

WebSphere Edge Server (Multiplattform)



Network Dispatcher Administratorhandbuch

Version 2.0

WebSphere Edge Server (Multiplattform)



Network Dispatcher Administratorhandbuch

Version 2.0

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen in „Anhang I. Bemerkungen“ auf Seite 413 gelesen werden.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business Symbol ist eine Marke der International Business Machines Corporation
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle Java-basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Siebte Auflage (Oktober 2001)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
WebSphere Edge Server for Multiplatforms, Administration Guide,
IBM Form GC31-8496-06,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2001
© Copyright IBM Deutschland GmbH 2001

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Oktober 2001

Inhaltsverzeichnis

Tabellen	xi	Vorteile von Network Dispatcher	28
Abbildungsverzeichnis	xiii	Neue Merkmale	30
Willkommen	xv	Komponenten von Network Dispatcher	36
Senden von Kommentaren	xv	Dispatcher im Überblick	36
Kapitel 1. Erste Schritte...für einen schnellen Start!	1	Content Based Routing (CBR) im Überblick	40
Voraussetzungen	2	Mailbox Locator im Überblick	41
Vorbereitungen	2	Site Selector im Überblick	43
Dispatcher konfigurieren	3	Consultant für Cisco CSS Switches im Überblick	45
Konfiguration von der Befehlszeile aus	4	Hohe Verfügbarkeit	48
Konfiguration mit dem Konfigurationsassistenten	5	Dispatcher	48
Mit der grafischen Benutzerschnittstelle (GUI) konfigurieren	6	CBR, Mailbox Locator, Site Selector	48
Konfiguration testen	8	Kapitel 4. Planung für Dispatcher	49
Arten von Cluster-, Port- und Serverkonfigurationen	8	Hardware- und Softwarevoraussetzungen	49
Kapitel 2. Network Dispatcher installieren	11	Überlegungen bei der Planung	50
Voraussetzungen für AIX	12	Hohe Verfügbarkeit	52
Installation unter AIX	13	Einfache hohe Verfügbarkeit	52
Installation vorbereiten	14	Gegenseitige hohe Verfügbarkeit	53
Installationsschritte	14	MAC-Weiterleitungsmethode (mac) des Dispatchers	54
Voraussetzungen für Red Hat Linux oder SuSE Linux	17	NAT/NAPT-Weiterleitungsmethode (nat) des Dispatchers	55
Installation unter Linux	18	Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)	57
Installation vorbereiten	18	Kapitel 5. Dispatcher konfigurieren	61
Installationsschritte	19	Konfigurations-Tasks im Überblick	61
Voraussetzungen für Solaris	21	Konfigurationsmethoden	61
Installation unter Solaris	21	Befehlszeile	62
Installation vorbereiten	22	Scripts	62
Installationsschritte	22	GUI	63
Voraussetzungen für Windows 2000	23	Konfigurationsassistent	64
Installation unter Windows 2000	24	Dispatcher-Maschine konfigurieren	64
Installationspakete	24	Schritt 1. Serverfunktion starten	66
Installation vorbereiten	24	Schritt 2. Executor-Funktion starten	67
Installationsschritte	25	Schritt 3. NFA definieren (falls vom Host-Namen abweichend)	67
Kapitel 3. Einführung in Network Dispatcher	27	Schritt 4. Cluster definieren und Cluster-Optionen festlegen	67
Was ist Network Dispatcher?	27	Schritt 5. Aliasnamen für die Netz-schnittstellenkarte erstellen	67
		Schritt 6. Ports definieren und Port-Optionen festlegen	69

Schritt 7. Am Lastausgleich beteiligte Servermaschinen definieren	70	Schritt 8. Regeln zur Konfiguration hinzufügen	98
Schritt 8. Manager-Funktion starten (optional)	70	Schritt 9. Server zu den Regeln hinzufügen	98
Schritt 9. Advisor-Funktion starten (optional)	71	Schritt 10. Manager-Funktion starten (optional)	98
Schritt 10. Cluster-Proportionen festlegen	71	Schritt 11. Advisor-Funktion starten (optional)	99
Servermaschinen für Lastausgleich konfigurieren	71	Schritt 12. Cluster-Proportionen festlegen	99
Schritt 1. Aliasnamen für die Loopback-Einheit festlegen	71	Schritt 13. Caching Proxy starten	99
Schritt 2. Überprüfung auf zusätzliche Route	74	CBR-Konfigurationsbeispiel	100
Schritt 3. Zusätzliche Routes löschen	75	Kapitel 8. Planung für Mailbox Locator	101
Schritt 4. Serverkonfiguration prüfen	75	Hardware- und Softwarevoraussetzungen	101
Patch-Code für Linux-Kernel (zum Unterdrücken von ARP-Antworten an der Loopback-Schnittstelle) installieren	77	Überlegungen bei der Planung	102
Kapitel 6. Planung für Content Based Routing.	81	Affinitätsfunktion verwenden	104
Hardware- und Softwarevoraussetzungen	81	Inaktivitätszeitgeber für POP3/IMAP überschreiben	104
Überlegungen bei der Planung	81	Kapitel 9. Mailbox Locator konfigurieren	105
Lastausgleich für sichere Verbindungen (SSL)	84	Übersicht über die Konfigurations-Tasks	105
SSL-Datenverkehr vom Client zum Proxy und HTTP-Datenverkehr vom Proxy zum Server verteilen	85	Konfigurationsmethoden	106
Kapitel 7. Content Based Routing konfigurieren	87	Befehlszeile	106
Konfigurations-Tasks im Überblick	87	Scripts	107
Konfigurationsmethoden	87	GUI	107
Befehlszeile	88	Konfigurationsassistent	108
Scripts	90	Maschine mit Mailbox Locator konfigurieren	109
GUI	90	Schritt 1. Serverfunktion starten	109
Konfigurationsassistent	92	Schritt 2. Cluster definieren und Cluster-Optionen festlegen	109
CBR-Maschine konfigurieren	93	Schritt 3. Ports definieren und Port-Optionen festlegen	110
Schritt 1. Caching Proxy für die Verwendung von CBR konfigurieren	93	Schritt 4. Am Lastausgleich beteiligte Servermaschinen definieren	110
Schritt 2. Serverfunktion starten	95	Schritt 5. Manager-Funktion starten (optional)	110
Schritt 3. Executor-Funktion starten	96	Schritt 6. Advisor-Funktion starten (optional)	110
Schritt 4. Cluster definieren und Cluster-Optionen festlegen	96	Schritt 7. Cluster-Proportionen festlegen	111
Schritt 5. Aliasnamen für die Netz-schnittstellenkarte erstellen (optional)	96	Kapitel 10. Planung für Site Selector	113
Schritt 6. Ports definieren und Port-Optionen festlegen	97	Hardware- und Softwarevoraussetzungen	113
Schritt 7. Am Lastausgleich beteiligte Servermaschinen definieren	98	Überlegungen bei der Planung	113
		Hinweise zu TTL	116
		Netzproximität verwenden	117
		Kapitel 11. Site Selector konfigurieren	119
		Konfigurations-Tasks im Überblick	119
		Konfigurationsmethoden	119
		Befehlszeile	120
		Scripts	120

GUI	121
Konfigurationsassistent	122
Maschine mit Site Selector konfigurieren	123
Schritt 1. Serverfunktion starten	123
Schritt 2. Namensserver starten	123
Schritt 3. Sitenamen definieren und Optionen für Sitenamen festlegen	123
Schritt 4. Am Lastausgleich beteiligte Servermaschinen definieren	124
Schritt 5. Manager-Funktion starten (optional)	124
Schritt 6. Advisor-Funktion starten (optional)	124
Schritt 7. Systemmesswert definieren (optional)	124
Schritt 8. Proportionen für den Sitenamen festlegen	124
Servermaschinen für Lastausgleich konfigurieren	125

Kapitel 12. Planung für Consultant für Cisco CSS Switches	127
Hardware- und Softwarevoraussetzungen	127
Überlegungen bei der Planung	127

Kapitel 13. Consultant für Cisco CSS Switches konfigurieren	133
Übersicht über die Konfigurations-Tasks	133
Konfigurationsmethoden	134
Befehlszeile	134
Scripts	135
GUI	135
Maschine mit Consultant für Cisco CSS Switches konfigurieren	136
Schritt 1. Serverfunktion starten	137
Schritt 2. Executor-Funktion konfigurieren	137
Schritt 3. Cluster definieren und Cluster-Optionen festlegen	137
Schritt 4. Ports definieren und Port-Optionen festlegen	137
Schritt 5. Am Lastausgleich beteiligte Servermaschinen definieren	137
Schritt 6. Manager-Funktion starten	138
Schritt 7. Advisor-Funktion starten (optional)	138
Schritt 8. Cluster-Proportionen festlegen	138
Schritt 9. Metric Server starten (optional)	138
Konfiguration testen	139

Kapitel 14. Erweiterte Funktionen von Network Dispatcher	141
Lastausgleich mit Network Dispatcher optimieren	144
Proportionale Bedeutung von Statusinformationen	145
Wertigkeiten	146
Manager-Intervalle	147
Sensitivitätsschwelle	148
Glättungsfaktor	148
Scripts zum Generieren eines Alerts oder Protokollieren eines Serverausfalls verwenden	149
Advisor-Funktionen	149
Arbeitsweise der Advisor-Funktionen	150
Advisor-Funktion starten und stoppen	150
Advisor-Intervalle.	151
Berichtszeitlimit für Advisor-Funktion	152
Serververbindungs- und -empfangszeitlimit mit der Advisor-Funktion	152
Liste der Advisor-Funktionen	153
Kundenspezifische (anpassbare) Advisor-Funktion erstellen.	155
WAS-Advisor-Funktion	156
Namenskonvention	157
Kompilierung	157
Ausführung.	158
Erforderliche Routinen	158
Suchreihenfolge	159
Benennung und Pfad	159
Beispiel-Advisor-Funktion	159
Advisor-Funktion Workload Manager	159
Einschränkung für Metric Server.	160
Metric Server	161
WLM-Einschränkung	161
Vorbedingungen	161
Metric Server verwenden	161
Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)	163
Option 'Anforderung/ Antwort (URL)' der HTTP-Advisor-Funktion	165
Verknüpfte Server verwenden.	166
Für Dispatcher.	166
Für CBR	167
Für Mailbox Locator	167
Für Site Selector	168
Für Cisco Consultant.	168
Dispatcher-WAN-Unterstützung konfigurieren.	168

Befehlssyntax	169	Platzhalter-Port für die Übertragung von Datenverkehr mit nicht konfiguriertem Port verwenden	201
Ferne Advisor mit der Weitverkehrsunter- stützung verwenden	170	Funktionsweise der Affinität für Network Dispatcher	202
Konfigurationsbeispiel	172	Verhalten bei Inaktivierung der Affinität	202
Anmerkungen	174	Verhalten bei Aktivierung der Affinität	202
Unterstützung für GRE (Generic Routing Encapsulation).	175	SDA-API zur Steuerung der Client- /Serveraffinität	202
Advisor-Funktion 'self' in einer Client/Server-WAND-Konfiguration . . .	176	Port-übergreifende Affinität	204
Hohe Verfügbarkeit	177	Affinitätsadressmaske	204
Hohe Verfügbarkeit konfigurieren . . .	178	Überschreibung der Regelaaffinität . . .	205
Fehlererkennung mit Hilfe von Überwachungssignal und Erreichbarkeits- ziel	181	Stilllegung gehaltener Verbindungen . .	206
Wiederherstellungsstrategie	181	Affinitätsoption für Regeln.	207
Scripts verwenden	182	Aktive Cookie-Affinität	207
Regelbasierten Lastausgleich konfigurieren	185	Passive Cookie-Affinität.	209
Wie werden Regeln ausgewertet? . . .	187	URI-Affinität	210
Regeln verwenden, die auf der Client-IP- Adresse basieren	188	Erkennung von DoS-Attacken.	211
Regeln verwenden, die auf der Uhrzeit basieren	188	Binäres Protokollieren verwenden, um Serverstatistiken zu analysieren	213
Regeln auf der Basis der Verbindungen pro Sekunde an einem Port verwenden .	188	Zusätzliche Informationen zu den erweiter- ten Funktionen von Cisco Consultant . .	215
Regeln auf der Grundlage der an einem Port insgesamt aktiven Verbindungen ver- wenden	189	Wertigkeiten von Cisco Consultant . . .	216
Auf dem Client-Port basierende Regeln verwenden	190	Kapitel 15. Betrieb und Verwaltung von Network Dispatcher	219
Regeln verwenden, die auf der Service- Art (Type of Service = TOS) basieren . .	190	Authentifizierte Fernverwaltung	219
Regeln auf der Basis der reservierten und gemeinsam benutzten Bandbreite verwen- den	190	Protokolle von Network Dispatcher verwen- den	221
Regel 'Messwert für alle'	193	Pfade für die Protokolldatei ändern. . .	222
Regel "Durchschnitt der Messwerte" . .	193	Dispatcher-Komponente verwenden . . .	223
Regeln verwenden, die immer wahr sind	194	Dispatcher starten und stoppen	223
Regeln verwenden, die auf dem Inhalt der Anforderung basieren	195	Inaktivitätszeitlimit verwenden	223
Regeln zur Konfiguration hinzufügen . .	195	Über Anzahl beendeter Verbindungen die Speicherbereinigungsfunktion steuern . .	224
Regeloption für Serverauswertung . . .	196	Berichte der GUI — Menüoption 'Über- wachen'	225
Explizite Verbindungen benutzen	197	Simple Network Management Protocol mit Dispatcher verwenden.	225
Konfiguration für ein privates Netz verwen- den	198	Gesamten Datenverkehr zur Sicherheit der Network-Dispatcher-Maschine mit ipchains oder iptables zurückweise (unter Linux)	230
Platzhalter-Cluster verwenden, um Server- konfigurationen zusammenzufassen . . .	199	Komponente Content Based Routing ver- wenden	231
Platzhalter-Cluster für den Lastausgleich von Firewalls verwenden.	200	CBR starten und stoppen	231
Platzhalter-Cluster mit Caching Proxy für transparente Weiterleitung verwenden . .	201	CBR steuern	231
		CBR-Protokolle verwenden	232
		Mailbox Locator verwenden	232
		Mailbox Locator starten und stoppen . .	232

Mailbox Locator steuern	232	Problem: Fehlernachricht "Datei nicht gefunden..." beim Anzeigen der Onlinehilfe (Windows 2000)	248
Protokolle von Mailbox Locator verwenden	232	Problem: Irrelevante Fehlernachricht beim Starten von ndserver unter Solaris 2.7	249
Site Selector verwenden.	233	Problem: Die grafische Benutzerschnittstelle (GUI) wird nicht richtig gestartet	249
Site Selector starten und stoppen.	233	Problem: Fehler bei der Ausführung von Dispatcher mit installiertem Caching Proxy	249
Site Selector steuern	233	Problem: Die grafische Benutzerschnittstelle (GUI) wird nicht richtig angezeigt	250
Protokolle von Site Selector verwenden	233	Problem: Unter 2000 sind die Hilfefenster manchmal von anderen offenen Fenstern verdeckt	250
Cisco Consultant verwenden	233	Problem: Network Dispatcher kann Rahmen nicht verarbeiten und weiterleiten	250
Cisco Consultant starten und stoppen	233	Problem: Beim Starten des Executors von Network Dispatcher erscheint eine blaue Anzeige	250
Cisco Consultant steuern	233	Problem: Automatische Pfaderkennung verhindert Datenrückfluss mit Network Dispatcher	251
Protokolle von Cisco Consultant verwenden	234	Problem: Die Advisor-Funktionen zeigen alle Server als inaktiv an	252
Metric Server verwenden	234	Problem: Keine hohe Verfügbarkeit im Weitverkehrsmodus von Network Dispatcher	252
Metric Server starten und stoppen	234	Problem: Beim Laden einer großen Konfigurationsdatei blockiert die GUI oder verhält sich nicht erwartungsgemäß	253
Protokolle von Metric Server verwenden	234	Allgemeine Probleme lösen — CBR	254
Kapitel 16. Fehlerbehebung.	235	Problem: CBR wird nicht ausgeführt	254
Fehlerbehebungstabellen	235	Problem: Der Befehl cbrcontrol oder ndadmin scheitert.	254
Port-Nummern für Dispatcher überprüfen	242	Problem: Anforderungen werden nicht verteilt	254
Port-Nummern für CBR überprüfen	243	Problem: Unter Solaris scheitert der Befehl cbrcontrol executor start	255
Port-Nummern für Mailbox Locator überprüfen	243	Problem: Syntax- oder Konfigurationsfehler	255
Port-Nummern für Site Selector überprüfen	244	Allgemeine Probleme lösen—Mailbox Locator	255
Port-Nummern für Cisco Consultant überprüfen	245	Problem: Mailbox Locator wird nicht ausgeführt	255
Allgemeine Probleme lösen — Dispatcher	245	Problem: Der Befehl mlserver wird gestoppt	255
Problem: Dispatcher wird nicht ausgeführt	245		
Problem: Dispatcher und Server antworten nicht	245		
Problem: Dispatcher-Anforderungen werden nicht verteilt	246		
Problem: Die Dispatcher-Funktion für hohe Verfügbarkeit arbeitet nicht.	246		
Problem: Es kann kein Überwachungssignal hinzugefügt werden (Windows 2000)	246		
Problem: Zusätzliche Routes (Windows 2000)	247		
Problem: Advisor arbeiten nicht korrekt	247		
Problem: SNMPD wird nicht korrekt ausgeführt (Windows 2000).	247		
Problem: Dispatcher, Microsoft IIS und SSL funktionieren nicht (Windows 2000)	247		
Problem: Dispatcher-Verbindung zu einer fernen Maschine	247		
Problem: Befehl ndcontrol oder ndadmin schlägt fehl	248		

Problem: Der Befehl mlcontrol oder ndadmin scheitert	256	ndcontrol executor — Executor steuern	280
Problem: Ein Port kann nicht hinzugefügt werden	256	ndcontrol file — Konfigurationsdateien verwalten	285
Problem: Empfang eines Proxy-Fehlers beim Hinzufügen eines Ports	256	ndcontrol help — Hilfetext für diesen Befehl anzeigen oder drucken	287
Allgemeine Fehler beheben — Site Selector	257	ndcontrol highavailability — Hohe Verfügbarkeit steuern.	289
Problem: Site Selector wird nicht ausgeführt	257	ndcontrol host — Ferne Maschine konfigurieren	294
Problem: Site Selector verteilt den Datenverkehr von Solaris-Clients nicht nach der RoundRobin-Methode	257	ndcontrol log — Binäre Protokolldatei steuern.	295
Problem: Der Befehl sscontrol oder ndadmin scheitert	257	ndcontrol manager — Manager steuern	296
Problem: ssserver wird unter Windows 2000 nicht gestartet	257	ndcontrol metric — Systemmesswerte konfigurieren	303
Problem: Site Selector führt bei duplizierten Routes den Lastausgleich nicht korrekt durch	258	ndcontrol port — Ports konfigurieren	305
Allgemeine Probleme lösen—Consultant für Cisco CSS Switches	258	ndcontrol rule — Regeln konfigurieren.	312
Problem: lbcsrvr wird nicht gestartet	258	ndcontrol server — Server konfigurieren	320
Problem: Der Befehl lbcscontrol oder ndadmin scheitert.	258	ndcontrol set — Serverprotokoll konfigurieren.	327
Problem: Für Port 14099 kann kein Eintrag in der Registrierungsdatenbank erstellt werden.	259	ndcontrol status — Aktivitätsanzeige für Manager und Advisor-Funktionen	328
Allgemeine Fehler beheben — Metric Server	259	ndcontrol subagent — SNMP-Subagenten konfigurieren	329
Problem: IOException für Metric Server unter Windows 2000 bei Ausführung von benutzerdefinierten Messwertdateien mit der Erweiterung .bat oder .cmd	259	Anhang C. Syntax der content-Regel	331
Problem: Metric Server meldet die Last nicht an die Network-Dispatcher-Maschine.	259	Syntax der content-Regel	331
Problem: Metric-Server-Protokoll meldet, dass für den Zugriff auf den Agenten eine Kennung erforderlich ist	260	Reservierte Schlüsselwörter	331
Anhang A. Syntaxdiagramm lesen	261	Anhang D. Befehlsreferenz für Site Selector	335
Symbole und Interpunktion	261	sscontrol advisor — Advisor-Funktion steuern.	336
Parameter	261	sscontrol file — Konfigurationsdateien verwalten	341
Beispiele für die Syntax.	262	sscontrol help — Hilfetext für diesen Befehl anzeigen oder drucken	343
Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator	265	sscontrol manager — Manager steuern.	344
Konfigurationsunterschiede bei CBR, Mailbox Locator und Dispatcher	266	sscontrol metric — Systemmesswerte konfigurieren	349
ndcontrol advisor — Advisor steuern	268	sscontrol nameserver — Namensserver steuern.	350
ndcontrol cluster — Cluster konfigurieren	274	sscontrol rule — Regeln konfigurieren	351
		sscontrol server — Server konfigurieren	355
		sscontrol set — Serverprotokoll konfigurieren.	357
		sscontrol sitename — Sitenamen konfigurieren.	358
		sscontrol status — Aktivitätsanzeige für Manager und Advisor-Funktionen	362

Anhang E. Befehlsreferenz für Consultant für Cisco CSS Switches	363
lbcontrol advisor — Advisor steuern	364
lbcontrol cluster — Cluster konfigurieren	369
lbcontrol executor — Executor steuern	371
lbcontrol file — Konfigurationsdateien verwalten	373
lbcontrol help — Hilfetext für diesen Befehl anzeigen oder drucken	375
lbcontrol host — Ferne Maschine konfigurieren	376
lbcontrol log — Binäre Protokolldatei steuern.	377
lbcontrol manager — Manager steuern	378
lbcontrol metric — Systemmesswerte konfigurieren	384
lbcontrol port — Ports konfigurieren	386
lbcontrol server — Server konfigurieren	388
lbcontrol set — Serverprotokoll konfigurieren.	390
lbcontrol status — Aktivitätsanzeige für Manager und Advisor-Funktionen	391
Anhang F. Beispielkonfigurationsdateien	393
Beispielkonfigurationsdateien für Network Dispatcher	393

Dispatcher-Konfigurationsdatei—AIX, Red Hat Linux und Solaris.	393
Dispatcher-Konfigurationsdatei—Windows	397
Beispiel-Advisor-Funktion	400

Anhang G. Beispiel für eine Client-/Serverkonfiguration mit hoher Verfügbarkeit unter Verwendung von Dispatcher, CBR und Caching Proxy	407
Servermaschine einrichten	407

Anhang H. Weitere Ressourcen	411
Zugriff auf die Befehlszeile.	411
Onlinehilfefunktion aufrufen	411
Referenzinformationen	411

Anhang I. Bemerkungen	413
Marken	415

Glossar	417
--------------------------	------------

Index	429
------------------------	------------

Tabellen

1.	installp-Images für AIX	13	12.	Konfigurations-Tasks für Consultant für Cisco CSS Switches	133
2.	AIX-Installationsbefehle	16	13.	Erweiterte Konfigurations-Tasks für Network Dispatcher	141
3.	Konfigurations-Tasks für Dispatcher	61	14.	Tabelle zur Fehlerbehebung für Dispat- cher	235
4.	Befehle zum Festlegen eines Alias- namens für die Loopback-Einheit (lo0) für Dispatcher	72	15.	Tabelle zur Fehlerbehebung für CBR	238
5.	Befehle zum Löschen zusätzlicher Rou- tes für Dispatcher	75	16.	Tabelle zur Fehlerbehebung für Mail- box Locator	239
6.	Konfigurations-Tasks für die CBR-Kom- ponente	87	17.	Tabelle zur Fehlerbehebung für Site Selector	239
7.	Befehle zum Erstellen eines Aliasnamens für die NIC	97	18.	Tabelle zur Fehlerbehebung für Consul- tant für Cisco CSS Switches	240
8.	Konfigurations-Tasks für Mailbox Loca- tor	105	19.	Tabelle zur Fehlerbehebung für Metric Server	241
9.	Konfigurations-Tasks für Site Selector	119			
10.	Begriffe für die Konfiguration von Con- sultant und des Cisco CSS Switch . . .	129			
11.	Beispiel für eine in der Consultant- Konfiguration abgebildete Konfigura- tion des Cisco CSS Switch	131			

Abbildungsverzeichnis

1. Einfache lokale Dispatcher-Konfiguration	1	15. Beispiel der für die Dispatcher-Maschine	
2. Die grafische Benutzerschnittstelle (GUI)	6	erforderlichen IP-Adressen	66
3. Dispatcher-Beispielkonfiguration mit		16. CBR-Konfigurationsdatei für AIX	94
einem Cluster und zwei Ports	8	17. CBR-Konfigurationsdatei für Linux	94
4. Dispatcher-Beispielkonfiguration mit zwei		18. CBR-Konfigurationsdatei für Solaris	95
Clustern mit jeweils einem Port	9	19. CBR-Konfigurationsdatei für Windows	
5. Dispatcher-Beispielkonfiguration mit		2000	95
zwei Clustern mit jeweils zwei Ports	10	20. Beispiel für eine DNS-Umgebung	114
6. Beispiel für die physische Darstellung		21. Konfigurationsbeispiel für Consultant	
einer Site mit Network Dispatcher für		mit 2 Clustern mit jeweils 3 Ports	130
die Verwaltung lokaler Server	37	22. Beispiel einer Konfiguration mit einem	
7. Beispielsite mit Dispatcher und Metric		LAN-Segment	168
Server für die Serververwaltung	38	23. Beispiel einer Konfiguration mit loka-	
8. Beispiel für eine Site mit Dispatcher für		len und fernen Servern	169
die Verwaltung lokaler und ferner Ser-		24. WAN-Beispielkonfiguration mit fernen	
ver	39	Network-Dispatcher-Maschinen	172
9. Beispielsite mit CBR für die Verwaltung		25. WAN-Beispielkonfiguration mit einer	
lokaler Server	41	Serverplattform, die GRE unterstützt	175
10. Beispielsite mit Mailbox Locator für die		26. Beispiel für eine Client/Server-WAND-	
Verwaltung lokaler Server	42	Konfiguration mit Advisor-Funktion	
11. Beispielsite mit Site Selector und Metric		"self"	176
Server für die Verwaltung lokaler und		27. Beispiel für ein privates Netz mit dem	
ferner Server	44	Dispatcher	199
12. Beispielsite mit Cisco Consultant und		28. SNMP-Befehle für AIX und Solaris	226
Metric Server für die Verwaltung lokaler		29. SNMP-Befehle für Windows 2000	227
Server	47	30. Beispiel für eine Client-	
13. Beispiel für einen Dispatcher mit einfa-		/Serverkonfiguration mit hoher Verfüg-	
cher hoher Verfügbarkeit	52	barkeit unter Verwendung von Dispat-	
14. Beispiel für einen Dispatcher mit gegen-		cher, CBR und Caching Proxy	407
seitiger hoher Verfügbarkeit	53		

Willkommen

In diesem Handbuch sind die Planung, Installation, Konfiguration, Verwendung und Fehlerbehebung für IBM® WebSphere Edge Server Network Dispatcher für AIX, Linux, Solaris und Windows 2000 beschrieben. Zuvor hatte dieses Produkt den Namen SecureWay Network Dispatcher, eNetwork Dispatcher und Interactive Network Dispatcher.

Die neueste Version dieses Handbuchs ist im HTML- und PDF-Format auf der Website zu WebSphere Edge Server verfügbar. Sie können über den folgenden URL auf das Onlinebuch zugreifen:

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

Die Website zu WebSphere Edge Server enthält die neuesten Informationen zur Verwendung von Network Dispatcher für die Leistungsoptimierung Ihrer Server. Konfigurationsbeispiele und Szenarien sind eingeschlossen. Um auf diese Website zuzugreifen, rufen Sie den folgenden URL auf:

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

Die letzten Aktualisierungen und Verwendungshinweise zu Network Dispatcher finden Sie auf der Webseite mit Unterstützung zu WebSphere Edge Server. Klicken Sie auf dieser Webseite auf den Eintrag *Search for Network Dispatcher hints and tips*. Die genannte Webseite hat den folgenden URL:

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

Senden von Kommentaren

Ihre Rückmeldung ist uns wichtig, damit wir möglichst genaue und hochwertige Informationen bieten können. Falls Sie Kommentare zum vorliegenden Handbuch oder einem anderen Dokument zu WebSphere Edge Server abgeben möchten:

- Senden Sie Ihren Kommentar per E-Mail an fsdoc@us.ibm.com. Geben Sie dabei Folgendes an: Handbuchtitel, Teilenummer des Handbuchs, Version von WebSphere Edge Server und wenn möglich die Position der Textstelle, auf die sich Ihr Kommentar bezieht (z. B. Seitenzahl oder Tabellenummer).

Kapitel 1. Erste Schritte...für einen schnellen Start!

Wie schnell können Sie Network Dispatcher nutzen? Das folgende Szenario gibt ein Beispiel.

Angenommen, Sie sind der Webadministrator des Unternehmens Intersplash. Sie verwalten eine lokale Website mit zwei HTTP-Servern. Bisher haben Sie die Auslastung der beiden Server nach der RoundRobin-Methode verwaltet. In letzter Zeit hat das Unternehmen jedoch expandiert, und die Kunden beschweren sich zunehmend, dass sie nicht auf die Site zugreifen können. Was ist zu tun?

Rufen Sie <http://www.ibm.com/software/webervers/edgeserver> auf und laden Sie die neueste Version von Network Dispatcher herunter. Dieses Produkt umfasst fünf Komponenten: Dispatcher, Content Based Routing (CBR), Mailbox Locator, Site Selector und Consultant für Cisco CSS Switches (Cisco Consultant). Im Augenblick soll nur die Komponente **Dispatcher** erläutert werden.

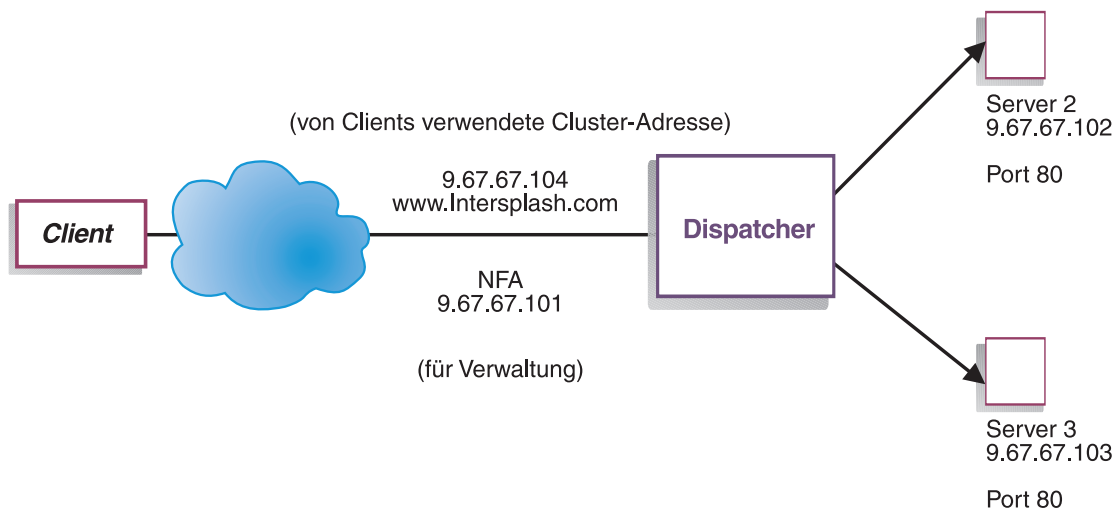


Abbildung 1. Einfache lokale Dispatcher-Konfiguration

Dieses Beispiel zeigt die Konfiguration von drei lokal angeschlossenen Workstations, die die MAC-Weiterleitungsmethode der Dispatcher-Komponente verwenden, um den Webdatenverkehr auf zwei Webserver zu verteilen.

Für die Verteilung des Datenverkehrs einer anderen TCP-Anwendung oder einer kontextlosen UDP-Anwendung würde die Konfiguration im Wesentlichen genauso aussehen.

Anmerkung: Bei Verwendung der AIX-, Linux- oder Solaris-Version von Dispatcher würden zwei Workstations für die Konfiguration reichen. Der Dispatcher würde sich dabei auf einer der Webserver-Workstations befinden. Dies wäre dann eine verknüpfte Konfiguration. Prozeduren für das Erstellen komplexer Konfigurationen finden Sie im Abschnitt „Dispatcher-Maschine konfigurieren“ auf Seite 64.

Voraussetzungen

In dem Beispiel für einen schnellen Start werden drei Workstations und vier IP-Adressen benötigt. Eine Workstation wird als Dispatcher verwendet; die beiden anderen Workstations werden als Webserver verwendet. Jeder Webserver benötigt eine IP-Adresse. Die Dispatcher-Workstation benötigt eine eigene Adresse und eine Adresse für den Lastausgleich.

Vorbereitungen

1. Stellen Sie sicher, dass die Vorbedingungen erfüllt sind, die in „Kapitel 2. Network Dispatcher installieren“ auf Seite 11 aufgelistet sind.
2. Konfigurieren Sie Ihre Workstations so, dass sie sich innerhalb eines LAN-Segments befinden. Stellen Sie sicher, dass der Datenaustausch im Netz zwischen den drei Maschinen nicht über Router oder Brücken erfolgen muss.
3. Konfigurieren Sie die Netzwerkadapter der drei Workstations. In diesem Beispiel wird die folgende Netzkonfiguration angenommen:

Workstation	Name	IP-Adresse
1	server1.intersplash.com	9.67.67.101
2	server2.intersplash.com	9.67.67.102
3	server3.intersplash.com	9.67.67.103
Netzmaske = 255.255.255.0		

Jede Workstation enthält nur eine Standard-Ethernet-Netzschnittstellenkarte.

4. Stellen Sie sicher, dass server1.intersplash.com ping-Aufrufen an server2.intersplash.com und server3.intersplash.com senden kann.
5. Stellen Sie sicher, dass server2.intersplash.com und server3.intersplash.com ping-Aufrufe an server1.intersplash.com senden können.

