cambiar su ponderación para el servidor, de acuerdo con información externa.

peso

Un número del 0 al 100 que se utiliza como porcentaje de peso. El valor por omisión 5 crea una sensibilidad mínima del 5%.

smoothing

Establece un índice que corrige las variaciones de peso al repartir el tráfico. Cuanto más alto sea el índice de corrección, menos acusadamente cambiarán los pesos de los servidores cuando se modifiquen las condiciones de la red. Un índice más bajo ocasionará que los pesos de los servidores se modifiquen más acusadamente.

valor

Un número positivo de coma flotante. El valor por omisión es 1,5.

start

Arranca el gestor.

nombre_archivo_anotaciones

Nombre de archivo en el que se anotan los datos del gestor. Cada registro del archivo de anotaciones contiene una indicación horaria.

El archivo por omisión se instala en el directorio **logs**. Consulte “Apéndice F. Ejemplos de archivos de configuración” en la página 377. Consulte “Cambio de la vía de acceso de los archivos de anotaciones” en la página 208 para conocer cómo cambiar el directorio donde se guardan los archivos de anotaciones.

puerto_métrica

Es el puerto que Metric Server utiliza para comunicarse. Si especifica un puerto de métrica, debe especificar un nombre de archivo de anotaciones. El puerto de métrica por omisión es 10004.

status

Muestra el estado actual de todos los valores globales del gestor y sus valores por omisión.

stop

Detiene el gestor.

unquiesce

Especifica que el gestor puede empezar a otorgar un peso mayor que 0 a un servidor que se desactivó anteriormente en cada puerto para el que está definido. El gestor envía un mandato active al Cisco CSS Switch.

servidor

La dirección IP expresada como nombre simbólico o en formato decimal con puntos.

version

Muestra la versión actual del gestor.

Ejemplos

- Para establecer el intervalo de actualización del gestor a cada 5 segundos:
`lbcontrol manager interval 5`
- Para establecer el nivel de anotaciones a 0 para mejorar el rendimiento:
`lbcontrol manager loglevel 0`
- Para establecer el tamaño de las anotaciones del gestor a 1.000.000 bytes:
`lbcontrol manager logsize 1000000`
- Para especificar que no se envíen más conexiones al servidor de 130.40.52.153:
`lbcontrol manager quiesce 130.40.52.153`
- Para establecer en 3 el número de intervalos de actualización antes de renovar los pesos:
`lbcontrol manager refresh 3`
- Para obtener una instantánea de las estadísticas del gestor:
`lbcontrol manager report`

Este mandato produce una salida similar a la siguiente:

lbccontrol>>manager report

HOST TABLE LIST	STATUS
server6	ACTIVE
server5	ACTIVE
server4	ACTIVE
server3	ACTIVE
server2	ACTIVE
server1	ACTIVE

9.67.154.35		WEIGHT		ACTIVE % 49		NEW % 50		PORT % 1		SYSTEM % 0	
PORT: 80		NOW	NEW	WT	CONNECT	WT	CONNECT	WT	LOAD	WT	LOAD
server1		4	4	5	0	5	0	3	301	-9999	-1
server2		5	5	5	0	5	0	6	160	-9999	-1
PORT TOTALS:		9	9		0		0		461		-2

9.67.154.35	WEIGHT		ACTIVE % 49		NEW % 50		PORT % 1		SYSTEM % 0	
PORT: 443	NOW	NEW	WT	CONNECT	WT	CONNECT	WT	LOAD	WT	LOAD
server3	4	4	5	0	5	0		0	-9999	-1
server4	5	5	5	0	5	0	0	0	-9999	-1
PORT TOTALS:	9	9		0		0		0		-2

9.67.154.34	WEIGHT		ACTIVE % 49		NEW % 50		PORT % 1		SYSTEM % 0	
PORT: 80	NOW	NEW	WT	CONNECT	WT	CONNECT	WT	LOAD	WT	LOAD
server5	5	5	5	0	5	0	5	160	-9999	-1
server6	0	0	5	0	5	0	-9999	-1	-9999	-1
PORT TOTALS:	5	5		0		0		159		-2

ADVISOR	PORT	TIMEOUT
http	80	unlimited

- Para reiniciar todos los servidores con pesos normalizados y escribir un mensaje en el archivo de anotaciones del gestor:

lbcontrol manager restart Restarting the manager to update code

Este mandato produce una salida similar a la siguiente:

320-14:04:54 Restarting the manager to update code

- Para establecer en 10 la sensibilidad a los cambios de peso:

lbcontrol manager sensitivity 10

- Para establecer el índice de corrección en 2.0:

lbcontrol manager smoothing 2.0

- Para iniciar el gestor y especificar el archivo de anotaciones denominado ndmgr.log (la vía de acceso no puede establecerse):

lbcontrol manager start ndmgr.log

- Para visualizar el estado actual de los valores asociados al gestor:

lbcontrol manager status

Este mandato produce una salida similar al ejemplo siguiente:

Manager

status:

=====

Metric port 10004
Manager log filename manager.log
Manager log level 1
Maximum manager log size (bytes) unlimited
Sensitivity level 0.05
Smoothing index 1.5
Update interval (seconds) 2
Weights refresh cycle 1
Reach log level 1
Maximum reach log size (bytes) unlimited
Reach update interval (seconds) 7

- Para detener el gestor:

lbcontrol manager stop

- Para visualizar el número de la versión actual del gestor:

lbcontrol manager version

lbcontrol metric — configurar métricas del sistema

```
►►—lbcontrol—metric—┬—add—cluster+c2+...+cN:métrica+métrica1+...+métricaN—►
                      │—remove—cluster+c2+...+cN:métrica+métrica1+...+métricaN—
                      │—proportions—cluster+c2+...+cN:prop1 prop2 prop3...propN—
                      └—status—cluster+c2+...+cN:métrica+métrica1+...+métricaN—
```

add

Añade una métrica.

cluster

La dirección a la que se conectan los clientes. La dirección puede ser el nombre de sistema principal de la máquina o la dirección IP en formato decimal con puntos. Los clusters adicionales se separan mediante un signo más (+).

Nota: para Cisco Consultant, la dirección de cluster corresponde la dirección IP virtual (dirección VIP) de la norma de contenido del propietario en la configuración de Cisco CSS Switch.

métrica

Es el nombre de la métrica del sistema. Las opciones posibles para la métrica son:

- cpuload
- memload
- puerto
- métricas del sistema

remove

Elimina la métrica.

proportions

Establece las proporciones para todas las métricas asociadas al objeto.

status

Muestra los valores actuales de la métrica.

Ejemplos

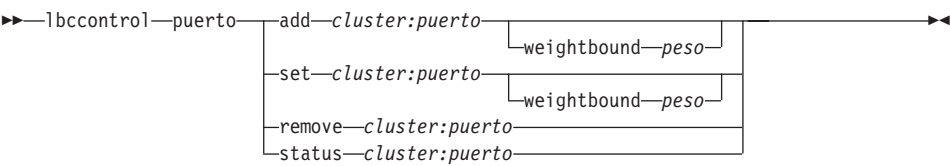
- Para añadir una métrica del sistema:
`lbcontrol metric add 10.10.10.20:metric1`
- Para establecer las proporciones de un cluster con dos métricas del sistema:
`lbcontrol metric proportions 10.10.10.20 48 52`
- Para visualizar el estado actual de los valores asociados a la métrica especificada:
`lbcontrol metric status 10.10.10.20:metric1`

Este mandato produce una salida similar a la siguiente:

Metric Status:

```
Cluster ..... 10.10.10.20
Metric name ..... metric1
Metric proportion ..... 52
    Server ..... 9.37.56.100
    Metric data .... -1
```

lbcontrol port — configurar puertos



add

Añade un puerto a un cluster. Ha de añadir un puerto a un cluster antes de poder añadir servidores a este puerto. Si no existen puertos para un cluster, todas las peticiones de los clientes se procesan localmente. Puede añadir más de un puerto a la vez utilizando este mandato.

weightbound

Establece el peso máximo para los servidores del puerto. Este valor determina la diferencia que puede haber entre el número de peticiones que el Cisco CSS Switch proporcionará a cada servidor. El valor por omisión es 10.

peso

Un número del 1 al 10 que representa el peso máximo.

set

Establece los campos de un puerto.

remove

Elimina el puerto.

status

Muestra el estado de los servidores del puerto. Si desea ver el estado de todos los puertos, no especifique un *puerto* en este mandato, pero debe especificar los dos puntos (:).

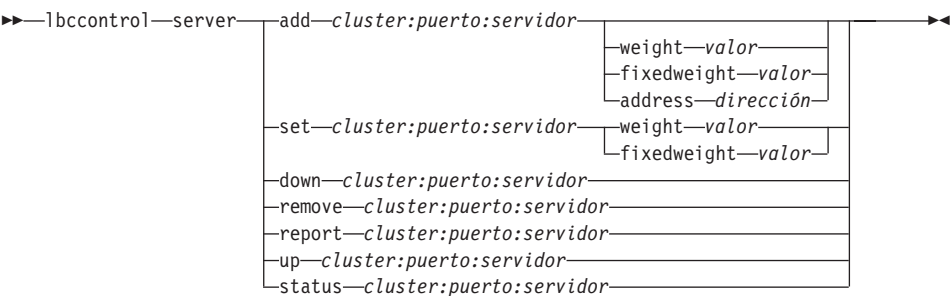
Ejemplos

- Para añadir los puertos 80 y 23 a la dirección del cluster 130.40.52.153:
`lbccontrol port add 130.40.52.153:80+23`
- Para establecer el peso máximo 10 en el puerto 80 de la dirección de cluster 130.40.52.153:
`lbccontrol port set 130.40.52.153:80 weightbound 10`
- Para eliminar el puerto 23 de la dirección de cluster 130.40.52.153:
`lbccontrol port remove 130.40.52.153:23`
- Para obtener el estado del puerto 80 de la dirección de cluster 9.67.131.153:
`lbccontrol port status 9.67.131.153:80`

Este mandato produce una salida similar a la siguiente:

```
Port
Status:
-----
Port number ..... 80
Cluster address ..... 9.67.131.153
Number of servers ..... 2
Weight bound ..... 10
```

lbcontrol server — configurar servidores



add
Añade este servidor.

cluster
La dirección del cluster expresada como nombre simbólico o en formato decimal con puntos.

Nota: Los clusters adicionales se separan mediante un signo más (+).

puerto
El número del puerto.

Nota: Los puertos adicionales se separan mediante un signo más (+).

servidor
Es la dirección IP exclusiva del servidor TCP expresada como nombre simbólico o en el formato decimal con puntos. Si utiliza un nombre simbólico exclusivo que no da lugar a una dirección IP, debe proporcionar el atributo address en el mandato **lbcontrol server add**.

weight
Un número del 0 al 10 que representa el peso asignado al servidor. Si el peso se establece en 0, se impide el envío de nuevas peticiones al servidor, pero no finalizan las conexiones que actualmente están activas para ese servidor. El valor por omisión es la mitad del peso máximo del puerto especificado. Si el gestor está en ejecución y fixedweight se establece en no, este valor se sobregabarará rápidamente.

valor
Valor del peso.

fixedweight
La opción fixedweight le permite especificar si desea que el gestor modifique el peso del servidor. Si establece el valor de fixedweight en sí,

cuando se ejecute el gestor, éste no podrá modificar el peso del servidor. Para obtener más información, consulte “Pesos fijos del gestor” en la página 137.

valor

Es el valor del peso fijo (fixedweight). El valor por omisión es no.

address

Es la dirección IP exclusiva del servidor TCP expresada como nombre simbólico o en el formato decimal con puntos. Si el nombre del servidor no se puede resolver (por ejemplo, un nombre de servidor lógico), debe proporcionar la dirección del servidor físico.

valor

Es el identificador exclusivo del servidor. Si el nombre del servidor no se puede resolver, debe proporcionar el atributo de dirección (address).

down

Marca el servidor como inactivo. El Cisco CSS Switch dejará de enviar conexiones a este servidor.

remove

Elimina este servidor.

report

Informa sobre este servidor.

set

Establece valores para este servidor.

up

Marca este servidor como activo. El Cisco CSS Switch enviará ahora nuevas conexiones a este servidor.

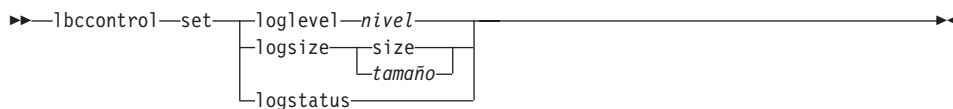
status

Muestra el estado de los servidores.

Ejemplos

- Para añadir el servidor con dirección 27.65.89.42 al puerto 80 de la dirección de cluster 130.40.52.153:
`lbcontrol server add 130.40.52.153:80:27.65.89.42`
- Para eliminar el servidor con dirección 27.65.89.42 de todos los puertos de todos los clusters:
`lbcontrol server remove ::27.65.89.42`
- Para establecer en 10 el peso del servidor 27.65.89.42 en el puerto 80 de la dirección de cluster 130.40.52.153:
`lbcontrol server set 130.40.52.153:80:27.65.89.42 weight 10`

lbcontrol set — configurar archivo de anotaciones del servidor



loglevel

El nivel para el cual lbcservidor registra sus actividades.

nivel

El valor por omisión de **loglevel** es 1. El rango es 0-5. Los valores posibles son: 0 para None, 1 para Minimal, 2 para Basic, 3 para Moderate, 4 para Advanced, 5 para Verbose.

logsize

El número máximo de bytes que se registran en el archivo de anotaciones.

tamaño

El valor por omisión de logsize es 1 MB.

logstatus

Muestra los valores referentes al archivo de anotaciones del servidor (nivel de registro de anotaciones y tamaño del archivo de anotaciones).

lbcontrol status — visualizar si el gestor y los asesores están en ejecución

➤—lbcontrol—status—➤

Ejemplos

- Para ver lo que está en funcionamiento:
lbcontrol status

Este mandato produce una salida similar a la siguiente:

Manager has been started.

ADVISOR	PORT	TIMEOUT
http	80	unlimited
ftp	21	unlimited

Apéndice F. Ejemplos de archivos de configuración

Este apéndice contiene archivos de configuración de ejemplo para el componente Dispatcher de Network Dispatcher.

Archivos de configuración de ejemplo para Network Dispatcher

Los archivos de ejemplo están situados en el directorio
.../nd/servers/samples/.