6. Stellen Sie sicher, dass der Inhalt auf den beiden Webservern (Server 2 und 3) identisch ist. Dies kann durch die Vervielfältigung der Daten auf beiden Workstations, durch die Verwendung eines gemeinsamen Dateisystems, wie beispielsweise NFS, AFS oder DFS, oder durch eine andere für Ihre Site geeignete Methode erreicht werden.
7. Stellen Sie sicher, dass die Webserver auf `server2.intersplash.com` und `server3.intersplash.com` betriebsbereit sind. Fordern Sie mit einem Webbrowser Seiten direkt von **`http://server2.intersplash.com`** und **`http://server3.intersplash.com`** an.
8. Definieren Sie eine andere gültige IP-Adresse für dieses LAN-Segment. Dies ist die Adresse, die Sie den Clients zur Verfügung stellen, die auf Ihre Site zugreifen möchten. In diesem Beispiel wird folgende Adresse verwendet:

Name=`www.intersplash.com`
IP=`9.67.67.104`

9. Konfigurieren Sie die beiden Webserver-Workstations so, dass sie Datenverkehr für `www.intersplash.com` akzeptieren.

Fügen Sie zur **Loopback**-Schnittstelle von `server2.intersplash.com` und `server3.intersplash.com` einen Aliasnamen für `www.intersplash.com` hinzu.

- Für AIX:
`ifconfig lo0 alias www.intersplash.com netmask 255.255.255.0`
- Für Solaris 7:
`ifconfig lo0:1 www.intersplash.com 127.0.0.1 up`
- Für andere Betriebssysteme: siehe Tabelle 4 auf Seite 72.

10. Löschen Sie alle zusätzlichen Routes, die unter Umständen infolge des Aliasing für die Loopback-Schnittstelle erstellt wurden. Weitere Informationen hierzu finden Sie in „Schritt 2. Überprüfung auf zusätzliche Route“ auf Seite 74.

Sie haben jetzt alle für die beiden Webserver-Workstations erforderlichen Konfigurationsschritte ausgeführt.

Dispatcher konfigurieren

Für den Dispatcher können Sie eine Konfiguration unter Verwendung der Befehlszeile, des Konfigurationsassistenten oder der grafischen Benutzerschnittstelle (GUI) erstellen.

Anmerkung: Die Parameterwerte müssen mit Ausnahme der Parameterwerte für Host-Namen und Dateinamen in englischen Zeichen eingegeben werden.

Konfiguration von der Befehlszeile aus

Führen Sie folgende Schritte aus, wenn Sie die Befehlszeile verwenden:

1. Starten Sie wie folgt den ndserver für Dispatcher:
 - Führen Sie unter AIX, Linux oder Solaris den folgenden Befehl als Benutzer "root" aus: **ndserver**
 - Unter Windows 2000 ist ndserver ein Dienst, der automatisch gestartet wird.
2. Starten Sie wie folgt die Executor-Funktion des Dispatchers:
ndcontrol executor start
3. Fügen Sie wie folgt die Cluster-Adresse zur Dispatcher-Konfiguration hinzu:
ndcontrol cluster add www.intersplash.com
4. Fügen Sie wie folgt den Port für das Protokoll HTTP zur Dispatcher-Konfiguration hinzu:
ndcontrol port add www.intersplash.com:80
5. Fügen Sie wie folgt alle Webserver zur Dispatcher-Konfiguration hinzu:
ndcontrol server add www.intersplash.com:80:server2.intersplash.com
ndcontrol server add www.intersplash.com:80:server3.intersplash.com
6. Konfigurieren Sie wie folgt die Workstation, so dass sie den Datenverkehr für die Cluster-Adresse akzeptiert:
ndcontrol cluster configure www.intersplash.com
7. Starten Sie wie folgt die Manager-Funktion des Dispatchers:
ndcontrol manager start
Der Dispatcher führt den Lastausgleich jetzt ausgehend von der Serverleistung durch.
8. Starten Sie wie folgt die Advisor-Funktion des Dispatchers:
ndcontrol advisor start http 80
Der Dispatcher stellt jetzt sicher, dass keine Client-Anforderungen an einen ausgefallenen Webserver gesendet werden.

Die Basiskonfiguration mit lokal angeschlossenen Servern ist damit vollständig.

Konfiguration mit dem Konfigurationsassistenten

Führen Sie folgende Schritte aus, wenn Sie den Konfigurationsassistenten verwenden:

1. Starten Sie wie folgt den ndserver für Dispatcher:
 - Führen Sie unter AIX, Linux oder Solaris den folgenden Befehl als Benutzer "root" aus:
ndserver
 - Unter Windows 2000 ist ndserver ein Dienst, der automatisch gestartet wird.
2. Starten Sie den Assistenten des Dispatchers, **ndwizard**.

Der Assistent führt Sie schrittweise durch den Prozess zum Erstellen einer Basiskonfiguration für die Dispatcher-Komponente. Der Assistent stellt Ihnen Fragen zu Ihrem Netz. Sie erhalten eine Anleitung für die Konfiguration eines Clusters, bei der der Dispatcher den Datenverkehr auf eine Gruppe von Servern verteilt.

Bei Verwendung des Konfigurationsassistenten erscheinen die folgenden Anzeigen:

- Einführung in den Assistenten
- Erwartungen
- Konfiguration vorbereiten
- Auswahl eines Hosts für die Konfiguration (falls erforderlich)
- Cluster definieren
- Port hinzufügen
- Server hinzufügen
- Advisor starten
- Servermaschine konfigurieren

Mit der grafischen Benutzerschnittstelle (GUI) konfigurieren

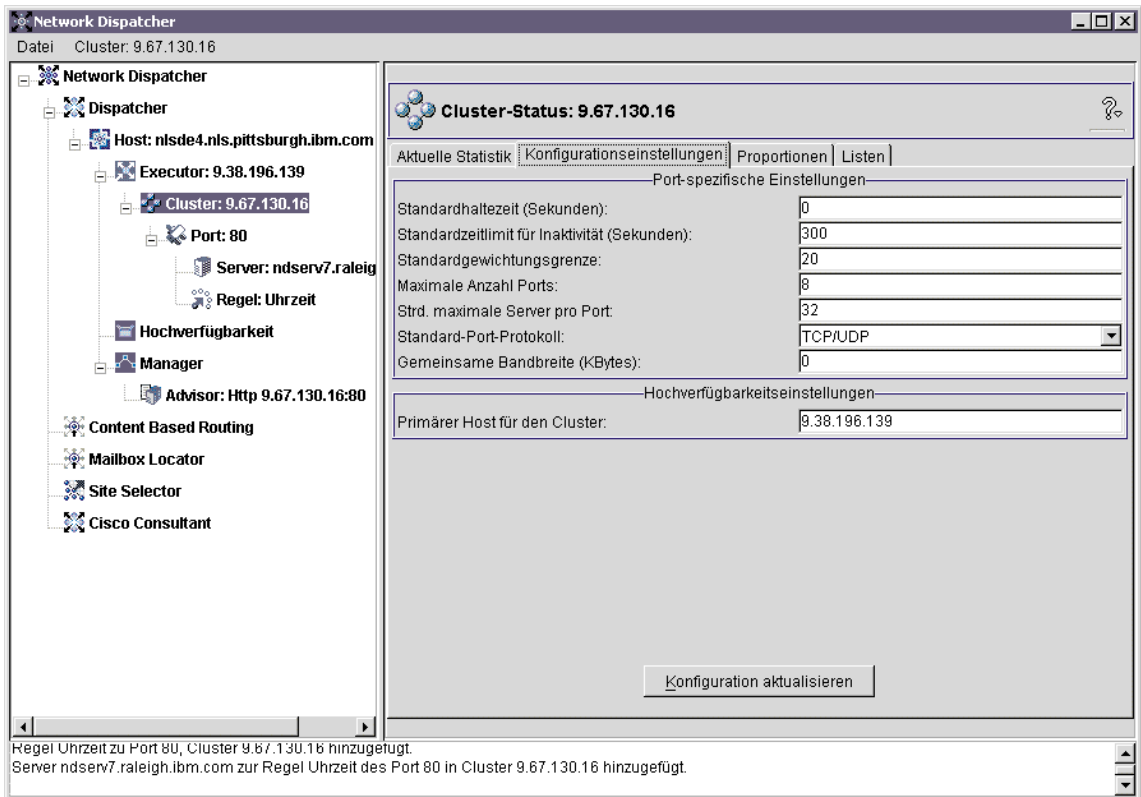


Abbildung 2. Die grafische Benutzerschnittstelle (GUI)

Führen Sie die folgenden Schritte aus, um die grafische Benutzerschnittstelle zu starten:

1. Stellen Sie sicher, dass ndserver ausgeführt wird:
 - Führen Sie unter AIX, Linux oder Solaris den folgenden Befehl als Benutzer "root" aus:
ndserver
 - Unter Windows 2000 ist ndserver ein Dienst, der automatisch gestartet wird.
2. Führen Sie anschließend einen der folgenden Schritte aus:
 - Geben Sie unter AIX, Linux oder Solaris **ndadmin** ein.
 - Klicken Sie unter Windows 2000 nacheinander auf **Start, Programme, IBM WebSphere, Edge Server, IBM Network Dispatcher** und **Network Dispatcher**.

Allgemeine Anweisungen zur Verwendung der GUI

Auf der linken Seite der Anzeige erscheint eine Baumstruktur mit Network Dispatcher als Ausgangsebene und Dispatcher, Content Based Routing, Mailbox Locator, Site Selector sowie Cisco Consultant als Komponenten. Siehe Abb. 2 auf Seite 6.

Alle Komponenten können über die GUI konfiguriert werden. Sie können Elemente in der Baumstruktur auswählen, indem Sie mit der ersten Maustaste (normalerweise der linken Maustaste) darauf klicken. Zum Aufrufen von Popup-Menüs müssen Sie die zweite Maustaste (normalerweise die rechte Maustaste) drücken. Auf die Popup-Menüs für die Baumstrukturelemente kann auch über die Menüleiste zugegriffen werden, die sich oben in der Anzeige befindet.

Durch Klicken auf das Plus- oder Minuszeichen können Sie die Elemente der Baumstruktur ein- bzw. ausblenden.

Auf der rechten Seite der Anzeige erscheinen Registerseiten mit Statusanzeigen für das derzeit ausgewählte Element.

- Die Registerseite **Aktuelle Statistik** stellt statistische Daten zum Element bereit.
- Durch Klicken auf den Knopf **Statistik aktualisieren** können Sie die aktuellen statistischen Daten aufrufen. Sollte kein Knopf "Statistik aktualisieren" vorhanden sein, wird die Statistik automatisch aktualisiert und ist somit immer auf dem neuesten Stand.
- Die Registerseite **Konfigurationseinstellungen** stellt Konfigurationsparameter bereit, die wie in den Kapiteln zur Konfiguration der einzelnen Komponenten beschrieben definiert werden können. Diese Registerseite wird nicht für alle Elemente der Baumstruktur angezeigt.
- Mit dem Knopf **Konfiguration aktualisieren** werden die letzten Änderungen auf die gegenwärtig aktive Konfiguration angewendet.
- Die Registerseite **Proportionen** enthält Proportionsparameter (oder Wertigkeitsparameter), die wie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141 beschrieben konfiguriert werden können. Diese Registerseite wird nicht für alle Elemente der Baumstruktur angezeigt.
- Die Registerseite **Listen** stellt zusätzliche Details zum ausgewählten Baumstrukturelement zur Verfügung. Diese Registerseite wird nicht für alle Elemente der Baumstruktur angezeigt.
- Mit dem Knopf **Entfernen** können Sie die hervorgehobenen Einträge löschen.

Falls Sie **Hilfe** benötigen, klicken Sie oben rechts im Network-Dispatcher-Fenster auf das Fragezeichen.

- **Hilfe für Feld** — beschreibt jedes Feld und gibt die Standardwerte an.
- **Vorgehensweise** — listet Tasks auf, die in der aktuellen Anzeige ausgeführt werden können.
- **Inhaltsverzeichnis** — zeigt ein Inhaltsverzeichnis aller Hilfetexte an.
- **Index** — zeigt einen alphabetischen Index der Hilfethemen an.

Konfiguration testen

Testen Sie, ob die Konfiguration korrekt ist.

1. Rufen Sie mit einem Webbrowser die Adresse **<http://www.intersplash.com>** auf. Wird eine Seite angezeigt, ist die Konfiguration korrekt.
2. Laden Sie die Seite erneut im Webbrowser.
3. Überprüfen Sie die Ergebnisse des folgenden Befehls: **ndcontrol server report www.intersplash.com:80**: Die Einträge der Spalte "Summe Verbindungen" für beide Server sollten addiert "2" ergeben.

Arten von Cluster-, Port- und Serverkonfigurationen

Es gibt viele Möglichkeiten, Network Dispatcher für die Unterstützung Ihrer Site zu konfigurieren. Wenn Sie für Ihre Site nur einen Host-Namen haben, zu dem alle Kunden eine Verbindung herstellen, können Sie einen Cluster mit Servern definieren. Für jeden dieser Server konfigurieren Sie einen Port, über den Network Dispatcher kommuniziert. Siehe Abb. 3.

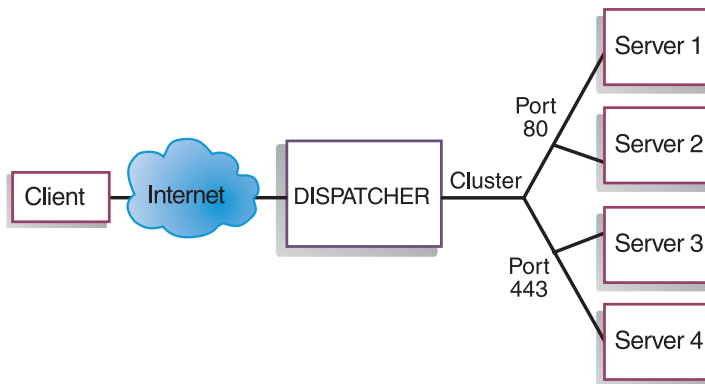


Abbildung 3. Dispatcher-Beispielkonfiguration mit einem Cluster und zwei Ports

In diesem Beispiel ist für die Dispatcher-Komponente ein Cluster mit der Adresse www.productworks.com definiert. Dieser Cluster hat zwei Ports: Port 80 für HTTP und Port 443 für SSL. Ein Client, der eine Anforderung an <http://www.productworks.com> (Port 80) richtet, wird einem anderen Server zugeordnet als ein Client, der eine Anforderung an <http://www.productworks.com> (Port 443) richtet.

Wenn Ihre Site sehr groß ist und Sie für jedes unterstützte Protokoll mehrere dedizierte Server haben, sollten Sie Network Dispatcher auf andere Weise konfigurieren. In diesem Fall könnten Sie für jedes Protokoll einen Cluster mit nur einem Port, aber mehreren Servern definieren (siehe Abb. 4).

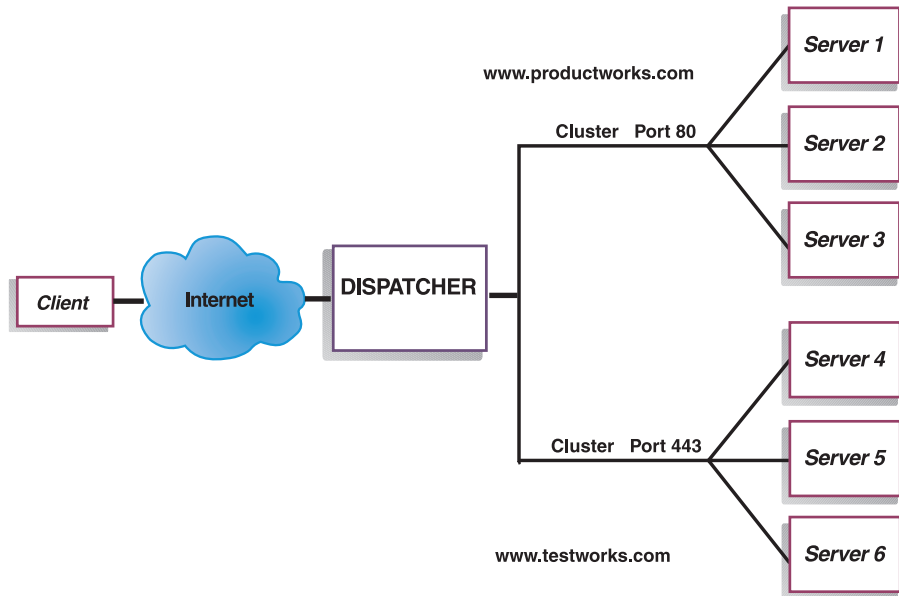


Abbildung 4. Dispatcher-Beispielkonfiguration mit zwei Clustern mit jeweils einem Port

In diesem Beispiel für die Dispatcher-Komponente sind zwei Cluster definiert: `www.productworks.com` für Port 80 (HTTP) und `www.testworks.com` für Port 443 (SSL).

Wenn Ihre Site Inhalte für mehrere Unternehmen oder Abteilungen bereitstellt, die jeweils mit einem eigenen URL auf Ihre Site zugreifen, muss Network Dispatcher auf eine dritte Art konfiguriert werden. In diesem Fall könnten Sie für jede Firma oder Abteilung einen Cluster definieren und anschließend die Ports, an denen Verbindungen mit dem jeweiligen URL empfangen werden sollen (siehe Abb. 5 auf Seite 10).

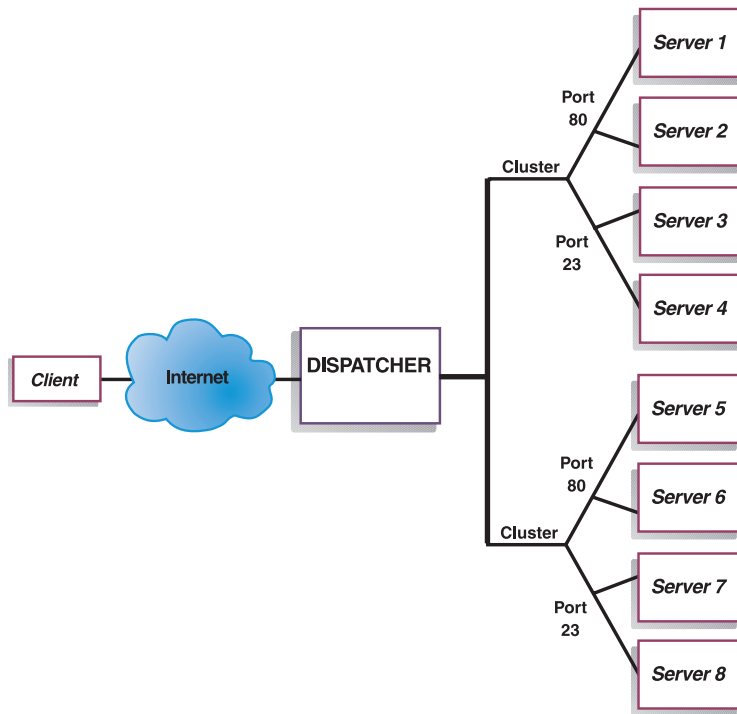


Abbildung 5. Dispatcher-Beispielkonfiguration mit zwei Clustern mit jeweils zwei Ports

In diesem Beispiel für die Dispatcher-Komponente wurden für die Sites www.productworks.com und www.testworks.com jeweils zwei Cluster mit Port 80 (HTTP) und Port 23 (Telnet) definiert.

Kapitel 2. Network Dispatcher installieren

Dieses Kapitel enthält Informationen zu den Hardwarevoraussetzungen und zur Installation von Network Dispatcher unter AIX, Linux, Solaris und Windows 2000. Beginnen Sie mit einem der folgenden Abschnitte:

- „Voraussetzungen für AIX“ auf Seite 12
- „Voraussetzungen für Red Hat Linux oder SuSE Linux“ auf Seite 17
- „Voraussetzungen für Solaris“ auf Seite 21
- „Voraussetzungen für Windows 2000“ auf Seite 23.

Anmerkungen:

1. Falls Sie eine Migration von einer früheren Version durchführen möchten, beachten Sie, dass sich die Struktur des Installationsverzeichnis für Network Dispatcher geändert hat. Sie müssen alle eigenen Konfigurationsdateien in das Verzeichnis `...nd/servers/configurations/Komponente` verschieben. (*Komponente* steht hier für dispatcher, cbr, ml, ss oder lbc.) Außerdem müssen Sie alle eigenen Scripts (z. B. goldle und goStandby) in das Verzeichnis `...nd/servers/bin` verschieben, um diese ausführen zu können.
2. Wenn Sie eine Maschine nach der Installation von Network Dispatcher abmelden, müssen Sie nach einer erneuten Anmeldung alle Network-Dispatcher-Dienste neu starten.
3. Für Network Dispatcher Release 2.0 ist Java ab Version 1.3.0 erforderlich. Da einige auf der Network-Dispatcher-Maschine enthaltene Anwendungen unter Umständen eine andere Java-Version erfordern, müssen Sie nach einem Upgrade sicherstellen, dass auf der Maschine die richtigen Java-Versionen installiert sind.

Sie können wie folgt gewährleisten, dass die Network-Dispatcher-Komponenten beim Vorhandensein mehrerer Java-Versionen die richtige Version verwenden:

- a. Installieren Sie die für das Betriebssystem erforderliche Version von Java 1.3 (wie in diesem Kapitel unter "Voraussetzungen" angegeben).
- b. Editieren Sie die Script-Dateien für Network Dispatcher so, dass Java 1.3 verwendet wird. Die Script-Dateien befinden sich standardmäßig in den folgenden Verzeichnissen:

UNIX `/usr/bin/<Script-Datei>`

Windows

`C:\WINNT\System32\<Script-Datei.cmd>`

Editieren Sie die Script-Dateien für jede Komponente von Network Dispatcher, für die Sie ein Upgrade durchführen. Die Script-Dateien für die einzelnen Komponenten haben die folgenden Namen:

Administration

ndadmin

Dispatcher

ndserver, ndcontrol, ndwizard, ndkeys

Content Based Routing (CBR)

cbrserver, cbrcontrol, cbrwizard, cbrkeys

Site Selector

ssserver, sscontrol

Cisco Consultant

lbserver, lbcontrol

Anmerkung: Diese Dateien stehen standardmäßig nur im Lesezugriff zur Verfügung. Sie müssen deshalb die Berechtigungen für diese Dateien ändern, bevor Sie die Änderungen sichern können.

- c. Fügen Sie für jeden in den Script-Dateien vorkommenden Befehl `java` oder `javaw` einen Pfad als Präfix hinzu, um anzugeben, wo sich der Befehl im Installationsverzeichnis von Java 1.3 befindet.

Beispiel für Windows 2000: Wenn Java 1.3 im Verzeichnis

C:\Programme\IBM\Java13\jre\bin installiert ist, müssen Sie die Zeile in `ndserver.cmd` wie folgt ändern:

Alt: `javaw %END_ACCESS%
-DEND_INSTALL_PATH=%IBMNDPATH% ..`

Neu: `C:\Programme\IBM\Java13\jre\bin\javaw %END_ACCESS%
-DEND_INSTALL_PATH=%IBMNDPATH% ...`

Voraussetzungen für AIX

- Eine IBM RS/6000
- IBM AIX 5.1 mit APAR IY19177. Es wird der 32-Bit-Power-PC unterstützt (*nicht* der 64-Bit-Kernel).

IBM AIX 4.3.3.10 mit APARs (um die Unterstützung für Java 1.3 zu gewährleisten). Eine Liste der erforderlichen AIX APARs finden Sie in der Readme-Datei zum IBM AIX Developer Kit.

- 50 MB freier Plattenspeicherplatz für die Installation.

Anmerkung: Für Protokolle wird zusätzlicher Plattenspeicherplatz benötigt.

- Die folgenden Netzschnittstellenkarten (Network Interface Cards = NICs) werden unterstützt:
 - 16 Mbit Token-Ring
 - 10 Mbit Ethernet
 - 100 Mbit Ethernet
 - 1 Gbit Ethernet
 - Fiber Distributed Data Interface (FDDI)
 - Ethernet-NICs mit mehreren Anschlüssen

Anmerkung: Die Implementierung der NICs mit mehreren Anschlüssen ist je nach Lieferant verschieden. Deshalb kann die Unterstützung bestimmter NICs mit mehreren Anschlüssen eingeschränkt sein.

- IBM AIX Developer Kit, Java 2 Technology Edition, Version 1.3.0 für JRE (Java Runtime Environment). (Weitere Informationen zur Ausführung mehrerer Java-Versionen können Sie der Anmerkung 3 auf Seite 11 entnehmen.)
- Edge Server Caching Proxy Version 2.0, falls Sie zum Verteilen von HTTP- oder SSL-Datenverkehr die CBR-Komponente verwenden.
- Netscape Navigator ab Version 4.07 oder Netscape Communicator ab Version 4.61 zum Anzeigen von Onlinehilfetexten.
- Für Consultant für Cisco CSS Switches müssen Sie den Cisco CSS 11000 Series Switch installiert und konfiguriert haben.

Installation unter AIX

In Tabelle 1 sind die installp-Images von Network Dispatcher für AIX aufgelistet.

Tabelle 1. installp-Images für AIX

Dispatcher (Komponente, Verwaltung, Lizenz und Nachrichten)	intnd.nd.driver intnd.nd.rte intnd.msg.nd.<Sprache>.nd intnd.admin.rte intnd.msg.<Sprache>.admin
Administration (nur Komponente)	intnd.admin.rte intnd.msg.<Sprache>.admin
Dokumentation	intnd.doc.rte
Lizenz	intnd.nd.license
Metric Server	intnd.ms.rte

Dabei gibt <Sprache> einen der folgenden Sprachencodes an:

- en_US
- de
- es_ES
- fr
- it
- ja_JP
- Ja_JP
- ko_KR
- pt_BR
- zh_CN
- zh_TW
- Zh_TW

Falls Sie eine Probeversion des Produkts von der Website herunterladen, verwenden Sie die im Dokument

<http://www.ibm.com/software/webservers/edgeserver/download.html> enthaltenen Installationsanweisungen.

Installation vorbereiten

Bei der Installation des Produkts können Sie auswählen, ob Sie nur bestimmte oder alle der in der folgenden Liste aufgeführten Optionen installieren wollen:

- Network Dispatcher Administration
- Einheitentreiber für Network Dispatcher (erforderlich)
- Lizenz für Network Dispatcher (erforderlich)
- Dokumentation zu Network Dispatcher
- Network Dispatcher Metric Server
- Lizenz.

Installationsschritte

Anmerkung: Falls Sie eine frühere Version installiert haben, sollten Sie diese Kopie vor Installation der aktuellen Version deinstallieren. Vergewissern Sie sich zunächst, dass alle Steuerprogramme und Server gestoppt wurden. Geben Sie dann **installp -u intnd** ein, um die Installation des gesamten Produkts zu entfernen. Wenn Sie bestimmte Dateigruppen deinstallieren möchten, listen Sie diese anstelle des Paketnamens einzeln auf.

Führen Sie die folgenden Schritte aus, um Network Dispatcher für AIX zu installieren:

1. Melden Sie sich als Root an.
2. Legen Sie den Datenträger mit dem Produkt ein oder, falls Sie das Produkt aus dem Web installieren, kopieren Sie die Installationsimages in ein Verzeichnis.
3. Installieren Sie das Installationsimage. Es wird empfohlen, Network Dispatcher für AIX mit SMIT zu installieren, da in diesem Fall alle Nachrichten automatisch installiert werden.

Verwendung von SMIT:

Auswahl

Softwareinstallation und Wartung

Auswahl

Software installieren und aktualisieren

Auswahl

Aus gesamter verfügbarer Software installieren und aktualisieren

Eingabe

Die Einheit oder das Verzeichnis mit den installp-Images

Eingabe

In der Zeile '*Zu installierende SOFTWARE' die entsprechende Optionsangabe (oder wählen Sie 'Liste' aus)

Taste OK

Ist der Befehl vollständig ausgeführt, drücken Sie die Taste für **Ende**. Wählen Sie dann im Menü "Beenden" den Eintrag **SMIT beenden** aus oder drücken Sie die Taste **F12**. Drücken Sie bei Verwendung von SMITTY die Taste **F10**, um das Programm zu verlassen.

Verwendung der Befehlszeile:

Führen Sie die Installation von einer CD aus, müssen Sie die folgenden Befehle eingeben, um die CD einzulegen:

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

Stellen Sie anhand der folgenden Tabelle fest, welche Befehle Sie eingeben müssen, um die gewünschten Pakete von Network Dispatcher für AIX zu installieren:

Tabelle 2. AIX-Installationsbefehle

Network Dispatcher (mit Nachrichten); umfasst Dispatcher, CBR, Mailbox Locator, Site Selector und Cisco Consultant.	installp -acXgd <i>Einheit</i> intnd.nd.rte intnd.admin.rte intnd.nd.driver intnd.msg.<Sprache>.nd intnd.msg.<Sprache>.admin
Dokumente	installp -acXgd <i>Einheit</i> intnd.doc.rte intnd.msg.<Sprache>.doc
Administration (nur Komponente)	installp -acXgd <i>Einheit</i> intnd.admin.rte intnd.msg.<Sprache>.admin
Lizenz	installp -acXgd <i>Einheit</i> intnd.nd.license
Metric Server	installp -acXgd <i>Einheit</i> intnd.ms.rte intnd.msg.<Sprache>.admin

Einheit steht hier für Folgendes:

- /cdrom, wenn die Installation von einer CD erfolgt.
- /dir (das Verzeichnis mit den installp-Images), wenn die Installation von einem Dateisystem aus erfolgt.

Achten Sie darauf, dass die Ergebnisspalte in der Zusammenfassung für alle installierten Komponenten von Network Dispatcher jeweils die Angabe **ERFOLGREICH** enthält. Fahren Sie erst fort, wenn alle ausgewählten Komponenten erfolgreich installiert wurden.

Anmerkung: Wenn Sie für ein installp-Image eine Liste der Dateigruppen einschließlich aller verfügbaren Nachrichtenkataloge generieren möchten, geben Sie folgendes ein:

```
installp -ld Einheit
```

Einheit steht hier für Folgendes:

- /cdrom, wenn die Installation von einer CD erfolgt.
- /dir (das Verzeichnis mit den installp-Images), wenn die Installation von einem Dateisystem aus erfolgt.

Geben Sie folgendes ein, um die CD abzuhängen:

```
umount /cdrom
```

4. Überprüfen Sie, ob das Produkt installiert ist. Geben Sie den folgenden Befehl ein:

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

Wurde das gesamte Produkt installiert, gibt dieser Befehl folgendes zurück:

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

Für Network Dispatcher gelten die folgenden Installationspfade:

- Administration - **/usr/lpp/nd/admin**
- Network-Dispatcher-Komponenten - **/usr/lpp/nd/servers**
- Metric Server - **/usr/lpp/nd/ms**
- Dokumentation (*Administratorhandbuch*) - **/usr/lpp/nd/documentation**

Voraussetzungen für Red Hat Linux oder SuSE Linux

- Red Hat Linux Version 7.1 (Linux-Kernel Version 2.4.2-2) oder SuSE Linux Version 7.1 (Linux-Kernel Version 2.4.0 - 4 GB). Es werden sowohl Einzelprozessor- als auch Multiprozessor-Kernels unterstützt.

Anmerkung: Wenn Sie die MAC-Weiterleitungsmethode von Dispatcher mit hoher Verfügbarkeit und Verknüpfung verwenden möchten, müssen Sie einen Patch-Code für den Linux-Kernel installieren. Informationen zum Download und zur Installation des Patch-Codes finden Sie im Abschnitt „Patch-Code für Linux-Kernel (zum Unterdrücken von ARP-Antworten an der Loopback-Schnittstelle) installieren“ auf Seite 77.

- 50 MB freier Plattenspeicherplatz für die Installation.

Anmerkung: Für Protokolle wird zusätzlicher Plattenspeicherplatz benötigt.

- Die folgenden Netzschnittstellenkarten (Network Interface Cards = NICs) werden unterstützt:
 - 10 Mbit Ethernet
 - 100 Mbit Ethernet
 - 1 Gbit Ethernet
 - Ethernet-NICs mit mehreren Anschlüssen (Nur Unterstützung für Modus 1. Fehlertoleranz (Modus 2) und Anschlussbündelung (Modus 3) werden nicht unterstützt.)

Anmerkung: Die Implementierung der NICs mit mehreren Anschlüssen ist je nach Lieferant verschieden. Deshalb kann die Unterstützung bestimmter NICs mit mehreren Anschlüssen eingeschränkt sein.

- Eine Version der Korn-Shell (ksh) muss installiert werden.
- IBM Runtime Environment für Linux, Java 2 Technology Edition, ab Version 1.3.0. (Weitere Informationen zur Ausführung mehrerer Java-Versionen können Sie der Anmerkung 3 auf Seite 11 entnehmen.)
- Die Umgebungsvariablen JAVA_HOME und PATH müssen mit dem Befehl **export** gesetzt werden. Der Inhalt der Variablen JAVA_HOME ist von der Position abhängig, an der der Benutzer Java installiert hat. Beispiel:
 - JAVA_HOME=/opt/IBMJava2-13/jre
 - PATH=\$JAVA_HOME/bin:\$PATH
- Edge Server Caching Proxy Version 2.0, falls Sie zum Verteilen von HTTP- oder SSL-Datenverkehr die CBR-Komponente verwenden.
- Netscape Navigator ab Version 4.07 oder Netscape Communicator ab Version 4.61 zum Anzeigen von Onlinehilfetexten.
- Für Consultant für Cisco CSS Switches müssen Sie den Cisco CSS 11000 Series Switch installiert und konfiguriert haben.

Installation unter Linux

In diesem Abschnitt wird erklärt, wie Network Dispatcher unter Red Hat Linux oder SuSE Linux unter Verwendung der Produkt-CD oder der von der Website heruntergeladenen Probeversion installiert wird. Installationsanweisungen finden Sie auf der Website (<http://www.ibm.com/software/webservers/edgeserver/download.html>).

Installation vorbereiten

Vergewissern Sie sich vor Beginn des Installationsverfahrens, dass Sie die Root-Berechtigung für die Installation der Software haben.

Installationsschritte

Anmerkung: Falls Sie eine frühere Version installiert haben, sollten Sie diese Kopie vor Installation der aktuellen Version deinstallieren. Vergewissern Sie sich zunächst, dass alle Steuerprogramme und Server gestoppt wurden. Geben Sie anschließend **rpm -e Paketname** ein, um das gesamte Produkt zu deinstallieren. Bei der Deinstallation ist die Reihenfolge umzukehren, die für die Installation der Pakete verwendet wurde. Damit wird sichergestellt, dass die Verwaltungspakete zuletzt deinstalliert werden.

Gehen Sie wie folgt vor, um Network Dispatcher zu installieren:

1. Bereiten Sie die Installation vor.

- Melden Sie sich als Root an.
- Legen Sie den Produktdatenträger ein oder laden Sie das Produkt von der Website herunter und installieren Sie das Installationsimage mit Hilfe von RPM (Red Hat Packaging Manager).

Anmerkung: Das Installationspaket für Red Hat Linux bzw. für SuSE Linux kann unter keiner anderen Produktversion von Linux ausgeführt werden.

Das Installationsimage ist eine Datei im Format **ndlinux-Version.tar**.

- Entpacken Sie die tar-Datei in einem temporären Verzeichnis, indem Sie **tar -xf ndlinux-Version.tar** eingeben. Das Ergebnis ist eine Gruppe von Dateien mit der Erweiterung .rpm.

Die folgende Liste enthält die von RPM installierbaren Pakete.

- **ibmnd-adm-Releaseversion.i386.rpm** (Network Dispatcher Administration)
- **ibmnd-doc-Releaseversion.i386.rpm** (Dokumentation)
- **ibmnd-ms-Releaseversion.i386.rpm** (Metric Server)
- **ibmnd-srv-Releaseversion.i386.rpm** (Network-Dispatcher-Laufzeit)
- **ibmnd-lic-Releaseversion.i386.rpm** (Lizenz)

- Die Reihenfolge, in der die Pakete installiert werden, ist wichtig. Die folgende Liste zeigt die für jede Komponente erforderlichen Pakete und die Reihenfolge, in der sie installiert werden müssen:
 - Administration (adm)
 - Lizenz (lic)
 - Network-Dispatcher-Komponenten (srv)
 - Metric Server (ms)
 - Dokumentation (doc).

Der Befehl zum Installieren der Pakete sollte von dem Verzeichnis mit den RPM-Dateien aus abgesetzt werden. Setzen Sie zum Installieren der einzelnen Pakete den Befehl **rpm -i *Paket.rpm*** ab.

Anmerkung: Mindestens eine der RPM-Dateien erfordert, dass Java installiert und in der RPM-Datenbank registriert ist. Ist Java installiert, aber nicht in der RPM-Datenbank registriert, verwenden Sie den Installationsbefehl wie folgt mit der Option 'no dependencies':

rpm -i --nodeps *Paket.rpm*

- Für Network Dispatcher gelten die folgenden Installationspfade:
 - Administration - **/opt/nd/admin**
 - Network-Dispatcher-Komponenten - **/opt/nd/servers**
 - Metric Server - **/opt/nd/ms**
 - Dokumentation (*Administratorhandbuch*) - **/opt/nd/documentation**
 - Bei der Deinstallation der Pakete ist die Reihenfolge umzukehren, die für die Installation der Pakete verwendet wurde. Damit wird sichergestellt, dass die Verwaltungspakete zuletzt deinstalliert werden.
2. Überprüfen Sie, ob das Produkt installiert ist. Geben Sie den folgenden Befehl ein:

rpm -qa | grep ibmnd

Wurde das gesamte Produkt installiert, sollte eine Liste wie die folgende generiert werden:

- *ibmnd-adm-Releaseversion*
- *ibmnd-doc-Releaseversion*
- *ibmnd-ms-Releaseversion*
- *ibmnd-srv-Releaseversion*
- *ibmnd-lic-Releaseversion*.

Voraussetzungen für Solaris

- Eine von Solaris Version 7 oder 8 unterstützte SPARC-Workstation bzw. ein von diesen Versionen unterstützter Ultra-60-Server. Network Dispatcher unterstützt nur Solaris-Plattformen im 32-Bit-Modus.
- 50 MB freier Plattenspeicherplatz für die Installation.

Anmerkung: Für Protokolle wird zusätzlicher Plattenspeicherplatz benötigt.

- Die folgenden Netzschnittstellenkarten (Network Interface Cards = NICs) werden unterstützt:
 - 10 Mbit Ethernet
 - 100 Mbit Ethernet
 - 1 Gbit Ethernet (nur auf Ultra-60-Server unterstützt)
 - Ethernet-NICs mit mehreren Anschlüssen (Nur Unterstützung für Modus 1. Fehlertoleranz (Modus 2) und Anschlussbündelung (Modus 3) werden nicht unterstützt.)

Anmerkung: Die Implementierung der NICs mit mehreren Anschlüssen ist je nach Lieferant verschieden. Deshalb kann die Unterstützung bestimmter NICs mit mehreren Anschlüssen eingeschränkt sein.

- Java 2 JRE, Standard Edition, ab Version 1.3.0. (Weitere Informationen zur Ausführung mehrerer Java-Versionen können Sie der Anmerkung 3 auf Seite 11 entnehmen.)
- Edge Server Caching Proxy Version 2.0, falls Sie zum Verteilen von HTTP- oder SSL-Datenverkehr die CBR-Komponente verwenden.
- Für Solaris 7: Sun Microsystems HotJava Browser ab Version 1.0.1 zum Anzeigen der Onlinehilfe.
Für Solaris 8: Netscape Navigator ab Version 4.07 oder Netscape Communicator ab Version 4.61 zum Anzeigen der Onlinehilfe.
- Für Consultant für Cisco CSS Switches müssen Sie den Cisco CSS 11000 Series Switch installiert und konfiguriert haben.

Installation unter Solaris

In diesem Abschnitt wird erklärt, wie Network Dispatcher unter Solaris von der Produkt-CD installiert wird. Falls Sie eine Probeversion des Produkts aus dem Internet downloaden, verwenden Sie die auf der Website enthaltenen Installationsanweisungen

(<http://www.ibm.com/software/webserver/edgeserver/download.html>).

Installation vorbereiten

Vergewissern Sie sich vor Beginn des Installationsverfahrens, dass Sie die Root-Berechtigung für die Installation der Software haben.

Installationsschritte

Anmerkung: Haben Sie eine frühere Version installiert, sollten Sie die Installation dieser Kopie entfernen, bevor Sie die aktuelle Version installieren. Vergewissern Sie sich zunächst, dass das Steuerprogramm und der Server gestoppt wurde. Geben Sie dann zum Deinstallieren von Network Dispatcher **pkgrm Paketname** ein.

Gehen Sie wie folgt vor, um Network Dispatcher zu installieren:

1. Bereiten Sie die Installation vor.

- Melden Sie sich als Benutzer "root" an.
- Legen Sie die CD-ROM mit der Network Dispatcher-Software in das entsprechende Laufwerk ein.

Geben Sie an der Eingabeaufforderung **pkgadd -d Pfadname** ein. Dabei ist **-d Pfadname** der Einheitenname des CD-ROM-Laufwerks oder das Verzeichnis auf dem Festplattenlaufwerk, in dem sich das Paket befindet. Beispiel: **pkgadd -d /cdrom/cdrom0/**.

Es wird eine Liste mit Paketen angezeigt, die installiert werden können. Diese Pakete sind:

- ibmdsp IBM ND für Solaris (Network-Dispatcher-Komponenten)
- ibmndadm IBM ND Basisverwaltung für Solaris
- ibmnddoc IBM ND Dokumentation für Solaris
- ibmndms IBM ND Metric Server für Solaris
- ibmdsplic Lizenz für Solaris

Sollen alle Pakete installiert werden, geben Sie einfach "all" ein und drücken Sie die Rückföhrtaste. Sollen einzelne Komponenten installiert werden, geben Sie die Namen der zu installierenden Pakete durch ein Leerzeichen oder Komma getrennt ein und drücken Sie die Rückföhrtaste. Möglicherweise werden Sie aufgefordert, Berechtigungen für vorhandene Verzeichnisse oder Dateien zu ändern. Drücken Sie einfach die Rückföhrtaste oder antworten Sie mit "yes". Sie müssen vorausgesetzte Pakete installieren (da die Installation in alphabetischer Reihenfolge und nicht in der Reihenfolge der vorausgesetzten Pakete erfolgt). Haben Sie "all" eingegeben, antworten Sie auf alle Bedienerföhungen mit "yes". Die Installation wird dann erfolgreich ausgeföhrt.

Alle Pakete sind von dem allgemeinen Paket `ibmndadm` abhängig. Dieses allgemeine Paket muss zusammen mit allen anderen Paketen installiert werden.

Falls Sie das gesamte Produkt Network Dispatcher installieren möchten, müssen Sie die fünf Komponenten `ibmdsp`, `ibmdsplic`, `ibmndadm`, `ibmnddoc` und `ibmndms` installieren. Wenn Sie die Fernverwaltung installieren möchten, muss nur die Komponente `ibmndadm` installiert werden.

Die Network-Dispatcher-Komponenten sind wie folgt im Installationsverzeichnis `/opt/nd/servers` enthalten.

2. Die installierte Verwaltungskomponente befindet sich im Verzeichnis `/opt/nd/admin`.
3. Der installierte Metric Server befindet sich im Verzeichnis `/opt/nd/ms`.
4. Die installierte Dokumentation (*Administratorhandbuch*) befindet sich im Verzeichnis `/opt/nd/documentation`.
5. Überprüfen Sie, ob das Produkt installiert ist. Setzen Sie den folgenden Befehl ab: `pkginfo | grep ibm`

Wurde das gesamte Produkt installiert, sollte eine Liste wie die folgende generiert werden:

- `ibmdsp`
- `ibmndadm`
- `ibmnddoc`
- `ibmndms`
- `ibmdsplic`

Voraussetzungen für Windows 2000

- Ein von Microsoft Windows 2000 unterstützter PC Intel x86
- Windows 2000 Professional, Server oder Advanced Server
- 50 MB freier Plattenspeicherplatz für die Installation.

Anmerkung: Für Protokolle wird zusätzlicher Plattenspeicherplatz benötigt.

- Die folgenden Netzschnittstellenkarten (Network Interface Cards = NICs) werden unterstützt:
 - 16 Mbit Token-Ring
 - 10 Mbit Ethernet
 - 100 Mbit Ethernet
 - 1 Gbit Ethernet
 - Ethernet-NICs mit mehreren Anschlüssen

Anmerkung: Die Implementierung der NICs mit mehreren Anschlüssen ist je nach Lieferant verschieden. Deshalb kann die Unterstützung bestimmter NICs mit mehreren Anschlüssen eingeschränkt sein.

- IBM Cross Platform Technologies für Windows Version 2.0 (SDK ab Version 1.3.0).

Beachten Sie, dass Sie sowohl das Installationspaket für das Developer Kit herunterladen müssen als auch das Installationspaket für Runtime Environment (Laufzeitumgebung), bevor Sie das InstallShield-Programm ausführen. (Weitere Informationen zur Ausführung mehrerer Java-Versionen können Sie der Anmerkung 3 auf Seite 11 entnehmen.)

- Edge Server Caching Proxy Version 2.0, falls Sie zum Verteilen von HTTP- oder SSL-Datenverkehr die CBR-Komponente verwenden.
- Stellen Sie sicher, dass Ihr Standardbrowser Netscape Navigator ab Version 4.07, Netscape Communicator ab Version 4.61 oder Internet Explorer ab Version 4.0 ist. Der Standardbrowser wird zum Anzeigen der Onlinehilfe verwendet.
- Für Consultant für Cisco CSS Switches müssen Sie den Cisco CSS 11000 Series Switch installiert und konfiguriert haben.

Installation unter Windows 2000

In diesem Abschnitt wird erklärt, wie Network Dispatcher von der Produkt-CD unter Windows 2000 installiert wird. Falls Sie eine Probeversion des Produkts von der Website downloaden, verwenden Sie die auf der Website enthaltenen Installationsanweisungen

(<http://www.ibm.com/software/webserver/edgeserver/download.html>).

Installationspakete

Es wird eine Liste mit Paketen angezeigt, die installiert werden können.

Diese Pakete sind:

- Laufzeit
- Administration
- Lizenz
- Dokumentation
- Metric Server.

Installation vorbereiten

Die Produktversion von Network Dispatcher für Windows 2000 wird von den folgenden Betriebssystemen unterstützt:

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

Anmerkung: Unter anderen Windows-Versionen kann die Produktversion von Network Dispatcher für Windows 2000 *nicht* ausgeführt werden.

Einschränkungen: Die Version von Network Dispatcher für Windows 2000 kann nicht auf derselben Maschine wie IBM Firewall installiert werden.

Vergewissern Sie sich vor Beginn der Installation, dass Sie als Administrator oder Benutzer mit Administratorberechtigung angemeldet sind.

Installationsschritte

Falls Sie eine frühere Version installiert haben, sollten Sie diese Kopie vor Installation der aktuellen Version deinstallieren. Gehen Sie zum Deinstallieren mit der Option **Software** wie folgt vor:

1. Klicken Sie nacheinander auf **Start**→**Einstellungen**→**Systemsteuerung**.
2. Klicken Sie doppelt auf **Software**.
3. Wählen Sie *Network Dispatcher* aus.
4. Klicken Sie auf die Schaltfläche **Ändern/Entfernen**.

Gehen Sie wie folgt vor, um Network Dispatcher zu installieren:

1. Legen Sie die CD-ROM mit Network Dispatcher in das CD-ROM-Laufwerk ein. Das Installationsfenster sollte automatisch angezeigt werden.
2. Der folgende Schritt ist nur erforderlich, wenn die automatische Ausführung der CD auf Ihrem Computer nicht funktionierte. Verwenden Sie für die folgenden Tasks die erste (linke) Maustaste:
 - Klicken Sie auf **Start**.
 - Wählen Sie **Ausführen** aus.
 - Geben Sie das CD-ROM-Laufwerk gefolgt von setup.exe an. Beispiel:
`E:\setup`
3. Wählen Sie die **Sprache** aus, die für den Installationsprozess verwendet werden soll.
4. Klicken Sie auf **OK**.
5. Befolgen Sie die Anweisungen des Installationsprogramms.
6. Wollen Sie das Ziellaufwerk oder -verzeichnis ändern, klicken Sie auf **Durchsuchen**.
7. Sie können "Das gesamte Produkt Network Dispatcher" oder "Ihre Auswahl der Komponenten" auswählen.
8. Nach Abschluss der Installation erscheint eine Nachricht, in der Sie aufgefordert werden, vor der Benutzung von Network Dispatcher einen Warmstart auszuführen. Dies ist erforderlich, um sicherzustellen, dass alle Dateien installiert sind und die Umgebungsvariable IBMNDPATH zur Registrierungsdatenbank hinzugefügt wurde.

Für Network Dispatcher gelten die folgenden Installationspfade:

- Administration – **c:\Progra~1\IBM\edge\nd\admin**
- Network-Dispatcher-Komponenten – **c:\Progra~1\IBM\edge\nd\servers**
- Metric Server – **c:\Progra~1\IBM\edge\nd\ms**
- Dokumentation (Administratorhandbuch) –
c:\Progra~1\IBM\edge\nd\documentation

Kapitel 3. Einführung in Network Dispatcher

Dieses Kapitel gibt einen Überblick über Network Dispatcher und ist in die folgenden Abschnitte gegliedert:

- „Was ist Network Dispatcher?“
- „Vorteile von Network Dispatcher“ auf Seite 28
- „Neue Merkmale“ auf Seite 30
- „Komponenten von Network Dispatcher“ auf Seite 36
- „Hohe Verfügbarkeit“ auf Seite 48.

Was ist Network Dispatcher?

Network Dispatcher ist eine Softwarelösung für den Lastausgleich von Servern. Dieses Produkt verbessert die Leistung von Servern erheblich, indem es TCP/IP-Sitzungsanforderungen an verschiedene Server einer Gruppe verteilt. Dieser Lastausgleich ist für Benutzer und andere Anwendungen transparent. Network Dispatcher ist vor allem bei Anwendungen wie E-Mail-Servern, WWW-Servern, parallelen Abfragen verteilter Datenbanken und anderen TCP/IP-Anwendungen nützlich.

Beim Einsatz mit Webservern kann Network Dispatcher zur optimalen Nutzung des Potenzials Ihrer Site beitragen, da er eine leistungsfähige, flexible und skalierbare Lösung für Probleme bietet, die durch eine sehr hohe Belastung auftreten können. Haben Besucher zu Zeiten höchster Belastung Schwierigkeiten, auf Ihre Site zuzugreifen, können Sie mit Network Dispatcher automatisch den optimalen Server zur Bearbeitung eingehender Anforderungen suchen.

Network Dispatcher besteht aus fünf Komponenten, die separat oder zusammen verwendet werden können, um bessere Ergebnisse beim Lastausgleich zu erzielen:

- Sie können allein mit der **Dispatcher**-Komponente einen Lastausgleich auf Servern in einem lokalen Netz oder Weitverkehrsnetz durchführen, indem Sie die von Dispatcher dynamisch festgelegten Wertigkeiten und Messungen verwenden. Diese Komponente führt den Lastausgleich auf der Ebene bestimmter Dienste aus, beispielsweise für HTTP, FTP, SSL, NNTP, IMAP, POP3, SMTP und Telnet. Die Komponente benutzt für die Zuordnung von Domännennamen zu IP-Adressen keinen Domännennamensserver.

Wenn Sie mit dem Protokoll HTTP arbeiten, können Sie auch die Dispatcher-Funktion für inhaltsabhängige Weiterleitung verwenden, um die Last

ausgehend vom Inhalt der Client-Anfrage zu verteilen. Der ausgewählte Server ist das Ergebnis des Abgleichs des URL mit einer angegebenen Regel.

- Wenn Sie mit den Protokollen HTTP und HTTPS (SSL) arbeiten, können Sie die Komponente **Content Based Routing** (CBR) für einen Lastausgleich ausgehend vom Inhalt der Client-Anfrage verwenden. Ein Client sendet eine Anfrage an Caching Proxy, und Caching Proxy sendet diese Anfrage an einen geeigneten Server. Der ausgewählte Server ist das Ergebnis des Abgleichs des URL mit einer angegebenen Regel.
- Wenn Sie mit dem Protokoll IMAP oder POP3 arbeiten, können Sie die Komponente **Mailbox Locator** verwenden, die wie ein Proxy funktioniert und ausgehend von der vom Client angegebenen Benutzer-ID mit Kennwort einen geeigneten Server auswählt.
- Mit der Komponente **Site Selector** können Sie einen Lastausgleich für Server in einem lokalen oder Weitverkehrsnetz durchführen. Sie können dazu nach einer DNS-RoundRobin-Methode oder nach einer komplexeren benutzerdefinierten Methode vorgehen. Site Selector ordnet zusammen mit einem Namensserver IP-Adressen DNS-Namen zu.
- Mit der Komponente **Consultant für Cisco CSS Switches** können Sie Messwerte für die Servergewichtung generieren, die dann zur Erreichung einer optimalen Serverauswahl sowie von Lastoptimierung und Fehlertoleranz an den Cisco CSS Switch gesendet werden.

Weitere Informationen zu den Komponenten Dispatcher, CBR, Mailbox Locator, Site Selector und Consultant für Cisco CSS Switches finden Sie im Abschnitt „Komponenten von Network Dispatcher“ auf Seite 36.

Vorteile von Network Dispatcher

Die Anzahl von Benutzern und Netzen, die mit dem globalen Internet verbunden sind, wächst mit rasanter Geschwindigkeit. Dieses Wachstum verursacht Probleme hinsichtlich der Skalierbarkeit, da der Benutzerzugriff auf attraktive Sites bei einem hohen Anforderungsaufkommen möglicherweise eingeschränkt wird.

Derzeit benutzen Netzadministratoren verschiedene Methoden zur Optimierung des Zugriffs. Bei einigen dieser Methoden können Benutzer nach dem Zufallsprinzip einen anderen Server auswählen, wenn der vorher ausgewählte Server zu langsam oder überhaupt nicht antwortet. Diese Vorgehensweise ist jedoch mühsam und ineffektiv. Eine weitere Methode ist die Standard-RoundRobin-Methode, bei der der Domänennamensserver der Reihe nach Server zur Bearbeitung von Anforderungen auswählt. Dieser Ansatz ist zwar besser, aber immer noch ineffizient, da der Datenverkehr ohne Berücksichtigung der Serverauslastung weitergeleitet wird. Zudem werden bei dieser Methode auch dann noch Anforderungen an einen Server gesendet, wenn er ausgefallen ist.

Der Bedarf an einer leistungsfähigeren Lösung hat zur Entwicklung von Network Dispatcher geführt. Dieses Produkt bietet gegenüber früheren Lösungen und Lösungen von anderer Anbieter eine Vielzahl von Vorteilen:

Skalierbarkeit

Wenn die Anzahl der Client-Anforderungen steigt, können Sie Server dynamisch hinzufügen und Millionen von Anforderungen pro Tag auf Hunderten von Servern unterstützen.

Effektive Nutzung der Ausrüstung

Der Lastausgleich gewährleistet, dass jede Servergruppe die zugehörige Hardware optimal nutzen kann, da die bei einer Standard-Round-Robin-Methode häufig auftretenden Spitzenbelastungen auf ein Minimum reduziert werden.

Problemlose Integration

Network Dispatcher benutzt TCP/IP-Standardprotokolle. Das Produkt kann zu einem vorhandenen Netz hinzugefügt werden, ohne dass physische Änderungen am Netz erforderlich sind. Es ist leicht zu installieren und zu konfigurieren.

Geringer Systemaufwand

Bei Anwendung der einfachen MAC-Weiterleitung muss der Dispatcher nur auf den beim Server eingehenden Datenverkehr vom Client achten, nicht aber auf den vom Server zum Client abgehenden Datenverkehr. Dies führt im Vergleich zu anderen Methoden zu einer erheblichen Reduzierung der Auswirkungen auf die Anwendung und zu einer verbesserten Leistung im Netz.

Hohe Verfügbarkeit

Der Dispatcher verfügt über eine integrierte Funktion für hohe Verfügbarkeit, bei der eine Partnermaschine benutzt wird, die jederzeit die Weiterleitung von Paketen übernehmen kann, wenn die primäre Dispatcher-Maschine ausfällt. Die Dispatcher-Komponente gewährleistet außerdem eine gegenseitige hohe Verfügbarkeit, so dass zwei Maschinen aktiv sein und die jeweils andere Maschine als Ausweichmaschine nutzen können. Weitere Informationen hierzu finden Sie im Abschnitt „Hohe Verfügbarkeit“ auf Seite 48.

Content Based Routing (mit der Komponente CBR oder Dispatcher)

Zusammen mit Caching Proxy kann die Komponente CBR HTTP- und HTTPS-Anforderungen (SSL) ausgehend vom angefragten Inhalt an bestimmte Server weiterleiten. Wenn eine Anforderung im Verzeichnisabschnitt des URL beispielsweise die Zeichenfolge `"/cgi-bin/"` enthält und der Servername ein lokaler Server ist, kann CBR die Anfor-

derung an den besten Server einer speziell für die Bearbeitung von cgi-Anforderungen zugeordneten Servergruppe übertragen.

Die Dispatcher-Komponente erlaubt auch eine inhaltsabhängige Weiterleitung, erfordert jedoch nicht die Installation von Caching Proxy. Da die inhaltsabhängige Weiterleitung der Dispatcher-Komponente bei Empfang von Paketen im Kernel ausgeführt wird, ist die inhaltsabhängige Weiterleitung der Dispatcher-Komponente *schneller* als die der CBR-Komponente. Die Dispatcher-Komponente führt das Content Based Routing für HTTP (unter Verwendung des Regeltyps "content") und für HTTPS (unter Verwendung der Affinität von SSL-Sitzungs-IDs) durch.

Anmerkung: Für HTTPS (SSL) kann die CBR-Komponente den Regeltyp "content" nur für den Lastausgleich von Datenverkehr verwenden, der auf dem Inhalt der HTTP-Anforderung basiert, was das Entschlüsseln und erneute Verschlüsseln von Nachrichten erfordert.

Neue Merkmale

Network Dispatcher für IBM WebSphere Edge Server Version 2.0 ist durch eine Reihe neuer Merkmale gekennzeichnet. Die wichtigsten dieser Merkmale sind nachfolgend aufgelistet.

- **Unterstützung für AIX Version 5.1**

Dieses Merkmal gilt für alle Komponenten von Network Dispatcher.

Network Dispatcher bietet jetzt Unterstützung für eine neuere Version von AIX, für AIX Version 5.1. Weitere Informationen hierzu finden Sie im Abschnitt „Voraussetzungen für AIX“ auf Seite 12.

- **Unterstützung für SuSE Linux Version 7.1**

Dieses Merkmal gilt für alle Komponenten von Network Dispatcher.

Network Dispatcher bietet jetzt Unterstützung für SuSE Linux Version 7.1 (Kernel-Version 2.4.0 - 4 GB). Früher hat Network Dispatcher nur Red Hat Linux unterstützt. Weitere Informationen hierzu finden Sie im Abschnitt „Voraussetzungen für Red Hat Linux oder SuSE Linux“ auf Seite 17.

- **Unterstützung für Red Hat Linux Version 7.1**

Dieses Merkmal gilt für alle Komponenten von Network Dispatcher.

Network Dispatcher bietet jetzt Unterstützung für eine neuere Version von Red Hat Linux, für Red Hat Linux Version 7.1 (Kernel-Version 2.4.2-2). Weitere Informationen hierzu finden Sie im Abschnitt „Voraussetzungen für Red Hat Linux oder SuSE Linux“ auf Seite 17.

- **Unterstützung der Landessprache für Linux und Solaris**

Dieses Merkmal gilt für alle Komponenten von Network Dispatcher.

Unter den Betriebssystemen Linux und Solaris bietet Network Dispatcher Unterstützung der Landessprache für Länder der Gruppe 1.

- **Unterstützung für neuen Chinesisch-Standard**

Dieses Merkmal gilt für alle Komponenten von Network Dispatcher.

Network Dispatcher bietet Unterstützung der Landessprache gemäß dem neuen Chinesisch-Standard GB 18030.

- **Komponente Consultant für Cisco CSS Switches (Cisco Consultant)**

Dies ist eine neue Komponente von Network Dispatcher.

In Zusammenarbeit mit Cisco und dem CDN (Content Distribution Network) von Cisco wurde eine zusätzliche Komponente für Network Dispatcher entwickelt, Cisco Consultant. Diese Komponente (die ursprünglich als Standalone-Komponente eingeführt wurde) ermöglicht Network Dispatcher, Wertigkeiten für den Cisco CSS Switch zu generieren und Lastausgleichsentscheidungen für den Switch zu treffen.

Weitere Informationen hierzu finden Sie in „Kapitel 12. Planung für Consultant für Cisco CSS Switches“ auf Seite 127 und „Kapitel 13. Consultant für Cisco CSS Switches konfigurieren“ auf Seite 133.

- **Komponente Site Selector**

Dies ist eine neue Komponente von Network Dispatcher.

Die Komponente Site Selector verteilt die Last für eine Gruppe von Servern, indem sie für eine Namensserviceanforderung die IP-Adresse des "richtigen" Servers auswählt. Dadurch kann der Client für seine gesamte Kommunikation eine direkte Verbindung zu diesem Server herstellen. Site Selector ersetzt die in früheren Releases von Network Dispatcher enthaltene Komponente Interactive Session Support (ISS). Die Funktionalität von Site Selector ist mit der von ISS vergleichbar. Site Selector erfordert für das Einrichten einer typischen DNS-Konfiguration mit Lastausgleich jedoch weniger Schritte.

Weitere Informationen hierzu finden Sie in „Kapitel 10. Planung für Site Selector“ auf Seite 113 und „Kapitel 11. Site Selector konfigurieren“ auf Seite 119.

- **Metric Server**

Diese Funktion ist für alle Komponenten von Network Dispatcher verfügbar.

Metric Server liefert Network Dispatcher Informationen zur Serverauslastung in Form systemspezifischer Messwerte. Der Agent Metric Server ist eine Komponente von Network Dispatcher, die auf Servern installiert und aufgeführt werden kann, für die Network Dispatcher einen Lastausgleich durchführt. Metric Server ersetzt den System Monitoring Agent (SMA), der in früheren Releases unter Linux unterstützt wurde. Metric Ser-

ver wird von allen Plattformen unterstützt. Sie sollten Metric Server zusammen mit der Komponente Site Selector verwenden.

Weitere Informationen hierzu finden Sie im Abschnitt „Metric Server“ auf Seite 161.

- **Komponente Mailbox Locator**

Dies ist eine neue Komponente für Network Dispatcher.

Die Komponente Mailbox Locator war früher Bestandteil der CBR-Komponente und wurde bei IMAP- und POP3-Postservern für einen Lastausgleich ausgehend von Benutzer-ID und Kennwort verwendet. Durch die Untergliederung von CBR in zwei Komponenten können Mailbox Locator (bisher als "CBR für IMAP/POP3" bekannt) und CBR mit Caching Proxy auf einer Maschine ausgeführt werden.

Weitere Informationen hierzu finden Sie in „Kapitel 8. Planung für Mailbox Locator“ auf Seite 101 und „Kapitel 9. Mailbox Locator konfigurieren“ auf Seite 105.

- **Verbesserte Benutzerfreundlichkeit der Komponente CBR (Content Based Routing)**

Das Konfigurieren der Caching-Proxy-Konfigurationsdatei (ibmproxy.conf) für die Verwendung von CBR wurde optimiert, so dass auf einer Maschine mehrere Instanzen des Caching Proxy parallel bei gleichzeitiger Integration von CBR ausgeführt werden können. Weitere Informationen zum Konfigurieren von CBR mit Caching Proxy finden Sie im Abschnitt „CBR-Maschine konfigurieren“ auf Seite 93.

- **Unterstützung für NAT (Network Address Translation, Konvertierung von Netzadressen) und NAPT (Network Address Port Translation, Port-Umsetzung für Netzadressen)**

Dieses Merkmal gilt für die Dispatcher-Komponente.

Durch NAT/NAPT entfällt die Einschränkung, dass sich Back-End-Server im lokal angeschlossenen Netz befinden müssen. Durch NAT/NAPT kann der Dispatcher außerdem die Last der TCP-Anforderungen von Clients auf mehrere Serverdämonen, die auf einer physischen Maschine ausgeführt werden, verteilen. Server mit mehreren Dämonen können Sie auf zwei verschiedene Arten konfigurieren. Mit NAT können Sie mehrere Serverdämonen für die Beantwortung von Anfragen, die an verschiedene IP-Adressen gerichtet sind, konfigurieren. Dieses Konfiguration wird auch als Bindung eines Serverdämons an eine IP-Adresse bezeichnet. Mit NAPT können Sie mehrere Serverdämonen so konfigurieren, dass sie an unterschiedlichen Port-Nummern empfangsbereit sind.

Die Weiterleitungsmethode "nat" von Dispatcher bietet den Vorteil, dass sie auf Port-Ebene konfiguriert wird und Ihnen so ein höheres Maß an Detailierung ermöglicht.

Anmerkung: Network Dispatcher kann NAT/NAPT nicht für Anwendungsprotokolle wie FTP verwenden, die die Adressen oder Port-Nummern in den Datenabschnitt von Nachrichten einbetten. Dies ist eine allgemein bekannte Einschränkung für die Header-bezogene NAT/NAPT.

Weitere Informationen hierzu finden Sie im Abschnitt „NAT/NAPT-Weiterleitungsmethode (nat) des Dispatchers“ auf Seite 55.

- **Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (unter Verwendung des Regeltyps "content" und der Affinität von SSL-Sitzungs-IDs)**

Dieses Merkmal gilt für die Dispatcher-Komponente.

In früheren Releases von Network Dispatcher war das Content Based Routing nur bei Verwendung der CBR-Komponente zusammen mit Caching Proxy verfügbar. Jetzt können Sie mit der Dispatcher-Komponente das Content Based Routing für HTTP (unter Verwendung des Regeltyps "content") und für HTTPS (unter Verwendung der Affinität von SSL-Sitzungs-IDs) ohne Caching Proxy ausführen. Für HTTP- und HTTPS-Datenverkehr ist das Content Based Routing der Dispatcher-Komponente schneller als das der CBR-Komponente.

Weitere Informationen zur Verwendung des Regeltyps "content" und der Affinität von SSL-Sitzungs-IDs finden Sie im Abschnitt „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)“ auf Seite 57.

- **Passive Cookie-Affinität**

Dieses Merkmal gilt für die inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (Weiterleitungsmethode cbr) und die CBR-Komponente.

Die passive Cookie-Affinität ermöglicht die Verteilung von Webdatenverkehr mit Affinität zu einem Server ausgehend von den Identifizierungs-Cookies, die von den Servern generiert werden. Weitere Informationen finden Sie im Abschnitt „Passive Cookie-Affinität“ auf Seite 209.

- **URI-Affinität (Lastverteilung auf Caching Proxies)**

Dieses Merkmal gilt für die inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (Weiterleitungsmethode cbr) und die CBR-Komponente.

Die URI-Affinität ermöglicht eine Lastverteilung für Webdatenverkehr auf Caching-Proxy-Server mit effektiver Vergrößerung des Cache. Weitere Informationen finden Sie im Abschnitt „URI-Affinität“ auf Seite 210.

- **Cluster- oder sitespezifische Proportionen**

Dieses Merkmal gilt für alle Komponenten von Network Dispatcher.

In früheren Releases wurde die proportionale Bedeutung, die aktiven Verbindungen, neuen Verbindungen, Port und Systemmesswerten für Entscheidungen bezüglich des Lastausgleichs beigemessen wurde, von der Verwaltungsfunktion bestimmt. Diese Proportion wurde in der Konfiguration für die Komponente auf jeden Cluster angewendet. Alle Cluster wurden unabhängig von der Site, für die der Lastausgleich durchgeführt wurde, unter Verwendung derselben Proportion gemessen.

Dank dieser Verbesserung können Sie die proportionale Bedeutung pro Cluster (oder Site) festlegen. Weitere Informationen finden Sie im Abschnitt „Proportionale Bedeutung von Statusinformationen“ auf Seite 145.

- **Serverpartitionierung**

Dieses Merkmal gilt für alle Komponenten von Network Dispatcher.

Network Dispatcher bietet jetzt die Möglichkeit, einen physischen Server in mehrere logische Server zu partitionieren. Dadurch können Sie beispielsweise bei einem bestimmten Dienst auf der Maschine nachfragen, ob eine Servlet-Steuerkomponente oder eine Datenbankanforderung schneller oder gar nicht ausgeführt wird. Durch diese Verbesserung können Sie die Last ausgehend von einer detaillierteren dienstspezifischen Auslastung verteilen. Weitere Informationen hierzu finden Sie im Abschnitt „Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)“ auf Seite 163.