Archivo de configuración de Dispatcher—para AIX, Red Hat Linux y Solaris

```
#!/bin/ksh
#
# configuration.sample - Archivo de configuración de ejemplo para el componente
# Dispatcher
#
#
# Comprobar que es el usuario root quien ejecuta este script.
#
# iam='whoami'

# if [ "$iam" != "root" ]if [ "$iam" != "root" ]
# then
# echo "Debe iniciar la sesión como usuario root para ejecutar este script"
# exit 2
# fi

#
# Primero se arranca el servidor
#
# ndserver start
# sleep 5

#
# Seguidamente arrancar el ejecutor
#
# ndcontrol executor start

#
# El Dispatcher puede eliminarse en cualquier momento con los mandatos
# "ndcontrol executor stop" y "ndserver stop" para detener el
# ejecutor y el servidor respectivamente antes de eliminar el
# software de Dispatcher.
#
# El siguiente paso de configuración de Dispatcher es definir la
# NFA (dirección de no reenvío) y la dirección o direcciones de cluster.
#
# La dirección de no reenvío se utiliza para acceder de forma remota a la
```

```

# máquina Dispatcher con fines de administración o configuración. Dicha
# dirección es necesaria, puesto que Dispatcher reenviará los paquetes
# a la dirección o direcciones de cluster.
#
# La dirección de cluster (CLUSTER) es el nombre del sistema principal
# (o dirección IP) al que se conectarán los clientes remotos.
#
# En cualquier parte de este archivo, puede utilizar nombres de
# sistema principal y direcciones IP indistintamente.
#

# NFA=nombsistprinc.dominio.nombre
# CLUSTER=www.sucompañía.com

# echo "Cargando la dirección de no reenvío"
# ndcontrol executor set nfa $NFA

#
# El siguiente paso en la configuración de Dispatcher es crear
# un cluster. Dispatcher encaminará las peticiones enviadas a la
# dirección de cluster a las máquinas servidor correspondientes
# definidas para ese cluster. Puede configurar y dar servicio a
# varias direcciones de cluster mediante la utilización de Dispatcher.

# Se debe utilizar una configuración similar para CLUSTER2, CLUSTER3, etc.
#

# echo "Cargando la primera dirección de CLUSTER "
# ndcontrol cluster add $CLUSTER

#
# Ahora se deben definir los puertos que utilizará este cluster.
# Las peticiones recibidas por Dispatcher en un puerto definido se
# reenviarán al puerto correspondiente de una de las máquinas
# servidor.
#

# echo "Creando puertos para CLUSTER: $CLUSTER"

# ndcontrol port add $CLUSTER:20+21+80

#
# El último paso consiste en añadir cada máquina servidor a los
# puertos de este cluster.
# De nuevo, puede utilizar el nombre de sistema principal o la dirección IP
# de las máquinas servidor.
#

# SERVER1=nombreserv1.dominio.nombre
# SERVER2=nombreserv2.dominio.nombre
# SERVER3=nombreserv3.dominio.nombre

# echo "Añadiendo máquinas servidor"
# ndcontrol server add $CLUSTER:20+21+80:
# $SERVER1+$SERVER2+$SERVER3

```

```

#
# Ahora iniciaremos los componentes de reparto del tráfico de
# Dispatcher. El componente principal de reparto del tráfico se conoce
# como el gestor y los componentes secundarios de reparto del tráfico
# se conocen como asesores.
# Si el gestor y los asesores no se están ejecutando,
# Dispatcher envía peticiones en un formato rotatorio
# ("round-robin"). Una vez que se arranca
# el gestor, se emplean las decisiones sobre el peso según el número de
# conexiones nuevas y activas, y las peticiones entrantes
# se envían al mejor servidor. Los asesores proporcionan al
# gestor más información sobre la capacidad de los servidores de dar servicio a
# peticiones, y detectan si un servidor está activado. Si
# un asesor detecta que un servidor está desactivado, estará marcado
# como inactivo (siempre y cuando las proporciones del gestor se hayan
# establecido para incluir la información del asesor) y no se encaminarán
# más peticiones hacia el servidor.
# El último paso en la configuración de los componentes del reparto
# del tráfico es establecer las proporciones del gestor. Éste actualiza
# el peso de los servidores basándose en cuatro políticas:
# 1. El número de conexiones activas de cada servidor.
# 2. El número de conexiones nuevas a cada servidor.
# 3. La información de entrada procedente de los asesores.
# 4. La información de entrada procedente del asesor a nivel de sistema.
# Estas proporciones deben sumar 100. Por ejemplo,
# si establece las proporciones del gestor mediante
# ndcontrol manager proportions 48 48 4 0
# las conexiones nuevas y activas contribuirán en un 48%
# en la asignación de pesos, los asesores contribuirán en
# en un 4% y la información del sistema no se tendrá en cuenta.
#
# NOTA: Las proporciones por omisión del gestor están
# establecidas en 50 50 0 0
#

# echo "Iniciando el gestor..."
# ndcontrol manager start

# echo "Iniciando el asesor FTP en el puerto 21 ..."
# ndcontrol advisor start ftp 21
# echo "Iniciando el asesor HTTP en el puerto 80 ..."
# ndcontrol advisor start http 80
# echo "Iniciando el asesor Telnet en el puerto 23 ..."
# ndcontrol advisor start telnet 23
# echo "Iniciando el asesor SMTP en el puerto 25 ..."
# ndcontrol advisor start smtp 25
# echo "Iniciando el asesor POP3 en el puerto 110 ..."
# ndcontrol advisor start pop3 110
# echo "Iniciando el asesor NNTP en el puerto 119 ..."
# ndcontrol advisor start nntp 119
# echo "Iniciando el asesor SSL en el puerto 443 ..."
# ndcontrol advisor start ssl 443
#

```

```

# echo "Estableciendo las proporciones del gestor..."
# ndcontrol manager proportions 58 40 2 0

#
# El último paso en la configuración de la máquina Dispatcher es asignar
# un alias a la tarjeta de interfaz de red (NIC).
#
# NOTA: NO utilice este mandato en un entorno de alta
# disponibilidad. Los scripts go* configurarán la NIC y el
# bucle de retorno tal como sea necesario.
# ndcontrol cluster configure $CLUSTER

# Si la dirección de cluster está en una subred o NIC diferente de la
# dirección de no reenvío, utilice el siguiente formato para el
# mandato de configuración de cluster.
# ndcontrol cluster configure $CLUSTER tr0 0xfffff800
# donde tr0 es la NIC (tr1 para la segunda tarjeta de Red en Anillo, en0
# para la primera tarjeta Ethernet) y 0xfffff800 es una máscara de
# subred válida para su sitio Web.
#

#
# Los mandatos siguientes están establecidos en sus valores por omisión.
# Utilice estos mandatos como guía para cambiar los valores por omisión.
# ndcontrol manager loglevel 1
# ndcontrol manager logsize 1048576
# ndcontrol manager sensitivity 5,000000
# ndcontrol manager interval 2
# ndcontrol manager refresh 2
#
# ndcontrol advisor interval ftp 21 5
# ndcontrol advisor loglevel ftp 21 1
# ndcontrol advisor logsize ftp 21 1048576
# ndcontrol advisor timeout ftp 21 unlimited
# ndcontrol advisor interval telnet 23 5
# ndcontrol advisor loglevel telnet 23 1
# ndcontrol advisor logsize telnet 23 1048576
# ndcontrol advisor timeout telnet 23 unlimited
# ndcontrol advisor interval smtp 25 5
# ndcontrol advisor loglevel smtp 25 1
# ndcontrol advisor logsize smtp 25 1048576
# ndcontrol advisor timeout smtp 25 unlimited
# ndcontrol advisor interval http 80 5
# ndcontrol advisor loglevel http 80 1
# ndcontrol advisor logsize http 80 1048576
# ndcontrol advisor timeout http 80 unlimited
# ndcontrol advisor interval pop3 110 5
# ndcontrol advisor loglevel pop3 110 1
# ndcontrol advisor logsize pop3 110 1048576
# ndcontrol advisor timeout pop3 110 unlimited
# ndcontrol advisor interval nntp 119 5
# ndcontrol advisor loglevel nntp 119 1
# ndcontrol advisor logsize nntp 119 1048576
# ndcontrol advisor timeout nntp 119 unlimited
# ndcontrol advisor interval ssl 443 5

```

```
# ndcontrol advisor loglevel ssl 443 1
# ndcontrol advisor logsize ssl 443 1048576
# ndcontrol advisor timeout ssl 443 unlimited
#
```

Archivo de configuración de Dispatcher—Windows

El siguiente es un archivo de configuración de ejemplo de Network Dispatcher denominado **configuration.cmd.sample** que se puede utilizar con Windows.

```
@echo off
rem configuration.cmd.sample - Archivo de configuración de ejemplo para
rem el componente Dispatcher.
rem

rem ndserver ha de iniciarse a través de Servicios

rem

rem
rem Seguidamente arrancar el ejecutor
rem
rem call ndcontrol executor start

rem

rem El siguiente paso de configuración del Dispatcher es definir la
rem dirección de no reenvío (NFA) y la dirección o direcciones
rem de cluster.
rem

rem La dirección de no reenvío se utiliza para acceder de forma
rem remota a la máquina Dispatcher para la configuración de la
rem administración. Esta dirección es necesaria, puesto que Dispatcher
rem reenviará los paquetes a la dirección o direcciones de cluster.

rem
rem La dirección del cluster (CLUSTER) es el nombre de sistema principal
rem (o dirección IP) a la que se conectarán los clientes remotos.
rem

rem Puede utilizar nombres de sistema principal y direcciones IP
rem indistintamente en cualquier parte del archivo.
rem NFA=[dirección de no reenvío]
rem CLUSTER=[nombre del cluster]
rem

rem set NFA=nombresistpral.dominio.nombre
rem set CLUSTER=www.suempresa.com

rem echo "Cargando la dirección de no reenvío"
rem call ndcontrol executor set nfa %NFA%

rem
rem Los mandatos siguientes están establecidos en los valores por omisión.
```

```

rem Utilícelos para cambiar los valores por omisión

rem call ndcontrol executor set fintimeout 30
rem call ndcontrol executor set fincount 4000
rem
rem El siguiente paso de configuración del Dispatcher es crear
rem un cluster. El Dispatcher encaminará las peticiones enviadas a la
rem dirección de cluster a las máquinas servidor correspondientes
rem definidas para dicho cluster. Puede configurar y dar servicio a
rem varias direcciones de cluster utilizando el Dispatcher.
rem Utilice una configuración parecida para un CLUSTER2, CLUSTER3, etc.
rem

rem echo "Cargando la primera dirección de CLUSTER "
rem call ndcontrol cluster add %CLUSTER%

rem
rem Ahora se deben definir los puertos que utilizará este cluster. Todas
rem las peticiones recibidas por Dispatcher en un puerto definido se
rem reenviarán al puerto correspondiente
rem de una de las máquinas servidor.
rem

rem echo "Creando puertos para CLUSTER: %CLUSTER%"
rem call ndcontrol port add %CLUSTER%:20+21+80

rem
rem El último paso consiste en añadir cada máquina servidor a
rem los puertos de este cluster. De nuevo, se puede utilizar el nombre
rem de sistema principal o la dirección IP de las máquinas servidor.
rem

rem set SERVER1=nombreservidor1.dominio.nombre
rem set SERVER2=nombreservidor2.dominio.nombre
rem set SERVER3=nombreservidor3.dominio.nombre

rem echo "Añadiendo máquinas servidor"
rem call ndcontrol server add %CLUSTER%:20+21+80:
rem %SERVER1%+%SERVER2%+%SERVER3%

rem
rem Ahora, iniciaremos los componentes de reparto del tráfico del
rem Dispatcher. El componente principal de reparto del tráfico se llama
rem gestor y los componentes secundarios de reparto del tráfico son los
rem asesores. Si el gestor y los asesores no se están ejecutando,
rem el Dispatcher envía peticiones en un formato rotatorio.
rem Una vez iniciado el gestor, se emplean decisiones de peso
rem según el número de conexiones nuevas y activas,
rem y las peticiones entrantes se envían al mejor
rem servidor. Los asesores facilitan al gestor más información
rem sobre la capacidad de los servidores para dar servicio a las peticiones
rem y detectan si un servidor está activo. Si un asesor detecta
rem que un servidor está desactivado, se marcará como desactivado (siempre
rem que las proporciones del gestor se hayan definido para incluir
rem la entrada del asesor) y no se encaminarán más peticiones al servidor.

```



```

rem El último paso para configurar los componentes del reparto del
rem tráfico es establecer las proporciones del gestor. Éste actualiza
rem el peso de cada servidor basándose en cuatro
rem políticas:

rem 1. El número de conexiones activas de cada servidor
rem 2. El número de conexiones nuevas de cada servidor
rem 3. La información de entrada procedente de los asesores.
rem 4. La información de entrada procedente del asesor a nivel de sistema.
rem
rem Estas proporciones deben sumar 100. Por ejemplo,
rem si establece las proporciones del cluster mediante
rem     ndcontrol cluster set <cluster> proportions 48 48 4 0
rem las conexiones nuevas y activas contribuirán en un 48%
rem en la asignación de pesos, el asesor contribuirá en un 4%
rem y la información del sistema no se tendrá en cuenta.
rem
rem NOTA: Las proporciones por omisión del gestor están
rem     establecidas en 50 50 0 0
rem echo "Iniciando el gestor..."
rem call ndcontrol manager start

rem echo "Iniciando el asesor FTP en el puerto 21 ..."
rem call ndcontrol advisor start ftp 21
rem echo "Iniciando el asesor HTTP en el puerto 80 ..."
rem call ndcontrol advisor start http 80
rem echo "Iniciando el asesor Telnet en el puerto 23..."
rem call ndcontrol advisor start telnet 23
rem echo "Iniciando el asesor SMTP en el puerto 25..."
rem call ndcontrol advisor start smtp 25
rem echo "Iniciando el asesor POP3 en el puerto 110..."
rem call ndcontrol advisor start pop3 110
rem echo "Iniciando el asesor NNTP en el puerto 119..."
rem call ndcontrol advisor start nntp 119
rem echo "Iniciando el asesor SSL en el puerto 443..."
rem call ndcontrol advisor start ssl 443
rem

rem echo "Estableciendo las proporciones del cluster..."
rem call ndcontrol cluster set %CLUSTER% proportions 58 40 2 0

rem
rem El paso final para configurar la máquina del Dispatcher
rem es asignar un alias a la NIC (tarjeta de interfaz de red).
rem
rem NOTA: NO utilice este mandato en un entorno de alta disponibilidad.
rem Los scripts go* configurarán la NIC y el
rem bucle de retorno según sea necesario.
rem
rem ndcontrol cluster configure %CLUSTER%

rem Si la dirección de cluster se encuentra en una NIC o subred
rem diferentes de la dirección de no reenvío (NFA), utilice el formato
rem siguiente para el mandato de configuración del cluster:
rem ndcontrol cluster configure %CLUSTER% tr0 0xfffff800

```

```

rem donde tr0 es su NIC (tr1 para la segunda tarjeta de Red en Anillo,
rem en0 para la primera tarjeta Ethernet) y 0xfffff800 es una
rem máscara de subred válida para su sitio Web.
rem
rem
rem Los mandatos siguientes están establecidos en los valores por omisión.
rem Utilice estos mandatos como guía para cambiar los valores por omisión.
rem call ndcontrol manager loglevel 1
rem call ndcontrol manager logsize 1048576
rem call ndcontrol manager sensitivity 5,000000
rem call ndcontrol manager interval 2
rem call ndcontrol manager refresh 2
rem
rem call ndcontrol advisor interval ftp 21 5
rem call ndcontrol advisor loglevel ftp 21 1
rem call ndcontrol advisor logsize ftp 21 1048576
rem call ndcontrol advisor timeout ftp 21 unlimited
rem call ndcontrol advisor interval telnet 23 5
rem call ndcontrol advisor loglevel telnet 23 1
rem call ndcontrol advisor logsize telnet 23 1048576
rem call ndcontrol advisor timeout telnet 23 unlimited
rem call ndcontrol advisor interval smtp 25 5
rem call ndcontrol advisor loglevel smtp 25 1
rem call ndcontrol advisor logsize smtp 25 1048576
rem call ndcontrol advisor timeout smtp 25 unlimited
rem call ndcontrol advisor interval http 80 5
rem call ndcontrol advisor loglevel http 80 1
rem call ndcontrol advisor logsize http 80 1048576
rem call ndcontrol advisor timeout http 80 unlimited
rem call ndcontrol advisor interval pop3 110 5
rem call ndcontrol advisor loglevel pop3 110 1
rem call ndcontrol advisor logsize pop3 110 1048576
rem call ndcontrol advisor timeout pop3 110 unlimited
rem call ndcontrol advisor interval nntp 119 5
rem call ndcontrol advisor loglevel nntp 119 1
rem call ndcontrol advisor logsize nntp 119 1048576
rem call ndcontrol advisor timeout nntp 119 unlimited
rem call ndcontrol advisor interval ssl 443 5
rem call ndcontrol advisor loglevel ssl 443 1
rem call ndcontrol advisor logsize ssl 443 1048576
rem call ndcontrol advisor timeout ssl 443 unlimited
rem

```

Asesor de ejemplo

A continuación se muestra un archivo de asesor de ejemplo llamado **ADV_sample**.

```

/**
 * ADV_sample: El asesor HTTP de Network Dispatcher
 *
 *
 * Esta clase define un asesor de ejemplo personalizado para Network
 * Dispatcher.
 * Al igual que todos los asesores, este asesor personalizado amplía la función

```

```

* del asesor base, denominado ADV_Base. Es el asesor base el que realmente
* efectúa la mayoría de las funciones del asesor, como informar del tráfico
* a Network Dispatcher para que se utilicen estos datos en el algoritmo
* de peso de Network Dispatcher.
* El asesor base también realiza las operaciones de conexión
* y cierre de socket, además de proporcionar los métodos de envío y recepción
* para que el asesor los utilice.
* El asesor en sí solamente se utiliza para enviar y recibir
* datos hacia y desde el puerto del servidor que se asesora.
* Los métodos TCP incluidos en el asesor base están temporizados para calcular el
* tráfico. Si se desea, un indicador dentro del constructor en el ADV_base
* sobregraba el tráfico existente con el nuevo tráfico devuelto por
* el asesor.
*
* Nota: De acuerdo con un valor establecido en el constructor, la base
* del asesor notifica periódicamente el tráfico al algoritmo de
* ponderación. Si el asesor real no ha finalizado y no puede devolver
* un valor válido de tráfico, la base del asesor utiliza el valor de
* tráfico anterior.
*
* NOMENCLATURA
*
* El convenio de nomenclatura es el siguiente:
*
* - El archivo debe estar situado en los directorios siguientes
*   de Network Dispatcher:
*
*   nd/servers/lib/CustomAdvisors/
*   (nd\servers\lib\CustomAdvisors en Windows 2000)
*
* - El nombre del asesor debe ir precedido de "ADV_". Sin embargo, el
*   asesor puede arrancarse simplemente con el nombre; por ejemplo,
*   el asesor "ADV_sample" puede arrancarse con "sample".
*
* - El nombre del asesor debe estar en minúsculas.
*
* Por lo tanto, teniendo en cuenta estas normas, este ejemplo
* se identifica de la siguiente manera:
*
*   <directorio base>/lib/CustomAdvisors/ADV_sample.class
*
*
* Los asesores, al que el resto de Network Dispatcher, se deben compilar
* con la versión necesaria de Java.
*
* Para asegurar el acceso a las clases de Network Dispatcher,
* la variable CLASSPATH del sistema debe incluir el archivo
* ibmnd.jar (situado en el subdirectorio lib del directorio base)
*
* Métodos proporcionados por ADV_Base:
*
* - ADV_Base (Constructor):
*

```

```

*   - Parámetros
*     - String sName = Nombre del asesor
*     - String sVersion = Versión del asesor
*     - int iDefaultPort = Número de puerto por omisión a asesorar
*     - int iInterval = Intervalo durante el cual se asesora a los servidores
*     - String sDefaultLogFileName = No utilizado. Debe pasarse como "".
*     - boolean replace = True - sustituir el valor de tráfico calculado
*                               por la base del asesor
*                               False - añadir al valor de tráfico calculado
*                               por la base del asesor
*   - Retorno
*     - Los constructores no tienen valores de retorno.
*
* Debido a que la base del asesor utiliza subprocesos, dispone
* de otros varios métodos que pueden ser utilizados por un asesor. Estos
* métodos se pueden invocar utilizando el parámetro CALLER pasado con
* getLoad().
*
* Estos métodos son los siguientes:
*
*   - send - Enviar un paquete de información en la conexión de socket
*            establecida con el servidor del puerto especificado
*   - Parámetros
*     - String sDataString - Los datos a enviar se envían en forma
*                           de serie de caracteres
*   - Retorno
*     - int RC - Indicación de si los datos se enviaron correctamente:
*               un 0 indica que los datos se enviaron; un entero negativo
*               denota un error.
*
*   - receive - Recibir información desde la conexión de socket.
*   - Parámetros
*     - StringBuffer sbDataBuffer - Los datos recibidos durante la
*                                   llamada de recepción
*   - Retorno
*     - int RC - Indicación de si los datos se enviaron correctamente:
*               un 0 indica que los datos se enviaron; un entero negativo
*               denota un error.
*
* Si la función proporcionada por la base del asesor no es
* suficiente, puede crear la función apropiada dentro del asesor y
* no se tendrán en cuenta los métodos proporcionados por la base
* del asesor.
*
* Una cuestión importante relativa al valor de tráfico devuelto
* es si debe aplicarse al valor de tráfico que se está generando en
* la base del asesor o si debe sustituirlo; existen casos válidos de ambas
* situaciones.
*
* Este ejemplo es en esencia el asesor HTTP de Network Dispatcher.
* Funciona de una manera muy simple:
* Se emite una petición de transmisión (una petición de cabecera
* http). Una vez recibida la respuesta, el método getLoad termina y
* marca la base del asesor para detener la temporización de la petición.
* El método entonces se completa. La información devuelta no se analiza;

```

```

* el valor de tráfico está basado en el tiempo necesario
* para realizar las operaciones de transmisión y recepción.
*/

package CustomAdvisors;
import com.ibm.internet.nd.advisors.*;

public class ADV_sample extends ADV_Base implements ADV_MethodInterface
{
    String COPYRIGHT = "(C) Copyright IBM Corporation 1997,
                        All Rights Reserved.\n";

    static final String  ADV_NAME           = "Sample";
    static final int     ADV_DEF_ADV_ON_PORT = 80;
    static final int     ADV_DEF_INTERVAL   = 7;

    // Nota: La mayoría de los protocolos de servidor precisan un retorno
    // de carro ("\r") y un salto de página ("\n") al final de los mensajes.
    // Si es así, inclúyalos aquí.
    static final String  ADV_SEND_REQUEST   =
        "HEAD / HTTP/1.0\r\nAccept: */*\r\nUser-Agent: " +
        "IBM_Network_Dispatcher_HTTP_Advisor\r\n\r\n";

    /**
     * Constructor.
     *
     * Parámetros: ninguno, pero el constructor de ADV_Base tiene varios
     * parámetros que se le deben pasar.
     */
    public ADV_sample()
    {
        super( ADV_NAME,
            "2.0.0.0-03.27.98",
            ADV_DEF_ADV_ON_PORT,
            ADV_DEF_INTERVAL,
            "", // no se utiliza
            false);
        super.setAdvisor( this );
    }

    /**
     * ADV_AdvisorInitialize
     *
     * Cualquier inicialización específica del asesor que deba
     * efectuarse una vez iniciada la base del asesor.
     * Este método se invoca una sola vez y generalmente no se utiliza.
     */
    public void ADV_AdvisorInitialize()
    {
        return;
    }
}

```

```

/**
 * getLoad()
 *
 * Este método es invocado por la base del asesor para completar la
 * operación del asesor, de acuerdo con datos específicos del protocolo.
 * En este asesor de ejemplo, sólo son necesarias una única transmisión
 * y recepción; para códigos más complejos, se pueden emitir varias
 * operaciones de transmisión y recepción.
 *
 * Parámetros:
 *
 * - iConnectTime - El tráfico actual de acuerdo con el período de
 *                  tiempo que fue necesario para establecer la conexión
 *                  con el servidor a través del puerto especificado.
 *
 * - caller - Una referencia a la clase de la base del asesor en la que
 *             los métodos proporcionados por Network Dispatcher deben realizar
 *             peticiones TCP simples, principalmente de transmisión y recepción.
 *
 * Resultados:
 *
 * - El tráfico - Un valor, expresado en milisegundos, que se puede
 *               sumar al valor de tráfico existente o sustituirlo, según determine el
 *               indicador "replace" del constructor.
 *
 *               Cuanto mayor sea el tráfico, más tiempo necesitará el servidor
 *               para responder; por lo tanto, mayor será el peso utilizado por
 *               Network Dispatcher para el reparto del tráfico.
 *
 *               Si el valor es negativo, se supone que se ha producido un error.
 *               Un error procedente de un asesor indica que el asesor no puede
 *               acceder al servidor y éste se ha marcado como inactivo.
 *               Network Dispatcher no intentará repartir el tráfico hacia un
 *               servidor que esté inactivo.
 *               Network Dispatcher reanudará el reparto de tráfico hacia el
 *               servidor cuando se reciba un valor positivo.
 *
 *               Raramente se devuelve un valor 0 de tráfico; Network Dispatcher
 *               trata esta situación de una forma especial.
 *               Se considera que el valor 0 indica un estado desconocido y, como
 *               respuesta, Network Dispatcher otorga al servidor un peso alto.
 */
public int getLoad(int iConnectTime, ADV_Thread caller)
{
    int iRc;
    int iLoad = ADV_HOST_INACCESSIBLE; // -1

    // Enviar petición tcp
    iRc = caller.send(ADV_SEND_REQUEST);
    if (iRc >= 0)
    {
        // Realizar una recepción
        StringBuffer sbReceiveData = new StringBuffer("");
        iRc = caller.receive(sbReceiveData);
    }
}

```

```

// Si la operación de recepción es satisfactoria, se devuelve un valor 0
// de tráfico.
// Esto es debido al valor "false" del indicador "replace",
// que denota que debe utilizarse el valor de tráfico creado dentro de la
// base del asesor.
// Debido a que no se han utilizado los datos devueltos, no es necesario
// un tráfico adicional.

// Nota: Se sabe que el valor de tráfico devuelto por la base del asesor
// no será 0, por lo tanto no se devolverá un tráfico 0
// para calcular el peso.
if (iRc >= 0)
{
    iLoad = 0;
}
}
return iLoad;
}

} // End - ADV_sample

```

Apéndice G. Ejemplo de una configuración de alta disponibilidad de 2 niveles utilizando Dispatcher, CBR y Caching Proxy

Este apéndice describe cómo realizar una configuración de alta disponibilidad de 2 niveles combinando las funciones de los dos componentes de Network Dispatcher (el componente Dispatcher y el componente CBR) junto con Caching Proxy.

Configuración de la máquina servidor

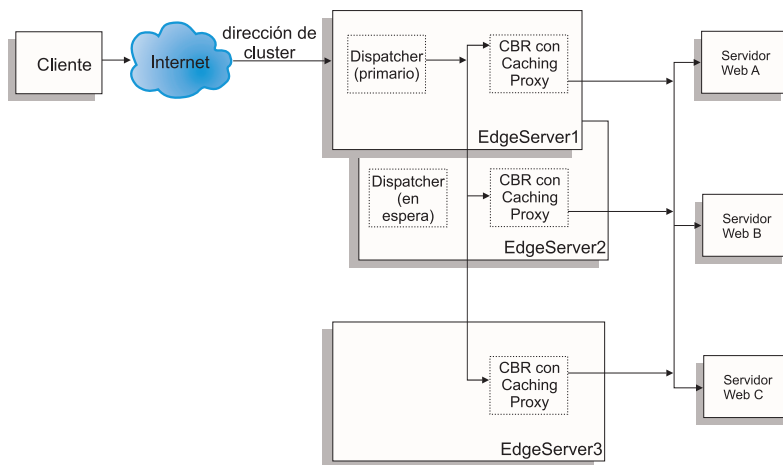


Figura 30. Ejemplo de una configuración de alta disponibilidad de 2 niveles utilizando Dispatcher, CBR y Caching Proxy

La configuración de la máquina servidor correspondiente a Figura 30 es la siguiente:

- EdgeServer1: máquina Dispatcher principal (alta disponibilidad) con ubicación compartida con CBR y Caching Proxy que reparte el tráfico entre servidores Web
- EdgeServer2: máquina Dispatcher en espera (alta disponibilidad) con ubicación compartida con CBR y Caching Proxy
- EdgeServer3: máquina CBR y Caching Proxy
- WebServerA, WebServerB, WebServerC: servidores Web de fondo

La Figura 30 en la página 391 muestra una representación básica de varios servidores (EdgeServer1, EdgeServer2, EdgeServer3) distribuyendo el tráfico entre varios servidores Web de fondo. El componente CBR utiliza Caching Proxy para reenviar peticiones basándose en el contenido del URL a los servidores Web de fondo. El componente Dispatcher se utiliza para repartir el tráfico a los componentes CBR a través de Edge Servers. La función de alta disponibilidad del componente Dispatcher se utiliza para asegurar que las peticiones a los servidores de fondo continúan aunque la máquina principal de alta disponibilidad (EdgeServer1) falle en algún momento.

Líneas generales de la configuración básica:

- Configure Caching Proxy para que sea igual en todos los Edge Servers. Para mejorar la capacidad general de acceso a las páginas Web de los servidores de fondo, configure Caching Proxy para que realice colocación en antememoria. Esto permitirá a los Edge Servers colocar en antememoria las páginas Web que se solicitan con más frecuencia. Para obtener más información sobre cómo configurar Caching Proxy, consulte el manual *IBM WebSphere Edge Server for Multiplatforms Administration Guide*.
- Defina la dirección del cluster y los puertos para que sean los mismos en los componentes CBR y Dispatcher de Network Dispatcher.
- Configure el componente CBR para que sea igual en todos los Edge Servers. Utilice Web Servers A, B y C como servidores en los puertos que desee definir para el cluster. Para obtener más información sobre cómo configurar CBR, consulte el “Capítulo 7. Configuración del componente Content Based Routing” en la página 81.
- Configure el componente Dispatcher para que sea igual en los Edge Servers 1 y 2. Defina todos los Edge Servers como sus servidores en los puertos que desee que se definan en el cluster para que Dispatcher reparta su tráfico. Para obtener más información sobre cómo configurar Dispatcher, consulte el “Capítulo 5. Configuración del componente Dispatcher” en la página 55.
- Configure Edge Server 1 como máquina principal de alta disponibilidad y Edge Server 2 como máquina de alta disponibilidad en espera (reserva). Para obtener más información, consulte “Alta disponibilidad” en la página 165.

Nota:

1. El nombre del sistema principal (por ejemplo, www.company.com) asociado con la dirección del cluster se tendrá que actualizar en el archivo de configuración de Caching Proxy para la directriz “Hostname”.
2. Para evitar que las direcciones del servidor de fondo se muestren en el URL, es posible que tenga que definir para la directriz “SendRevProxyName” el valor “yes” en el archivo de configuración de Caching Proxy.