- **Option 'Anforderung/Antwort (URL)' der HTTP-Advisor-Funktion**

Diese Funktion ist für die Komponenten Dispatcher und CBR verfügbar.

Mit dieser Erweiterung der HTTP-Advisor-Funktion können Sie den Status einzelner Dienste auf einem Server bewerten. Sie können für jeden logischen Server am HTTP-Port eine eindeutige HTTP-URL-Zeichenfolge festlegen, die speziell für den Dienst gilt, den Sie vom Server abfragen möchten. Weitere Informationen hierzu finden Sie im Abschnitt „Option 'Anforderung/Antwort (URL)' der HTTP-Advisor-Funktion“ auf Seite 165.

- **Cluster- oder sitespezifische Advisor-Funktionen**

Diese Funktionen sind für alle Komponenten von Network Dispatcher verfügbar.

Mit Network Dispatcher können Sie verschiedene Advisor-Funktionen starten, die über einen Port ausgeführt werden, jedoch für unterschiedliche Cluster (Sites) konfiguriert wurden. Sie können beispielsweise eine HTTP-Advisor-Funktion am Port 80 für einen Cluster (eine Site) und eine angepasste Advisor-Funktion am Port 80 für einen anderen Cluster (eine andere Site) verwenden. Weitere Informationen hierzu finden Sie im Abschnitt „Advisor-Funktion starten und stoppen“ auf Seite 150.

- **DoS-Erkennung (Denial of Service)**

Dieses Merkmal gilt für die Dispatcher-Komponente.

Dank dieser Erweiterung kann der Dispatcher potenzielle DoS-Attacks (Denial of Service) erkennen und Administratoren per Alert darauf aufmerksam machen. Zu diesem Zweck analysiert der Dispatcher eingehende Anforderungen auf eine verdächtig hohe Anzahl halboffener Verbindungen, die ein allgemeines Kennzeichen einfacher DoS-Attacks sind.

Weitere Informationen hierzu finden Sie im Abschnitt „Erkennung von DoS-Attacks“ auf Seite 211.

- **Erweiterte Benutzer-Exits**

Dieses Merkmal gilt für alle Komponenten mit Ausnahme von Consultant für Cisco CSS Switches und Site Selector.

Network Dispatcher stellt zusätzliche Benutzer-Exits bereit, die Scripts aktivieren, die von Ihnen angepasst werden können. Sie können Scripts für die Ausführung automatisierter Aktionen erstellen. Eine solche Aktion wäre beispielsweise das Protokollieren der Änderung einer hohen Verfügbarkeit oder das Informieren eines Administrators über nicht aktive Server per Alert. Network Dispatcher stellt die folgenden neuen Beispiel-Script-Dateien bereit:

- serverDown, serverUp, managerAlert und managerClear — weitere Informationen hierzu finden Sie im Abschnitt „Scripts zum Generieren eines Alerts oder Protokollieren eines Serverausfalls verwenden“ auf Seite 149.
- highavailChange — weitere Informationen hierzu finden Sie im Abschnitt „Scripts verwenden“ auf Seite 182.
- halfOpenAlert — es wurde eine mögliche DoS-Attacke (Denial of Service) festgestellt (weitere Informationen hierzu finden Sie im Abschnitt „Erkennung von DoS-Attacks“ auf Seite 211).
- halfOpenAlertDone — die DoS-Attacke ist beendet (weitere Informationen hierzu finden Sie im Abschnitt „Erkennung von DoS-Attacks“ auf Seite 211).

- **DB2-Advisor-Funktion**

Diese Funktion ist für die Dispatcher-Komponente verfügbar.

Der Dispatcher stellt eine DB2-Advisor-Funktion bereit, die mit den DB2-Servern kommuniziert. Weitere Informationen zur DB2-Advisor-Funktion finden Sie im Abschnitt „Liste der Advisor-Funktionen“ auf Seite 153.

Komponenten von Network Dispatcher

Die fünf Komponenten von Network Dispatcher sind Dispatcher, Content Based Routing (CBR), Mailbox Locator, Site Selector und Consultant für Cisco CSS Switches. Network Dispatcher bietet Ihnen die Möglichkeit, die Komponenten flexibel entsprechend der Konfiguration Ihrer Site einzeln oder zusammen zu verwenden. Dieser Abschnitt gibt einen Überblick über die Komponenten.

Dispatcher im Überblick

Die Dispatcher-Komponente verteilt den Datenverkehr mit einer Kombination von Lastausgleichs- und Verwaltungssoftware auf Ihre Server. Der Dispatcher kann auch einen ausgefallenen Server erkennen und den Datenverkehr entsprechend umleiten. Dispatcher unterstützt HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3, Telnet sowie alle anderen TCP-basierten bzw. kontextlosen UDP-basierten Anwendungen.

Alle an die Dispatcher-Maschine gesendeten Client-Anforderungen werden auf der Basis dynamisch festgelegter Wertigkeiten an den "besten" Server übertragen. Für diese Wertigkeiten können Sie Standardwerte benutzen oder die Werte während des Konfigurationsprozesses ändern.

Dispatcher kann drei Weiterleitungsmethoden anwenden (die für den Port angegeben werden):

- MAC-Weiterleitungsmethode (**mac**). Bei dieser Methode der Weiterleitung führt der Dispatcher einen Lastausgleich für die beim Server eingehenden Anforderungen durch. Der Server gibt die Antwort direkt, d. h. ohne Eingreifen des Dispatchers, an den Client zurück.
- NAT/NAPT-Weiterleitungsmethode (**nat**). Bei Verwendung der Dispatcher-Methode NAT (Konvertierung von Netzadressen) bzw. NAPT (Port-Umsetzung für Netzadressen) entfällt die Einschränkung, dass die Back-End-Server sich in einem lokal angeschlossenen Netz befinden müssen. Falls Sie Server an fernen Standorten haben, sollten Sie anstelle einer GRE/WAND-Kapselungstechnik die NAT-Technik anwenden. Bei der NAT-Weiterleitungsmethode verteilt der Dispatcher die eingehenden Anforderungen auf den Server. Der Server gibt die Antwort an den Dispatcher zurück. Die Dispatcher-Maschine gibt die Antwort dann an den Client zurück.
- Inhaltsabhängige Weiterleitungsmethode (**cbr**). Ohne Caching Proxy können Sie mit der Dispatcher-Komponente ein Content Based Routing für HTTP (unter Verwendung des Regeltyps "content") und für HTTPS (unter Verwendung der Affinität von SSL-Sitzungs-IDs) durchführen. Für HTTP- und HTTPS-Datenverkehr ist das Content Based Routing der Dispatcher-Komponente *schneller* als das der CBR-Komponente.

Bei der Weiterleitungsmethode cbr verteilt der Dispatcher für die eingehenden Anforderungen auf den Server. Der Server gibt die Antwort an den Dispatcher zurück. Die Dispatcher-Maschine gibt die Antwort dann an den Client zurück.

Die Dispatcher-Komponente ist der Schlüssel für eine stabile, effiziente Verwaltung eines großen skalierbaren Servernetzes. Mit Network Dispatcher können Sie viele einzelne Server so verbinden, dass sie ein virtueller Server zu sein scheinen. Besucher halten Ihre Site daher für eine einzelne IP-Adresse. Der Dispatcher arbeitet unabhängig von einem Domännennamensserver. Alle Anforderungen werden an die IP-Adresse der Dispatcher-Maschine gesendet.

Der Dispatcher bringt klare Vorteile bei der Lastverteilung auf geclusterte Server und ermöglicht daher eine stabile und effiziente Verwaltung Ihrer Site.

Lokale Server mit dem Dispatcher verwalten

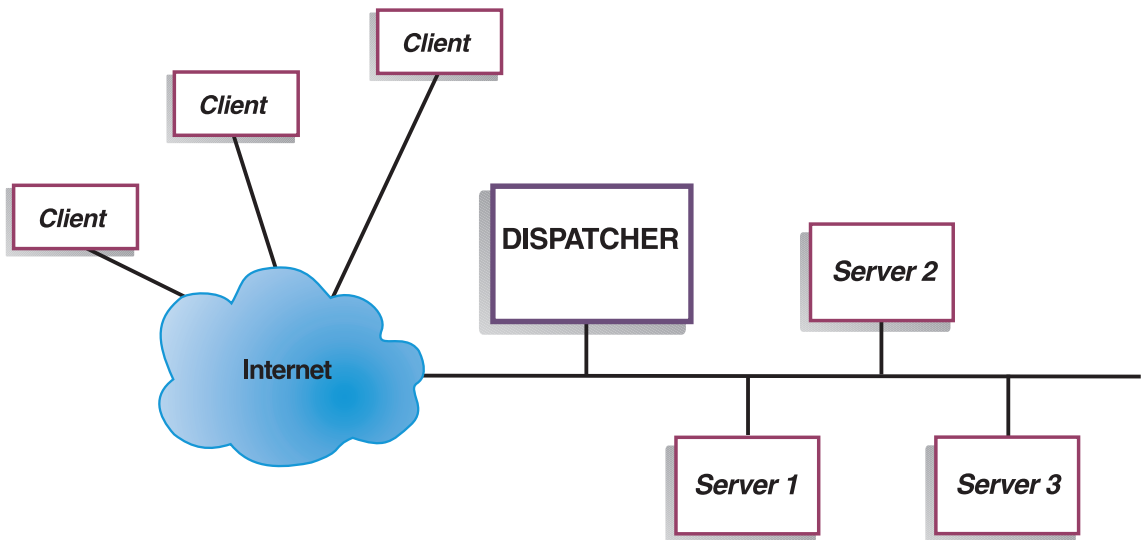


Abbildung 6. Beispiel für die physische Darstellung einer Site mit Network Dispatcher für die Verwaltung lokaler Server

In Abb. 6 wird die physische Darstellung der Site mit einer Ethernet-Netzkonfiguration gezeigt. Die Dispatcher-Maschine kann installiert werden, ohne dass physische Änderungen am Netz erforderlich sind. Nachdem der Dispatcher eine Client-Anforderung an den optimalen Server übertragen hat, wird die Antwort mit der MAC-Weiterleitungsmethode ohne Eingriff des Dispatchers direkt vom Server an den Client gesendet.

Server mit Metric Server verwalten

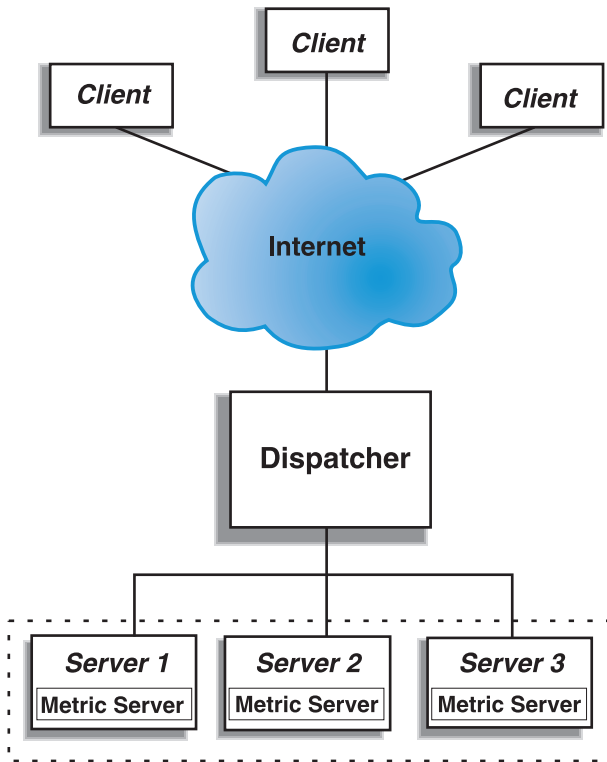


Abbildung 7. Beispielsite mit Dispatcher und Metric Server für die Serververwaltung

In Abb. 7 wird eine Site gezeigt, in der sich alle Server in einem lokalen Netz befinden. Die Dispatcher-Komponente leitet Anforderungen weiter und Metric Server stellt der Dispatcher-Maschine Informationen zur Systembelastung zur Verfügung.

In diesem Beispiel ist der Metric-Server-Dämon auf allen Servern installiert. Sie können Metric Server zusammen mit der Dispatcher-Komponente oder einer beliebigen anderen Komponente von Network Dispatcher verwenden.

Lokale und ferne Server mit Dispatcher verwalten

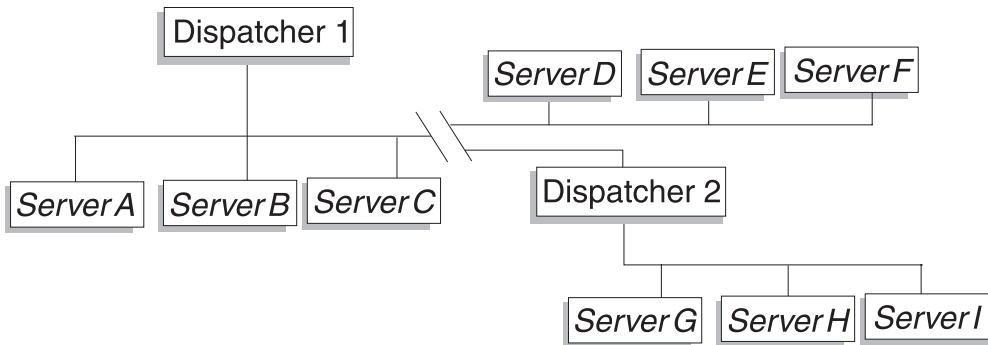


Abbildung 8. Beispiel für eine Site mit Dispatcher für die Verwaltung lokaler und ferner Server

Die Weitverkehrsunterstützung von Dispatcher ermöglicht Ihnen die Verwendung lokaler und ferner Server (d. h. Server in anderen Teilnetzen). Abb. 8 zeigt eine Konfiguration, bei der ein lokaler Dispatcher (Dispatcher 1) als Eingangspunkt für alle Anforderungen dient. Er verteilt diese Anforderungen auf seine lokalen Server (ServerA, ServerB, ServerC) und den fernen Dispatcher (Dispatcher 2), der die Last auf seine lokalen Server (ServerG, ServerH, ServerI) verteilt.

Wenn Sie die NAT-Weiterleitungsmethode oder die GRE-Unterstützung von Dispatcher nutzen, können Sie eine Weitverkehrsunterstützung auch ohne Verwendung eines Dispatchers am fernen Standort (wo sich ServerD, ServerE und ServerF befinden) erreichen. Weitere Informationen hierzu finden Sie in den Abschnitten „NAT/NAPT-Weiterleitungsmethode (nat) des Dispatchers“ auf Seite 55 und „Unterstützung für GRE (Generic Routing Encapsulation)“ auf Seite 175.

Content Based Routing (CBR) im Überblick

CBR arbeitet mit Caching Proxy zusammen, um Client-Anforderungen an angegebene HTTP- oder HTTPS-Server (SSL) weiterzuleiten. Diese Komponente ermöglicht die Bearbeitung von Caching-Angaben für ein schnelleres Abrufen von Webdokumenten mit geringen Anforderungen an die Netzbandbreite. CBR überprüft zusammen mit Caching Proxy HTTP-Anforderungen anhand angegebener Regeltypen.

Bei Verwendung von CBR können Sie eine Gruppe von Servern angeben, die eine Anforderung ausgehend von der Übereinstimmung eines regulären Ausdrucks mit dem Inhalt der Anforderung bearbeiten. Da CBR die Angabe mehrerer Server für jede Art von Anforderung zulässt, können die Anforderungen so verteilt werden, dass eine optimale Client-Antwortzeit erreicht wird. CBR erkennt auch, wenn ein Server in einer Gruppe ausgefallen ist. In diesem Fall werden keine weiteren Anforderungen an diesen Server weitergeleitet. Der von der CBR-Komponente verwendete Lastausgleichsalgorithmus ist mit dem bewährten Algorithmus identisch, der von der Dispatcher-Komponente verwendet wird.

Wenn Caching Proxy eine Anfrage empfängt, wird diese mit den Regeln, die für die CBR-Komponente definiert wurden, abgeglichen. Wird eine Übereinstimmung gefunden, wird einer der Server, die dieser Regel zugeordnet sind, für die Bearbeitung der Anforderung ausgewählt. Caching Proxy führt dann die normale Verarbeitung aus, um die Anfrage an den ausgewählten Server weiterzuleiten.

CBR stellt mit Ausnahme der hohen Verfügbarkeit, des Subagenten, der Weitverkehrsunterstützung und einiger anderer Konfigurationsbefehle dieselben Funktionen wie der Dispatcher bereit.

CBR kann erst mit dem Lastausgleich für Client-Anfragen beginnen, wenn Caching Proxy aktiv ist.

Lokale Server mit CBR verwalten

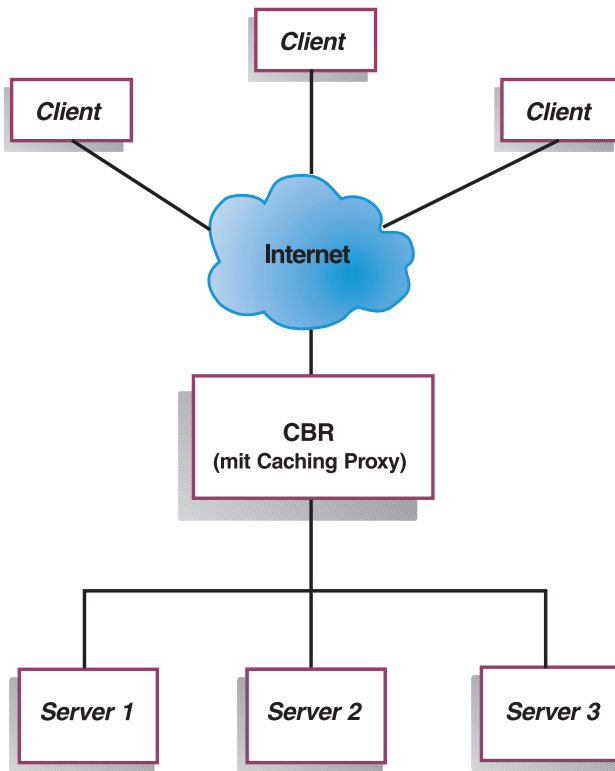


Abbildung 9. Beispielsite mit CBR für die Verwaltung lokaler Server

Abb. 9 zeigt die logische Darstellung einer Site, bei der ein Teil der Inhalte von lokalen Server mit CBR weitergeleitet wird. Die CBR-Komponente leitet mit Caching Proxy Client-Anfragen (HTTP oder HTTPS) ausgehend vom Inhalt des URL an die Server weiter.

Mailbox Locator im Überblick

Mailbox Locator kann ein Anlaufpunkt für viele IMAP- oder POP3-Server sein. Jeder Server kann einen Teil der Benutzer-Mailboxes vom Anlaufpunkt bedienen lassen. Für IMAP- und POP3-Datenverkehr ist Mailbox Locator ein Proxy, der ausgehend von der vom Client bereitgestellten Benutzer-ID mit Kennwort einen geeigneten Server auswählt. Mailbox Locator bietet keine Unterstützung für den regelgestützten Lastausgleich.

Anmerkung: Die Komponente Mailbox Locator war früher Teil der CBR-Komponente und wurde für den Lastausgleich bei IMAP- und POP3-Postservern verwendet. Durch die Untergliederung von CBR in zwei Komponenten *entfällt* die Einschränkung, dass "CBR für IMAP/POP3" (Mailbox Locator) und "CBR für HTTP/HTTPS" (CBR mit Caching Proxy) nicht auf einer Maschine ausgeführt werden können.

Lokale Server mit Mailbox Locator verwalten

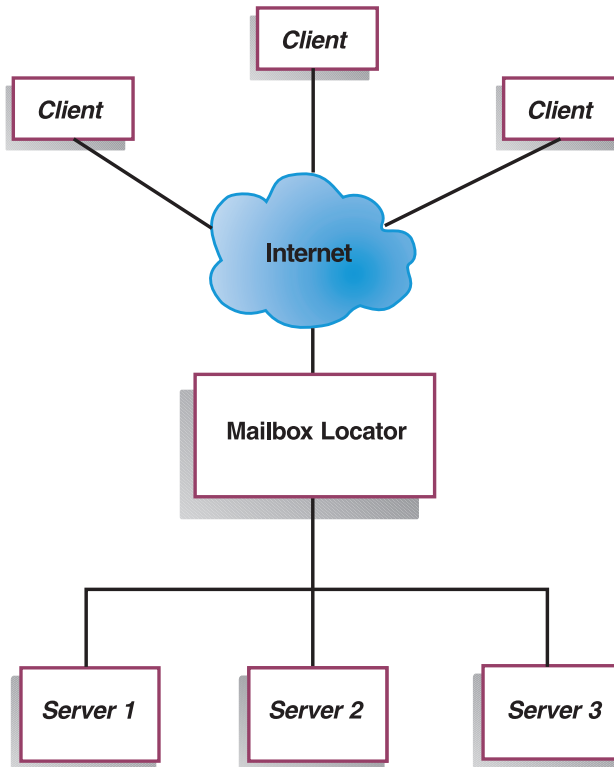


Abbildung 10. Beispielsite mit Mailbox Locator für die Verwaltung lokaler Server

Abb. 10 zeigt die logische Darstellung einer Site, bei der Mailbox Locator Client-Anfragen (Protokoll IMAP oder POP3) ausgehend von Benutzer-ID und Kennwort an einen geeigneten Server weiterleitet.

Site Selector im Überblick

Site Selector fungiert als Namensserver und führt zusammen mit anderen Namensservern in einem Domänennamenssystem auf der Grundlage abgerufener Messungen und Wertigkeiten einen Lastausgleich für Servergruppen durch. Sie können eine Sitekonfiguration erstellen, bei der die Last innerhalb einer Servergruppe auf der Grundlage des für eine Client-Anfrage verwendeten Domänennamens verteilt wird.

Ein Client fordert die Auflösung eines Domänennamens bei einem Namensserver innerhalb seines Netzes an. Der Namensserver leitet die Anforderung an die Site-Selector-Maschine weiter. Site Selector löst den Domänennamen dann in die IP-Adresse eines der Server auf, die für den Sitenamen konfiguriert wurden. Anschließend gibt Site Selector die IP-Adresse des ausgewählten Servers an den Namensserver zurück. Der Namensserver liefert die IP-Adresse an den Client.

Metric Server ist eine Systemüberwachungskomponente von Network Dispatcher, die auf jedem am Lastausgleich beteiligten Server innerhalb der Konfiguration installiert sein muss. Mit Metric Server kann Site Selector das Aktivitätsniveau eines Servers überwachen, den Server mit der geringsten Auslastung ermitteln und einen ausgefallenen Server erkennen. Die Auslastung eines Servers ist ein Maß für das Arbeitsvolumen des Servers. Durch Anpassung der Script-Dateien für Systemmesswerte können Sie steuern, auf welche Art die Last gemessen wird. Sie können Site Selector an die Anforderungen der eigenen Umgebung anpassen und dabei Faktoren wie die Zugriffshäufigkeit, die Gesamtzahl der Benutzer und die Zugriffsarten (beispielsweise kurze Abfragen, lange Abfragen, Transaktionen mit hoher CPU-Belastung) berücksichtigen.

Lokale und ferne Server mit Site Selector und Metric Server verwalten

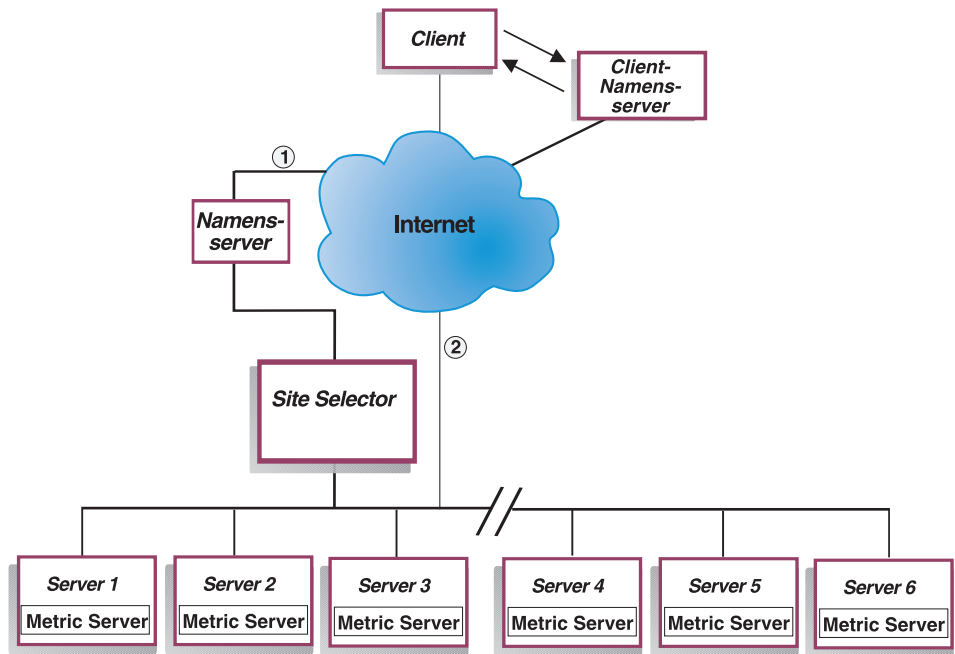


Abbildung 11. Beispielsite mit Site Selector und Metric Server für die Verwaltung lokaler und ferner Server

Abb. 11 stellt eine Site dar, bei der die Komponente Site Selector Anfragen beantwortet. Server1, Server2 und Server3 sind lokale Server. Server4, Server5 und Server6 sind ferne Server. Ein Client fordert die Auflösung eines Domännennamens bei einem Client-Namensserver an. Der Client-Namensserver leitet die Anfrage über den DNS an die Site-Selector-Maschine weiter (Pfad 1). Site Selector löst den Domännennamen dann in die IP-Adresse eines der Server auf. Anschließend gibt Site Selector die IP-Adresse des ausgewählten Servers an den Client-Namensserver zurück. Der Namensserver liefert die IP-Adresse an den Client.

Sobald der Client die IP-Adresse des Servers empfangen hat, leitet er alle folgenden Anfragen direkt an den ausgewählten Server weiter (Pfad 2).

Anmerkung: In diesem Beispiel liefert Metric Server Informationen zur Systembelastung an die Site-Selector-Maschine. Der Agent Metric Server ist auf jedem Back-End-Server installiert. Sie sollten Site Selector zusammen mit Metric Server verwenden, da Site Selector sonst nur eine RoundRobin-Auswahlmethode für den Lastausgleich anwenden kann.

Consultant für Cisco CSS Switches im Überblick

Consultant für Cisco CSS Switches ist eine ergänzende Lösung für die CSS 11000 Series Switches von Cisco. Die kombinierte Lösung verbindet die zuverlässige Paket- und Inhaltsweiterleitung der CSS 11000 Series mit den ausgeklügelten Erkennungsalgorithmen von Network Dispatcher, um die Verfügbarkeit von Back-End-Servern, Anwendungen und Datenbanken festzustellen und Informationen zu laden. Cisco Consultant verwendet den Manager, die standardmäßigen und benutzerdefinierten Advisor-Funktionen von Network Dispatcher sowie Metric Server, um die Messwerte, den Zustand und die Belastung von Back-End-Servern, Anwendungen und Datenbanken zu ermitteln. Aus diesen Informationen generiert Cisco Consultant Messwerte für die Servergewichtung, die dann zur Erreichung einer optimalen Serverauswahl sowie von Lastoptimierung und Fehlertoleranz an den Cisco CSS Switch gesendet werden.

Der Cisco CSS Switch trifft seine Entscheidungen bezüglich des Lastausgleichs auf der Grundlage benutzerdefinierter Kriterien.

Cisco Consultant protokolliert zahlreiche Kriterien. Dazu gehören unter anderem:

- aktive und neue Verbindungen
- Verfügbarkeit von Anwendungen und Datenbanken (was durch standardmäßige und angepasste Advisor-Funktionen sowie durch serverresidente und für bestimmte Anwendungen maßgeschneiderte Agenten erleichtert wird)
- CPU-Auslastung
- Speicherauslastung
- vom Benutzer anpassbare Servermesswerte.

Wenn ein Cisco CSS Switch ohne Cisco Consultant den Zustand eines Inhalte bereitstellenden Servers ermittelt, greift er dabei auf die Antwortzeiten für Inhaltsanfragen und andere Netzmesswerte zurück. Wird Cisco Consultant verwendet, gehen diese Aktivitäten vom Cisco CSS Switch auf Cisco Consultant über. Cisco Consultant beeinflusst die Fähigkeit des Servers, Inhalte bereitzustellen, und aktiviert einen Server als geeigneten Server, wenn dieser verfügbar ist, bzw. stellt ihn als geeigneten Server zurück, wenn dieser nicht mehr verfügbar ist.

Cisco Consultant:

- empfängt über eine veröffentlichte SNMP-Schnittstelle Verbindungsdaten vom Cisco CSS Switch
- analysiert die Verbindungsdaten anhand der Vorgaben von Advisor-Funktionen
- analysiert den relativen Zustand von Servern anhand der Informationen von Metric Server
- generiert Wertigkeiten für jeden Server der Konfiguration.

Wertigkeiten gelten für alle Server an einem Port. An einem bestimmten Port werden die Anfragen ausgehend von einem Vergleich der Wertigkeiten der einzelnen Server verteilt. Wenn ein Server beispielsweise die Wertigkeit 10 und ein anderer die Wertigkeit 5 hat, sollte der Server mit der Wertigkeit 10 doppelt so viele Anfragen erhalten wie der Server mit der Wertigkeit 5. Diese Wertigkeiten werden dem Cisco CSS Switch mit SNMP zur Verfügung gestellt. Wird ein Server mit einer höheren Wertigkeit eingestuft, überträgt der Cisco CSS Switch mehr Anfragen an diesen Server.

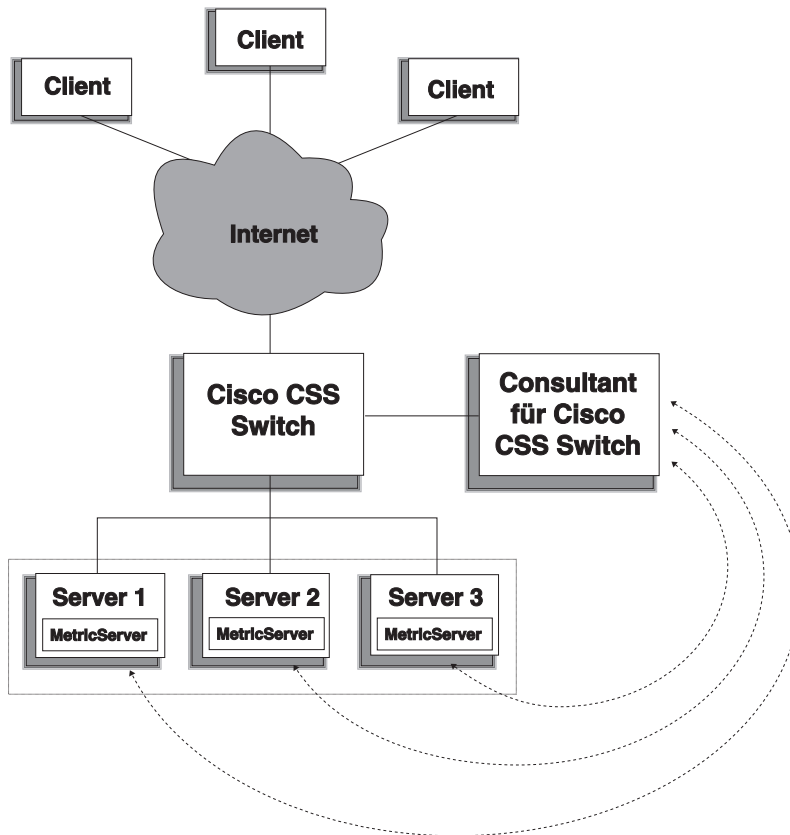


Abbildung 12. Beispielsite mit Cisco Consultant und Metric Server für die Verwaltung lokaler Server

Cisco Consultant ist in Verbindung mit dem Cisco CSS Switch eine Lösung, die das "Beste aus zwei Welten" auf sich vereint, super schnelles Content-Switching und ausgeklügelte Anwendungserkennung, Fehlertoleranz sowie optimale Serverauslastung. Cisco Consultant ist Bestandteil einer ergänzenden Lösung für den Cisco CSS Switch und IBM WebSphere Edge Server.

In „Kapitel 2. Network Dispatcher installieren“ auf Seite 11 finden Sie eine Liste der Voraussetzungen für Cisco Consultant.

Hohe Verfügbarkeit

Dispatcher

Die Dispatcher-Komponente stellt eine integrierte Funktion für hohe Verfügbarkeit bereit. Für diese Funktion ist eine zweite Dispatcher-Maschine erforderlich, die die primäre Maschine überwacht und den Lastausgleich übernehmen kann, wenn die primäre Maschine ausfällt. Die Dispatcher-Komponente gewährleistet außerdem eine gegenseitige hohe Verfügbarkeit, so dass sowohl die primäre als auch die sekundäre Maschine die jeweils andere Maschine als Ausweichmaschine nutzen kann. Lesen Sie hierzu die Informationen im Abschnitt „Hohe Verfügbarkeit konfigurieren“ auf Seite 178.

CBR, Mailbox Locator, Site Selector

Durch eine Client-/Serverkonfiguration mit einer Dispatcher-Maschine, bei der der Datenverkehr auf zwei oder mehr Servermaschinen mit CBR, Mailbox Locator oder Site Selector verteilt wird, können Sie für diese Komponenten von Network Dispatcher ein hohes Maß an Verfügbarkeit erreichen.

Kapitel 4. Planung für Dispatcher

In diesem Kapitel wird beschrieben, was die für die Planung des Netzes zuständige Person vor der Installation und Konfiguration der Dispatcher-Komponente berücksichtigen muss.