3. Para asegurar que la colocación en antememoria de Web se utiliza de forma eficiente, defina para la directriz "Caching" el valor "ON" y aumente la directriz "CacheMemory" al tamaño necesario en el archivo de configuración de Caching Proxy.
4. Para realizar la colocación en antememoria por el nombre del URL de entrada en lugar de la dirección IP, añada una línea adicional con la directriz Proxy bajo la sección Mapping Rules del archivo de configuración de Caching Proxy.

Líneas de ejemplo a las que se hace referencia en las notas 1-4 (anteriores):

```

Hostname                www.company.com
SendRevProxyName        yes
Caching                 ON
CacheMemory             128000 K
Proxy                   /* http://www.company.com/* www.company.com

```

5. Recuerde unir mediante un alias la dirección del cluster en la tarjeta de interfaz de red correspondiente EdgeServer1 y de unir mediante un alias la dirección del cluster en el dispositivo loopback en los demás Edge Servers.
6. Si utiliza la plataforma Linux para los Edge Servers, tendrá que instalar un parche en el kernel de Linux. Para obtener más información, consulte "Instalación del parche del kernel de Linux (para suprimir las respuestas a arp en la interfaz de bucle de retorno)" en la página 70.
7. Para CBR, no se debe utilizar la afinidad de puertos (stickytime) cuando se utilicen normas de contenido; si se hace, las normas de contenido no se activarán cuando procesen peticiones a los servidores Web de fondo.

Archivos de configuración de ejemplo:

Los siguientes archivos de configuración de ejemplo son parecidos a los archivos que se crean cuando se prepara una configuración de Edge Server tal como se muestra en la Figura 30 en la página 391. Los archivos de configuración de ejemplo muestran los archivos correspondientes a los componentes Dispatcher y CBR de Network Dispatcher. En la configuración de ejemplo, se utiliza un solo adaptador Ethernet para cada una de las máquinas Edge Server y todas las direcciones están representadas dentro de una subred privada. Los archivos de configuración de ejemplo utilizan las siguientes direcciones IP para las máquinas especificadas:

- EdgeServer1 (Edge Server principal de alta disponibilidad): 192.168.1.10
- EdgeServer2 (Edge Server de reserva de alta disponibilidad): 192.168.1.20
- EdgeServer3 (Edge Server de colocación en antememoria de Web): 192.168.1.30

- Dirección del cluster del sitio Web: 192.168.1.11
- WebServersA-C (Web Servers de fondo): 192.168.1.71, 192.168.1.72 y 192.168.1.73

Archivo de configuración de ejemplo correspondiente al componente Dispatcher en el Edge Server principal de alta disponibilidad:

```
ndcontrol executor start

ndcontrol cluster add 192.168.1.11 primaryhost 192.168.1.10

ndcontrol port add 192.168.1.11:80

ndcontrol server add 192.168.1.11:80:edgeserver1 address 192.168.1.10
ndcontrol server add 192.168.1.11:80:edgeserver2 address 192.168.1.20
ndcontrol server add 192.168.1.11:80:edgeserver3 address 192.168.1.30

ndcontrol manager start manager.log 10004

ndcontrol highavailability heartbeat add 192.168.1.10 192.168.1.20
ndcontrol highavailability backup add primary auto 4567
```

Archivo de configuración de ejemplo correspondiente al componente CBR en los Edge Servers:

```
cbrcontrol set loglevel 1
cbrcontrol executor start

cbrcontrol cluster add 192.168.1.11

cbrcontrol port add 192.168.1.11:80

cbrcontrol server add 192.168.1.11:80:webserverA address 192.168.1.71
cbrcontrol server add 192.168.1.11:80:webserverB address 192.168.1.72
cbrcontrol server add 192.168.1.11:80:webserverC address 192.168.1.73

cbrcontrol rule add 192.168.1.11:80:webA_rule type content
    pattern (URI=*WSA*)|(URI=*wsA*) priority 21
cbrcontrol rule useserver 192.168.1.11:80:webA_rule webserverA

cbrcontrol rule add 192.168.1.11:80:webB_rule type content
    pattern (URI=/WS_B*) priority 22
cbrcontrol rule useserver 192.168.1.11:80:webB_rule webserverB

cbrcontrol rule add 192.168.1.11:80:webC_rule type content
    pattern URI=*webC* priority 23
cbrcontrol rule useserver 192.168.1.21:80:webC_rule webserverC
```

Apéndice H. Otros recursos

Acceso desde la línea de mandatos

En muchos casos, puede utilizar teclas o combinaciones de teclas para realizar operaciones que también se pueden efectuar mediante acciones del ratón. Muchas acciones de menú se pueden iniciar desde el teclado.

Consulte la documentación de su sistema operativo para obtener instrucciones sobre el uso del teclado.

Obtención de ayuda en línea

Network Dispatcher incluye un recurso de ayuda en línea, que describe las tareas que el usuario realiza al instalar, planificar, configurar y utilizar el producto.

Para obtener ayuda para la ventana actual, pulse el signo de interrogación (?) de la esquina superior derecha. Puede elegir entre estas opciones:

Ayuda para campos

Contiene ayuda sensible al contexto para la tarea que está realizando.

Cómo puedo

Es una lista de tareas correspondientes a la ventana actual.

Contenido

Es una tabla de contenido de toda la información de la Ayuda.

Índice Es un índice alfabético de temas de la Ayuda.

Información de consulta

Para obtener más información sobre la utilización de Network Dispatcher, consulte:

- El sitio Web de WebSphere Edge Server, situado en:
<http://www.ibm.com/software/webservers/edgeserver>
- El sitio Web de notas técnicas de Network Dispatcher, situado en:
<http://www.ibm.com/software/webservers/edgeserver/support.html>
Pulse en **Search for Network Dispatcher hints and tips**.

Apéndice I. Avisos

Las referencias hechas en esta publicación a productos, programas o servicios IBM no implican que IBM tenga previsto comercializarlos en todos los países en los que IBM realiza operaciones comerciales. Las referencias a productos, programas o servicios IBM no pretenden afirmar ni implican que únicamente puedan utilizarse dichos productos, programas o servicios IBM. En su lugar puede utilizarse cualquier otro producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM ni ningún otro tipo de derecho protegido legalmente. La evaluación y verificación del funcionamiento conjunto con otros productos, excepto los que IBM indica expresamente, son responsabilidad del usuario.

IBM puede tener patentes o solicitudes de patentes en tramitación que afecten al tema tratado en este documento. La entrega de este documento no otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a: IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, Estados Unidos.

Los licenciarios de este programa que deseen información sobre el mismo con el fin de posibilitar: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) la utilización mutua de la información intercambiada, deben dirigirse a:

Site Counsel
IBM Corporation
P.O. Box 12195
3039 Cornwallis Avenue
Research Triangle Park, NC 27709-2195
Estados Unidos

IBM facilita el programa bajo licencia descrito en este documento, así como todo el material bajo licencia disponible para él, sujeto a las condiciones generales para la contratación de programas IBM bajo licencia.

Este documento no está pensado para su uso en un entorno de trabajo real y se entrega tal cual sin garantías de ninguna clase; por el presente documento se deniega cualquier garantía, incluidas las de comercialización y las de adecuación a un propósito determinado.

Este producto incluye software informático creado y disponible por medio de CERN. Esta notificación debe mencionarse en su totalidad en cualquier producto que incluya, en parte o en su totalidad, el software informático CERN.

Marcas registradas

Los términos siguientes son marcas registradas o marcas comerciales de IBM Corporation en los Estados Unidos o en otros países.

AIX

IBM

IBMLink

LoadLeveler

OS/2

NetView

WebSphere

Lotus es una marca registrada de Lotus Development Corporation en los Estados Unidos o en otros países.

Domino es una marca registrada de Lotus Development Corporation en los Estados Unidos o en otros países.

Tivoli es una marca registrada de Tivoli Systems, Inc. en los Estados Unidos o en otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas o marcas comerciales de Sun Microsystems, Inc. en los Estados Unidos o en otros países.

Solaris es una marca registrada de Sun Microsystems, Inc. en los Estados Unidos o en otros países.

Microsoft y Windows 2000 son marcas registradas o marcas comerciales de Microsoft Corporation en los Estados Unidos o en otros países.

Cisco es una marca registrada de Cisco Systems, Inc. en los Estados Unidos o en otros países.

HP es una marca registrada de Hewlett-Packard Company en los Estados Unidos o en otros países.

Linux es una marca registrada de Linus Torvalds.

Red Hat es una marca registrada de Red Hat, Inc.

UNIX es una marca registrada de The Open Group en los Estados Unidos o en otros países.

Otros nombres de empresas, productos y servicios, que pueden estar señalados con dos asteriscos (**), pueden ser marcas registradas o marcas de servicio de terceros.

Glosario

A

ACK. Bit de control (de acuse de recibo) que no ocupa ningún espacio en la secuencia. Este bit indica que el campo de acuse de recibo de este segmento contiene el siguiente número de secuencia que espera recibir el remitente de este segmento, con lo que se efectúa un acuse de recibo de todos los números de secuencia anteriores.

afinidad entre puertos. La afinidad entre puertos es la función de persistencia que se ha ampliado para abarcar varios puertos. Véase también tiempo de persistencia.

agente. (1) En gestión de sistemas, un usuario que, para una interacción particular, ha asumido la función de agente. (2) Una entidad que representa uno o más objetos gestionados por medio de (a) la emisión de notificaciones concernientes a los objetos y (b) el manejo de peticiones de los gestores para operaciones de gestión para modificar o consultar los objetos.

alcance. En Dispatcher, asesor que emite señales de prueba a un destino determinado e informa de si dicho destino responde.

alias. Nombre adicional asignado a un servidor. Independiza al servidor del nombre de su sistema principal. Debe estar definido en el servidor de nombres de dominio.

alias de bucle de retorno. Dirección IP alternativa asociada con la interfaz de bucle de retorno. La dirección alternativa tiene la ventaja de no anunciarse en una interfaz real.

alta disponibilidad. Característica del Dispatcher mediante la cual un Dispatcher puede asumir las funciones de otro, en el caso de que éste último falle.

alta disponibilidad mutua. La alta disponibilidad mutua permite que dos máquinas Dispatcher sean al mismo tiempo la máquina principal y la máquina de reserva la una respecto de la otra. Véase también máquina de reserva, alta disponibilidad y máquina principal.

ancho de banda. Diferencia entre las frecuencia más alta y más baja de un canal de transmisión; volumen de datos que se pueden enviar cada segundo a través de un circuito de comunicación determinado.

anotaciones en binario. Permite que la información del servidor se almacene en archivos binarios y luego se procese para analizar la información del servidor que se recoge con el paso del tiempo.

API. Interfaz de programación de aplicaciones. La interfaz (convenios de denominación) mediante la cual un programa de aplicación accede al sistema operativo y otros servicios. Una API se define a nivel de código fuente y proporciona un nivel de abstracción entre la aplicación y el kernel (u otros programas de utilidad privilegiados) para asegurar la portabilidad del código.

asesor. Los asesores con una función de Network Dispatcher. Los asesores reúnen y analizan la información de retorno de los servidores individuales e informan a la función de gestor.

asistente. Diálogo dentro una aplicación que utiliza instrucciones paso a paso para ayudar a un usuario a realizar una tarea determinada.

C

Caching Proxy. Servidor proxy de antememoria que puede ayudar a acelerar el tiempo de respuesta del usuario final mediante esquemas de antememoria muy efectivos. El filtro de PICS flexible ayuda a los administradores de la red a controlar el acceso a la información basada en la Web en una ubicación central.

Calidad de Servicio (Quality of Service, QoS). Propiedades funcionales de un servicio de red, tales como el rendimiento, el tiempo de respuesta y la prioridad. Algunos protocolos aplicar requisitos de QoS a los paquetes o corrientes de datos.

CBR. Content Based Routing (Encaminamiento basado en el contenido). Componente de Network Dispatcher. CBR trabaja en combinación con Caching Proxy para repartir el tráfico de peticiones entrantes destinadas a servidores HTTP o HTTPS, de acuerdo con el contenido de las páginas Web y utilizando tipos de normas especificadas.

cbrcontrol. Proporciona la interfaz con el componente Content Based Router de Network Dispatcher.

cbrserver. En Content Based Router, gestiona las peticiones procedentes del ejecutor, el gestor y los asesores.

CGI. Siglas de Common Gateway Interface, que significan interfaz de pasarela común. Es una norma para el intercambio de información entre un servidor Web y un programa externo. El programa externo puede estar escrito en cualquier lenguaje soportado por el sistema operativo y ejecuta tareas que el servidor no realiza habitualmente, como el proceso de formularios.

Cisco Consultant. Componente de IBM Network Dispatcher. Cisco Consultant utiliza la tecnología Network Dispatcher para proporcionar información sobre distribución de tráfico en tiempo real a Cisco Content Services Switch.

Cisco CSS Switch. Cualquiera de los conmutadores Cisco de la serie CSS 11000, que se utilizan para el reenvío de paquetes y el encaminamiento por contenido.

cliente. Un sistema o proceso que solicita un servicio a otro sistema o proceso. Por ejemplo, una estación de trabajo o un PC que solicita documentos HTML de un servidor Web Lotus Domino Go es un cliente de dicho servidor.

cluster. En Dispatcher, un grupo de servidores TCP o UDP que se utilizan para el mismo propósito y se identifican por un sólo nombre de sistema principal. Véase también célula.

colocar en estado activo. Permitir que un servidor reciba nuevas conexiones.

colocar en estado inactivo. Interrumpir todas las conexiones activas con un servidor y detener cualquier conexión o paquete nuevo que se envíe a ese servidor.

cortafuegos. Sistema que conecta una red privada, tal como una red corporativa, a una red pública, tal como Internet. Este sistema contiene programas que limitan el acceso entre las dos redes. Véase también *pasarela proxy*.

D

daemon. Siglas de "Disk And Execution Monitor". Programa que no interviene explícitamente, pero que permanece en estado latente a la espera de que se produzca una determinada condición o condiciones. El causante de la condición no necesita conocer la existencia del daemon (pero a menudo un programa ejecuta una acción para invocar explícitamente un daemon).

detención progresiva. Finalizar un proceso permitiendo que las operaciones finalicen normalmente.

dirección. Código exclusivo asignado a cada estación de trabajo o dispositivo conectado a una red. Una dirección IP estándar es un campo de dirección de 32 bits. Este campo contiene dos partes. La primera es la dirección de red; la segunda es el número del sistema principal.

dirección de alcance. En la modalidad de alta disponibilidad del Dispatcher, dirección del destino al que el asesor debe enviar señales de prueba para determinar si el destino responde.

dirección de cluster. En el Dispatcher, la dirección a la que se conectan los clientes.

dirección de destino. La dirección de la máquina remota de alta disponibilidad a la que se envían señales de prueba y respuestas.

dirección de no reenvío (nfa). La dirección IP principal de la máquina Network Dispatcher, utilizada para administración y configuración.

dirección de origen. En la modalidad de alta disponibilidad de Dispatcher, dirección de la máquina asociada de alta disponibilidad que envía señales de prueba.

dirección de retorno. Dirección IP exclusiva o nombre de sistema principal. Se configura en la máquina Dispatcher y es utilizada por Dispatcher como dirección de origen cuando reparte el tráfico de peticiones de los clientes destinadas al servidor.

dirección de servidor. Código exclusivo asignado a cada sistema que proporciona servicios compartidos a otros sistema de una red; por ejemplo, un servidor de archivos, un servidor de impresión o un servidor de correo. Una dirección IP estándar es un campo de dirección de 32 bits. La dirección del servidor puede ser la dirección IP en formato decimal separado por puntos o el nombre del sistema principal.

dirección IP. Dirección de protocolo Internet. Es la dirección exclusiva de 32 bits que especifica la ubicación real de cada dispositivo o estación de trabajo en una red. También se la conoce como dirección Internet.

dirección MAC. Concepto de LAN o de emulación de LAN.

Dispatcher. Componente de Network Dispatcher que reparte de forma eficiente el tráfico TCP o UDP entre los grupos de servidores individuales asociados. La máquina Dispatcher es el servidor que ejecuta el código Dispatcher.

E

ejecutor. Una de varias funciones de Dispatcher. El ejecutor encamina las peticiones a los servidores TCP o UDP; también supervisa el número de conexiones nuevas, activas y finalizadas y realiza la recogida de basura de las conexiones completadas o restauradas. El ejecutor proporciona a la función de

gestor las conexiones nuevas y las conexiones activas. En Cisco Consultant, el ejecutor contiene información de configuración y la información necesaria para conectar con Cisco CSS Switch.

encaminador. Dispositivo que reenvía paquetes entre redes. La ruta seleccionada para el reenvío está basada en información sobre las capas de red y en tablas de encaminamiento, que a menudo son generadas por productos de encaminamiento.

escalable. Relativo a la capacidad de un sistema para adaptarse fácilmente a una mayor o menor intensidad de uso, volumen o demanda. Por ejemplo, un sistema escalable puede adaptarse de forma eficiente para trabajar con redes de mayor o menor tamaño ejecutando tareas con un grado diverso de complejidad.

estación de gestión de red. En el Protocolo Simple de Gestión de Red (SNMP), estación que ejecuta los programas de aplicación de gestión que supervisan y controlan los elementos de la red.

estado FIN. Estado de una transacción que ha finalizado. Una vez que una transacción se encuentra en estado de finalización, el recolector de basura de Network Dispatcher puede vaciar la memoria reservada para la conexión.

estrategia. En la modalidad de alta disponibilidad de Dispatcher, palabra clave que especifica la manera de efectuar la recuperación tras producirse un error en la máquina activa.

Ethernet. Tipo estándar de red de área local (LAN). Permite que varias estaciones accedan a voluntad al medio de transmisión sin una coordinación previa, evita la contención utilizando detección de portadora y transmisión diferida, y resuelve la contención mediante detección de colisión y transmisión. Los sistemas Ethernet utilizan diversos protocolos de software, entre ellos TCP/IP.

F

FIN. Un bit de control (final) que ocupa un número de secuencia y que indica que el remitente no enviará más datos ni información de control que ocupe espacio de secuencia.

final de rango. En el reparto del tráfico basado en normas, un valor superior especificado en una norma. El valor por omisión de este parámetro depende del tipo de norma.

FQDN. Fully Qualified Domain Name (nombre de dominio totalmente calificado). Es el nombre completo de un sistema, que consta de su nombre de sistema principal local y su nombre de dominio, incluido un dominio de nivel superior (TLD, "top-level domain"). Por ejemplo, "venera" es un nombre de sistema principal y "venera.isi.edu" es un FQDN. Normalmente un FQDN es suficiente para definir una dirección Internet exclusiva para cualquier sistema principal de la red. Este proceso se denomina "resolución de nombres" y hace uso del Sistema de Nombres de Dominio ("Domain Name System", DNS).

FTP (Protocolo de transferencia de archivos). Protocolo de aplicación utilizado para transferir archivos entre los sistemas de una red. FTP necesita un ID de usuario y a veces una contraseña para permitir el acceso a los archivos de un sistema principal remoto.

G

gestor. Una de las diversas funciones de Network Dispatcher. El gestor establece los pesos basándose en contadores internos del ejecutor y en la realimentación proporcionada por los asesores. A continuación el ejecutor utiliza los pesos para realizar el reparto del tráfico.

GRE. Generic Routing Encapsulation. Protocolo que permite que un protocolo de red arbitrario A se transmita sobre cualquier otro protocolo arbitrario B, mediante la encapsulación de paquetes de A dentro de paquetes de GRE, que a su vez están contenidos dentro de paquetes de B.

H

HTML. Siglas de "Hypertext Markup Language" (lenguaje de códigos de hipertexto). Es el lenguaje utilizado para crear documentos de hipertexto. Los documentos de hipertexto incluyen enlaces a otros documentos que contienen información adicional sobre el término o tema resaltado. HTML controla el formato del texto y la posición de las áreas de entrada de formularios, por ejemplo, así como los enlaces navegables.

HTTP (Protocolo de transferencia de hipertexto). El protocolo utilizado para transferir y visualizar documentos de hipertexto.

I

ICMP. Internet Control Message Protocol (Protocolo de control de mensajes de Internet). Protocolo de control de mensaje e informe de errores entre un servidor de sistema principal y una pasarela a Internet.

IMAP. Internet Message Access Protocol (protocolo de acceso de mensajes de Internet). Protocolo que permite a un cliente acceder y manipular mensajes de correo electrónico en un servidor. Permite manipular las carpetas de mensajes remotos (buzones de correo) de un modo funcionalmente equivalente a los buzones locales.

inicio de rango. En el reparto del tráfico basado en normas, un valor inferior especificado en una norma. El valor por omisión de este parámetro depende del tipo de norma.

interfaz de bucle de retorno. Interfaz que elude las funciones de comunicación innecesarias cuando la información está dirigida a una entidad dentro del mismo sistema.

Internet. El conjunto mundial de redes interconectadas que utilizan el conjunto de protocolos Internet y permiten el acceso público.

intranet. Una red segura y privada que integra los estándares y las aplicaciones de Internet (como por ejemplo los navegadores Web) en la estructura de red informática existente de una organización.

IP. (Internet Protocol). Protocolo Internet. Protocolo no orientado a la conexión que encamina datos a través de una red o redes interconectadas. IP actúa como intermediario entre las capas superiores de protocolo y la capa física.

IPSEC. Internet Protocol Security (Seguridad de protocolo Internet). Estándar en desarrollo para la seguridad de la capa de proceso del paquete o la red de la comunicación por la red.

L

LAN. Red de área local. Una red de sistemas de dispositivos conectados dentro de un área geográfica limitada para las comunicaciones entre sí y que puede conectarse a una red mayor.

lbc. Load-Balancing Consultant

lbccontrol. En Cisco Consultant, proporciona la interfaz con el Cisco CSS Switch.

lbcserver. En Cisco Consultant, contiene la información de configuración y ejecuta los mandatos.

M

Mailbox Locator. Componente de Network Dispatcher. Para los protocolos IMAP o POP3, Mailbox Locator es un proxy que selecciona un servidor apropiado de acuerdo con el ID de usuario y la contraseña.

máquina servidor. Servidor que el Dispatcher agrupa con otros servidores en un único servidor virtual. El Dispatcher reparte el tráfico entre las máquinas servidor. Es sinónimo de servidor agrupado en cluster.

máquina servidor TCP. Servidor que Network Dispatcher enlaza con otros servidores en un único servidor virtual. Network Dispatcher reparte el tráfico TCP entre las máquinas servidor TCP. Es sinónimo de servidor agrupado en cluster.

máscara de red. Para subredes en Internet, máscara de 32 bits que se utiliza para identificar los bits de dirección de subred en la parte de una dirección IP referente al sistema principal.

máscara de subred. Para subredes en Internet, máscara de 32 bits que se utiliza para identificar los bits de dirección de subred en la parte de una dirección IP referente al sistema principal.

métrica. Proceso o mandato que devuelve un valor numérico que se puede utilizar para repartir el tráfico en la red; por ejemplo, el número de usuarios conectados actualmente.

Metric Server. Antes denominado Server Monitor Agent (SMA). Metric Server proporciona la métrica específica del sistema al gestor de Network Dispatcher.

MIB. (1) Management Information Base (base de información de gestión). Conjunto de objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) Una definición para la información de gestión que especifica la información disponible en un sistema principal o en una pasarela y las operaciones permitidas.

mlcontrol. Proporciona la interfaz con el componente Mailbox Locator de Network Dispatcher.

mlserver. En Mailbox Locator, contiene la información de configuración y ejecuta los mandatos.

N

ndcontrol. Proporciona la interfaz con el componente Dispatcher de Network Dispatcher.

ndserver. En Dispatcher, gestiona las peticiones procedentes de la línea de mandatos y destinadas al ejecutor, el gestor y los asesores.

Network Address Port Translation. NAPT, también conocido como correlación de puertos. Permite configurar varios daemons de servidor dentro de un mismo servidor físico para recibir las peticiones en números de puerto diferentes.

Network Address Translation. LAN Virtual de NAT (Network Address Translator). Mecanismo de hardware que actualmente se desarrolla y utiliza para ampliar las direcciones Internet que ya están en uso. Permite utilizar direcciones IP duplicadas dentro de una empresa y direcciones exclusivas fuera de ella.

NIC. Network Interface Card (tarjeta de interfaz de red). Tarjeta adaptadora que se instala en un sistema para proporcionar una conexión física a una red.

NNTP. Siglas de Network News Transfer Protocol, que significan protocolo de red de transferencia de artículos de debate. Protocolo TCP/IP para transferir artículos de debate.

nodo gestionado. En las comunicaciones de Internet, una estación de trabajo, servidor o encaminador que contiene un agente de gestión de red. En el protocolo Internet (IP), el nodo gestionado contiene generalmente un agente SNMP (Protocolo simple de gestión de red).

nombre de sistema principal. Nombre simbólico asignado a un sistema principal. Los nombres de sistema principal se convierten en direcciones IP por medio de un servidor de nombres de dominio.

nombre de sitio. Un nombre de sitio es un nombre de sistema principal que no se puede resolver y que el cliente solicitará. Por ejemplo, considere un sitio Web que tiene 3 servidores (1.2.3.4, 1.2.3.5 y 1.2.3.6) configurados para el mismo sitio *www.dnsload.com*. Cuando un cliente solicita este nombre de sitio, el resultado de la resolución de nombres será una de estas tres direcciones IP de servidor. El nombre de sitio debe ser un nombre de dominio totalmente calificado, por ejemplo: *dnsload.com*. Un nombre no calificado, por ejemplo, *dnsload* no sería un nombre de sitio válido.

norma. En el reparto del tráfico basado en normas, un mecanismo para agrupar servidores de manera que se pueda seleccionar un servidor basándose en una información distinta de la dirección de destino y el puerto.

notación decimal con puntos. Representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits, escritos en base 10 y separados por puntos. Se utiliza para representar las direcciones IP.

P

paquete. La unidad de datos que se dirige entre un origen y un destino en Internet o en cualquier otra red con paquetes.

pasarela. Unidad funcional que interconecta dos redes de sistemas con arquitecturas distintas.

PICS. Platform for Internet Content Selection (Plataforma para la selección del contenido de Internet). Los clientes habilitados para PICS permiten a los usuarios determinar los servicios de clasificación que desean utilizar y, para cada servicio, las clasificaciones aceptables y las inaceptables.

ping. Un mandato que envía paquetes de petición de eco de Protocolo de mensajes de control Internet (ICMP) a un sistema principal, una pasarela o un encaminador, con la esperanza de recibir una respuesta.

POP3. Post Office Protocol 3 (protocolo de oficina de correos 3). Protocolo utilizado para intercambiar correo en una red y acceder a buzones de correo.

principal. En la modalidad de alta disponibilidad de Dispatcher, máquina tras arrancar encamina activamente los paquetes. Su máquina asociada, la máquina de reserva, supervisa el estado de la máquina principal y toma el control si es necesario. Véase también máquina de reserva y alta disponibilidad.

prioridad. En el reparto del tráfico basado en normas, nivel de importancia asignado a una norma determinada cualquiera. El Dispatcher evalúa las normas desde el nivel de prioridad más alta hasta el nivel de prioridad más baja.

protocolo. Conjunto de normas que gobiernan la actividad de unidades funcionales de un sistema de comunicación para que ésta pueda tener lugar. Los protocolos pueden determinar características de bajo nivel de las interfaces entre máquina y máquina, tales como el orden en el que se envían los bits de un byte; también pueden determinar intercambios de alto nivel entre programas de aplicación, tal como la transferencia de archivos.

proximidad en la red. Proximidad de dos entidades de red, como un cliente y un servidor, que Site Selector determina midiendo el tiempo de ida y vuelta.

puerto. Número que identifica un dispositivo de comunicación abstracto. Los servidores Web utilizan por omisión el puerto 80.

R

red privada. Red separada en la que el Dispatcher se comunica con servidores agrupados en cluster por razones de rendimiento.

reserva. En la modalidad de alta disponibilidad de Dispatcher, máquina asociada a la máquina principal. Supervisa el estado de la máquina principal y toma el control si es necesario. Véase también alta disponibilidad y máquina principal.

RMI. Remote Method Invocation (invocación de método remoto). Parte la biblioteca de lenguajes de programación Java que permite que un programa Java que se ejecuta en un sistema acceda a objetos y métodos de otro programa Java que se ejecuta en un sistema diferente.

RPM. Red Hat Package Manager.

ruta. Camino que sigue el tráfico de la red desde el punto de origen hasta el punto de destino.

S

script CGI. Programa CGI escrito en un lenguaje de scripts, como por ejemplo Perl o REXX, que utiliza la interfaz de pasarela común para ejecutar tareas que el servidor no realiza habitualmente, como el proceso de formularios.

señal de prueba. Paquete simple que se envía entre dos máquinas Dispatcher en la modalidad de alta disponibilidad y que es utilizado por el Dispatcher de reserva para supervisar el estado del Dispatcher activo.

servicio. Función ofrecida por uno o más nodos; por ejemplo, HTTP, FTP y Telnet.

servidor. Sistema que proporciona servicios compartidos a otros sistemas de una red. Un servidor de archivos, un servidor de impresión o un servidor de correo son ejemplos de servidores.

servidor de nombres de dominio. DNS. Servicio general de consulta de datos, distribuido y duplicado, que se utiliza principalmente en Internet para convertir nombres de sistema principal en direcciones de Internet. También designa el estilo de nombre de sistema principal utilizado en Internet, aunque más propiamente ese nombre se denomina nombre de dominio totalmente calificado. DNS se puede configurar para que utilice una secuencia de servidores de nombres, de acuerdo con los dominios contenidos en el nombre buscado, hasta que se encuentre una coincidencia.

servidor en cluster. Servidor que el Dispatcher agrupa con otros servidores en un único servidor virtual. Network Dispatcher reparte el tráfico TCP o UDP entre estos servidores agrupados en cluster.

shell. Software que acepta y procesa las líneas de mandatos de la estación de trabajo de un usuario. Korn es uno de los diversos shell disponibles para UNIX.

sistema principal. Sistema, conectado a una red, que proporciona un punto de acceso a esa red. Un sistema principal puede ser un cliente, un servidor o ambas cosas a la vez.