- Informationen zum Konfigurieren der Lastausgleichsparameter von Dispatcher finden Sie in „Kapitel 5. Dispatcher konfigurieren“ auf Seite 61.
- Informationen zum Konfigurieren von Network Dispatcher für erweiterte Funktionen finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Dieses Kapitel enthält die folgenden Abschnitte:

- „Hardware- und Softwarevoraussetzungen“
- „Überlegungen bei der Planung“ auf Seite 50
- „Hohe Verfügbarkeit“ auf Seite 52
- „MAC-Weiterleitungsmethode (mac) des Dispatchers“ auf Seite 54
- „NAT/NAPT-Weiterleitungsmethode (nat) des Dispatchers“ auf Seite 55
- „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)“ auf Seite 57

Hardware- und Softwarevoraussetzungen

Plattformvoraussetzungen:

- für AIX finden Sie im Abschnitt „Voraussetzungen für AIX“ auf Seite 12.
- für Linux finden Sie im Abschnitt „Voraussetzungen für Red Hat Linux oder SuSE Linux“ auf Seite 17.
- für Solaris finden Sie im Abschnitt „Voraussetzungen für Solaris“ auf Seite 21.
- für Windows 2000 finden Sie im Abschnitt „Voraussetzungen für Windows 2000“ auf Seite 23.

Überlegungen bei der Planung

Der Dispatcher stellt die folgenden Funktionen bereit:

- Der Befehl **ndserver** bearbeitet Anfragen von der Befehlszeile an den Executor, den Manager und die Advisor-Funktionen.
- Der **Executor** unterstützt die Verteilung von TCP- und UDP-Verbindungen auf Port-Basis. Der Executor kann Verbindungen ausgehend vom Typ der empfangenen Anforderung (HTTP, FTP, SSL usw.) an Server weiterleiten. Er wird immer ausgeführt, wenn die Dispatcher-Komponente für den Lastausgleich verwendet wird.
- Der **Manager** definiert Wertigkeiten, die vom Executor verwendet werden und auf folgenden Kriterien basieren:
 - interne Zähler des Executors
 - von den Advisor-Funktionen bereitgestellte Rückmeldungen von den Servern
 - Rückmeldungen von einem Systemüberwachungsprogramm wie Metric Server oder WLM.

Die Benutzung des Managers ist optional. Ohne den Manager wird der Lastausgleich nach einer gewichteten RoundRobin-Zeitplanung und ausgehend von den aktuellen Serverwertigkeiten durchgeführt. Es stehen keine Advisor-Funktionen zur Verfügung.

- Die **Advisor-Funktionen** richten Abfragen an die Server und analysieren die Ergebnisse nach Protokoll, bevor sie den Manager zum Festlegen der entsprechenden Wertigkeiten aufrufen. Derzeit sind Advisor-Funktionen für die folgenden Protokolle verfügbar: HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3 und Telnet.

Dispatcher bietet außerdem Advisor-Funktionen an, die keine protokoll-spezifischen Informationen austauschen. Dazu gehören unter anderem die DB2-Advisor-Funktion, die Angaben zum Status von DB2-Servern macht, und die Ping-Advisor-Funktion, die meldet, ob der Server auf ein gesendetes "ping" antwortet. Eine vollständige Liste der Advisor-Funktionen finden Sie im Abschnitt „Liste der Advisor-Funktionen“ auf Seite 153.

Sie haben auch die Möglichkeit, eigene Advisor-Funktionen zu schreiben. (Lesen Sie hierzu die Informationen im Abschnitt „Kundenspezifische (anpassbare) Advisor-Funktion erstellen“ auf Seite 155.)

Die Benutzung der Advisor-Funktionen ist optional, wird jedoch empfohlen.

- Zum Konfigurieren und Verwalten des Executors, der Advisor-Funktionen und des Managers können Sie die Befehlszeile (**ndcontrol**) oder die grafische Benutzerschnittstelle (**ndadmin**) verwenden.

- Für die Konfiguration und Verwaltung der Dispatcher-Maschine steht eine **Beispielkonfigurationsdatei** bereit (siehe „Anhang F. Beispielkonfigurationsdateien“ auf Seite 393). Nach der Installation des Produkts finden Sie diese Datei im Unterverzeichnis **nd/servers/samples** des Verzeichnisses mit Network Dispatcher.
- Der **SNMP-Subagent** ermöglicht es einer SNMP-gestützten Verwaltungsanwendung, den Status des Dispatchers zu überwachen.

Die drei Schlüsselfunktionen des Dispatchers (Executor, Manager und Advisor) kommunizieren miteinander, um die eingehenden Anforderungen auf die Server zu verteilen. Neben Lastausgleichsanforderungen überwacht der Executor die Anzahl neuer, aktiver und beendeter Verbindungen. Der Executor übernimmt auch die Garbage Collection für beendete oder zurückgesetzte Verbindungen und stellt diese Informationen dem Manager zur Verfügung.

Der Manager stellt Informationen vom Executor, von den Advisor-Funktionen und von einem Systemüberwachungsprogramm wie Metric Server zusammen. Der Manager passt anhand der erhaltenen Informationen die Wertigkeit der Servermaschinen an den einzelnen Ports an und teilt dem Executor die neue Wertigkeit mit, die dieser dann beim Lastausgleich für neue Verbindungen verwendet.

Die Advisor-Funktionen überwachen die einzelnen Server am zugeordneten Port, um Antwortzeit und Verfügbarkeit der Server zu ermitteln, und übergeben diese Informationen an den Manager. Die Advisor-Funktionen überwachen zudem, ob ein Server aktiv oder inaktiv ist. Ohne Manager und Advisor-Funktionen wendet der Executor eine RoundRobin-Zeitplanung auf der Basis der aktuellen Serverwertigkeiten an.

Hohe Verfügbarkeit

Einfache hohe Verfügbarkeit

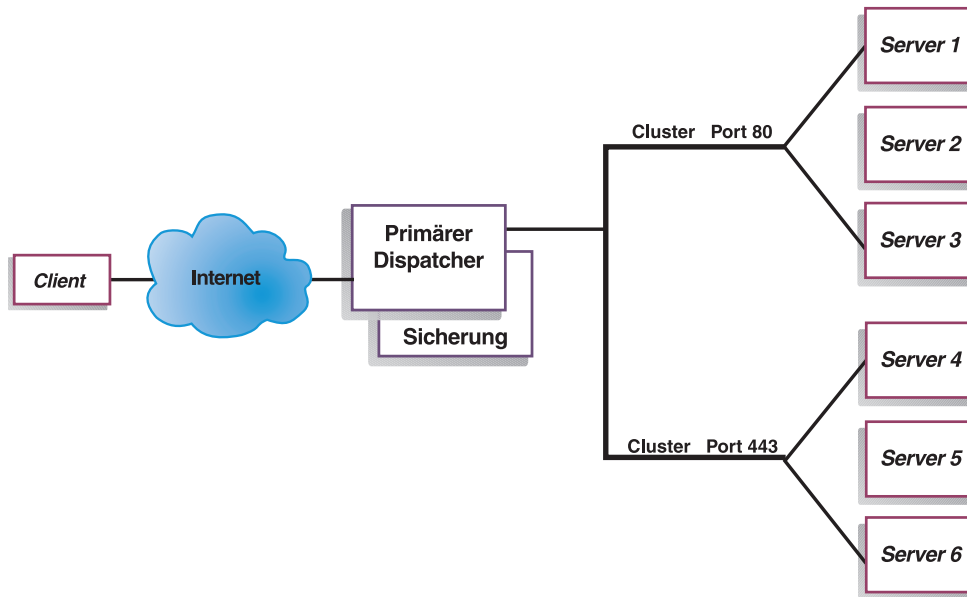


Abbildung 13. Beispiel für einen Dispatcher mit einfacher hoher Verfügbarkeit

Die Funktion für hohe Verfügbarkeit erfordert eine zweite Dispatcher-Maschine. Die erste Dispatcher-Maschine führt den Lastausgleich für den gesamten Client-Datenverkehr aus, wie dies in einer Konfiguration mit einem einzelnen Dispatcher geschehen würde. Die zweite Dispatcher-Maschine überwacht den "Zustand" der ersten Maschine und übernimmt die Task des Lastausgleichs, wenn sie erkennt, dass die erste Dispatcher-Maschine ausgefallen ist.

Jeder der beiden Maschinen wird eine bestimmte Rolle zugewiesen, entweder die der primären Maschine (*primary*) oder die der Ausweichmaschine (*backup*). Die primäre Maschine sendet ständig Verbindungsdaten an die Partnermaschine. Während die primäre Maschine *aktiv* ist (den Lastausgleich durchführt), befindet sich die Partnermaschine in *Bereitschaft*. Sie wird ständig aktualisiert und ist bereit, den Lastausgleich zu übernehmen, falls dies erforderlich ist.

Die Übertragungssitzungen zwischen den beiden Maschinen werden als *Überwachungssignale* bezeichnet. Mit Hilfe der Überwachungssignale kann jede Maschine den Zustand der anderen Maschine überwachen.

Stellt die Ausweichmaschine fest, dass die aktive Maschine ausgefallen ist, übernimmt sie deren Aufgaben und beginnt mit dem Lastausgleich. An diesem Punkt kehrt sich der *Status* der beiden Maschinen um: die Partnermaschine wird zur *aktiven Maschine* und die primäre Maschine wird zur *Maschine in Bereitschaft*.

In der Konfiguration mit hoher Verfügbarkeit müssen sich die primäre Maschine und die Partnermaschine innerhalb eines Teilnetzes befinden.

Informationen zum Konfigurieren der hohen Verfügbarkeit finden Sie im Abschnitt „Hohe Verfügbarkeit“ auf Seite 177.

Gegenseitige hohe Verfügbarkeit

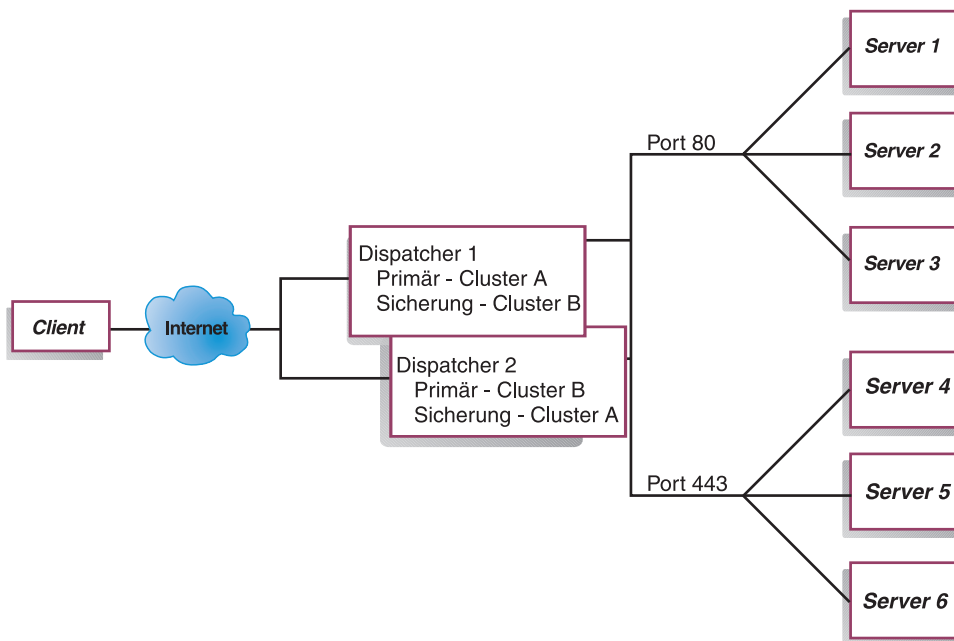


Abbildung 14. Beispiel für einen Dispatcher mit gegenseitiger hoher Verfügbarkeit

Für die gegenseitige hohe Verfügbarkeit sind zwei Dispatcher-Maschinen erforderlich. Beide Maschinen führen aktiv den Lastausgleich des Client-Datenverkehrs aus und beide Maschinen sind gleichzeitig Partnermaschinen. In einer Konfiguration mit einfacher hoher Verfügbarkeit führt nur eine Maschine den Lastausgleich durch. In einer Konfiguration mit gegenseitiger hoher Verfügbarkeit verteilen beide Maschinen einen Teil des Client-Datenverkehrs.

Bei der gegenseitigen hohen Verfügbarkeit wird jeder der Client-Datenverkehr den Dispatcher-Maschinen auf der Basis einer Cluster-Adresse zugeordnet. Jeder Cluster kann mit der nicht für Weiterleitungszwecke bestimmten Adresse (NFA, nonforwarding Address) seines primären Dispatchers konfiguriert werden. Die primäre Dispatcher-Maschine führt normalerweise den Lastausgleich für diesen Cluster durch. Fällt die Maschine aus, führt die andere Maschine den Lastausgleich für ihren eigenen Cluster und für den Cluster des ausgefallenen Dispatchers durch.

Abb. 14 auf Seite 53 zeigt eine Beispielkonfiguration mit gegenseitiger hoher Verfügbarkeit, bei der die "Cluster-Gruppe A" und die "Cluster-Gruppe B" gemeinsam benutzt werden. Jeder Dispatcher kann aktiv für seinen *primären* Cluster bestimmte Pakete weiterleiten. Fällt einer der Dispatcher aus, so dass er nicht länger aktiv für seinen primären Cluster bestimmte Pakete weiterleiten kann, übernimmt der andere Dispatcher die Weiterleitung der Pakete zu seinem *Ausweich*-Cluster.

Anmerkung: Auf beiden Maschinen müssen die gemeinsam benutzten Cluster-Gruppen identisch konfiguriert werden.

Informationen zum Konfigurieren der hohen Verfügbarkeit und der gegenseitigen hohen Verfügbarkeit finden Sie im Abschnitt „Hohe Verfügbarkeit“ auf Seite 177.

MAC-Weiterleitungsmethode (mac) des Dispatchers

Wenn der Dispatcher seine Standardweiterleitungsmethode, die MAC-Weiterleitung, anwendet, werden die eingehenden Anforderungen an den ausgewählten Server weitergeleitet. Der Server gibt die Antwort *direkt*, d. h. ohne Eingreifen des Dispatchers, an den Client zurück. Bei dieser Methode der Weiterleitung achtet der Dispatcher nur auf den beim Server eingehenden Datenfluss vom Client, nicht aber auf den abgehenden Datenfluss vom Server zum Client. Dies führt zu einer erheblichen Reduzierung der Auswirkungen auf die Anwendung und zu einem verbesserten Durchsatz im Netz.

Sie können die Weiterleitungsmethode auswählen, wenn Sie mit dem Befehl **ndcontrol port add Cluster:Port method Wert** einen Port hinzufügen. Der Wert für die Standardweiterleitungsmethode ist **mac**. Die Parameter für die Methode können Sie nur beim Hinzufügen des Ports angeben. Ist der Port hinzugefügt, können Sie die Einstellung für die Weiterleitungsmethode nicht mehr ändern. Weitere Informationen hierzu finden Sie im Abschnitt „ndcontrol port — Ports konfigurieren“ auf Seite 305.

NAT/NAPT-Weiterleitungsmethode (nat) des Dispatchers

Bei Verwendung der Dispatcher-Methode NAT (Konvertierung von Netz-adressen) bzw. NAPT (Port-Umsetzung für Netzadressen) entfällt die Einschränkung, dass sich die am Lastausgleich beteiligten Server in einem lokal angeschlossenen Netz befinden müssen. Falls Sie Server an fernen Standorten haben, sollten Sie anstelle einer GRE/WAND-Kapselungstechnik die NAT-Weiterleitungsmethode anwenden. Mit NAPT können Sie außerdem auf mehrere Serverdämonen zugreifen, die sich auf den einzelnen am Lastausgleich beteiligten Servermaschinen befinden und jeweils an einem eindeutigen Port empfangsbereit sind.

Einen Server mit mehreren Dämonen können Sie auf die beiden folgenden Arten konfigurieren:

- Mit NAT können Sie mehrere Serverdämonen für die Beantwortung von Anfragen, die an verschiedene IP-Adressen gerichtet sind, konfigurieren. Dieses Konfiguration wird auch als Bindung eines Serverdämons an eine IP-Adresse bezeichnet.
- Mit NAPT können Sie mehrere Serverdämonen (die auf einem physischen Server aktiv sind) so konfigurieren, dass sie an unterschiedlichen Port-Nummern empfangsbereit sind.

Diese Anwendung funktioniert gut mit höheren Anwendungsprotokollen wie HTTP, SSL, IMAP, POP3, NNTP, SMTP, Telnet usw.

Einschränkungen:

- Die NAT/NAPT-Implementierung durch den Dispatcher ist eine *einfache* Implementierung dieser Funktion. Sie analysiert lediglich den Inhalt der Header von TCP/IP-Paketen und kann nur auf diese angewendet werden. Der Inhalt des Datenabschnitts der Pakete kann nicht analysiert werden. Der Dispatcher kann NAT/NAPT nicht für Anwendungsprotokolle wie FTP verwenden, die die Adressen oder Port-Nummern in den Datenabschnitt von Nachrichten einbetten. Dies ist eine allgemein bekannte Einschränkung für die Header-bezogene NAT/NAPT.
- Die NAT/NAPT-Funktion von Dispatcher kann nicht zusammen mit Platzhalter-Clustern oder -Ports verwendet werden.

Sie können NAT/NAPT wie folgt implementieren:

- Geben Sie den Befehl **ndcontrol executor set** mit dem Parameter **clientgateway** an. Der Parameter **clientgateway** ist eine IP-Adresse, die als Router-Adresse verwendet wird, über die Network Dispatcher den Antwortdatenverkehr an die Clients weiterleitet. Sie können NAT/NAPT erst verwenden, wenn dieser Wert auf eine IP-Adresse ungleich null gesetzt ist. Weitere Informationen hierzu finden Sie im Abschnitt „ndcontrol executor — Executor steuern“ auf Seite 280.

- Fügen Sie mit dem Befehl **ndcontrol port add Cluster:Port method Wert** einen Port hinzu. Der Wert für die Weiterleitungsmethode sollte auf **nat** gesetzt werden. Die Parameter für die Methode können Sie nur beim Hinzufügen des Ports angeben. Ist der Port hinzugefügt, können Sie die Einstellung für die Weiterleitungsmethode nicht mehr ändern. Weitere Informationen hierzu finden Sie im Abschnitt „ndcontrol port — Ports konfigurieren“ auf Seite 305.

Anmerkung: Wenn Sie die Client-Gateway-Adresse nicht auf einen Wert ungleich null gesetzt haben, kann als Weiterleitungsmethode nur **mac** (MAC-basierte Weiterleitung) angegeben werden.

- Fügen Sie mit den Parametern "mapport", "returnaddress" und "router" des Befehls **ndcontrol** einen Server hinzu. Beispiel:

ndcontrol server add Cluster:Port:Server mapport Wert returnaddress Rückkehradresse router Router-Adresse

– **mapport**

Dieser Parameter ordnet die (für den Dispatcher bestimmte) Nummer des Ziel-Ports für die Client-Anforderung der Nummer des Server-Ports zu, an dem der Dispatcher die Client-Anforderungen verteilt. Mit "mapport" kann Network Dispatcher die Anforderung eines Clients an einem Port empfangen und an einen anderen Port der Servermaschine übertragen. Mit "mapport" können Sie den Lastausgleich für die Anforderungen eines Clients auf einer Servermaschine mit mehreren Serverdämonen durchführen. Der Standardwert für "mapport" ist die Nummer des Ziel-Ports für die Client-Anforderung.

– **returnaddress**

Die Rückkehradresse ist eine eindeutige Adresse oder ein Host-Name, die bzw. den Sie auf der Dispatcher-Maschine konfigurieren. Der Dispatcher verwendet die Rückkehradresse beim Lastausgleich für die Client-Anforderung auf dem Server als Quellenadresse. Auf diese Weise wird sichergestellt, dass der Server das Paket an die Dispatcher-Maschine zurückgibt und es nicht direkt an den Client sendet. (Der Dispatcher leitet das IP-Paket dann an den Client weiter.) Sie müssen den Wert für die Rückkehradresse beim Hinzufügen des Servers angeben. Die Rückkehradresse kann nur geändert werden, wenn Sie den Server entfernen und dann erneut hinzufügen. Die Rückkehradresse darf nicht mit dem Wert für Cluster, Server oder NFA übereinstimmen.

– **router**

Die Adresse des Routers zum fernen Server.

Weitere Informationen zum Befehl **ndcontrol server** mit den Parametern "mapport", "returnaddress" und "router" finden Sie im Abschnitt „ndcontrol server — Server konfigurieren“ auf Seite 320.

Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)

In früheren Releases von Network Dispatcher war das Content Based Routing nur bei Verwendung der CBR-Komponente zusammen mit Caching Proxy verfügbar. Jetzt können Sie mit der Dispatcher-Komponente das Content Based Routing für HTTP (unter Verwendung des Regeltyps "content") und für HTTPS (unter Verwendung der Affinität von SSL-Sitzungs-IDs) ohne Caching Proxy ausführen. Für HTTP- und HTTPS-Datenverkehr ist das Content Based Routing der Dispatcher-Komponente schneller als das der CBR-Komponente.

Für HTTP: Die Serverauswahl für die inhaltsabhängige Weiterleitung basiert auf dem Inhalt eines URL oder eines HTTP-Headers. Sie wird mit dem Regeltyp "content" konfiguriert. Wenn Sie die content-Regel konfigurieren, geben Sie für die Regel den Suchbegriff (das Muster) und eine Gruppe von Servern an. Beim Verarbeiten einer neu eingehenden Anforderung vergleicht diese Regel die angegebene Zeichenfolge mit dem URL des Clients oder mit dem in der Client-Anforderung angegebenen HTTP-Header.

Findet der Dispatcher die Zeichenfolge in der Client-Anforderung, leitet er diese an einen der für die Regel definierten Server weiter. Anschließend gibt der Dispatcher die Antwortdaten vom Server an den Client zurück (Weiterleitungsmethode "cbr").

Findet der Dispatcher die Zeichenfolge nicht in der Client-Anforderung, wählt er *keinen* der für die Regel definierten Server aus.

Anmerkung: Die content-Regel wird für die Dispatcher-Komponente auf die gleiche Weise wie für die CBR-Komponente konfiguriert. Der Dispatcher kann die content-Regel für HTTP-Datenverkehr verwenden. Die CBR-Komponente kann die content-Regel für HTTP- und HTTPS-Datenverkehr (SSL) verwenden.

Für HTTPS (SSL): Bei der inhaltsabhängigen Weiterleitung von Dispatcher erfolgt der Lastausgleich ausgehend vom Feld für die SSL-Sitzungs-ID in der Client-Anforderung. Bei Verwendung von SSL enthält eine Client-Anforderung die SSL-Sitzungs-ID einer früheren Sitzung und Server speichern ihre früheren SSL-Verbindungen im Cache. Durch die Dispatcher-Funktion für Affinität der SSL-Sitzungs-ID können Client und Server eine neue Verbindung aufbauen und dafür die Sicherheitsparameter der vorherigen Verbindung zum Server verwenden. Da SSL-Sicherheitsparameter wie gemeinsam verwendete Schlüssel und Verschlüsselungsalgorithmen nicht neu ausgehandelt werden müssen, benötigen die Server weniger CPU-Zyklen und der Client erhält schneller eine Antwort. Zum Aktivieren der Affinität von SSL-Sitzungs-IDs muss **stickytime** für den Port auf einen Wert ungleich null gesetzt werden. Wenn die Haltezeit (stickytime) abgelaufen ist, wird der Client unter Umständen an einen anderen als den vorherigen Server verwiesen.

Sie können die inhaltsabhängige Weiterleitung (Weiterleitungsmethode `cbr`) wie folgt implementieren:

- Geben Sie den Befehl **ndcontrol executor set** mit dem Parameter **clientgateway** an. Der Parameter `clientgateway` ist eine IP-Adresse, die als Router-Adresse verwendet wird, über die der Dispatcher den Antwortdatenverkehr an die Clients weiterleitet. Der Standardwert für "clientgateway" ist null. Sie können eine CBR-Weiterleitungsmethode erst verwenden, wenn dieser Wert auf eine IP-Adresse ungleich null gesetzt ist. Weitere Informationen hierzu finden Sie im Abschnitt „ndcontrol executor — Executor steuern“ auf Seite 280.
- Verwenden Sie den Befehl **ndcontrol port add** mit dem Parameter **method**, um einen Port hinzuzufügen. Der Wert für die Weiterleitungsmethode sollte auf `cbr` gesetzt werden. Weitere Informationen hierzu finden Sie im Abschnitt „ndcontrol port — Ports konfigurieren“ auf Seite 305.

Anmerkung: Wenn Sie die Client-Gateway-Adresse nicht auf einen Wert ungleich null gesetzt haben, kann als Weiterleitungsmethode nur **mac** angegeben werden.

- Fügen Sie mit den Parametern "mapport", "returnaddress" und "router" einen Server hinzu.

ndcontrol server add *Cluster:Port:Server* **mapport** *Wert* **returnaddress** *Rückkehradresse* **router** *Router-Adresse*

Anmerkung: Informationen zum Konfigurieren des Servers mit den Parametern "mapport", "returnaddress" und "router" finden Sie auf Seite 56.

- **Für HTTP:** Verwenden Sie für die Konfiguration Regeln, die auf dem Inhalt der Client-Anforderung basieren (Regeltyp **content**). Beispiel:

ndcontrol rule 125.22.22.03:80:content-Regel1 **type** content **pattern** *Muster*
Muster gibt hier das für den Regeltyp "content" zu verwendende Muster an. Weitere Informationen zum Regeltyp "content" finden Sie im Abschnitt „Regeln verwenden, die auf dem Inhalt der Anforderung basieren“ auf Seite 195. Weitere Informationen zu gültigen Ausdrücken für *Muster* können Sie „Anhang C. Syntax der content-Regel“ auf Seite 331 entnehmen.

Für HTTPS (SSL): Zum Konfigurieren der Affinität von SSL-Sitzungs-IDs muss der Parameter **stickytime** für den Port auf einen Wert ungleich null gesetzt werden. Weitere Informationen zum Parameter **stickytime** des port-Befehls finden Sie im Abschnitt „ndcontrol rule — Regeln konfigurieren“ auf Seite 312.

Anmerkung: Die für eine hohe Verfügbarkeit ausgeführte Vervielfältigung von Verbindungseinträgen stellt sicher, dass die Verbindung eines Clients nicht unterbrochen wird, wenn eine Ausweich-Dispatcher-Maschine die Aufgaben der primären Maschine übernimmt. Diese Vervielfältigung wird bei der inhaltsabhängigen Weiterleitung durch den Dispatcher *nicht* unterstützt.

Kapitel 5. Dispatcher konfigurieren

Lesen Sie vor Ausführung der in diesem Kapitel beschriebenen Schritte „Kapitel 4. Planung für Dispatcher“ auf Seite 49. Dieses Kapitel erläutert das Erstellen einer Basiskonfiguration für die Dispatcher-Komponente von Network Dispatcher.

- Komplexere Konfigurationen für Network Dispatcher finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Konfigurations-Tasks im Überblick

Anmerkung: Vergewissern Sie sich vor Ausführung der Konfigurationsschritte in dieser Tabelle, dass die Dispatcher-Maschine und alle Servermaschinen mit dem Netz verbunden sind, gültige IP-Adressen haben und sich gegenseitig mit ping-Aufrufen erreichen können.

Tabelle 3. Konfigurations-Tasks für Dispatcher

Task	Beschreibung	Referenzinformationen
Dispatcher-Maschine konfigurieren	Definieren Sie Ihre Lastausgleichskonfiguration.	„Dispatcher-Maschine konfigurieren“ auf Seite 64
Am Lastausgleich beteiligte Maschinen konfigurieren.	Definieren Sie einen Aliasnamen für die Loopback-Einheit. Überprüfen Sie, ob eine zusätzliche Route vorhanden ist und löschen Sie zusätzliche Routes.	„Servermaschinen für Lastausgleich konfigurieren“ auf Seite 71

Konfigurationsmethoden

Es gibt vier grundlegende Methoden für die Konfiguration des Dispatchers:

- Befehlszeile
- Scripts
- grafische Benutzerschnittstelle (GUI)
- Konfigurationsassistent.

Befehlszeile

Dies ist die direkte Methode für die Konfiguration des Dispatchers. Die Werte der Befehlsparameter müssen in englischen Zeichen eingegeben werden. Die einzige Ausnahme hiervon bilden Host-Namen (die in den Befehlen "cluster", "server" und "highavailability" verwendet werden) und (die in Dateibefehlen verwendeten) Dateinamen.

Starten Sie den Dispatcher wie folgt von der Befehlszeile aus:

- Setzen Sie an der Eingabeaufforderung den Befehl **ndserver** ab. Unter Windows 2000 ist "ndserver" ein Dienst, der automatisch gestartet wird.

Anmerkung: Mit dem Befehl **ndserver stop** können Sie den Dienst stoppen.

- Setzen Sie anschließend die gewünschten Dispatcher-Steuerbefehle ab, um die Konfiguration einzurichten. Bei den in diesem Handbuch beschriebenen Prozeduren wird von der Verwendung der Befehlszeile ausgegangen. Der Befehl lautet **ndcontrol**. Weitere Informationen zu Befehlen finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Sie können eine Minimalversion der Parameter für den Befehl "ndcontrol" eingeben. Sie müssen nur die eindeutigen Buchstaben der Parameter eingeben. Beispiel: Wenn Sie Hilfe für den Befehl zum Speichern von Dateien aufrufen möchten, können Sie **ndcontrol he f** anstelle von **ndcontrol help file** angeben.

Wenn Sie die Befehlszeilenschnittstelle starten möchten, setzen Sie den Befehl **ndcontrol** ab, um die Eingabeaufforderung "ndcontrol" aufzurufen.

Sie können die Befehlszeilenschnittstelle verlassen, indem Sie den Befehl **exit** oder **quit** absetzen.

Scripts

Die Befehle für die Konfiguration des Dispatchers können in eine Konfigurations-Script-Datei eingegeben und zusammen ausgeführt werden. Lesen Sie hierzu die Informationen im Abschnitt „Beispielkonfigurationsdateien für Network Dispatcher“ auf Seite 393.

Anmerkung: Falls Sie den Inhalt einer Script-Datei (z. B. meinScript) schnell ausführen möchten, verwenden Sie einen der folgenden Befehle:

- Führen Sie zum Aktualisieren der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:

ndcontrol file appendload *meinScript*

- Führen Sie zum vollständigen Ersetzen der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:

```
ndcontrol file newload meinScript
```

GUI

Abb. 2 auf Seite 6 zeigt ein Beispiel für die grafische Benutzerschnittstelle (GUI).

Gehen Sie zum Starten der GUI wie folgt vor:

1. Vergewissern Sie sich, dass ndserver aktiv ist.
 - Führen Sie unter AIX, Linux oder Solaris den folgenden Befehl als Root aus:
ndserver
 - Unter Windows 2000 ist "ndserver" ein Dienst, der automatisch gestartet wird.
2. Führen Sie anschließend einen der folgenden Schritte aus:
 - Geben Sie unter AIX, Linux oder Solaris **ndadmin** ein.
 - Klicken Sie unter Windows 2000 nacheinander auf **Start, Programme, IBM WebSphere, Edge Server, IBM Network Dispatcher** und **Network Dispatcher**.

Zum Konfigurieren von Dispatcher auf der GUI müssen Sie zunächst in der Baumstruktur **Dispatcher** auswählen. Sie können den Executor und den Manager starten, sobald Sie eine Verbindung zu einem Host hergestellt haben. Sie können auch Cluster mit Ports und Servern erstellen und Advisor-Funktionen für den Manager starten.

Mit der GUI können Sie dieselben Tasks wie mit dem Befehl **ndcontrol** ausführen. Zum Definieren eines Clusters von der Befehlszeile aus müssten Sie beispielsweise den Befehl **ndcontrol cluster add Cluster** eingeben. Zum Definieren eines Clusters von der GUI aus müssen Sie mit der rechten Maustaste auf "Executor" klicken und im daraufhin angezeigten Popup-Menü mit der linken Taste auf **Cluster hinzufügen**. Geben Sie die Cluster-Adresse in das Dialogfenster ein und klicken Sie dann auf **OK**.

Bereits vorhandene Dispatcher-Konfigurationsdateien können Sie mit der im Popup-Menü **Host** angezeigten Option **Neue Konfiguration laden** (zum vollständigen Ersetzen der derzeitigen Konfiguration) oder **An aktuelle Konfiguration anfügen** (zum Aktualisieren der derzeitigen Konfiguration) laden. Sie sollten Ihre Dispatcher-Konfiguration von Zeit zu Zeit mit der Option **Konfigurationsdatei sichern unter** in einer Datei sichern. Diese Option ist ebenfalls im Popup-Menü **Host** enthalten. Das oben auf der GUI befindliche Menü **Datei** bietet Ihnen die Möglichkeit, die aktuellen Host-Verbindungen in

einer Datei zu speichern oder Verbindungen aus vorhandenen Dateien für alle Komponenten von Network Dispatcher wiederherzustellen.

Die Konfigurationsbefehle können auch auf einem fernen System ausgeführt werden. Weitere Informationen hierzu finden Sie im Abschnitt „Authentifizierte Fernverwaltung“ auf Seite 219.

Sie können auf **Hilfe** zugreifen, indem Sie auf das Fragezeichen in der oberen rechten Ecke des Fensters von Network Dispatcher klicken.

- **Hilfe für Feld** — beschreibt jedes Feld und gibt die Standardwerte an.
- **Vorgehensweise** — listet Tasks auf, die von dieser Anzeige aus ausgeführt werden können.
- **Inhaltsverzeichnis** — zeigt ein Inhaltsverzeichnis mit allen Hilfetexten an.
- **Index** — zeigt einen alphabetischen Index der Hilfethemen an.

Weitere Informationen zur Verwendung der GUI finden Sie im Abschnitt „Allgemeine Anweisungen zur Verwendung der GUI“ auf Seite 7.

Konfigurationsassistent

Weitere Informationen zur Verwendung des Konfigurationsassistenten finden Sie im Abschnitt „Konfiguration mit dem Konfigurationsassistenten“ auf Seite 5.

Dispatcher-Maschine konfigurieren

Vor dem Konfigurieren der Dispatcher-Maschine müssen Sie (unter AIX, Linux oder Solaris) als Benutzer „root“ oder (unter Windows 2000) als Administrator registriert sein.

Unter AIX, Linux und Solaris kann Network Dispatcher mit einem Server **verknüpft** sein. Dies bedeutet, dass sich der Network Dispatcher physisch auf einer Servermaschine befinden kann, für die er einen Lastausgleich durchführt.