Site Selector. Componente de reparto del tráfico basado en DNS de Network Dispatcher. Site Selector reparte el tráfico para los servidores de una red de área amplia (WAN), utilizando mediciones y valores de ponderación recogidos a partir del Metric Server que se ejecuta en esos servidores.

SMTP. Simple Mail Transfer Protocol (protocolo simple de transferencia de correo). En el conjunto de protocolos de Internet, protocolo de aplicación para transferir correo entre usuarios en el entorno Internet. SMTP especifica las secuencias de intercambio de correo y el formato de los mensajes. Presupone que el protocolo subyacente es TCP (protocolo de control de transmisión).

SNMP. Simple Network Management Protocol (protocolo simple de gestión de red). Protocolo estándar de Internet, definido en STD 15, RFC 1157, que está diseñado para gestionar los nodos de una red IP. SNMP no está limitado a la utilización de TCP/IP. Se puede utilizar para gestionar y supervisar toda clase de dispositivos, tales como sistemas PC, encaminadores de red, concentradores de cableado, tostadores y máquinas de jukebox.

SPARC. Arquitectura de procesador escalable

sscontrol. Proporciona la interfaz con el componente Site Selector de Network Dispatcher.

SSL. Siglas de "Secure Sockets Layer". Estrategia de seguridad, de uso generalizado, desarrollada por Netscape Communications Corp. en colaboración con RSA Data Security Inc. SSL permite a la máquina cliente autenticar al servidor, y cifrar todos los datos y peticiones. El URL de un servidor seguro protegido por SSL empieza por https (en lugar de http).

ssserver. En Site Selector, gestiona las peticiones procedentes de la línea de mandatos y destinadas al nombre de sitio, el gestor y los asesores.

SYN. Un bit de control en el segmento entrante que ocupa un número de secuencia y que se utiliza en la inicialización de una conexión para indicar dónde comenzará la numeración de la secuencia.

T

TCP. Siglas de Transmission Control Protocol, que significan protocolo de control de transmisión. Es un protocolo de comunicaciones utilizado en Internet. TCP proporciona el intercambio fiable de información de sistema a sistema. Utiliza IP como protocolo subyacente.

TCP/IP . Siglas de Transmission Control Protocol/Internet Protocol, que significan protocolo de control de transmisión/protocolo Internet. Un conjunto de protocolos diseñados para permitir la comunicación entre redes sin tener en cuenta las tecnologías de comunicación utilizadas en cada una de ellas.

Telnet. Protocolo de emulación de terminal. Protocolo de aplicación TCP/IP para servicios de conexión remota. Telnet permite a un usuario situado en una ubicación acceder a un sistema principal remoto como si la estación de trabajo del usuario estuviera conectada directamente a dicho sistema remoto.

tiempo de persistencia. Intervalo que transcurre entre el cierre de una conexión y la apertura de una nueva conexión y durante el cual las peticiones del cliente se envían al mismo servidor utilizado en la primera conexión. Después de transcurrido el tiempo de persistencia, las peticiones del cliente se pueden enviar a un servidor diferente del primero.

timeout. El intervalo de tiempo permitido a una operación para que se produzca.

tipo de norma. En el reparto del tráfico basado en normas, un indicador de la información que debe evaluarse para determinar si una norma es cierta.

TOS. Tipo de servicio. Un campo de un byte de la cabecera IP del paquete SYN.

TTL. Un TTL (tiempo de vida) de DNS es el número de segundos durante los que un cliente puede poner en antememoria la respuesta dirigida a la resolución de nombres.

U

ubicación compartida. Cuando no se dispone de una máquina dedicada, el Dispatcher se instala en la misma máquina en la que realiza el reparto del tráfico.

Nota: La ubicación compartida sólo es aplicable a los sistemas operativos AIX, Red Hat Linux y Solaris.

ubicación compartida con varias direcciones. La ubicación compartida con varias direcciones permite al usuario especificar una dirección del servidor con ubicación compartida diferente de la dirección de no reenvío (NFA) de la configuración. Véase también ubicación compartida.

UDP. Siglas de User Datagram Protocol, que significan protocolo de datagrama de usuario. En el conjunto de protocolos de Internet, un protocolo que proporciona un servicio de datagrama no fiable y sin conexión. Permite que un programa de aplicación de una máquina o proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza el protocolo Internet (IP) para entregar datagramas.

URI. Universal Resource Identifier (identificador universal de recursos). Dirección codificada para cualquier recurso de la Web, como, por ejemplo, un documentoHTML, imagen, video clip, programa, etc.

URL. Uniform Resource Locator (localizador universal de recursos). Forma estándar de especificar la ubicación de un objeto, habitualmente una página Web, en Internet. El URL es el formato de dirección utilizado en la World-Wide Web. El URL se utiliza en los documentos HTML para especificar el destino de un hipervínculo, que a menudo es otro documento HTML (que puede residir en otro sistema).

usuario root. Autorización no restringida para modificar y acceder a cualquier parte del sistema operativo AIX, Red Hat Linux o Solaris, y que generalmente corresponde al usuario que gestiona el sistema.

V

valor por omisión. Un valor, atributo u opción que se presupone cuando no se indica ninguno explícitamente.

VPN. Virtual Private Network (Red privada virtual). Red compuesta de uno o varios túneles de IP seguros que se conectan a dos o más redes.

W

WAN. Wide Area Network (red de área amplia). Red que proporciona servicios de comunicaciones a una zona geográfica mayor que la atendida por una red de área local o red de área metropolitana, y que puede utilizar o proporcionar recursos de comunicaciones.

WAP. Wireless Application Protocol (protocolo de aplicación inalámbrica). Estándar internacional abierto para aplicaciones que hacen uso de comunicaciones inalámbricas, por ejemplo, el acceso a Internet desde un teléfono móvil.

WAS. Websphere Application Server (servidor de aplicaciones Websphere).

Web. Red de servidores HTTP que contienen programas y archivos, muchos de los cuales son documentos de hipertexto que contienen enlaces con otros documentos situados en servidores HTTP. También llamada World Wide Web.

WLM. Workload Manager (gestor de la carga de trabajo). Asesor incluido con Dispatcher. Está diseñado para funcionar sólo en combinación con servidores de sistemas OS/390 que ejecutan el componente Workload Manager (WLM) de MVS.

Índice

A

- activo, colocar un servidor en estado 307, 339
- administración remota 21, 205
- afinidad (persistencia)
 - activa de cookie 193, 298
 - afinidad entre puertos 189, 191, 288
 - alteración temporal de afinidad de norma 191
 - cómo funciona 188
 - desactivar ahora 192, 280, 284
 - Mailbox Locator 97
 - máscara de dirección de afinidad 190
 - opción de norma 193
 - pasiva de cookie 193, 194, 298
 - persistencia (alteración temporal de afinidad de norma) 191, 192, 303
 - SDA (Server Directed Affinity) 188
 - SSL ID (reenvío cbr) 53
 - stickymask 190, 288
 - stickytime 53, 289, 298
 - tiempo de persistencia 188, 190
 - URI 193, 195, 298
- afinidad activa de cookie 193, 298
- afinidad de URI 193, 195, 298
- afinidad entre puertos 189, 288
- afinidad pasiva de cookie 193, 194, 298
- AIX
 - instalación 13
 - requisitos 12
- alias
 - dispositivo de bucle de retorno 65
 - parche del kernel de Linux 65, 70
 - la NIC 61, 89
- alta disponibilidad 27, 44, 47, 165
 - configurar 166
 - mutua 48, 167, 260, 262, 274
 - ndcontrol 272
 - primaryhost 262
 - scripts 170
 - goActive 171
 - goldle 172
 - alta disponibilidad (continuación)
 - scripts (continuación)
 - goInOp 171
 - goStandby 171
 - highavailChange 172
 - sistema principal primario 260
 - alta disponibilidad mutua 48, 166, 167
 - primaryhost 260, 262
 - scripts 171
 - toma del control 170
 - alteración temporal de afinidad de norma
 - server 307
 - servidor 191
 - alteración temporal de la afinidad de norma
 - server 303
 - anotaciones
 - binario, para estadísticas de servidor 198
 - anotaciones en binario para estadísticas de servidores 198, 208
 - añadir
 - cluster 262, 354
 - puerto para un cluster 63, 292, 370, 371
 - servidor a un puerto 64, 307, 339, 373
 - apCnsvchits 201
 - apSvcConnections 200
 - archivo de anotaciones
 - archivo, establecer el nombre
 - para el asesor 320, 350
 - para el gestor 329, 364
 - nivel, establecer
 - para el asesor 207, 256, 322, 349, 351
 - para el gestor 207, 327, 362
 - para el servidor 207
 - para el subagente 207
 - tamaño, establecer
 - para el asesor 207, 256, 319, 322, 349, 351
 - para el gestor 207, 282, 327, 329, 362, 365
 - para el servidor 207
 - para el subagente 207
- archivo de anotaciones (continuación)
 - utilización de archivos de anotaciones de CBR 217
 - utilización de los archivos de anotaciones de Cisco Consultant 219
 - utilización de los archivos de anotaciones de Mailbox Locator 218
 - utilización de los archivos de anotaciones de Metric Server 219
 - utilización de los archivos de anotaciones de Network Dispatcher 207
 - utilización de los archivos de anotaciones de Site Selector 218
- archivo de correlación de direcciones
 - ejemplo de 185
- archivos de configuración de ejemplo 377
- asesor 384
 - componente Dispatcher (AIX) 377
 - componente Dispatcher (Windows) 381
- asesor ftp 252, 318
- asesor http 252, 318
- asesor personalizado (personalizable) 145
- asesor WAS (WebSphere Application Server) 146
- asesor WLM (Workload Manager) 149
- asesores
 - archivos de configuración de ejemplo 384
 - cbrcontrol 252
 - Cisco Consultant
 - detener 350, 352
 - informe sobre el estado de 351
 - iniciar 350, 352
 - intervalo de 348, 351
 - lista de 349, 350
 - mostrar estado 350, 352
 - nombre de 348
 - puerto de 348

asesores (continuación)

Cisco Consultant (continuación)

- tiempo de caducidad del informe 350, 352
- tiempo de espera de conexión de servidores 348, 351
- tiempo de espera de recepción de servidores 349, 351
- versión de 351, 352

componente Dispatcher

- asesor self 144
- asesor ssl2http 143
- ssl2http, asesor 78

Dispatcher, componente 139

- asesor self 164
- Caching Proxyasesor 143
- detección rápida de errores 142
- detener 255
- informe sobre el estado de 256
- iniciar 64, 255
- inicio/detención 140
- intervalo de 141, 256
- lista de 143, 256
- nombre de 252
- personalizar 145
- puerto de 259
- report 257
- tiempo de caducidad del informe 142, 255
- tiempo de espera de conexión de servidores 142, 252, 255
- tiempo de espera de recepción de servidores 142, 254, 256
- versión de 257

iniciar 130

lbcontrol 348

limitación en Linux 139

lista de 254, 350

mlcontrol 252

ndcontrol 252

opción de URL, asesor

HTTP 154

petición/respuesta del asesor

HTTP 154

Site Selector

- detener 321, 323
- informe sobre el estado de 320, 322
- iniciar 320, 322
- interval 318
- intervalo de 321
- list 319
- lista de 320, 321

asesores (continuación)

Site Selector (continuación)

- loglevel 319
- nombre de 318
- puerto de 252, 318
- tiempo de caducidad del informe 321, 323
- tiempo de espera de conexión de servidores 318, 321
- tiempo de espera de recepción de servidores 319, 322
- versión de 321, 323
- sscontrol 318, 326

asesores, componente de Network

Dispatcher

- informe sobre el estado de 349
- iniciar 64
- lista de 351

asistente, configuración

Dispatcher 4

ataques de denegación de servicio, detección 197

halfopenaddressreport 291

maxhalfopen 291

avisos 397

ayuda en línea 395

ayuda para campos 395

C

Caching Proxy 77

configurar para CBR 87

Caching Proxyasesor 143

cambiar

número de conexiones

finalizadas 210

temporizador de

inactividad 210

tiempo de espera de

finalización 210

capa de sockets seguros. 64

CBR

cbrcontrol falla 238

cbrcontrol falla en Solaris 239

con Caching Proxy

conexiones SSL 78

configurar 92

palabra clave mapport 78

ssl2http, asesor 78

visión general 76

configuración

configuración de la máquina

CBR 86

visión general de las

tareas 81

crear alias para la NIC 89

CBR (continuación)