Sie benötigen mindestens zwei gültige IP-Adressen für die Dispatcher-Maschine:

- Eine IP-Adresse speziell für die Dispatcher-Maschine
Diese IP-Adresse ist die primäre IP-Adresse der Dispatcher-Maschine und wird als NFA (Nonforwarding Address) bezeichnet. Dies ist standardmäßig dieselbe Adresse wie die vom Befehl **hostname** zurückgegebene. Benutzen Sie diese Adresse, wenn Sie zu Verwaltungszwecken (z. B. für eine Fernkonfiguration über Telnet oder für den Zugriff auf den SNMP-Subagenten) eine Verbindung zur Maschine herstellen möchten. Kann die Dispatcher-Maschine bereits andere Maschinen im Netz über ping-Aufrufe erreichen, sind keine weiteren Aktionen zum Konfigurieren der NFA erforderlich.

- Eine IP-Adresse pro Cluster

Eine Cluster-Adresse ist eine Adresse, die einem Host-Namen zugeordnet ist (beispielsweise `www.IhreFirma.com`). Diese IP-Adresse wird von einem Client benutzt, um die Verbindung zu den Servern in einem Cluster herzustellen. An dieser Adresse führt der Dispatcher den Lastausgleich durch.

Nur Solaris:

1. Der Dispatcher ist standardmäßig für den Lastausgleich für Datenverkehr auf 100-Mbit/s-Ethernet-Netzschnittstellenkarten konfiguriert. Zum Ändern der Standardeinstellung müssen Sie die Datei `/opt/nd/servers/ibmnd.conf` wie folgt editieren:
 - Der standardmäßige 100-Mbit/s-Ethernet-Adapter ist in `ibmnd.conf` als `hme` angegeben.
 - Wenn Sie einen 10-Mbit/s-Ethernet-Adapter verwenden, ersetzen Sie `hme` durch `le`.
 - Für einen 1-Gbit/s-Ethernet-Adapter müssen Sie `hme` durch `ge` ersetzen.
 - Wenn Sie einen Adapter mit mehreren Anschlüssen verwenden, ersetzen Sie `hme` durch `qfe`.
 - Sollen mehrere Adaptertypen unterstützt werden, kopieren Sie die Zeile in der Datei `ibmnd.conf` und passen Sie die einzelnen Zeilen an den Einheitentyp an.

Wenn Sie vorhaben, zwei 100-Mbit/s-Ethernet-Adapter zu verwenden, sollte die Datei `ibmnd.conf` eine Zeile mit der Einheitenangabe `hme` enthalten. Falls Sie einen 10-Mbit/s-Ethernet-Adapter und einen 100-Mbit/s-Ethernet-Adapter verwenden möchten, enthält die Datei `ibmnd.conf` zwei Zeilen, eine Zeile für die Einheit `le` und eine für die Einheit `hme`.

Die Datei **`ibmnd.conf`** stellt Vorgaben für den Solaris-Befehl **`autopush`** bereit und muss mit dem Befehl `"autopush"` kompatibel sein.

2. Beim Starten oder Stoppen des Dispatcher-Executors werden alle Aliasnamen für die in der Datei `ibmnd.conf` aufgelisteten Adapter aus der Konfiguration entfernt. Wenn Sie die Aliasnamen für diese Adapter (mit Ausnahme der von der Dispatcher-Komponente von Network Dispatcher verwendeten Adapter) automatisch neu konfigurieren möchten, verwenden Sie die Script-Datei **`goAliases`**. Im Verzeichnis `.../nd/servers/samples` finden Sie ein Beispiel-Script, das Sie vor der Ausführung in das Verzeichnis `...nd/servers/bin` verschieben *müssen*. Das Script `goAliases` wird beim Starten oder Stoppen des Dispatcher-Executors automatisch ausgeführt.

Sind die beiden Cluster X und Y für einen der in `ibmnd.conf` aufgelisteten Adapter beispielsweise für die Komponente Mailbox Locator konfiguriert, werden die Cluster X und Y aus der Konfiguration entfernt, sobald der Befehl **`ndcontrol executor start`** oder **`ndcontrol executor stop`** abgesetzt wird. Dieses Ergebnis ist unter Umständen nicht erwünscht.

Wenn die Cluster X und Y im Script goAliases konfiguriert sind, werden Sie nach dem Starten oder Stoppen des Dispatcher-Executors automatisch rekonfiguriert.

Nur Windows 2000: Vergewissern Sie sich, dass die IP-Weiterleitung für das TCP/IP-Protokoll nicht aktiviert ist. (Vergleichen Sie dazu Ihre TCP/IP-Konfiguration unter Windows 2000.)

Abb. 15 zeigt ein Beispiel für einen mit einem Cluster, zwei Ports und drei Servern konfigurierten Dispatcher.

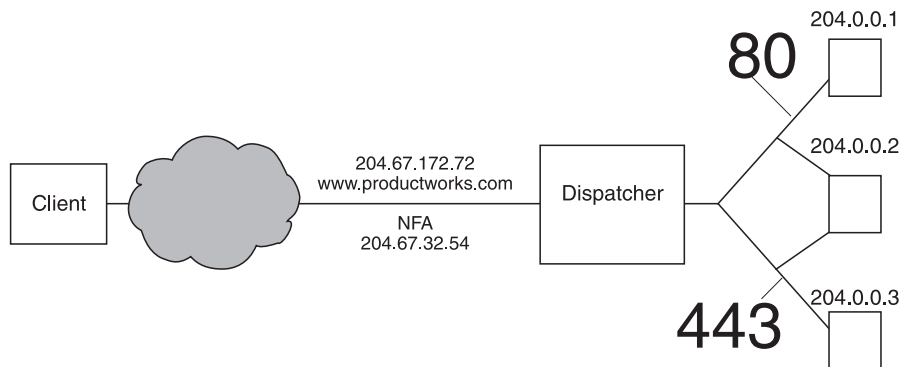


Abbildung 15. Beispiel der für die Dispatcher-Maschine erforderlichen IP-Adressen

Hilfe zu den in dieser Prozedur verwendeten Befehlen finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Eine Beispielfunktionsdatei finden Sie im Abschnitt „Beispielfunktionsdateien für Network Dispatcher“ auf Seite 393.

Schritt 1. Serverfunktion starten

AIX, Linux und Solaris: Geben Sie zum Starten der Serverfunktion **ndserver** ein.

Windows 2000: Die Serverfunktion wird automatisch als Dienst gestartet.

Anmerkung: Eine Standardkonfigurationsdatei (default.cfg) wird automatisch geladen, wenn ndserver gestartet wird. Entscheidet der Benutzer, dass die Dispatcher-Konfiguration in default.cfg gesichert werden soll, werden alle in dieser Datei gesicherten Daten automatisch geladen, wenn ndserver das nächste Mal gestartet wird.

Schritt 2. Executor-Funktion starten

Geben Sie zum Starten der Executor-Funktion den Befehl **ndcontrol executor start** ein. Sie können jetzt auch verschiedene Executor-Einstellungen ändern. Weitere Informationen hierzu finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Schritt 3. NFA definieren (falls vom Host-Namen abweichend)

Die NFA wird benutzt, um zu Verwaltungszwecken (z. B. für die Verwendung von Telnet oder SMTP) eine Verbindung zur Maschine herzustellen. Standardmäßig ist diese Adresse der Host-Name.

Geben Sie zum Definieren der NFA den Befehl **ndcontrol executor set nfa IP-Adresse** ein oder editieren Sie die Beispielkonfigurationsdatei. Die *IP-Adresse* ist entweder ein symbolischer Name oder die Adresse in Schreibweise mit Trennzeichen.

Schritt 4. Cluster definieren und Cluster-Optionen festlegen

Der Dispatcher verteilt die Last der an die Cluster-Adresse gesendeten Anforderungen auf die für die Ports dieses Clusters konfigurierten Server.

Der Cluster ist entweder der symbolische Name, die Adresse in Schreibweise mit Trennzeichen oder die spezielle Adresse 0.0.0.0, die einen Platzhalter-Cluster definiert. Setzen Sie zum Definieren eines Clusters den Befehl **ndcontrol cluster add** ab. Setzen Sie zum Definieren von Cluster-Optionen den Befehl **ndcontrol cluster set** ab oder verwenden Sie die GUI zum Absetzen von Befehlen. Platzhalter-Cluster können verwendet werden, wenn mehrere IP-Adressen für den Lastausgleich eingehender Pakete in Frage kommen. Weitere Informationen hierzu finden Sie in den Abschnitten „Platzhalter-Cluster verwenden, um Serverkonfigurationen zusammenzufassen“ auf Seite 199, „Platzhalter-Cluster für den Lastausgleich von Firewalls verwenden“ auf Seite 200 und „Platzhalter-Cluster mit Caching Proxy für transparente Weiterleitung verwenden“ auf Seite 201.

Schritt 5. Aliasnamen für die Netzschnittstellenkarte erstellen

Nachdem der Cluster definiert wurde, müssen Sie normalerweise die Cluster-Adresse auf einer der Netzschnittstellenkarten der Dispatcher-Maschine konfigurieren. Setzen Sie dazu den Befehl **ndcontrol cluster configure Cluster-Adresse ab**. Damit wird nach einem Adapter mit einer vorhandenen Adresse gesucht, die zu demselben Teilnetz wie die Cluster-Adresse gehört. Anschließend wird der Adapterkonfigurationsbefehl des Betriebssystems für die Cluster-Adresse unter Verwendung des gefundenen Adapters und der Netzmaske für die auf diesem Adapter vorhandene Adresse abgesetzt. Beispiel:

```
ndcontrol cluster configure 204.67.172.72
```

In manchen Fällen soll die Cluster-Adresse möglicherweise nicht konfiguriert werden. Dies gilt für Cluster, die zu einem Bereitschaftsserver im Modus für

hohe Verfügbarkeit hinzugefügt wurden, oder für Cluster, die zu einem Weitverkehrs-Dispatcher hinzugefügt wurden, der als ferner Server dient. Sie müssen den Befehl `cluster configure` auch nicht ausführen, wenn Sie im Standalone-Modus das Beispiel-Skript **goldle** verwenden. Informationen zum Skript **goldle** finden Sie im Abschnitt „Scripts verwenden“ auf Seite 182.

In seltenen Fällen haben Sie möglicherweise eine Cluster-Adresse, die mit keinem Teilnetz für vorhandene Adressen übereinstimmt. Verwenden Sie in diesem Fall die zweite Form des Befehls `cluster configure` und geben Sie explizit den Schnittstellennamen und die Netzmaske an. Verwenden Sie **ndcontrol cluster configure** *Cluster-Adresse Schnittstellenname Netzmaske*.

Beispiele:

```
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

Für die zweite Form des Befehls "cluster configure" müssen Sie unter Windows 2000 den zu verwendenden Schnittstellennamen ermitteln.

Befindet sich in Ihrer Maschine nur eine einzige Ethernet-Karte, lautet der Schnittstellenname `en0`. Befindet sich in Ihrer Maschine nur eine einzige Token-Ring-Karte, lautet der Schnittstellenname `tr0`. Befinden sich in Ihrer Maschine mehrere Karten beider Typen, müssen Sie die Zuordnung der Karten festlegen. Gehen Sie wie folgt vor:

1. Starten Sie **regedit** über die Eingabeaufforderung.
2. Klicken Sie auf **HKEY_LOCAL_MACHINE, Software, Microsoft, Windows NT und Current Version**.
3. Klicken Sie dann auf **Network Cards**.

Die Netzschnittstellenadapter sind unter **Network Cards** aufgeführt. Klicken Sie auf die einzelnen Karten, um festzustellen, ob es sich um eine Ethernet- oder Token-Ring-Schnittstelle handelt. Der Schnittstellentyp ist in der Spalte mit der Beschreibung aufgeführt. Die mit dem Befehl **ndconfig** zugeordneten Namen werden den Schnittstellentypen zugeordnet. Beispielsweise setzt **ndconfig** die erste Ethernet-Schnittstelle in der Liste auf `en0`, die zweite auf `en1` usw., die erste Token-Ring-Schnittstelle auf `tr0`, die zweite auf `tr1` usw.

Anmerkung: Die Nummerierung von Adaptern in der Registrierungsdatenbank von Windows 2000 beginnt bei **1** und nicht bei **0**.

Nachdem Sie diese Zuordnungsinformationen erhalten haben, können auf der Netzchnittstelle die Cluster-Adresse als Aliasnamen festlegen.

ifconfig/ndconfig zum Konfigurieren von Cluster-Aliasnamen verwenden
Der Befehl "cluster configure" führt nur ifconfig-Befehle (oder unter Windows 2000 ndconfig-Befehle) aus, so dass Sie bei Bedarf auch die ifconfig-Befehle (bzw. ndconfig-Befehle) verwenden können.

Windows 2000: Die Dispatcher-Komponente bietet den Befehl ndconfig an, um Cluster-Aliasnamen von der Befehlszeile aus zu konfigurieren. Der Befehl ndconfig hat dieselbe Syntax wie ein ifconfig-Befehl unter UNIX.

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

Anmerkung: Der Parameter für die Netzmaske ist erforderlich. Er muss in Schreibweise mit Trennzeichen (255.255.0.0) oder im Hexadezimalformat (0xffff0000) angegeben werden.

Verwenden Sie zur Bestimmung des Schnittstellennamens dieselbe Technik wie für die zweite Form des Befehls cluster configure.

Solaris: Bei Verwendung von bindungsspezifischen Serveranwendungen, die an eine Liste von IP-Adressen ohne die IP-Adresse des Servers gebunden werden, verwenden Sie anstelle von "ifconfig" den Befehl **arp publish**, um auf der Network-Dispatcher-Maschine dynamisch eine IP-Adresse festzulegen.
Beispiel:

```
arp -s <Cluster> <Network-Dispatcher-MAC-Adresse> pub
```

Schritt 6. Ports definieren und Port-Optionen festlegen

Zum Definieren eines Ports können Sie den Befehl **ndcontrol port add Cluster:Port** eingeben, die Beispielkonfigurationsdatei editieren oder die GUI verwenden. *Cluster* ist entweder der symbolische Name oder die Adresse in Schreibweise mit Trennzeichen. *Port* ist die Nummer des Ports, den Sie für dieses Protokoll verwenden. Sie können jetzt auch verschiedene Port-Einstellungen ändern. Sie müssen alle Server für einen Port definieren und konfigurieren. Lesen Sie hierzu die Informationen in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Mit der Port-Nummer 0 (null) wird ein Platzhalter-Port angegeben. Dieser Port akzeptiert Datenverkehr, der nicht für einen der definierten Ports eines Clusters bestimmt ist. Der Platzhalter-Port wird zum Konfigurieren von Regeln und Servern für alle Ports verwendet. Diese Funktion kann auch verwendet werden, wenn Sie eine identische Server-/Regelkonfiguration für mehrere Ports haben. Der Datenverkehr an einem Port könnte dann die Last-

ausgleichsentscheidungen für Datenverkehr an anderen Ports beeinflussen. Weitere Informationen zur Verwendung eines Platzhalter-Ports finden Sie im Abschnitt „Platzhalter-Port für die Übertragung von Datenverkehr mit nicht konfiguriertem Port verwenden“ auf Seite 201.

Anmerkung: Der mit Platzhalter-Port kann nicht für FTP-Datenverkehr verwendet werden.

Schritt 7. Am Lastausgleich beteiligte Servermaschinen definieren

Geben Sie zum Definieren einer am Lastausgleich beteiligten Servermaschine den Befehl **ndcontrol server add Cluster:Port:Server** ein. Sie können auch die Beispielkonfigurationsdatei editieren oder die GUI verwenden. *Cluster* und *Server* sind entweder symbolische Namen oder Adressen in Schreibweise mit Trennzeichen. *Port* ist die Nummer des Ports, den Sie für dieses Protokoll verwenden. Für einen Port eines Clusters müssen Sie mehrere Server definieren, um einen Lastausgleich durchführen zu können.

Bindungsspezifische Server: Wenn die Dispatcher-Komponente die Last auf bindungsspezifische Server verteilt, *müssen* die Server so konfiguriert werden, dass sie an die Cluster-Adresse gebunden werden. Da der Dispatcher Pakete ohne Änderung der Ziel-IP-Adresse weiterleitet, enthalten die beim Server eingehenden Pakete noch immer die Cluster-Adresse als Ziel. Wenn ein Server für die Bindung an eine andere IP-Adresse als die Cluster-Adresse konfiguriert ist, kann der Server für den Cluster bestimmte Pakete/Anforderungen nicht akzeptieren.

Anmerkung: Für Solaris und Linux: Bindungsspezifische Server dürfen nicht verknüpft werden.

Verknüpfung mehrerer Adressen: In einer verknüpften Konfiguration muss die Adresse der verknüpften Servermaschine *nicht* mit der NFA übereinstimmen. Wenn Ihre Maschine mit mehreren IP-Adressen definiert wurde, können Sie eine andere Adresse verwenden. Für die Dispatcher-Komponente muss die verknüpfte Servermaschine mit dem Befehl **ndcontrol server** als **verknüpft** definiert werden. Weitere Informationen zu verknüpften Servern finden Sie im Abschnitt „Verknüpfte Server verwenden“ auf Seite 166.

Weitere Informationen zur Syntax des Befehls **ndcontrol server** können Sie dem Abschnitt „ndcontrol server — Server konfigurieren“ auf Seite 320 entnehmen.

Schritt 8. Manager-Funktion starten (optional)

Die Manager-Funktion verbessert den Lastausgleich. Soll der Manager gestartet werden, geben Sie den Befehl **ndcontrol manager start** ein, editieren Sie die Beispielkonfigurationsdatei oder verwenden Sie die GUI.

Schritt 9. Advisor-Funktion starten (optional)

Die Advisor-Funktionen liefern dem Manager weitere Informationen über die Fähigkeit der am Lastausgleich beteiligten Servermaschinen, auf Anforderungen zu antworten. Advisor-Funktionen sind protokollspezifisch. Soll beispielsweise die HTTP-Advisor-Funktion gestartet werden, setzen Sie den folgenden Befehl ab:

```
cbrcontrol advisor start http Port
```

Eine Liste der Advisor-Funktionen mit den zugehörigen Standard-Ports finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265. Eine Beschreibung der einzelnen Advisor-Funktionen können Sie dem Abschnitt „Liste der Advisor-Funktionen“ auf Seite 153 entnehmen.

Schritt 10. Cluster-Proportionen festlegen

Wenn Sie Advisor-Funktionen starten, können Sie die Wichtigkeit ändern, die in Entscheidungen für den Lastausgleich einfließenden Informationen von Advisor-Funktionen beigemessen wird. Setzen Sie zum Festlegen von Cluster-Proportionen den Befehl **ndcontrol cluster set *Cluster* proportions** ab. Weitere Informationen hierzu finden Sie im Abschnitt „Proportionale Bedeutung von Statusinformationen“ auf Seite 145.

Servermaschinen für Lastausgleich konfigurieren

Wenn es sich um einen verknüpften Server handelt (d. h., sich der Dispatcher auf der Maschine befindet, für die er den Lastausgleich durchführt) oder eine der Weiterleitungsmethoden "nat" und "cbr" verwendet wird, führen Sie die folgenden Prozeduren *nicht* aus.

Wird die Weiterleitungsmethode "mac" verwendet, funktioniert der Dispatcher nur auf Back-End-Servern, bei denen der Loopback-Adapter mit einer zusätzlichen IP-Adresse konfiguriert werden kann, da der Back-End-Server nicht auf ARP-Anforderungen (Adressauflösungsprotokoll) reagiert. Führen Sie die Schritte in diesem Abschnitt aus, um die am Lastausgleich beteiligten Servermaschinen zu konfigurieren.

Schritt 1. Aliasnamen für die Loopback-Einheit festlegen

Damit die am Lastausgleich beteiligten Servermaschinen arbeiten können, müssen Sie die Loopback-Einheit (die häufig als lo0 bezeichnet wird) auf die Cluster-Adresse setzen (oder bevorzugt die Cluster-Adresse als Aliasnamen festlegen). Bei Verwendung der Weiterleitungsmethode "mac" ändert die Dispatcher-Komponente nicht die Ziel-IP-Adresse des TCP/IP-Pakets, bevor sie dieses an eine TCP-Servermaschine weiterleitet. Wird die Loopback-Einheit auf die Cluster-Adresse gesetzt oder diese Adresse als Aliasname der Loopback-Einheit festgelegt, akzeptieren die am Lastausgleich beteiligten Servermaschinen ein an die Cluster-Adresse gerichtetes Paket.

Falls Ihr Betriebssystem Aliasnamen für Netzschnittstellen unterstützt (wie es bei AIX, Linux, Solaris oder Windows 2000 der Fall ist), sollten Sie die Cluster-Adresse als Aliasnamen der Loopback-Einheit festlegen. Ein Betriebssystem mit Unterstützung für Aliasnamen bringt den Vorteil, dass die am Lastausgleich beteiligten Servermaschinen für mehrere Cluster-Adressen konfiguriert werden können.

Anmerkung: Es gibt einige wenige **Linux**-Kernel-Versionen, bei denen zum Festlegen eines Aliasnamens für die Loopback-Einheit ein Patch-Code erforderlich ist. Stellen Sie anhand der Informationen im Abschnitt „Patch-Code für Linux-Kernel (zum Unterdrücken von ARP-Antworten an der Loopback-Schnittstelle) installieren“ auf Seite 77 fest, ob Sie einen Patch-Code für Linux-Kernel benötigen.

Setzen Sie für **Linux**-Kernel ab Version 2.2.14 vor dem Befehl **ifconfig** den folgenden Befehl ab:

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

Wenn das Betriebssystem Ihres Servers keine Aliasnamen unterstützt, wie das z. B. bei HP-UX und OS/2 der Fall ist, müssen Sie die Loopback-Einheit auf die Cluster-Adresse setzen.

Verwenden Sie den in Tabelle 4 angegebenen betriebssystemspezifischen Befehl, um die Loopback-Einheit oder einen Aliasnamen für die Einheit zu definieren.

Tabelle 4. Befehle zum Festlegen eines Aliasnamens für die Loopback-Einheit (lo0) für Dispatcher

AIX	ifconfig lo0 alias <i>Cluster-Adresse</i> netmask <i>Netzmaske</i>
HP-UX	ifconfig lo0 <i>Cluster-Adresse</i>
Linux	ifconfig lo:1 <i>Cluster-Adresse</i> netmask 255.255.255.255 up
OS/2	ifconfig lo <i>Cluster-Adresse</i>
Solaris 7	ifconfig lo0:1 <i>Cluster-Adresse</i> 127.0.0.1 up
Solaris 8	ifconfig lo0:1 plumb <i>Cluster-Adresse</i> netmask <i>Netzmaske</i> up

Tabelle 4. Befehle zum Festlegen eines Aliasnamens für die Loopback-Einheit (lo0) für Dispatcher (Forts.)

Windows 2000	<ol style="list-style-type: none"> 1. Klicken Sie auf Start, Einstellungen und dann auf Systemsteuerung. 2. Fügen Sie den MS Loopback Adapter Driver hinzu (falls noch nicht erfolgt). <ol style="list-style-type: none"> a. Klicken Sie doppelt auf Hardware. Damit wird der Assistent zum Hinzufügen/Entfernen von Hardware gestartet. b. Klicken Sie auf Weiter, wählen Sie Gerät hinzufügen bzw. Problem beheben aus und klicken Sie dann auf Weiter. c. Die Anzeige blinkt. Anschließend erscheint die Anzeige Gerät wählen. d. Wenn der MS Loopbackadapter in der Liste aufgeführt ist, ist er bereits installiert— klicken Sie auf "Abbrechen", um die Anzeige zu verlassen. e. Ist der MS Loopbackadapter <i>nicht</i> aufgelistet, wählen Sie Neues Gerät hinzufügen aus und klicken Sie auf "Weiter". f. Falls Sie Hardware aus einer Liste auswählen möchten, wählen Sie für die Frage Soll nach neuen Hardwarekomponenten gesucht werden? als Antwort "Nein, die Hardwarekomponenten selbst in der Liste auswählen" aus und klicken Sie auf "Weiter". g. Wählen Sie Netzwerkadapter aus und klicken Sie auf "Weiter". h. Wählen Sie in der Anzeige Netzwerkadapter wählen unter "Hersteller" Microsoft und dann Microsoft Loopbackadapter aus. i. Klicken Sie auf "Weiter". Klicken Sie dann erneut auf "Weiter", um die Standardeinstellungen zu installieren (oder wählen Sie Datenträger aus, legen Sie die CD ein und installieren Sie von der CD). j. Klicken Sie auf "Fertig stellen", um die Installation zu beenden. 3. Klicken Sie in der Systemsteuerung doppelt auf Netzwerk- und DFÜ-Verbindungen. 4. Wählen Sie die Verbindung mit dem Einheitenamen "Microsoft Loopbackadapter" aus und klicken Sie mit der rechten Maustaste auf den Namen. 5. Wählen Sie im angezeigten Menü Eigenschaften aus. 6. Wählen Sie Internetprotokoll (TCP/IP) aus und klicken Sie auf Eigenschaften. 7. Klicken Sie auf Folgende IP-Adresse verwenden. Geben Sie für <i>IP-Adresse</i> die Cluster-Adresse und für <i>Subnetzmaske</i> die Standardteilnetzmaske (255.0.0.0) ein. Anmerkung: Geben Sie keine Router-Adresse ein. Verwenden Sie den lokalen Host als Standard-DNS-Server.
--------------	---

Tabelle 4. Befehle zum Festlegen eines Aliasnamens für die Loopback-Einheit (lo0) für Dispatcher (Forts.)

OS/390	<p>Konfigurieren eines Loopback-Aliasnamens auf einem OS/390-System</p> <ul style="list-style-type: none"> In der Teildatei mit den IP-Parametern muss ein Administrator einen Eintrag in der Liste der Ausgangsadressen erstellen. Beispiel: <table> <tr> <td>HOME</td><td></td></tr> <tr> <td>;Address</td><td>Link</td></tr> <tr> <td>192.168.252.11</td><td>tr0</td></tr> <tr> <td>192.168.100.100</td><td>ltr1</td></tr> <tr> <td>192.168.252.12</td><td>loopback</td></tr> </table> <ul style="list-style-type: none"> Für die Loopback-Einheit können mehrere Adressen definiert werden. Standardmäßig wird 127.0.0.1 konfiguriert. 	HOME		;Address	Link	192.168.252.11	tr0	192.168.100.100	ltr1	192.168.252.12	loopback
HOME											
;Address	Link										
192.168.252.11	tr0										
192.168.100.100	ltr1										
192.168.252.12	loopback										

Schritt 2. Überprüfung auf zusätzliche Route

Unter einigen Betriebssystemen wurde möglicherweise eine Standard-Route erstellt, die entfernt werden muss.

- Überprüfen Sie mit dem folgenden Befehl, ob unter Windows 2000 eine zusätzliche Route vorhanden ist:

```
route print
```

- Überprüfen auf allen UNIX-Systemen mit dem folgenden Befehl, ob eine zusätzliche Route vorhanden ist:

```
netstat -nr
```

Beispiel für Windows 2000:

- Nachdem **route print** eingegeben wurde, wird eine ähnliche Tabelle wie die folgende angezeigt. (Dieses Beispiel veranschaulicht das Auffinden und Entfernen einer zusätzlichen Route zu Cluster 9.67.133.158 mit der Standardnetzmaske 255.0.0.0.)

Aktive Routen:

Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Anzahl
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

- Suchen Sie die Cluster-Adresse in der Spalte "Gateway". Ist eine zusätzliche Route vorhanden, wird die Cluster-Adresse zweimal aufgeführt. In diesem Beispiel erscheint die Cluster-Adresse (9.67.133.158) in Zeile 2 und Zeile 8.
- Ermitteln Sie für jede Zeile, in der die Cluster-Adresse erscheint, die Netzadresse. Sie benötigen eine dieser Routes und müssen die überschüssige Route löschen. Die zu löschende zusätzliche Route ist die Route, deren dessen Netzadresse mit der ersten Ziffer der Cluster-Adresse beginnt, gefolgt von drei Nullen. In diesem Beispiel erscheint die zusätzliche Route in Zeile 2. Diese Route hat die Netzadresse **9.0.0.0**:

```
9.0.0.0    255.0.0.0    9.67.133.158  9.67.133.158    1
```

Schritt 3. Zusätzliche Routes löschen

Die zusätzliche Route muss gelöscht werden. Löschen Sie die zusätzliche Route mit dem in Tabelle 5 angegebenen betriebssystemspezifischen Befehl.

Beispiel: Geben Sie zum Löschen einer zusätzlichen Route wie in der Beispielaufstellung "Aktive Routen" für Schritt 2 Folgendes ein:

```
route delete 9.0.0.0 9.67.133.158
```

Tabelle 5. Befehle zum Löschen zusätzlicher Routes für Dispatcher

HP-UX	route delete <i>Cluster-Adresse Cluster-Adresse</i>
Windows 2000	route delete <i>Netzadresse Cluster-Adresse</i> (an einer MS-DOS-Eingabeaufforderung) Anmerkung: Die zusätzliche Route müssen Sie bei jedem Neustart des Servers löschen.

Wenn Sie für das in Abb. 15 auf Seite 66 gezeigte Beispiel eine Servermaschine mit AIX konfigurieren, würde der Befehl wie folgt lauten:

```
route delete -net 204.0.0.0 204.67.172.72
```

Schritt 4. Serverkonfiguration prüfen

Führen Sie zum Überprüfen der Konfiguration eines Back-End-Servers auf einer anderen Maschine im selben Teilnetz bei nicht aktivem Dispatcher und nicht konfiguriertem *Cluster* die folgenden Schritte aus:

- Setzen Sie den folgenden Befehl ab:

```
arp -d Cluster
```

2. Setzen Sie den folgenden Befehl ab:

```
ping Cluster
```

Sie sollten keine Antwort empfangen. Falls Sie eine Antwort auf das "ping" erhalten, vergewissern Sie sich, dass Sie nicht mit `iconfig` die Schnittstelle auf die Cluster-Adresse gesetzt haben. Vergewissern Sie sich, dass keine Maschine einen veröffentlichten Eintrag "arp" für die Cluster-Adresse hat.

Anmerkung: Für die **Linux**-Kernel-Versionen 2.2.12 und 2.2.13 müssen Sie sicherstellen, dass

```
/proc/sys/net/ipv4/conf/lo/arp_invisible
```

 eine "1" enthält.

Für **Linux**-Kernel ab Version 2.2.14 müssen

```
/proc/sys/net/ipv4/conf/lo/hidden
```

 und

```
/proc/sys/net/ipv4/conf/all/hidden
```

 eine "1" enthalten.

3. Senden Sie ein "ping" an den Back-End-Server und setzen Sie unmittelbar darauf den folgenden Befehl ab:

```
arp -a
```

Die Ausgabe des Befehls sollte die MAC-Adresse Ihres Servers enthalten. Setzen Sie den folgenden Befehl ab:

```
arp -s Cluster MAC-Adresse_des_Servers
```

4. Senden Sie ein "ping" an den Cluster. Sie sollten eine Antwort empfangen. Setzen Sie `http`, `telnet` oder eine andere an den Cluster adressierte Anfrage ab, die Ihr Back-End-Server verarbeiten können müsste. Vergewissern Sie sich, dass der Server ordnungsgemäß arbeitet.
5. Setzen Sie den folgenden Befehl ab:

```
arp -d Cluster
```
6. Senden Sie ein "ping" an den Cluster. Sie sollten keine Antwort empfangen.

Anmerkung: Falls Sie eine Antwort empfangen, setzen Sie die Anweisung **arp Cluster** ab, um die MAC-Adresse der falsch konfigurierten Maschine zu ermitteln. Wiederholen Sie dann die Schritte 1 bis 6.

Patch-Code für Linux-Kernel (zum Unterdrücken von ARP-Antworten an der Loopback-Schnittstelle) installieren

Bei Linux-Servern ist (je nach Linux-Kernel-Version) ein Patch-Code erforderlich, um der Loopback-Einheit einen Aliasnamen zuordnen zu können.

Der Patch-Code stellt sicher, dass eine ARP-Antwort nur von einem Netzwerkadapteranschluss gesendet wird, der die in der ARP-Anfrage angeforderte IP-Adresse hat. Ohne diesen Patch-Code setzt Linux im Netz ARP-Antworten für die Aliasnamen der Loopback-Einheit ab. Der Patch-Code beseitigt auch eine ARP-Konkurrenzbedingung, wenn in einem physischen Netzwerk mehrere Netzwerkadapteranschlüsse mit verschiedenen IP-Adressen vorhanden sind.

Sie müssen den Patch-Code unter den folgenden Bedingungen installieren.

- **Linux-Kernel-Versionen 2.4.x**

- Wenn Sie die MAC-Weiterleitungsmethode des Dispatchers mit hoher Verfügbarkeit und Verknüpfung verwenden, müssen Sie den Patch-Code auf der Dispatcher-Maschine installieren.

Anmerkung: Der Dispatcher kann auch dann als verknüpft angesehen werden, wenn er nur den Lastausgleich für eine auf derselben Maschine wie der Dispatcher installierte andere Komponente von Edge Server (wie Caching Proxy, Mailbox Locator, CBR usw.) durchführt.

- Wenn Sie den 2.4-Kernel auf einem Back-End-Server verwenden, dessen Lastausgleich ein für die MAC-Weiterleitungsmethode konfigurierter Dispatcher durchführt, müssen Sie den Patch-Code auf der Back-End-Servermaschine installieren.
- Falls die Maschine mehrere Netzwerkadapteranschlüsse in einem physischen Netz hat, müssen Sie den Patch-Code auf der Maschine installieren.

- **Linux-Kernel-Versionen 2.2.12 und 2.2.13**

Bei Verwendung des Kernels 2.2.12 oder 2.2.13 auf einem Back-End-Server gilt Folgendes:

Anmerkungen:

1. Network Dispatcher kann nicht auf einem 2.2-Kernel ausgeführt werden.
2. Im 2.2.14-Kernel ist der Patch-Code bereits enthalten.
3. Dieser Patch-Code für Linux-Kernel wurde für den Test des IBM Produkts verwendet und in der IBM Testumgebung mit zufriedenstellenden Ergebnissen getestet. Sie sollten die Brauchbarkeit dieses Codes in Ihrer eigenen Umgebung testen und entscheiden, ob der Code Ihren Bedürfnissen gerecht wird. Dieser Code kann möglicherweise in zukünftigen Versionen des Linux-Basisquellencodes enthalten sein.

Linux-Kernel-Versionen 2.4.x

Der Kernel-Patch-Code ist nicht für alle Konfigurationen erforderlich. Unter den folgenden Bedingungen müssen Sie einen Patch-Code für die Linux-Kernel-Versionen 2.4.x installieren:

- Wenn Sie die MAC-Weiterleitungsmethode des Dispatchers mit hoher Verfügbarkeit und Verknüpfung verwenden, müssen Sie den Patch-Code auf der Dispatcher-Maschine installieren.

Anmerkung: Der Dispatcher kann auch dann als verknüpft angesehen werden, wenn er nur den Lastausgleich für eine auf derselben Maschine wie der Dispatcher installierte andere Komponente von Edge Server (wie Caching Proxy, Mailbox Locator, CBR usw.) durchführt.

- Wenn Sie den 2.4-Kernel auf einem Back-End-Server verwenden, dessen Lastausgleich ein für die MAC-Weiterleitungsmethode konfigurierter Dispatcher durchführt, müssen Sie den Patch-Code auf dem Back-End-Server installieren.
- Falls die Maschine mehrere Netzwerkadapteranschlüsse in einem physischen Netz hat, müssen Sie den Patch-Code auf der Maschine installieren.

Sie können diesen Patch-Code von der Adresse

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

Wählen Sie in der Download-Liste den Eintrag "CVS Tree" aus.

Wenden Sie den Patch-Code wie folgt an:

1. Empfangen Sie den Loopback-Patch-Code von der Adresse <http://oss.software.ibm.com/developerworks/opensource/cvs/naslib>.
2. Installieren Sie wie folgt die Kernel-RPMs:

- a. Kopieren Sie die Patch-Codedatei **arp.c.2.4.0.patch** nach `/usr/src/linux-2.4/net/ipv4/`.
- b. Setzen Sie die folgenden Befehle ab:

```
cd /usr/src/linux-2.4/net/ipv4
patch -p0 -l < arp.c.2.4.0.patch
```

Anmerkung: Dies wurde mit den Linux-Kernel-Versionen 2.4.0 und 2.4.2 getestet.

3. Rufen Sie das Verzeichnis `/usr/src/linux-2.4` auf.
4. Editieren Sie die Datei `Makefile` und fügen Sie für den Wert `EXTRA-VERSION` **-arppatch** hinzu.
5. Setzen Sie den folgenden Befehl ab: `make mrproper`
6. Setzen Sie den Befehl `make config` ab. Wählen Sie die für Ihr System geeigneten Werte aus. Vergessen Sie nicht, Modulunterstützung zu konfigurieren.
7. Setzen Sie die folgenden Befehle ab:

```
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. Editieren Sie die Datei `lilo.conf` und kopieren Sie den Absatz **image=**. Nehmen Sie in der Kopie die folgenden Änderungen vor:

- Ändern Sie `/boot/vmlinuz-2.4.2-2` in `/boot/vmlinuz-2.4.2-2-arppatch`
- `label=linux` in `label=linux-arppatch`
- `default=linux` in `default=linux-arppatch`

9. Setzen Sie den folgenden Befehl ab: `/sbin/lilo`
10. Führen Sie einen Warmstart für den neuen Kernel durch.

Linux-Kernel-Versionen 2.2.12 und 2.2.13

Ein Patch-Code für die Linux-Kernel-Versionen 2.2.12 und 2.2.13 muss auf jeder Servermaschine, die die MAC-Weiterleitungsmethode anwendet, installiert werden. Sie können diesen Patch-Code von der Adresse <http://www.ibm.com/developer/linux> downloaden.