error sintáctico o de

configuración 239

ifconfig, mandato 89

inicio y detención 217

ndadmin falla 238

no se ejecuta 238

no se realiza el reparto del tráfico

para las peticiones 239

planificar 75

requisitos de hardware y de software 75

tabla de resolución de

problemas 224

utilización del componente

Dispatcher 52

valores de reparto del tráfico 134

Cisco Consultant

configuración

configurar la máquina

CSS 128

ejemplo 42

visión general de las tareas 125

ejecutor 120

gestor 120

iniciar 219

inicio y detención 219

lbcontrol 120

lbcontrol falla 242

lbserver 119

mandatos 347

ndadmin 120

ndadmin falla 242

no arranca 242

no se puede crear registro para puerto 14099 242

planificar 119

requisitos de hardware y de software 119

tabla de resolución de

problemas 226

utilización 219

valor de reparto de tráfico

tiempo de espera del asesor para servidores 348

valores de reparto del tráfico

tiempo de caducidad del

informe del asesor 350, 352

tiempo de espera del asesor

para servidores 349, 351

clave privada

para autenticación remota 205

- clave pública
 - para autenticación remota 205
 - claves
 - ndkeys 150, 206
 - cluster
 - añadir 262, 354
 - cambiar el tiempo de espera para estado de finalización 210
 - cambiar número de conexiones finalizadas 210
 - cbrcontrol 258
 - comodín 61
 - configurar la dirección 61
 - definir 61, 129, 262, 354
 - eliminar 262, 343, 353, 354
 - establecer proporciones 65, 130
 - lbcontrol 353
 - mlcontrol 258
 - ndcontrol 258
 - proporciones 258
 - visualizar
 - estado de este cluster 262, 354
 - cluster comodín 61, 262
 - con Caching Proxy para proxy transparente 187
 - para combinar las configuraciones de los servidores 185
 - para repartir tráfico de cortafuegos 186
 - colocar un servidor en estado
 - activo 307, 339
 - inactivo 307, 338, 339
 - collocated (palabra clave) 156, 307
 - cómo puedo 395
 - comprobar si hay
 - ruta adicional 68
 - conexiones, establecer el grado de importancia 135, 262
 - conexiones activas 200
 - conexiones nuevas 201
 - conexiones SSL
 - asesor 143
 - configuración de ibmproxy 78
 - para CBR 78
 - problema al habilitar 232
 - configuración
 - archivos de ejemplo 377
 - asistente 4
 - Cisco Consultant 125
 - Content Based Routing 81
 - correlación entre Consultant y CSS 121
 - definir cluster 129
 - configuración (continuación)
 - definir servidores con reparto del tráfico 129
 - Dispatcher, componente 55
 - establecer proporciones de cluster 130
 - iniciar el gestor 130
 - Mailbox Locator 99
 - métodos
 - asistente (CBR) 85
 - asistente (Mailbox Locator) 102
 - asistente (Site Selector) 116
 - asistente (Dispatcher) 58
 - GUI (CBR) 84
 - GUI (Cisco Consultant) 127
 - GUI (Dispatcher) 57
 - GUI (Mailbox Locator) 101
 - GUI (Site Selector) 115
 - línea de mandatos (CBR) 82
 - línea de mandatos (Cisco Consultant) 126
 - línea de mandatos (Dispatcher) 56
 - línea de mandatos (Mailbox Locator) 100
 - línea de mandatos (Site Selector) 114
 - scripts (CBR) 84
 - scripts (Cisco Consultant) 127
 - scripts (Dispatcher) 56
 - scripts (Mailbox Locator) 101
 - scripts (Site Selector) 114
 - Metric Server 130
 - probar 130
 - puerto 129
 - Site Selector 113
 - tareas, avanzadas 131
 - verificar 69
 - connecttimeout
 - Cisco Consultant 348
 - Site Selector 318
 - consulta de mandatos
 - lectura 245
 - Content Based Routing 27
 - configuración
 - configuración de la máquina CBR 86
 - visión general de las tareas 81
 - planificar 75
 - requisitos de hardware y de software 75
 - Content Based Routing (continuación)
 - tabla de resolución de problemas 224
 - utilización 217
 - utilización del componente Dispatcher 52
 - valores de reparto del tráfico 134
 - correlación entre Consultant y CSS 121
- D**
- DB2, asesor 144
 - default.cfg 60, 89, 103, 117
 - definir
 - cluster 262, 354
 - dirección de no reenvío 61, 267, 355, 356
 - puerto para un cluster 63, 292, 370, 371
 - servidor a un puerto 64, 307, 339, 373
 - desactivar un servidor 192, 280, 282, 284, 365
 - desinstalar
 - en AIX 14
 - en Linux 18
 - en Solaris 20
 - en Windows 2000 23
 - detener
 - asesor 255, 321, 323
 - Cisco Consultant 219
 - ejecutor 267
 - gestor 284, 329, 331, 365, 367
 - diagnóstico de problemas
 - aparece pantalla azul al iniciar ejecutor de Network Dispatcher 235
 - CBR no funcionará 238
 - cbrcontrol falla en Solaris 239
 - comportamiento inesperado al cargar un archivo de configuración grande 237
 - Dispatcher, Microsoft IIS y SSL no funcionan 232
 - Dispatcher no se ejecuta 230
 - Dispatcher y el servidor no responderán 230
 - el mandato cbrcontrol o ndadmin falla 238
 - el mandato lbcontrol o ndadmin falla 242
 - el mandato mlcontrol o ndadmin falla 240

diagnóstico de problemas

(continuación)

- el mandato ndcontrol o ndadmin falla 232
- el mandato sscontrol o ndadmin falla 241
- error al ejecutar Dispatcher cuando Caching Proxy está instalado 234
- Error sintáctico o de configuración 239
- excepción de E/S de Metric Server en Windows 2000 243
- GUI no arranca correctamente 234
- La alta disponibilidad de Dispatcher no funciona 231
- la alta disponibilidad en la modalidad de área amplia de Network Dispatcher no funciona 237
- la GUI no se visualiza correctamente 234
- la vía de acceso de descubrimiento impide la devolución de tráfico con Network Dispatcher 235
- las anotaciones de Metric Server indican que "se necesita una firma para poder acceder al agente" 244
- lbserver no arranca 242
- los asesores muestran que todos los servidores están inactivos 236
- los asesores no funcionan 232
- Mailbox Locator no se ejecuta 239
- mandato cbrserver detenido 240
- mensaje de error al intentar visualizar la ayuda en línea 233
- mensaje falso de error al iniciar ndserver en Solaris 2.7 234
- Metric Server no notifica cargas 243
- Network Dispatcher no puede procesar y reenviar una trama 235
- no se encaminan las peticiones Dispatcher 231
- No se puede añadir pulso 231
- no se puede añadir un puerto 240

diagnóstico de problemas

(continuación)

- no se puede crear registro para puerto 14099 242
- no se realiza el reparto del tráfico para las peticiones 239
- números de puerto que utiliza Dispatcher 227
- números de puerto utilizados por CBR 228
- números de puerto utilizados por Cisco Consultant 230
- números de puerto utilizados por Mailbox Locator 228
- números de puerto utilizados por Site Selector 229
- paneles de ayuda ocultos 234
- problemas habituales y su solución 230, 232, 238, 239, 241, 242, 243
- rutas sobrantes 232
- se recibe error de Mailbox Locator al intentar añadir un puerto 241
- Site Selector no efectúa reparto rotatorio (Solaris) 241
- Site Selector no reparte el tráfico correctamente 242
- Site Selector no se ejecuta 241
- SNMPD no funciona 232
- ssserver no se inicia en Windows 2000 241
- diagramas de sintaxis ejemplos 246
- lectura 245
- parámetros 245
- signos de puntuación 245
- símbolos 245
- dirección de no reenvío definir 61
- establecer 267, 355, 356
- Dispatcher configuración configuración de máquinas servidor TCP 65
- Dispatcher, componente alta disponibilidad no funcional 231
- aparece pantalla azul al iniciar ejecutor 235
- comportamiento inesperado al cargar un archivo de configuración grande 237
- conexión a una máquina remota 232

Dispatcher, componente

(continuación)

- configuración configurar la máquina Network Dispatcher 58
- configurar una red privada 184
- visión general de las tareas 55
- el servidor no responde 230
- encaminamiento por contenido 52
- error al iniciar ndserver en Solaris 2.7 234
- error cuando Caching Proxy está instalado 234
- GUI no arranca correctamente 234
- iniciar 209
- la alta disponibilidad en la modalidad de área amplia de Network Dispatcher no funciona 237
- la GUI no se visualiza correctamente 234
- la vía de acceso de descubrimiento impide la devolución de tráfico con Network Dispatcher 235
- los asesores muestran que todos los servidores están inactivos 236
- los asesores no funcionan 232
- MS IIS y SSL no funcionan 232
- NAT/ NAPT 50
- ndadmin falla 232
- ndcontrol falla 232
- no puede reenviar una trama 235
- no se ejecuta 230
- no se puede abrir ventana de ayuda 233
- no se puede añadir pulso 231
- peticiones no repartidas 231
- planificar 45
- reenvío MAC 49
- requisitos de hardware y de software 45
- rutas sobrantes (Windows 2000) 232
- SNMPD no funciona 232
- tabla de resolución de problemas 221
- utilización 209

- Dispatcher, componente
(*continuación*)
 - valores de reparto del tráfico 134
 - grado de importancia dado a la información de estado 135
 - índice de corrección 138
 - intervalos de asesor 141
 - intervalos de gestor 137
 - pesos 136
 - tiempo de caducidad del informe del asesor 142
 - tiempo de espera del asesor para servidores 142
 - umbral de sensibilidad 138
 - ventanas de ayuda ocultas 234
- DPID2 212

E

- ejecutor
 - detener 267
 - iniciar 267, 356
- ejemplo de iniciación rápida 1
- ejemplos
 - gestionar servidores locales 34, 35, 37, 39, 40, 42
 - iniciación rápida 1
- eliminar
 - cluster 262, 343, 353, 354
 - puerto de un cluster 292, 370, 371
 - ruta adicional 69
 - servidor de un puerto 307, 338, 339, 373
- en línea, ayuda 395
- enlaces explícitos 183
- específico de cluster
 - proportions 341
- establecer
 - con qué frecuencia debe el gestor consultar el ejecutor 138, 282, 363, 365
 - dirección de cluster 63
 - dirección de no reenvío 58
 - grado de importancia en el reparto del tráfico 262
 - índice de corrección 138, 283, 328, 330, 364, 367
 - nivel de anotaciones
 - para el asesor 207, 256, 322, 349, 351
 - para el gestor 327, 362
 - nombre del archivo de anotaciones 320, 350

- establecer (*continuación*)
 - para el gestor 329, 364
 - peso de un servidor 282, 284, 307, 339, 365, 373
 - peso máximo
 - para los servidores de un puerto específico 136, 292, 370, 371
 - sensibilidad a la actualización de pesos 138, 283, 328, 330, 364, 367
 - tamaño máximo de las anotaciones
 - para el asesor 207, 256, 319, 322, 349, 351
 - para el gestor 282, 327, 329, 362, 365
 - tiempo de intervalo
 - para que el asesor consulte los servidores 256, 321, 348, 351
 - para que el gestor actualice el servidor 137, 282, 327, 329, 362, 365
- estado, visualizar
 - servidores de un puerto específico 292, 370, 371
 - todos los clusters 354
 - un cluster 354
- Ethernet NIC
 - ibmnd.conf
 - configuración para Solaris 59
- executor
 - cbrcontrol 263
 - lbcontrol 355
 - mlcontrol 263
 - ndcontrol 263

F

- file
 - cbrcontrol 268
 - lbcontrol 357
 - mlcontrol 268
 - ndcontrol 268
 - sscontrol 324
- Firewall 23

G

- gestión de Network Dispatcher 205
- gestor
 - detener 284, 329, 331, 365, 367
 - iniciar 64, 130, 283, 329, 330, 364, 367
 - peso fijo 137
 - proporciones 135, 353

- gestor (*continuación*)
 - versión de 284, 329, 331, 365, 367
- goActive 171
- goIdle 172
- goInOp 171
- goStandby 171
- grado de importancia en el reparto del tráfico, establecer 135, 262
- GRE (Generic Routing Encapsulation)
 - OS/390 163
 - soporte de área amplia 163
- GUI 5
 - resolución 234
- H**
- help
 - cbrcontrol 270
 - lbcontrol 359
 - mlcontrol 270
 - ndcontrol 270
- highavailChange 172
- host
 - lbcontrol 360
- I**
- ibmnd.conf
 - configuración para Solaris 59
- ibmproxy 78, 87
 - asesor 143
- ifconfig, mandato 63, 66, 89, 160
- imap
 - alterar 97
- inactivo, colocar un servidor en estado 307, 338, 339
- índice de corrección, establecer 138, 283, 328, 330, 364, 367
- informe de instantánea de estadísticas, visualizar 282, 328, 329, 363, 365
- inhabilitación 395
- iniciar
 - asesor 64, 255, 320, 322
 - Cisco Consultant 219
 - Dispatcher 3
 - ejecutor 60, 267, 356
 - gestor 64, 283, 329, 330, 364, 367
 - Metric Server 219
 - servidor 60, 61
 - Site Selector 218
- inicio de sesión/fin de sesión 11
- inicio y detención
 - CBR 217
 - Dispatcher 209

inicio y detención (*continuación*)

Mailbox Locator 217

instalación

en AIX 13

en Linux 17

en Solaris 20

en Windows 2000 23

Network Dispatcher 11

interfaz gráfica de usuario (GUI) 5

intervalo, establecer frecuencia con que

el asesor consulta los

servidores 256, 321, 348, 351

el gestor actualiza los pesos para

el ejecutor 137, 282, 327, 329, 362, 365

el gestor consulta el

ejecutor 138, 282, 363, 365

J

Java Runtime Environment

(JRE) 13, 17, 20

L

lbcontrol, mandato

advisor 348

cluster 353

executor 355

file 357

help 359

host 360

log 361

manager 362

metric 368

puerto 370

servidor 372

set 374

status 375

lbserver

no arranca 230, 242

límite de conexiones finalizadas

cambiar 210

línea de mandatos

acceso 395

ejemplo de configuración 3

Linux

instalación 17

parche del kernel

versiones 2.2.12, 2.2.13 72

versiones 2.4.x 71

requisitos 16

log

binario, para estadísticas de

servidor 278, 361

cbrcontrol 278

log (*continuación*)

lbcontrol 361

mlcontrol 278

ndcontrol 278

M

Mailbox Locator

configuración

configuración de la

máquina 103

visión general de las

tareas 99

error de proxy al intentar añadir

un puerto 241

inicio y detención 217

mandato mlserver detenido 240

mlcontrol falla 240

mlserver 96

ndadmin falla 240

no se ejecuta 239

no se puede añadir un

puerto 240

planificar 95

protocolo del proxy 291, 292

requisitos de hardware y de

software 95

staletimeout 260, 264, 290

tabla de resolución de

problemas 224

tiempo de espera de

inactividad 260, 264, 290

utilización 217

valores de reparto del

tráfico 134

visión general 96

manager

cbrcontrol 279

lbcontrol 362

mlcontrol 279

ndcontrol 279

sscontrol 327

mandato cbrcontrol

advisor 252

cluster 258

executor 263

file 268

help 270

log 278

manager 279

metric 285

puerto 287

rule 294

servidor 302

set 308

sistema principal 277

mandato cbrcontrol (*continuación*)

status 309

mandato mlcontrol

advisor 252

cluster 258

executor 263

file 268

help 270

log 278

manager 279

metric 285

puerto 287

servidor 302

set 308

sistema principal 277

status 309

mandatos

cbrcontrol

advisor 252

cluster 258

executor 263

file 268

help 270

log 278

manager 279

metric 285

puerto 287

rule 294

servidor 302

set 308

sistema principal 277

status 309

Cisco Consultant 347

ifconfig 63, 160

para unir el dispositivo de
bucle de retorno por medio
de un alias 66

lbcontrol

asesor 348

cluster 353

executor 355

file 357

help 359

host 360

log 361

manager 362

metric 368

puerto 370

servidores, configurar 372

set 374

status 375

mlcontrol

advisor 252

cluster 258

executor 263

mandatos (*continuación*)

mlcontrol (*continuación*)

file 268
help 270
log 278
manager 279
metric 285
puerto 287
servidor 302
set 308
sistema principal 277
status 309

ndconfig 63, 160

ndcontrol

advisor 252
alta disponibilidad,
control 272
cluster 258
executor 263
file 268
help 270
indicador de mandatos 250
log 278
manager 279
metric 285
para controlar el asesor 64
para controlar el gestor 64
para definir la dirección de no
reenvío 61, 267, 355, 356
para definir un puerto 63
para definir un servidor 64
puerto 287
rule 294
servidor 302
set 308
sistema principal 277
status 309
subagente, configurar
SNMP 310

netstat

para comprobar las
direcciones IP y los alias 68

ruta

para suprimir una ruta
adicional 68, 69

Site Selector 317

sscontrol

advisor 318
file 324
help 326
manager 327
métrica 332
nameserver 333
rule 334
server 338

mandatos (*continuación*)

sscontrol (*continuación*)

set 340
sitename 341
status 345

marcas registradas 398

máscara de dirección de
afinidad 190, 288

método de reenvío cbr 52
stickytime 53

método de reenvío mac 49

método de reenvío NAT 50

metric

cbrcontrol 285
lbcccontrol 368
mlcontrol 285
ndcontrol 285

Metric Server

excepción de E/S de Metric
Server en Windows 2000 243

iniciar 130

inicio y detención 219

las anotaciones de Metric Server
indican que "se necesita una
firma para poder acceder al
agente" 244

Metric Server no notifica
cargas 243

tabla de resolución de
problemas 226

utilización 219

visión general 150

métrica

sscontrol 332

métricas del sistema

configurar 332, 368

configure 285

establecimiento de proporción de
importancia 135, 258, 259, 353

migración 11

mostrar

contadores internos 266, 356

estado de

servidores de un puerto 292,
370, 371

un cluster o todos los
clusters 262, 354

informe de estadísticas 282, 328,
329, 363, 365

informe sobre el estado de un
asesor 256, 320, 322, 349

lista de

asesores que proporcionan
métricas 256, 321, 351

mostrar (*continuación*)

número de versión

del asesor 257, 321, 323
del gestor 284, 329, 331, 365,
367

valores globales y sus valores por
omisión

de un asesor 257, 321, 322
para el gestor 284, 329, 330,
365, 367

N

nameserver

sscontrol 333

ndconfig 160

mandato 63

ndcontrol, mandato

abreviar parámetros de
mandatos 250

advisor 252

asesor 64

cluster 258

ejecutor 61

executor 263

file 268

gestor 64

help 270

highavailability 272

indicador de mandatos 250

log 278

manager 279

metric 285

puerto 63, 287

rule 294

servidor 64, 302

set 308

sistema principal 277

status 309

subagent 310

ndkeys 151, 206

ndserver

iniciar 3

netstat, mandato 68

Network Address Port Translation
(NAPT) 50

Network Address Translation
(NAT) 49, 50

Network Dispatcher

configuración

CBR 81

Cisco Consultant 125

Mailbox Locator 99

configurar

Dispatcher, componente 58,
86, 103, 116

- Network Dispatcher (*continuación*)
 - configurar (*continuación*)
 - Site Selector 113
 - consideraciones referentes a la
 - planificación 45, 107
 - ejemplo de iniciación rápida 1
 - funcionamiento y gestión 205, 218, 219
 - funciones 25, 33
 - instalación 11
 - requisitos de hardware 45, 75, 95, 107, 119
 - requisitos de software 45, 75, 95, 107, 119
 - resolución de problemas 221
 - tareas de configuración,
 - avanzadas 131
 - utilización y gestión 205
 - ventajas 26
 - visión general 25, 33
- NIC
 - alias 61
 - correlación (para Windows 2000) 62
 - Ethernet (para Solaris) 59
- norma de contenido 52, 181
- nuevas conexiones, establecer el
 - grado de importancia 135, 259, 353
- nuevas funciones, V2.0
 - afinidad de URI 31
 - afinidad pasiva de cookie 31
 - AIX v5.1, soporte de 28
 - Asesor DB2 33
 - Asesores específicos del cluster (o
 - sitio Web) 32
 - Cisco Consultant 29
 - Detección de denegación de
 - servicio 32
 - encaminamiento por contenido
 - del Dispatcher 30
 - HTTP Advisor Req/Rsp 32
 - idioma nacional para Linux y
 - Solaris 28
 - Mailbox Locator 29
 - mejoras en el manejo de CBR 30
 - Metric Server 29
 - NAT y NAPT 30
 - nuevo soporte estándar de
 - idioma nacional para el
 - chino 28
 - Particionamiento del
 - servidor 31
 - Proporciones específicas del
 - cluster 31

- nuevas funciones, V2.0 (*continuación*)
 - Red Hat Linux v7.1, soporte
 - de 28
 - Salidas de usuario mejoradas 32
 - Site Selector 29
 - SuSE Linux v7.1, soporte de 28
- número de conexiones
 - finalizadas 210

O

- opción de menú Supervisor 210
- opciones de proximidad 110
- OS/390
 - soporte de GRE 163

P

- persistencia (afinidad)
 - activa de cookie 193, 298
 - afinidad entre puertos 189, 191, 288
 - alteración temporal de afinidad
 - de norma 191
 - cómo funciona 188
 - desactivar ahora 192, 280, 284
 - máscara de dirección de
 - afinidad 190
 - pasiva de cookie 193, 194, 298
 - persistencia (alteración temporal
 - de afinidad de norma) 191, 192, 303
 - SDA (Server Directed
 - Affinity) 188
 - stickymask 190, 288
 - stickytime 53, 289, 298
 - tiempo de persistencia 188, 190
 - URI 193, 298
- peso
 - cómo lo establece el gestor 137, 203
 - ejemplo para xml 202
 - establecer
 - límite para todos los
 - servidores de un
 - puerto 136, 292, 370, 371
 - para un servidor 307, 339, 373
 - peso máximo, establecer
 - para los servidores de un puerto
 - específico 136, 292, 370, 371
- planificar
 - CBR 75
 - Cisco Consultant 119
 - Dispatcher, componente 45
 - Mailbox Locator 95
 - Site Selector 107

- planificar la instalación 25, 45, 107
- pop3
 - alterar 97
- posibilidad de acceso 395
- primaryhost 262
- probar
 - configuración 130
- productos componentes 45
- proporciones 130
- proximidad en la red 110
- puerto
 - cbrcontrol 287
 - configuración 129
 - lbcccontrol 370
 - mlcontrol 287
 - ndcontrol 287
- puerto comodín 63, 292
 - asesor ping 144
 - para dirigir el tráfico de puertos
 - no configurados 187
- puertos
 - añadir 292, 370, 371
 - comodín 63
 - definir para un cluster 63, 292, 370, 371
 - eliminar 292, 370, 371
 - establecer el peso máximo 136, 292, 370, 371
 - para asesores 252, 318
 - visualizar
 - estado de los servidores de
 - este puerto 292, 370, 371

R

- recogida de basura 210
- recursos 395
- red privada, utilizar con
 - Dispatcher 184
- reenvío, método
 - cbr 52
 - mac 49, 51
 - mac, nat o cbr 289
 - MAC, NAT o cbr 53
 - NAT 50
- reiniciar todos los servidores con
 - pesos normalizados 283, 328, 330, 364, 366
- reparto del tráfico basado en
 - normas 173
 - ancho de banda
 - compartido 177, 179, 295, 301
 - ancho de banda reservado 177, 178, 295, 301
 - conexiones activas en el
 - puerto 176, 295

- reparto del tráfico basado en normas (*continuación*)
 - conexiones por segundo 175, 295
 - contenido de la petición 52, 181, 296
 - dirección IP del cliente 175, 295, 300, 334, 337
 - gama de normas, por componente 173
 - hora del día 175, 295, 300, 334, 337
 - métrica promedio 180
 - métrica total 179
 - metricall 334
 - metricavg 334
 - opción de evaluación 182
 - opción de evaluación de servidor 182
 - puerto cliente 177, 295
 - siempre cierta 180, 296, 300, 335, 336
 - tipo de servicio (TOS) 177, 295, 300
- requisitos
 - AIX 12
 - Linux 16
 - Solaris 19
 - Windows 2000 22
- requisitos de hardware
 - CBR 75
 - Cisco Consultant 119
 - Dispatcher, componente 45
 - Mailbox Locator 95
 - Site Selector 107
- requisitos de software
 - CBR 75
 - Cisco Consultant 119
 - Dispatcher, componente 45
 - Mailbox Locator 95
 - Site Selector 107
- reserva, alta disponibilidad 47, 272
 - configurar 166
- resolución de la GUI 234
- resolución de problemas 221
 - aparece pantalla azul al iniciar ejecutor de Network Dispatcher 235
 - CBR no funcionará 238
 - cbrcontrol falla en Solaris 239
 - comportamiento inesperado al cargar un archivo de configuración grande 237
 - Dispatcher, Microsoft IIS y SSL no funcionan 232

- resolución de problemas (*continuación*)
 - Dispatcher no se ejecuta 230
 - Dispatcher y el servidor no responderán 230
 - el mandato cbrcontrol o ndadmin falla 238
 - el mandato lbcccontrol o ndadmin falla 242
 - el mandato mlcontrol o ndadmin falla 240
 - el mandato ndcontrol o ndadmin falla 232
 - el mandato sscontrol o ndadmin falla 241
 - error al ejecutar Dispatcher cuando Caching Proxy está instalado 234
 - Error sintáctico o de configuración 239
 - excepción de E/S de Metric Server en Windows 2000 243
 - GUI no arranca correctamente 234
 - La alta disponibilidad de Dispatcher no funciona 231
 - la alta disponibilidad en la modalidad de área amplia de Network Dispatcher no funciona 237
 - la GUI no se visualiza correctamente 234
 - la vía de acceso de descubrimiento impide la devolución de tráfico con Network Dispatcher 235
 - las anotaciones de Metric Server indican que "se necesita una firma para poder acceder al agente" 244
 - lbserver no arranca 242
 - los asesores muestran que todos los servidores están inactivos 236
 - los asesores no funcionan 232
 - Mailbox Locator no se ejecuta 239
 - mandato cbrserver detenido 240
 - mensaje de error al intentar visualizar la ayuda en línea 233
 - mensaje falso de error al iniciar ndserver en Solaris 2.7 234
 - Metric Server no notifica cargas 243

- resolución de problemas (*continuación*)
 - Network Dispatcher no puede procesar y reenviar una trama 235
 - no se encaminan las peticiones Dispatcher 231
 - No se puede añadir pulso 231
 - no se puede añadir un puerto 240
 - no se puede crear registro para puerto 14099 242
 - no se realiza el reparto del tráfico para las peticiones 239
 - números de puerto que utiliza Dispatcher 227
 - números de puerto utilizados por CBR 228
 - números de puerto utilizados por Cisco Consultant 230
 - números de puerto utilizados por Mailbox Locator 228
 - números de puerto utilizados por Site Selector 229
 - paneles de ayuda ocultos 234
 - problemas habituales y su solución 230, 232, 238, 239, 241, 242, 243
 - rutas sobrantes 232
 - se recibe error de Mailbox Locator al intentar añadir un puerto 241
 - Site Selector no efectúa reparto rotatorio (Solaris) 241
 - Site Selector no reparte el tráfico correctamente 242
 - Site Selector no se ejecuta 241
 - SNMPD no funciona 232
 - ssserver no se inicia en Windows 2000 241
- RMI (Remote Method Invocation) 205
- rule
 - cbrcontrol 294
 - ndcontrol 294
 - sscontrol 334
- ruta, mandato 68, 69
- rutas sobrantes 68, 69

S

- scripts 170
 - goActive 171
 - goldle 172
 - goInOp 171
 - goStandby 171

- scripts (*continuación*)
 - highavailChange 172
 - salida de usuario 139
 - scripts de salida de usuario 139
 - detección de la denegación de servicio 197
 - managerAlert 139
 - managerClear 139
 - serverDown 139
 - serverUp 139
 - SDA (Server Directed Affinity) 154, 188
 - sensibilidad a la actualización de pesos, establecer 138, 283, 328, 330, 364, 367
 - server
 - advisorrequest 305
 - advisorresponse 306
 - collocated 303, 307
 - cookievalue 305
 - dirección 303
 - fixedweight 304
 - mapport 304
 - returnaddress 305
 - router 304
 - sin persistencia (alteración temporal de afinidad de norma) 307
 - sin persistencia (alteración temporal de la afinidad de norma) 303
 - sscontrol 338
 - weight 303
 - Server Directed Affinity (SDA) 154, 188
 - servidor
 - activar 284, 365
 - añadir 307, 339, 373
 - cbrcontrol 302
 - colocar en estado activo 307, 339
 - colocar en estado inactivo 307, 338, 339
 - definir para un puerto 64, 307, 339, 373
 - desactivar 192, 280, 282, 284, 365
 - dirección 373
 - eliminar 307, 338, 339, 373
 - establecer el peso 307, 339, 373
 - físico 152
 - lbcontrol 372
 - lógico 152
 - mapport 78
 - mlcontrol 302
 - servidor (*continuación*)
 - ndcontrol 302
 - particionamiento 152
 - reiniciar todos con pesos normalizados 283, 328, 330, 364, 366
 - servidores de vinculación
 - específica 63, 64, 139, 159
 - set
 - cbrcontrol 308
 - lbcontrol 374
 - mlcontrol 308
 - ndcontrol 308
 - sscontrol 340
 - Simple Network Management Protocol (SNMP) 211
 - sistema principal
 - cbrcontrol 277
 - mlcontrol 277
 - ndcontrol 277
 - sistema principal primario 167
 - Site Selector
 - configuración
 - configuración de la máquina 116
 - visión general de las tareas 113
 - distribución de tráfico de HA Dispatchers 172
 - ejemplo de configuración 40
 - inicio y detención 218
 - mandatos 317
 - ndadmin falla 241
 - no efectúa reparto rotatorio para tráfico procedente de clientes Solaris 241
 - no reparte el tráfico correctamente con rutas duplicadas 242
 - no se ejecuta 241
 - planificar 107
 - requisitos de hardware y de software 107
 - sscontrol falla 241
 - ssserver no se inicia en Windows 2000 241
 - tabla de resolución de problemas 225
 - utilización 218
 - valores de reparto del tráfico 134
 - visión general 39
 - sitename
 - sscontrol 341
 - SNMP 207, 211
 - sobrantes, rutas 68
 - Solaris
 - apr publish, mandato 63
 - configurar la máquina Network Dispatcher 58
 - instalación 20
 - requisitos 19
 - soporte de área amplia 157
 - ejemplo de configuración 161
 - utilizando asesores remotos 159
 - utilizando Dispatcher remoto 157
 - utilizando GRE 163
 - sscontrol, mandato
 - advisor 318
 - file 324
 - help 326
 - manager 327
 - métrica 332
 - nameserver 333
 - rule 334
 - server 338
 - set 340
 - sitename 341
 - status 345
 - SSL 64
 - ssl2http, asesor 78, 143
 - status
 - cbrcontrol 309
 - lbcontrol 375
 - mlcontrol 309
 - ndcontrol 309
 - subagentes 207, 211
 - ndcontrol 310
 - suprimir
 - cluster 262, 343, 353, 354
 - puerto de un cluster 292, 370, 371
 - ruta adicional 69
 - servidor de un puerto 307, 338, 339, 373
 - suprimir rutas sobrantes 69
- T**
- tablas de resolución de problemas
 - CBR 224
 - Cisco Consultant 226
 - Dispatcher, componente 221
 - Mailbox Locator 224
 - Metric Server 226
 - Site Selector 225
 - teclado 395
 - tiempo de espera de inactividad 209, 260, 264, 290

tiempo de espera para estado de finalización
cambiar 210

U

ubicación compartida, Network
Dispatcher y servidor 58, 64, 155, 159, 303, 307
ubicación compartida con diferentes direcciones 64
utilización de Network
Dispatcher 205

V

Valores de reparto del tráfico (optimización) 134
valores globales, visualizar todos de un asesor 257, 321, 322
para el gestor 284, 329, 330, 365, 367
versión, visualizar
asesor 257, 321, 323
gestor 284, 329, 331, 365, 367
visión general
configuración de CBR 81
configuración de Cisco
Consultant 125
configuración de Mailbox
Locator 99
configuración de Site
Selector 113
configuración del componente
Dispatcher 55
visualizar
contadores internos 266, 356
estado de
servidores de un puerto 292, 370, 371
un cluster o todos los clusters 262, 354
informe de estadísticas 282, 328, 329, 363, 365
informe sobre el estado de un asesor 256, 320, 322, 349
lista de
asesores que proporcionan métricas 256, 321, 351
número de versión
del asesor 257, 321, 323
del gestor 284, 329, 331, 365, 367
valores globales y sus valores por omisión
de un asesor 257, 321, 322

visualizar (*continuación*)
valores globales y sus valores por omisión (*continuación*)
para el gestor 284, 329, 330, 365, 367

W

Windows 2000
cluster configure, mandato 62
configurar la máquina Network
Dispatcher 59
instalación 23
mandato ndconfig 63
requisitos 22



GC10-3180-04



Spine information:



WebSphere[™] Edge Server para
multiplataformas

Network Dispatcher
Guía de administración

Versión 2.0