Wenden Sie den Patch-Code wie folgt an:

1. Empfangen Sie den Patch-Code für die Loopback-Einheit von <http://www.ibm.com/developer/linux>.
2. Installieren Sie die Kernel-Quelle. Installationsanweisungen enthält die Datei **README.kernel-sources** im Verzeichnis `/usr/src/linux`.
3. Wenden Sie den Patch-Code an, indem Sie den `patch`-Befehl vom Verzeichnis `/usr/src` aus absetzen. Beispiel:

```
patch -p0 < Patch-Codedatei
```
4. Kompilieren Sie den Kernel. Kompilierungsanweisungen finden Sie in der Datei **README** im Verzeichnis `/usr/src/linux-2.4/`.
5. Installieren Sie den neuen Kernel und führen Sie den Befehl **lilo** aus. Anweisungen enthält die Datei **README** im Verzeichnis `/usr/src/linux`.
6. Führen Sie einen Warmstart mit dem neuen Kernel durch.
7. Suchen Sie nach der folgenden Datei:
`/proc/sys/net/ipv4/conf/lo/arp_invisible`. Ist die Datei vorhanden, wurde der Kernel-Patch-Code erfolgreich installiert. Ist die Datei *nicht* vorhanden, war entweder die Installation des Patch-Codes nicht erfolgreich oder es wurde ein Kernel ohne Patch-Code gebootet. Überprüfen Sie `/usr/src/linux/README`, um sicherzustellen, dass alle Installationsschritte korrekt ausgeführt wurden.
8. Setzen Sie den folgenden Befehl ab:

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

Dieser Befehl wird nur bis zum Warmstart der Maschine ausgeführt. Nach dem Warmstart ist es erforderlich, dass dieser und die nachfolgenden Schritte erneut ausgeführt werden.

9. Verwenden Sie beim Festlegen des Aliasnamens für die Loopback-Einheit die Netzmaske 255.255.255.255. Beispiel:

```
ifconfig lo:1 cluster netmask 255.255.255.255 up
```
10. Fügen Sie den Server zu Ihrem Cluster hinzu.

Kapitel 6. Planung für Content Based Routing

In diesem Kapitel wird beschrieben, was die für die Planung des Netzes zuständige Person vor der Installation und Konfiguration der CBR-Komponente mit Caching Proxy berücksichtigen muss.

- Informationen zum Konfigurieren der Lastausgleichsparameter von CBR finden Sie in „Kapitel 7. Content Based Routing konfigurieren“ auf Seite 87.
- Informationen zum Konfigurieren von Network Dispatcher für erweiterte Funktionen finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Dieses Kapitel enthält die folgenden Abschnitte:

- „Hardware- und Softwarevoraussetzungen“
- „Überlegungen bei der Planung“

Hardware- und Softwarevoraussetzungen

Plattformvoraussetzungen:

- für AIX finden Sie im Abschnitt „Voraussetzungen für AIX“ auf Seite 12.
- für Linux finden Sie im Abschnitt „Voraussetzungen für Red Hat Linux oder SuSE Linux“ auf Seite 17.
- für Solaris finden Sie im Abschnitt „Voraussetzungen für Solaris“ auf Seite 21.
- für Windows 2000 finden Sie im Abschnitt „Voraussetzungen für Windows 2000“ auf Seite 23.

Überlegungen bei der Planung

Mit der CBR-Komponente können Sie unter Verwendung von Caching Proxy zum Weiterleiten der Anforderung HTTP- und SSL-Datenverkehr verteilen.

Anmerkung: Wenn Sie CBR als Plug-In ausführen möchten, müssen Sie den Reverse-Proxy-Modus von Caching Proxy installieren.

CBR ist dem Dispatcher hinsichtlich der Komponentenstruktur sehr ähnlich. CBR umfasst die folgenden Funktionen:

- **cbrserver** bearbeitet Anforderungen von der Befehlszeile an den Executor, den Manager und die Advisor-Funktionen.
- Der **Executor** unterstützt die Verteilung von Client-Anforderungen. Vor Verwendung der CBR-Komponente muss der Executor gestartet sein.
- Der **Manager** definiert Wertigkeiten, die vom Executor benutzt werden und auf folgenden Kriterien basieren:
 - interne Zähler des Executors
 - von den Advisor-Funktionen bereitgestellte Rückmeldungen von den Servern
 - Rückmeldungen von einem Systemüberwachungsprogramm wie Metric Server.

Die Benutzung des Managers ist optional. Ohne den Manager wird der Lastausgleich nach einer gewichteten RoundRobin-Zeitplanung und ausgehend von den aktuellen Serverwertigkeiten durchgeführt. Es stehen keine Advisor-Funktionen zur Verfügung.

- Die **Advisor-Funktionen** richten Abfragen an die Server und analysieren die Ergebnisse nach Protokoll, bevor sie den Manager zum Festlegen der entsprechenden Wertigkeiten aufrufen. Es ist nicht immer sinnvoll, einige dieser Advisor-Funktionen in einer typischen Konfiguration zu verwenden. Sie können auch eigene Advisor-Funktionen schreiben. Die Benutzung der Advisor-Funktionen ist optional, wird jedoch empfohlen. Network Dispatcher stellt eine Caching-Proxy-Advisor-Funktion (ibmproxy) bereit. Weitere Informationen hierzu finden Sie im Abschnitt „Advisor-Funktionen“ auf Seite 149.
- Zum Konfigurieren und Verwalten des Executors, der Advisor-Funktionen und des Managers können Sie die Befehlszeile (**cbrcontrol**) oder die grafische Benutzerschnittstelle (**ndadmin**) verwenden.

Die drei wichtigsten Funktionen der CBR-Komponente (Executor, Manager und Advisor-Funktionen) arbeiten gemeinsam an der Verteilung der eingehenden Anforderungen auf die Server. Neben dem Verteilen von Anforderungen überwacht der Executor die Anzahl neuer und aktiver Verbindungen. Diese Informationen stellt er anschließend dem Manager zur Verfügung.

Die CBR-Komponente gibt Ihnen die Möglichkeit, eine Gruppe von Servern anzugeben, die eine Anforderung auf der Basis des Abgleichs eines regulären Ausdrucks mit dem Inhalt der Anforderung bearbeiten. Mit CBR können Sie Ihre Site partitionieren, so dass verschiedene Inhalte oder Anwendungsdienste von unterschiedlichen Servergruppen bearbeitet werden.

Diese Partitionierung ist für Clients, die auf Ihre Site zugreifen, transparent. Da CBR die Angabe mehrerer Server für jede Art von Anforderung zulässt, können die Anforderungen so verteilt werden, dass eine optimale Client-Antwortzeit erreicht wird. Aufgrund der Möglichkeit, jedem Inhaltstyp mehrere Server zuzuordnen, sind Sie geschützt, wenn eine Workstation oder ein Server ausfällt. CBR erkennt den Ausfall und verteilt die Client-Anforderungen auf die übrigen Server der Gruppe.

Eine Möglichkeit, Ihre Site zu partitionieren, besteht darin, einige Server ausschließlich für die Bearbeitung von cgi-Anforderungen und eine andere Gruppe von Servern für die Bearbeitung aller anderen Anforderungen zuzuordnen. Damit wird verhindert, dass die Server aufgrund der Verarbeitung umfangreicher cgi-Scripts für den normalen html-Datenverkehr zu langsam werden und resultiert in einer insgesamt besseren Antwortzeit für die Clients. Mit Hilfe dieses Schemas könnten Sie auch leistungsstärkere Workstations für normale Anforderungen zuordnen. Dadurch würde die Antwortzeit für Clients verbessert, ohne dass alle Ihre Server aufgerüstet werden müssen. Sie könnten auch für cgi-Anforderungen leistungsstärkere Workstations zur Verfügung stellen.

Eine andere Möglichkeit zur Partitionierung Ihrer Site besteht darin, Clients, die auf Seiten mit erforderlicher Registrierung zugreifen, an eine Servergruppe zu verweisen und alle anderen Anforderungen an eine zweite Servergruppe zu senden. Damit würde verhindert, dass Browser Ihrer Site Ressourcen binden, die von Clients verwendet werden könnten, die registriert wurden.

Außerdem könnten Sie leistungsstärkere Workstation verwenden, um Services für die Clients zur Verfügung zu stellen, die registriert wurden.

Sie könnten natürlich die oben genannten Methoden kombinieren, um eine noch größere Flexibilität und einen noch besseren Service zu erreichen.

Caching Proxy kommuniziert über die zugehörige Plug-In-Schnittstelle mit CBR. Caching Proxy muss auf derselben Maschine installiert sein. Mehrere Instanzen von Caching Proxy, die auf derselben Maschine ausgeführt werden, können gleichzeitig mit CBR kommunizieren. In früheren Releases konnte nur eine Instanz von Caching Proxy mit CBR kommunizieren.

CBR überprüft zusammen mit Caching Proxy HTTP-Anforderungen anhand angegebener Regeltypen. Wenn Caching Proxy aktiv ist, akzeptiert es Client-Anforderungen und fragt bei CBR den besten Server an. Bei dieser Abfrage gleicht CBR die Anforderung mit einer Gruppe von Regeln mit bestimmten Prioritäten ab. Wenn eine Regel erfüllt ist, wird aus einer vorkonfigurierten Servergruppe ein geeigneter Server ausgewählt. Abschließend teilt CBR Caching Proxy mit, welcher Server ausgewählt wurde. Die Anforderung wird dann an diesen Server weitergeleitet.

Nachdem Sie einen Cluster für den Lastausgleich definiert haben, müssen Sie sicherstellen, dass es für alle Anforderungen an diesen Cluster eine Regel für die Auswahl eines Servers gibt. Wird keine Regel gefunden, die zu einer bestimmten Anforderung passt, empfängt der Client von Caching Proxy eine Fehlerseite. Das Erstellen einer in allen Fällen gültigen Regel mit einer sehr hohen Prioritätsnummer ist der einfachste Weg zu gewährleisten, dass alle Anforderungen mit einer Regel übereinstimmen. Vergewissern Sie sich, dass die von dieser Regel verwendeten Server alle Anforderungen bearbeiten können, die nicht explizit von den Regeln mit einer kleineren Prioritätsnummer bearbeitet werden. (Anmerkung: Die Regeln mit kleinerer Prioritätsnummer werden zuerst ausgewertet.)

Lastausgleich für sichere Verbindungen (SSL)

CBR mit Caching Proxy kann SSL-Übertragungen vom Client zum Proxy empfangen und Übertragungen vom Proxy zu einem SSL-Server unterstützen. Wenn Sie für einen Server der CBR-Konfiguration einen SSL-Port für den Empfang der SSL-Anforderung vom Client definieren, können Sie den Datenverkehr mit CBR auf sichere Server (SSL-Server) verteilen und die Sicherheit Ihrer Site gewährleisten.

Zur Datei `ibmproxy.conf` für IBM Caching Proxy müssen Sie eine Konfigurationsanweisung hinzufügen, um die SSL-Verschlüsselung für Datenverkehr vom Proxy zum Server zu aktivieren. Diese Anweisung muss das folgende Format haben:

```
proxy uri-Muster url-Muster Adresse
```

Hier ist *uri-Muster* ein zu suchendes Muster (z. B. `/secure/*`), *url-Muster* ein Austausch-URL (z. B. `https://ClusterA/secure/*`) und *Adresse* die Cluster-Adresse (z. B. `ClusterA`).

SSL-Datenverkehr vom Client zum Proxy und HTTP-Datenverkehr vom Proxy zum Server verteilen

Die CBR-Komponente mit Caching Proxy kann auch SSL-Übertragungen vom Client empfangen und die SSL-Anfrage vor der Weiterleitung an einen HTTP-Server entschlüsseln. Für den Befehl "cbrcontrol server" gibt es das optionale Schlüsselwort **mapport**, damit CBR SSL-Datenverkehr vom Client zum Proxy und HTTP-Datenverkehr vom Proxy zum Server unterstützen kann. Verwenden Sie dieses Schlüsselwort, wenn der Port auf dem Server ein anderer als der vom Client ankommende Port ist. Nachfolgend sehen Sie ein Beispiel für das Hinzufügen eines Ports mit dem Schlüsselwort "mapport". Der Client-Port ist 443 (SSL) und der Server-Port 80 (HTTP):

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

Die Port-Nummer für "mapport" kann eine beliebige positive ganze Zahl sein. Die Standard-Port-Nummer ist der Wert des vom Client ankommenden Ports.

Da CBR in der Lage sein muss, Empfehlungen zu einer HTTP-Anforderung für einen am Port 443 (SSL) konfigurierten Server zu geben, gibt es die spezielle Advisor-Funktion *ssl2http*. Diese Advisor-Funktion wird an (dem vom Client ankommenden) Port 443 gestartet und gibt Empfehlungen zu den für diesen Port konfigurierten Servern. Wenn zwei Cluster konfiguriert sind und jeder der Cluster den Port 443 und die Server mit einem anderen "mapport" konfiguriert hat, kann eine Instanz der Advisor-Funktion den entsprechenden Port öffnen. Nachfolgend ist ein Beispiel dieser Konfiguration aufgeführt:

```
Executor
  Cluster1
    Port:443
      Server1 mapport 80
      Server2 mapport 8080
  Cluster2
    Port:443
      Server3 mapport 80
      Server4 mapport 8080
  Manager
    Advisor ssl2http 443
```

Kapitel 7. Content Based Routing konfigurieren

Lesen Sie vor Ausführung der in diesem Kapitel beschriebenen Schritte „Kapitel 6. Planung für Content Based Routing“ auf Seite 81. In diesem Kapitel wird erklärt, wie eine Basiskonfiguration für die CBR-Komponente von Network Dispatcher erstellt wird.

- Komplexere Konfigurationen für Network Dispatcher finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Konfigurations-Tasks im Überblick

Anmerkung: Vergewissern Sie sich vor Ausführung der Konfigurationsschritte in dieser Tabelle, dass die CBR-Maschine und alle Servermaschinen mit dem Netz verbunden sind, gültige IP-Adressen haben und sich mit ping-Aufrufen erreichen können.

Tabelle 6. Konfigurations-Tasks für die CBR-Komponente

Task	Beschreibung	Referenzinformationen
CBR-Maschine konfigurieren	Stellen Sie fest, welche Voraussetzungen zu erfüllen sind.	„CBR-Maschine konfigurieren“ auf Seite 93
Am Lastausgleich beteiligte Maschinen konfigurieren	Definieren Sie Ihre Lastausgleichskonfiguration.	„Schritt 7. Am Lastausgleich beteiligte Servermaschinen definieren“ auf Seite 98

Konfigurationsmethoden

Es gibt im Wesentlichen vier Methoden für das Erstellen einer Basiskonfiguration für die CBR-Komponente von Network Dispatcher:

- Befehlszeile
- Scripts
- Grafische Benutzerschnittstelle (GUI)
- Konfigurationsassistent.

Voraussetzung für die Verwendung von CBR ist die Installation von Caching Proxy.

Anmerkung: Caching Proxy ist ein Dienst, der nach der Installation standardmäßig automatisch gestartet wird. Vor dem Starten der CBR-Serverfunktion (cbrserver) müssen Sie Caching Proxy stoppen. Sie sollten den Dienst Caching Proxy so modifizieren, dass er manuell gestartet wird.

- Unter AIX, Linux und Solaris: Stoppen Sie Caching Proxy. Stellen Sie dazu mit dem Befehl `ps -ef|grep ibmproxy` die Prozesskennung des Dienstes fest. Beenden Sie dann den Prozess mit dem Befehl `kill Prozess-ID`.
- Unter Windows: Stoppen Sie Caching Proxy im Fenster "Dienste".

Befehlszeile

Dies ist die direkte Methode für die Konfiguration von CBR. Die Werte der Befehlsparameter müssen in englischen Zeichen eingegeben werden. Die einzige Ausnahme hiervon bilden Host-Namen (die z. B. in den Befehlen "cluster" und "server" verwendet werden) und Dateinamen.

Starten Sie CBR wie folgt von der Befehlszeile aus:

- Setzen Sie als Benutzer "root" an der Eingabeaufforderung den Befehl **cbrserver** ab.

Anmerkung: Mit dem Befehl **cbrserver stop** können Sie den Dienst stoppen.

- Setzen Sie anschließend die gewünschten CBR-Steuerbefehle ab, um die Konfiguration einzurichten. Bei den in diesem Handbuch beschriebenen Prozeduren wird von der Verwendung der Befehlszeile ausgegangen. Der Befehl lautet **cbrcontrol**. Weitere Informationen zu Befehlen finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.
- Starten Sie Caching Proxy. Setzen Sie an der Eingabeaufforderung den Befehl **ibmproxy** ab. (Vor dem Starten von Caching Proxy müssen Sie den Executor starten.)

Anmerkung: Für Windows 2000: Starten Sie Caching Proxy von der Anzeige "Dienste" aus, indem Sie nacheinander auf **Start -> Einstellungen -> Systemsteuerung -> Verwaltung -> Dienste** klicken.

Sie können eine gekürzte Version der Parameter für den Befehl "cbrcontrol" eingeben. Sie müssen nur die eindeutigen Buchstaben der Parameter eingeben.

Beispiel: Wenn Sie Hilfe für den Befehl zum Speichern von Dateien aufrufen möchten, können Sie **cbrcontrol he f** anstelle von **cbrcontrol help file** angeben.

Wenn Sie die Befehlszeilenschnittstelle starten möchten, setzen Sie den Befehl **cbrcontrol** ab, um die Eingabeaufforderung "cbrcontrol" aufzurufen.

Sie können die Befehlszeilenschnittstelle verlassen, indem Sie den Befehl **exit** oder **quit** absetzen.

Anmerkungen:

1. Unter Windows 2000 wird ndserver für die Dispatcher-Komponente automatisch gestartet. Falls Sie nur mit CBR und nicht mit der Dispatcher-Komponente arbeiten, können Sie den automatischen Start von ndserver wie folgt unterbinden:
 - a. Klicken Sie im Fenster "Dienste" von Windows 2000 mit der rechten Maustaste auf "IBM Dispatcher".
 - b. Wählen Sie den Menüeintrag "Eigenschaften" aus.
 - c. Wählen Sie im Feld **Starttyp** die Option "Manuell" aus.
 - d. Klicken Sie auf OK und schließen Sie das Fenster "Dienste".
2. Wenn Sie Content Based Routing (CBR) nicht von der Eingabeaufforderung "cbrcontrol>>" aus, sondern lieber von der Eingabeaufforderung des Betriebssystems aus konfigurieren möchten, seien Sie bei Verwendung der folgenden Zeichen vorsichtig:
 - () linke und rechte runde Klammer
 - & Et-Zeichen
 - | vertikaler Balken
 - ! Ausrufezeichen
 - * Stern.

Die Shell des Betriebssystems könnte diese Zeichen als Sonderzeichen interpretieren und in alternativen Text konvertieren, bevor sie von "cbrcontrol" ausgewertet werden.

Die oben aufgelisteten Sonderzeichen sind optionale Zeichen für den Befehl **cbrcontrol rule add** und werden zum Angeben eines Musters für eine content-Regel verwendet. Der folgende Befehl ist deshalb unter Umständen nur bei Verwendung der Eingabeaufforderung "cbrcontrol>>" gültig.

```
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/*
```

Wenn dieser Befehl an der Eingabeaufforderung des Betriebssystems funktionieren soll, müssen Sie das Muster wie folgt in Anführungszeichen setzen:

```
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/*"
```

Fehlen die Anführungszeichen, könnte beim Speichern der Regel in CBR ein Teil des Musters abgeschnitten werden. An der Eingabeaufforderung "cbrcontrol>>" wird die Verwendung von Anführungszeichen nicht unterstützt.

Scripts

Die Befehle zum Konfigurieren von CBR können in eine Konfigurations-Script-Datei eingegeben und dann zusammen ausgeführt werden.

Anmerkung: Falls Sie den Inhalt einer Script-Datei (z. B. *meinScript*) schnell ausführen möchten, verwenden Sie einen der folgenden Befehle:

- Führen Sie zum Aktualisieren der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:

```
cbrcontrol file appendload meinScript
```

- Führen Sie zum vollständigen Ersetzen der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:

```
cbrcontrol file newload meinScript
```

GUI

Abb. 2 auf Seite 6 zeigt ein Beispiel für die grafische Benutzerschnittstelle (GUI).

Gehen Sie zum Starten der GUI wie folgt vor:

1. Vergewissern Sie sich, dass cbrserver aktiv ist. Setzen Sie an einer Eingabeaufforderung als Benutzer "root" oder Administrator den Befehl **cbrserver** ab.
2. Führen Sie anschließend einen der folgenden Schritte aus:
 - Geben Sie unter AIX, Linux oder Solaris **ndadmin** ein.
 - Klicken Sie unter Windows 2000 nacheinander auf **Start, Programme, IBM WebSphere, Edge Server, IBM Network Dispatcher** und **Network Dispatcher**.
3. Starten Sie Caching Proxy. (Wenn Sie die GUI verwenden, müssen Sie zunächst eine Host-Verbindung herstellen und vor dem Start von Caching Proxy den Executor für die CBR-Komponente starten.) Führen Sie einen der folgenden Schritte aus:

- Unter AIX, Linux oder Solaris: Geben Sie zum Starten von Caching Proxy **ibmproxy** ein.
- Unter Windows 2000: Rufen Sie die Anzeige "Dienste" auf, indem Sie nacheinander auf **Start -> Einstellungen -> Systemsteuerung -> Verwaltung -> Dienste** klicken.

Zum Konfigurieren der Komponente CBR von der GUI aus müssen Sie zunächst in der Baumstruktur **Content Based Routing** auswählen. Sie können den Manager starten, sobald Sie eine Verbindung zu einem Host hergestellt haben. Sie können auch Cluster mit Ports und Servern erstellen und Advisor-Funktionen für den Manager starten.

Mit der GUI können Sie dieselben Tasks wie mit dem Befehl **cbrcontrol** ausführen. Wenn Sie beispielsweise einen Cluster von der Befehlszeile aus konfigurieren möchten, müssten Sie den Befehl **cbrcontrol cluster add Cluster** eingeben. Zum Definieren eines Clusters von der GUI aus müssen Sie mit der rechten Maustaste auf "Executor" klicken und in dem daraufhin angezeigten Popup-Menü mit der linken Maustaste auf **Cluster hinzufügen**. Geben Sie die Cluster-Adresse in das Dialogfenster ein und klicken Sie dann auf **OK**.

Bereits vorhandene CBR-Konfigurationsdateien können Sie mit der im Popup-Menü **Host** angezeigten Option **Neue Konfiguration laden** (zum vollständigen Ersetzen der derzeitigen Konfiguration) oder **An aktuelle Konfiguration anfügen** (zum Aktualisieren der derzeitigen Konfiguration) laden. Sie sollten Ihre CBR-Konfiguration von Zeit zu Zeit mit der Option **Konfigurationsdatei sichern unter** in einer Datei sichern. Diese Option ist ebenfalls im Popup-Menü **Host** enthalten. Über das Menü **Datei** oben auf der GUI können Sie Ihre aktuellen Host-Verbindungen in einer Datei speichern oder Verbindungen aus vorhandenen Dateien aller Network-Dispatcher-Komponenten wiederherstellen.

Sie können auf **Hilfe** zugreifen, indem Sie auf das Fragezeichen in der oberen rechten Ecke des Fensters von Network Dispatcher klicken.

- **Hilfe für Feld** — beschreibt jedes Feld und gibt die Standardwerte an.
- **Vorgehensweise** — listet Tasks auf, die von dieser Anzeige aus ausgeführt werden können.
- **Inhaltsverzeichnis** — zeigt ein Inhaltsverzeichnis mit allen Hilfetexten an.
- **Index** — zeigt einen alphabetischen Index der Hilfethemen an.

Weitere Informationen zur Verwendung der GUI finden Sie im Abschnitt „Allgemeine Anweisungen zur Verwendung der GUI“ auf Seite 7.

Konfigurationsassistent

Führen Sie folgende Schritte aus, wenn Sie den Konfigurationsassistenten verwenden:

1. Starten Sie cbrserver, indem Sie an der Eingabeaufforderung als Root oder Administrator den Befehl **cbrserver** absetzen.

2. Starten Sie wie folgt die Assistentenfunktion von CBR:

Starten Sie den Assistenten von der Eingabeaufforderung aus, indem Sie den Befehl **cbrwizard** absetzen. Sie können den Konfigurationsassistenten auch im CBR-Komponentenmenü auswählen, das auf der GUI angezeigt wird.

3. Starten Sie Caching Proxy zum Verteilen des HTTP- oder HTTPS-Datenverkehrs (SSL).

Unter AIX, Linux oder Solaris: Geben Sie zum Starten von Caching Proxy **ibmproxy** ein.

Unter Windows 2000: Rufen Sie die Anzeige "Dienste" auf, indem Sie nacheinander auf **Start -> Einstellungen -> Systemsteuerung -> Verwaltung -> Dienste** klicken.

Der CBR-Assistent führt Sie schrittweise durch den Prozess zum Erstellen einer Basiskonfiguration für die CBR-Komponente. Der Assistent stellt Ihnen Fragen bezüglich Ihres Netzes und führt Sie durch die Konfiguration eines Clusters, mit dem CBR den Datenverkehr auf eine Gruppe von Servern verteilen kann.

Der CBR-Konfigurationsassistent ruft die folgenden Anzeigen auf:

- Einführung in den Assistenten
- Was Sie erwarten können
- Vor dem Beginn
- Auswahl eines Hosts für die Konfiguration (falls erforderlich)
- Cluster definieren
- Port hinzufügen
- Server hinzufügen
- Regel hinzufügen
- Advisor starten.

CBR-Maschine konfigurieren

Vor dem Konfigurieren der CBR-Maschine müssen Sie (unter AIX, Linux oder Solaris) als Benutzer "root" oder (unter Windows 2000) als Administrator registriert sein.

Sie benötigen für jeden zu konfigurierenden Server-Cluster eine IP-Adresse. Eine Cluster-Adresse ist eine Adresse, die einem Host-Namen zugeordnet ist (beispielsweise `www.company.com`). Diese IP-Adresse wird von einem Client benutzt, um eine Verbindung zu den Servern eines Clusters herzustellen. Diese Adresse ist in der URL-Anforderung von dem Client enthalten. CBR verteilt alle Anforderungen, die an dieselbe Cluster-Adresse gerichtet sind.

Für Solaris: Vor Verwendung der Komponente CBR müssen die Systemstandardwerte für die prozessübergreifende Kommunikation (Inter-process Communication) geändert werden. Die maximale Größe des gemeinsam benutzten Speichersegments und die Anzahl von Semaphor-Kennungen müssen erhöht werden. Sie können Ihr System auf die Unterstützung für CBR einstellen, indem Sie die Datei `/etc/system` auf Ihrem System editieren und die folgenden Anweisungen hinzufügen, bevor Sie dann einen Warmstart durchführen:

```
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_semtime=30
```

Wenn Sie das gemeinsam benutzte Speichersegment nicht auf die oben gezeigten Werte vergrößern, kann der Befehl `cbrcontrol executor start` nicht ausgeführt werden.

Schritt 1. Caching Proxy für die Verwendung von CBR konfigurieren

Voraussetzung für die Verwendung von CBR ist die Installation von Caching Proxy.

Anmerkung: Caching Proxy ist ein Dienst, der nach der Installation standardmäßig automatisch gestartet wird. Vor dem Starten der CBR-Serverfunktion müssen Sie Caching Proxy stoppen. Sie sollten den Dienst Caching Proxy so modifizieren, dass er manuell gestartet wird.

- Unter AIX, Linux und Solaris: Stoppen Sie Caching Proxy. Stellen Sie dazu mit dem Befehl `ps -ef|grep ibmproxy` die Prozesskennung des Dienstes fest. Beenden Sie dann den Prozess mit dem Befehl `kill Prozess-ID`.
- Unter Windows: Stoppen Sie Caching Proxy im Fenster "Dienste".

Die Konfigurationsdatei für Caching Proxy (ibmproxy.conf) müssen Sie wie folgt ändern:

Setzen Sie die Anweisung für ankommenden URL **CacheByIncomingUrl** auf "on".

Für das CBR-Plug-In müssen Sie vier Einträge editieren:

- ServerInit
- PreExit
- PostExit
- ServerTerm

Jeder Eintrag muss sich jeweils in einer neuen Zeile befinden. Die Datei ibmproxy.conf enthält mehrere Einträge "ServerInit", einen für jedes Plug-In. Die Einträge für das CBR-Plug-In müssen editiert werden. Außerdem müssen Sie das Kommentarzeichen löschen.

Nachfolgend sehen Sie die spezifischen Zusätze zur Konfigurationsdatei für AIX, Linux, Solaris und Windows 2000.

Abbildung 16. CBR-Konfigurationsdatei für 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
```

Abbildung 17. CBR-Konfigurationsdatei für 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
```


Abbildung 18. CBR-Konfigurationsdatei für 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
```

Abbildung 19. CBR-Konfigurationsdatei für Windows 2000

Allgemeiner Installationsverzeichnispfad:

```
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
```

Interner Installationsverzeichnispfad:

```
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
```

Schritt 2. Serverfunktion starten

Anmerkung: Caching Proxy ist ein Dienst, der nach der Installation standardmäßig automatisch gestartet wird. Vor dem Starten der CBR-Serverfunktion müssen Sie Caching Proxy stoppen. Sie sollten den Dienst Caching Proxy so modifizierten, dass er manuell gestartet wird.

- Unter AIX, Linux und Solaris: Stoppen Sie Caching Proxy. Stellen Sie dazu mit dem Befehl `ps -ef|grep ibmproxy` die Prozesskennung des Dienstes fest. Beenden Sie dann den Prozess mit dem Befehl `kill Prozess-ID`.
- Unter Windows: Stoppen Sie Caching Proxy im Fenster "Dienste".

Geben Sie zum Starten der CBR-Serverfunktion in der Befehlszeile **cbrserver** ein.

Beim Starten von `cbrserver` wird automatisch eine Standardkonfigurationsdatei (`default.cfg`) geladen. Wenn Sie die CBR-Konfiguration in `default.cfg` sichern, werden alle in dieser Datei gesicherten Angaben beim nächsten Starten von `cbrserver` automatisch geladen.

Schritt 3. Executor-Funktion starten

Geben Sie zum Starten der Executor-Funktion den Befehl **cbrcontrol executor start** ein. Sie können jetzt auch verschiedene Executor-Einstellungen ändern. Lesen Sie hierzu die Informationen im Abschnitt „`ndcontrol executor` — Executor steuern“ auf Seite 280.

Schritt 4. Cluster definieren und Cluster-Optionen festlegen

CBR verteilt die an die Cluster-Adresse gesendeten Anforderungen auf die entsprechenden Server, die für die Ports dieses Clusters konfiguriert wurden.

Die Cluster-Adresse ist entweder ein symbolischer Name oder eine Adresse in Schreibweise mit Trennzeichen. Diese Adresse ist im Host-Abschnitt des URL enthalten.

Setzen Sie zum Definieren eines Clusters den folgenden Befehl ab:

```
cbrcontrol cluster add Cluster
```

Setzen Sie zum Festlegen von Cluster-Optionen den folgenden Befehl ab:

```
cbrcontrol cluster set Wert_der_Cluster-Option
```

Weitere Informationen hierzu finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Schritt 5. Aliasnamen für die Netzschnittstellenkarte erstellen (optional)

Wenn Sie Caching Proxy als Reverse Proxy konfiguriert haben und einen Lastausgleich für mehrere Websites durchführen, müssen Sie die Cluster-Adresse jeder Website zu mindestens einer Netzschnittstellenkarte der Network-Dispatcher-Maschine hinzufügen. Andernfalls kann dieser Schritt übergangen werden.

Unter AIX, Linux oder Solaris: Fügen Sie die Cluster-Adresse mit dem Befehl „`ifconfig`“ zur Netzschnittstellenkarte hinzu. Den Befehl für das von Ihnen verwendete Betriebssystem können Sie Tabelle 7 auf Seite 97 entnehmen.

Tabelle 7. Befehle zum Erstellen eines Aliasnamens für die NIC

AIX	ifconfig <i>Schnittstellename</i> alias <i>Cluster-Adresse</i> netmask <i>Netzmaske</i>
Linux	ifconfig <i>Schnittstellename</i> <i>Cluster-Adresse</i> netmask <i>Netzmaske</i> up
Solaris 7	ifconfig <i>Schnittstellename</i> <i>Cluster-Adresse</i> netmask <i>Netzmaske</i> up
Solaris 8	ifconfig addif <i>Schnittstellename</i> <i>Cluster-Adresse</i> netmask <i>Netzmaske</i> up

Anmerkung: Unter Linux und Solaris muss der *Schnittstellename* für jede hinzugefügte Cluster-Adresse eine eindeutige Nummer haben, z. B. eth0:1, eth0:2 usw.

Für Windows: Gehen Sie zum Hinzufügen der Cluster-Adresse zur Netz-schnittstelle wie folgt vor:

1. Klicken Sie auf **Start, Einstellungen** und dann auf **Systemsteuerung**.
2. Klicken Sie doppelt auf **Netzwerk- und DFÜ-Verbindungen**.
3. Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung**.
4. Wählen Sie den Eintrag **Eigenschaften** aus.
5. Wählen Sie **Internetprotokoll (TCP/IP)** aus und klicken Sie auf **Eigenschaften**.
6. Wählen Sie **Folgende IP-Adresse verwenden** aus und klicken Sie auf **Erweitert**.
7. Klicken Sie auf **Hinzufügen**. Geben Sie dann die **IP-Adresse** und die **Subnetzmaske** für den Cluster ein.

Schritt 6. Ports definieren und Port-Optionen festlegen

Die Port-Nummer bezeichnet den Port, an dem die Serveranwendungen empfangsbereit sind. Für HTTP-Datenverkehr ist dies bei Verwendung von CBR mit Caching Proxy in der Regel Port 80.

Setzen Sie den folgenden Befehl ab, um für den im vorherigen Schritt definierten Cluster einen Port zu definieren:

```
cbrcontrol port add Cluster:Port
```

Setzen Sie zum Festlegen von Port-Optionen den folgenden Befehl ab:

```
cbrcontrol port set Cluster:Wert_der_Port-Option
```

Weitere Informationen hierzu finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Schritt 7. Am Lastausgleich beteiligte Servermaschinen definieren

Die Servermaschinen sind die Maschinen, auf denen die Anwendungen ausgeführt werden, deren Last verteilt werden soll. Für den *Server* wird der symbolische Name der Servermaschine oder deren Adresse in Schreibweise mit Trennzeichen angegeben. Setzen Sie den folgenden Befehl ab, um für Cluster und Port einen Server zu definieren:

```
cbrcontrol server add Cluster:Port:Server
```

Für einen Cluster müssen Sie pro Port mehrere Server definieren, um einen Lastausgleich durchführen zu können.

Schritt 8. Regeln zur Konfiguration hinzufügen

Dies ist der wichtigste Schritt beim Konfigurieren von CBR mit Caching Proxy. Mit einer Regel wird definiert, wie zwischen URL-Anforderungen unterschieden wird und wie eine Anforderung an die entsprechende Gruppe von Servern gesendet wird. Der spezielle von CBR verwendete Regeltyp ist 'content'. Setzen Sie zum Definieren einer content-Regel den folgenden Befehl ab:

```
cbrcontrol rule  
add Cluster:Port:Regel type content pattern=Muster
```

Der Wert *Muster* ist der reguläre Ausdruck, der mit dem URL in den einzelnen Client-Anforderungen verglichen wird. Weitere Informationen über zum Konfigurieren des Musters finden Sie in „Anhang C. Syntax der content-Regel“ auf Seite 331.

Einige der anderen in Dispatcher definierten Regeltypen können ebenfalls für CBR verwendet werden. Weitere Informationen hierzu finden Sie im Abschnitt „Regelbasierten Lastausgleich konfigurieren“ auf Seite 185.

Schritt 9. Server zu den Regeln hinzufügen

Wenn für eine Client-Anforderung eine Übereinstimmung mit einer Regel gefunden wird, wird bei der der Regel zugeordneten Servergruppe der beste Server abgefragt. Die der Regel zugeordnete Servergruppe ist eine Untergruppe der Server, die für den Port definiert sind. Setzen Sie den folgenden Befehl ab, um Server zur Servergruppe einer Regel hinzuzufügen:

```
cbrcontrol rule useserver Cluster:Port:Regel server
```

Schritt 10. Manager-Funktion starten (optional)

Die Manager-Funktion verbessert den Lastausgleich. Setzen Sie zum Starten des Managers den folgenden Befehl ab:

```
cbrcontrol manager start
```

Schritt 11. Advisor-Funktion starten (optional)

Die Advisor-Funktionen liefern dem Manager weitere Informationen über die Fähigkeit der am Lastausgleich beteiligten Servermaschinen, auf Anforderungen zu antworten. Advisor-Funktionen sind protokollspezifisch. Soll beispielsweise die HTTP-Advisor-Funktion gestartet werden, setzen Sie den folgenden Befehl ab:

```
cbrcontrol advisor start http Port
```

Schritt 12. Cluster-Proportionen festlegen

Wenn Sie Advisor-Funktionen starten, können Sie die Wichtigkeit ändern, die in Entscheidungen für den Lastausgleich einfließenden Informationen von Advisor-Funktionen beigemessen wird. Setzen Sie zum Festlegen von Cluster-Proportionen den Befehl **cbrcontrol cluster set *Cluster proportions*** ab. Weitere Informationen hierzu finden Sie im Abschnitt „Proportionale Bedeutung von Statusinformationen“ auf Seite 145.

Schritt 13. Caching Proxy starten

- AIX-Plattform: Fügen Sie Folgendes zur Umgebungsvariablen LIBPATH hinzu:

```
/usr/lpp/nd/servers/lib
```

- Linux- oder Solaris-Plattform: Fügen Sie Folgendes zur Umgebungsvariablen LD_LIBRARY_PATH hinzu:

```
/opt/nd/servers/lib
```

- Windows-2000-Plattform: Fügen Sie Folgendes zur Umgebungsvariablen PATH hinzu:

Allgemeiner Installationsverzeichnispfad:

```
c:\Programme\IBM\edge\nd\servers\lib
```

Interner Installationsverzeichnispfad:

```
c:\Programme\IBM\nd\servers\lib
```

Starten Sie Caching Proxy in der neuen Umgebung, indem Sie an der Eingabeaufforderung den Befehl **ibmproxy** absetzen.

Anmerkung: Für Windows 2000: Starten Sie Caching Proxy von der Anzeige "Dienste" aus, indem Sie nacheinander auf **Start -> Einstellungen -> Systemsteuerung -> Verwaltung -> Dienste** klicken.

CBR-Konfigurationsbeispiel

Führen Sie die folgenden Schritte aus, um CBR zu konfigurieren:

1. Starten Sie CBR durch Absetzen des Befehls **cbrserver**.
2. Starten Sie die Befehlszeilenschnittstelle. Setzen Sie dazu den Befehl **cbrcontrol** ab.
3. Die Eingabeaufforderung **cbrcontrol** wird angezeigt. Setzen Sie die folgenden Befehle ab (*Cluster(c),Port(p),Regel(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 useserver c:p:r s`
4. Starten Sie Caching Proxy durch Absetzen des Befehls **ibmproxy**. (Unter Windows 2000 müssen Sie Caching Proxy von der Anzeige "Dienste" aus starten.)
5. Entfernen Sie alle Proxy-Konfigurationen aus dem Browser.
6. Laden Sie `http://c/` in Ihren Browser. Hier steht "c" für den Cluster, den Sie mit einem der vorherigen Schritte konfiguriert haben.
 - Server "s" wird aufgerufen.
 - Es wird die Webseite `http://s/` angezeigt.

Kapitel 8. Planung für Mailbox Locator

In diesem Kapitel wird beschrieben, was die für die Planung des Netzes zuständige Person vor der Installation und Konfiguration der Komponente Mailbox Locator berücksichtigen muss.

Anmerkung: Die Komponente Mailbox Locator war früher Bestandteil der CBR-Komponente und wurde bei IMAP- und POP3-Postservern für einen Lastausgleich ausgehend von Benutzer-ID und Kennwort verwendet. Durch die Untergliederung von CBR in zwei Komponenten *entfällt* die Einschränkung, dass "CBR für IMAP/POP3" (Mailbox Locator) und "CBR für HTTP/HTTPS" (CBR mit Caching Proxy) nicht auf einer Maschine ausgeführt werden können.

- Informationen zum Konfigurieren der Lastausgleichparameter von Mailbox Locator finden Sie in „Kapitel 9. Mailbox Locator konfigurieren“ auf Seite 105.
- Informationen zum Konfigurieren von Network Dispatcher für erweiterte Funktionen finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Dieses Kapitel enthält die folgenden Abschnitte:

- „Hardware- und Softwarevoraussetzungen“
- „Überlegungen bei der Planung“ auf Seite 102

Hardware- und Softwarevoraussetzungen

- für AIX finden Sie im Abschnitt „Voraussetzungen für AIX“ auf Seite 12.
- für Linux finden Sie im Abschnitt „Voraussetzungen für Red Hat Linux oder SuSE Linux“ auf Seite 17.
- für Solaris finden Sie im Abschnitt „Voraussetzungen für Solaris“ auf Seite 21.
- für Windows 2000 finden Sie im Abschnitt „Voraussetzungen für Windows 2000“ auf Seite 23.

Überlegungen bei der Planung

Mit Mailbox Locator können Sie IMAP- und POP3-Datenverkehr ausgehend von Benutzer-ID und Kennwort der Client-Anforderung weiterleiten.

Mailbox Locator ist Dispatcher hinsichtlich der Komponentenstruktur sehr ähnlich. Mailbox Locator stellt die folgenden Funktionen bereit:

- Der **mlserver** bearbeitet Anforderungen von der Befehlszeile an den Executor, den Manager und die Advisor-Funktionen.
- Der **Executor** unterstützt die Verteilung von Client-Anforderungen. Der Executor ist immer aktiv, wenn die Komponente Mailbox Locator verwendet wird.
- Der **Manager** definiert Wertigkeiten, die vom Executor verwendet werden und auf folgenden Kriterien basieren:
 - interne Zähler des Executors
 - von den Advisor-Funktionen bereitgestellte Rückmeldungen von den Servern
 - Rückmeldungen von einem Systemüberwachungsprogramm wie Metric Server.

Die Benutzung des Managers ist optional. Ohne den Manager wird der Lastausgleich nach einer gewichteten RoundRobin-Zeitplanung und ausgehend von den aktuellen Serverwertigkeiten durchgeführt. Es stehen keine Advisor-Funktionen zur Verfügung.

- Die **Advisor** fragen die Server ab und analysieren die Ergebnisse nach Protokoll, bevor sie den Manager zum Festlegen der entsprechenden Wertigkeiten aufrufen. Es ist nicht immer sinnvoll, einige dieser Advisor-Funktionen in einer typischen Konfiguration zu verwenden. Sie können auch eigene Advisor-Funktionen schreiben. Die Benutzung der Advisor-Funktionen ist optional, wird jedoch empfohlen. Weitere Informationen hierzu finden Sie im Abschnitt „Advisor-Funktionen“ auf Seite 149.
- Zum Konfigurieren und Verwalten des Executors, der Advisor-Funktionen und des Managers können Sie die Befehlszeile (**mlcontrol**) oder die grafische Benutzerschnittstelle (**ndadmin**) verwenden.

Die drei wichtigsten Funktionen von Mailbox Locator (Executor, Manager und Advisor-Funktionen) arbeiten gemeinsam an der Verteilung der eingehenden Anforderungen auf die Server. Neben dem Verteilen von Anforderungen überwacht der Executor die Anzahl neuer und aktiver Verbindungen. Diese Informationen stellt er anschließend dem Manager zur Verfügung.

Setzen Sie an der Eingabeaufforderung den Befehl **mlserver** ab.

Mailbox Locator kann ein Anlaufpunkt für viele IMAP- oder POP3-Server sein. Jeder Server kann eine Untergruppe aller Mailboxes haben, die von dem Ansprechpartner bedient werden. Für IMAP und POP3 ist Mailbox Locator ein Proxy, der ausgehend von der vom Client bereitgestellten Benutzer-ID mit Kennwort einen geeigneten Server auswählt.

Anmerkung: Mailbox Locator bietet *keine* Unterstützung für den regelgestützten Lastausgleich.

Nachfolgend finden Sie eine Beispielmethode für die Verteilung von Anforderungen ausgehend von der Client-Benutzer-ID. Wenn Sie zwei (oder mehr) POP3-Server haben, können Sie die Mailboxes bei Bedarf in alphabetischer Reihenfolge nach Benutzer-IDs unterteilen. Client-Anforderungen mit Benutzer-IDs, die mit den Buchstaben A-I beginnen, können an Server 1 weitergegeben werden, Client-Anforderungen mit Benutzer-IDs, die mit den Buchstaben J-R beginnen, an Server 2 usw.

Sie können auch auswählen, dass jede Mailbox auf mehreren Servern vorhanden ist. In diesem Fall muss der Inhalt jeder Mailbox für alle Server mit dieser Mailbox verfügbar sein. Bei einem Serverausfall kann ein anderer Server dennoch auf die Mailbox zugreifen.

Falls mehrere POP3-Postserver von nur einer Adresse repräsentiert werden sollen, kann Mailbox Locator mit einer Cluster-Adresse konfiguriert werden, die zur POP3-Postserveradresse für alle Clients wird. Die folgenden Befehle werden für diese Konfiguration verwendet:

```
mlcontrol cluster add POP3-Postserver
mlcontrol port add POP3-Postserver:110 protocol pop3
mlcontrol server add POP3-Postserver:110:POP3-Server1+POP3-Server2+POP3-Server3
```

In diesem Beispiel repräsentiert *POP3-Postserver* die Cluster-Adresse. Port 110 mit dem Weiterleitungsprotokoll POP3 wird zum *POP3-Postserver* hinzugefügt. *POP3-Server1*, *POP3-Server2* und *POP3-Server3* sind POP3-Postserver, die zum Port hinzugefügt werden. Bei dieser Konfiguration können Sie die eingehenden POP3-Anforderungen Ihrer Post-Clients mit der Cluster-Adresse *POP3-Postserver* konfigurieren.

Affinitätsfunktion verwenden

Wenn eine POP3- oder IMAP-Anforderung beim Proxy ankommt, versucht dieser, unter Verwendung von Benutzer-ID und Kennwort der Client-Anforderung alle für den Port konfigurierten Server zu erreichen. Die Client-Anforderung wird an den ersten Server gesendet, der antwortet. Sie sollten Mailbox Locator für IMAP- oder POP3-Server in Verbindung mit der Halte- bzw. Affinitätsfunktion verwenden. Mit der Affinitätsfunktion können nachfolgende Anforderungen mit derselben Client-Benutzer-ID an denselben Server übertragen werden. Setzen Sie **stickytime** für den Port auf einen Wert größer als null, um diese Affinitätsfunktion zu aktivieren. Weitere Informationen zur Affinitätsfunktion finden Sie im Abschnitt „Funktionsweise der Affinität für Network Dispatcher“ auf Seite 202.

Inaktivitätszeitgeber für POP3/IMAP überschreiben

Bei den Protokollen POP3 und IMAP liegt das Zeitlimit für autologout bei Inaktivität bei mindestens 10 Minuten bzw. 30 Minuten. Dieses Zeitlimit legt die Zeit der Inaktivität in Sekunden fest, nach der eine Verbindung entfernt wird. Für einen optimalen Durchsatz überschreibt Mailbox Locator das Inaktivitätszeitlimit und setzt es auf 60 Sekunden. Sie können das Inaktivitätszeitlimit ändern, indem Sie für den Befehl **mlcontrol port** den Wert **staletime-out** ändern. Informationen zum Konfigurieren dieses Befehls finden Sie im Abschnitt „ndcontrol port — Ports konfigurieren“ auf Seite 305.

Kapitel 9. Mailbox Locator konfigurieren

Lesen Sie vor Ausführung der in diesem Kapitel beschriebenen Schritte „Kapitel 8. Planung für Mailbox Locator“ auf Seite 101. Dieses Kapitel erläutert das Erstellen einer Basiskonfiguration für die Komponente Mailbox Locator von Network Dispatcher.

Anmerkung: Die Komponente Mailbox Locator war früher Bestandteil der CBR-Komponente und wurde bei IMAP- und POP3-Postservern für einen Lastausgleich ausgehend von Benutzer-ID und Kennwort verwendet. Durch die Untergliederung von CBR in zwei Komponenten *entfällt* die Einschränkung, dass "CBR für IMAP/POP3" (Mailbox Locator) und "CBR für HTTP/HTTPS" (CBR mit Caching Proxy) nicht auf einer Maschine ausgeführt werden können.

- Komplexere Konfigurationen für Network Dispatcher finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Übersicht über die Konfigurations-Tasks

Anmerkung: Vergewissern Sie sich vor Ausführung der Konfigurationsschritte in dieser Tabelle, dass die Mail-Locator-Maschine und alle Servermaschinen mit dem Netz verbunden sind, gültige IP-Adressen haben und sich gegenseitig durch ping-Aufrufe erreichen können.

Tabelle 8. Konfigurations-Tasks für Mailbox Locator

Task	Beschreibung	Referenzinformationen
Maschine mit Mailbox Locator konfigurieren	Stellen Sie fest, welche Voraussetzungen zu erfüllen sind.	„Maschine mit Mailbox Locator konfigurieren“ auf Seite 109
Am Lastausgleich beteiligte Maschinen konfigurieren	Definieren Sie Ihre Lastausgleichskonfiguration.	„Schritt 4. Am Lastausgleich beteiligte Servermaschinen definieren“ auf Seite 110

Konfigurationsmethoden

Es gibt im Wesentlichen vier Methoden für das Erstellen einer Basiskonfiguration für die Komponente Mailbox Locator von Network Dispatcher:

- Befehlszeile
- Scripts
- Grafische Benutzerschnittstelle (GUI)
- Konfigurationsassistent.

Befehlszeile

Dies ist die direkte Methode für die Konfiguration von Mailbox Locator. Die Werte der Befehlsparameter müssen in englischen Zeichen eingegeben werden. Die einzige Ausnahme hiervon bilden Host-Namen (die z. B. in den Befehlen "cluster" und "server" verwendet werden) und Dateinamen.

Starten Sie Mailbox Locator wie folgt von der Befehlszeile aus:

- Setzen Sie an der Eingabeaufforderung den Befehl **mlserver** ab.

Anmerkung: Mit dem Befehl **mlserver stop** können Sie den Dienst stoppen.

- Setzen Sie anschließend die gewünschten Steuerbefehle für Mailbox Locator ab, um die Konfiguration einzurichten. Bei den in diesem Handbuch beschriebenen Prozeduren wird von der Verwendung der Befehlszeile ausgegangen. Der Befehl lautet **mlcontrol**. Weitere Informationen zu Befehlen finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Sie können eine Minimalversion der Parameter für den Befehl "mlcontrol" eingeben. Sie müssen nur die eindeutigen Buchstaben der Parameter eingeben. Beispiel: Wenn Sie Hilfe für den Befehl zum Speichern von Dateien aufrufen möchten, können Sie **mlcontrol h e f** anstelle von **mlcontrol help file** angeben.

Wenn Sie die Befehlszeilenschnittstelle starten möchten, setzen Sie den Befehl **mlcontrol** ab, um die Eingabeaufforderung "mlcontrol" aufzurufen.

Sie können die Befehlszeilenschnittstelle verlassen, indem Sie den Befehl **exit** oder **quit** absetzen.

Anmerkung: Unter Windows 2000 wird ndserver für die Dispatcher-Komponente automatisch gestartet. Falls Sie nur mit Mailbox Locator und nicht mit der Dispatcher-Komponente arbeiten, können Sie den automatischen Start von ndserver wie folgt unterbinden:

1. Klicken Sie im Fenster "Dienste" von Windows 2000 mit der rechten Maustaste auf "IBM Dispatcher".
2. Wählen Sie den Menüeintrag "Eigenschaften" aus.

3. Wählen Sie im Feld **Starttyp** die Option "Manuell" aus.
4. Klicken Sie auf OK und schließen Sie das Fenster "Dienste".

Scripts

Die Befehle zum Konfigurieren von Mailbox Locator können in eine Konfigurations-Script-Datei eingegeben und dann zusammen ausgeführt werden.

Anmerkung: Falls Sie den Inhalt einer Script-Datei (z. B. *meinScript*) schnell ausführen möchten, verwenden Sie einen der folgenden Befehle:

- Führen Sie zum Aktualisieren der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:

```
mlcontrol file appendload meinScript
```

- Führen Sie zum vollständigen Ersetzen der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:

```
mlcontrol file newload meinScript
```

GUI

Ein Beispiel für die GUI zeigt Abb. 2 auf Seite 6.

Gehen Sie zum Starten der GUI wie folgt vor:

1. Vergewissern Sie sich, dass **mlserver** aktiv ist. Setzen Sie an einer Eingabeaufforderung als Benutzer "root" oder Administrator den Befehl **mlserver** ab.
2. Führen Sie anschließend einen der folgenden Schritte aus:
 - Geben Sie unter AIX, Linux oder Solaris **ndadmin** ein.
 - Klicken Sie unter Windows 2000 nacheinander auf **Start, Programme, IBM WebSphere, Edge Server, IBM Network Dispatcher** und **Network Dispatcher**.

Zum Konfigurieren von Mailbox Locator auf der GUI müssen Sie zunächst in der Baumstruktur **Mailbox Locator** auswählen. Sie können den Manager starten, sobald Sie eine Verbindung zu einem Host hergestellt haben. Sie können auch Cluster mit Ports und Servern erstellen und Advisor-Funktionen für den Manager starten.

Mit der GUI können Sie dieselben Tasks wie mit dem Befehl **mlcontrol** ausführen. Wenn Sie beispielsweise einen Cluster von der Befehlszeile aus konfigurieren möchten, müssten Sie den Befehl **mlcontrol cluster add Cluster** eingeben. Zum Definieren eines Clusters von der GUI aus müssen Sie mit der rechten Maustaste auf "Executor" klicken und im daraufhin angezeigten Popup-Menü mit der linken Taste auf **Cluster hinzufügen**. Geben Sie die Cluster-Adresse in das Dialogfenster ein und klicken Sie dann auf **OK**.

Bereits vorhandene Konfigurationsdateien für Mailbox Locator können Sie mit der im Popup-Menü **Host** angezeigten Option **Neue Konfiguration laden** (zum vollständigen Ersetzen der derzeitigen Konfiguration) oder **An aktuelle Konfiguration anfügen** (zum Aktualisieren der derzeitigen Konfiguration) laden. Sie sollten Ihre Mailbox-Locator-Konfiguration von Zeit zu Zeit mit der Option **Konfigurationsdatei sichern unter** in einer Datei sichern. Diese Option ist ebenfalls im Popup-Menü **Host** enthalten. Über das Menü **Datei** oben auf der GUI können Sie Ihre aktuellen Host-Verbindungen in einer Datei speichern oder Verbindungen aus vorhandenen Dateien aller Network-Dispatcher-Komponenten wiederherstellen.

Sie können auf **Hilfe** zugreifen, indem Sie auf das Fragezeichen in der oberen rechten Ecke des Fensters von Network Dispatcher klicken.

- **Hilfe für Feld** — beschreibt jedes Feld und gibt die Standardwerte an.
- **Vorgehensweise** — listet Tasks auf, die von dieser Anzeige aus ausgeführt werden können.
- **Inhaltsverzeichnis** — zeigt ein Inhaltsverzeichnis mit allen Hilfetexten an.
- **Index** — zeigt einen alphabetischen Index der Hilfethemen an.

Weitere Informationen zur Verwendung der GUI finden Sie im Abschnitt „Allgemeine Anweisungen zur Verwendung der GUI“ auf Seite 7.

Konfigurationsassistent

Führen Sie folgende Schritte aus, wenn Sie den Konfigurationsassistenten verwenden:

1. Setzen Sie an der Eingabeaufforderung als Root oder Administrator den Befehl **mlserver** ab.
2. Starten Sie die Assistentenfunktion von Mailbox Locator, **mlwizard**.
Sie können den Assistenten von der Eingabeaufforderung aus starten, indem Sie den Befehl **mlwizard** absetzen. Sie können den Konfigurationsassistenten aber auch auf der GUI unter der Komponente Mailbox Locator auswählen.

Der Mailbox-Locator-Assistent führt Sie schrittweise durch den Prozess zum Erstellen einer Basiskonfiguration für die Komponente Mailbox Locator. Er stellt Ihnen Fragen zu Ihrem Netz und leitet Sie beim Konfigurieren eines Clusters an, mit dem Mailbox Locator den Datenverkehr auf eine Gruppe von Servern verteilen kann.

Bei Verwendung des Konfigurationsassistenten für Mailbox Locator erscheinen die folgenden Anzeigen:

- Einführung in den Assistenten
- Was Sie erwarten können
- Vor dem Beginn

- Auswahl eines Hosts für die Konfiguration (falls erforderlich)
- Cluster definieren
- Port hinzufügen
- Server hinzufügen
- Advisor starten

Maschine mit Mailbox Locator konfigurieren

Vor dem Konfigurieren der Maschine mit Mailbox Locator müssen Sie (unter AIX, Linux oder Solaris) als Benutzer "root" oder (unter Windows 2000) als Administrator registriert sein.

Sie benötigen für jeden zu konfigurierenden Server-Cluster eine IP-Adresse. Eine Cluster-Adresse ist eine Adresse, die einem Host-Namen zugeordnet ist (beispielsweise `www.IhreFirma.com`). Diese IP-Adresse wird von einem Client benutzt, um die Verbindung zu den Servern in einem Cluster herzustellen. Mailbox Locator verteilt alle Anforderungen, die an dieselbe Cluster-Adresse gerichtet sind.

Schritt 1. Serverfunktion starten

Geben Sie zum Starten der Serverfunktion in der Befehlszeile **mlserver** ein.

Anmerkung: Beim Starten von "mlserver" wird automatisch eine Standard-konfigurationsdatei (`default.cfg`) geladen. Entscheidet der Benutzer, dass die Konfiguration in `default.cfg` gesichert werden soll, werden alle in dieser Datei gesicherten Angaben beim nächsten Starten von "mlserver" automatisch geladen.

Schritt 2. Cluster definieren und Cluster-Optionen festlegen

Mailbox Locator verteilt die an die Cluster-Adresse gesendeten Anforderungen auf die entsprechenden Server, die für die Ports dieses Clusters konfiguriert sind.

Die Cluster-Adresse ist ein symbolischer Name oder eine Adresse in Schreibweise mit Trennzeichen.

Setzen Sie zum Definieren eines Clusters den folgenden Befehl ab:

```
mlcontrol cluster add Cluster
```

Setzen Sie zum Festlegen von Cluster-Optionen den folgenden Befehl ab:

```
mlcontrol cluster set Wert_der_Cluster-Option
```

Weitere Informationen hierzu finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Schritt 3. Ports definieren und Port-Optionen festlegen

Die Port-Nummer bezeichnet den Port, an dem die Serveranwendungen empfangsbereit sind. Für IMAP-Datenverkehr ist dies in der Regel Port 143 und für POP3-Datenverkehr Port 110.

Setzen Sie den folgenden Befehl ab, um für den im vorherigen Schritt definierten Cluster einen Port zu definieren:

```
mlcontrol port add Cluster:Port protocol [pop3|imap]
```

Setzen Sie zum Festlegen von Port-Optionen den folgenden Befehl ab:

```
mlcontrol port set Cluster:Wert_der_Port-Option
```

Anmerkung: Wenn Sie einen Port hinzufügen, müssen Sie das Proxy-Protokoll angeben (pop3 oder imap). Nach dem Hinzufügen des Ports können Sie den vorhandenen Protokollwert für diesen Port nicht mehr ändern (festlegen).

Weitere Informationen hierzu finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Schritt 4. Am Lastausgleich beteiligte Servermaschinen definieren

Die Postserver sind die Maschinen, auf denen die Anwendungen ausgeführt werden, für die Sie einen Lastausgleich durchführen möchten. Für den *Server* wird der symbolische Name der Servermaschine oder deren Adresse in Schreibweise mit Trennzeichen angegeben. Setzen Sie zum Definieren eines Servers für den Cluster und Port aus Schritt 3 den folgenden Befehl ab:

```
mlcontrol server add Cluster:Port:Server
```

Für einen Cluster müssen Sie pro Port mehrere Server definieren, um einen Lastausgleich durchführen zu können.

Schritt 5. Manager-Funktion starten (optional)

Die Manager-Funktion verbessert den Lastausgleich. Setzen Sie zum Starten des Managers den folgenden Befehl ab:

```
mlcontrol manager start
```

Schritt 6. Advisor-Funktion starten (optional)

Die Advisor-Funktionen liefern dem Manager weitere Informationen über die Fähigkeit der am Lastausgleich beteiligten Servermaschinen, auf Anforderungen zu antworten. Advisor-Funktionen sind protokollspezifisch. Network Dispatcher stellt eine IMAP- und eine POP3-Advisor-Funktion bereit. Zum Starten der IMAP-Advisor-Funktion müssen Sie beispielsweise den folgenden Befehl absetzen:

```
mlcontrol advisor start imap Port
```


Eine Liste der Advisor-Funktionen mit den zugehörigen Standard-Ports finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265. Eine Beschreibung der einzelnen Advisor-Funktionen können Sie dem Abschnitt „Liste der Advisor-Funktionen“ auf Seite 153 entnehmen.

Schritt 7. Cluster-Proportionen festlegen

Wenn Sie Advisor-Funktionen starten, können Sie die Wichtigkeit ändern, die in Entscheidungen für den Lastausgleich einfließenden Informationen von Advisor-Funktionen beigemessen wird. Setzen Sie zum Festlegen von Cluster-Proportionen den Befehl **mlcontrol cluster set *Cluster proportions*** ab. Weitere Informationen hierzu finden Sie im Abschnitt „Proportionale Bedeutung von Statusinformationen“ auf Seite 145.

Kapitel 10. Planung für Site Selector

In diesem Kapitel wird beschrieben, was die für die Planung des Netzes zuständige Person vor der Installation und Konfiguration der Komponente Site Selector berücksichtigen muss.

- Informationen zum Konfigurieren der Lastausgleichparameter von Site Selector finden Sie in „Kapitel 11. Site Selector konfigurieren“ auf Seite 119.
- Informationen zum Konfigurieren von Network Dispatcher für erweiterte Funktionen finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Dieses Kapitel enthält die folgenden Abschnitte:

- „Hardware- und Softwarevoraussetzungen“
- „Überlegungen bei der Planung“

Hardware- und Softwarevoraussetzungen

- für AIX finden Sie im Abschnitt „Voraussetzungen für AIX“ auf Seite 12.
- für Linux finden Sie im Abschnitt „Voraussetzungen für Red Hat Linux oder SuSE Linux“ auf Seite 17.
- für Solaris finden Sie im Abschnitt „Voraussetzungen für Solaris“ auf Seite 21.
- für Windows 2000 finden Sie im Abschnitt „Voraussetzungen für Windows 2000“ auf Seite 23.

Überlegungen bei der Planung

Site Selector verteilt zusammen mit einem Domänennamensserver die Last auf eine Gruppe von Servern. Dazu verwendet Site Selector erfasste Messwerte und Wertigkeiten. Sie können eine Sitekonfiguration erstellen, die innerhalb einer Servergruppe einen Lastausgleich auf der Grundlage des für eine Client-Anfrage verwendeten Domänennamens durchführt.

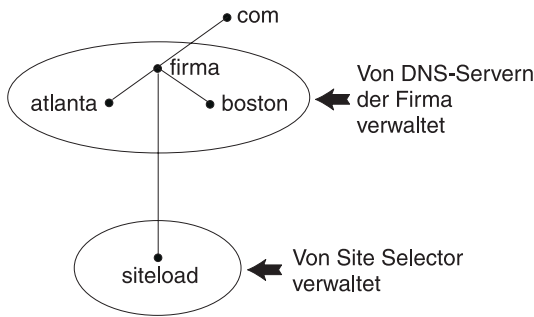


Abbildung 20. Beispiel für eine DNS-Umgebung

Wenn Sie innerhalb Ihrer DNS-Umgebung eine Unterdomäne für Site Selector einrichten, sollte Site Selector die Berechtigung für diese Unterdomäne haben. Beispiel (siehe Abb. 20): Ihre Firma hat die Berechtigung für die Domäne **firma.com** erhalten. Innerhalb der Firma gibt es mehrere Unterdomänen. Site Selector hätte in diesem Fall die Berechtigung für **siteload.firma.com** und die DNS-Server hätten weiterhin die Berechtigung für **atlanta.firma.com** und **boston.firma.com**.

Damit der Namensserver der Firma erkennt, dass Site Selector die Berechtigung für die Unterdomäne siteload hat, muss zur benannten Datendatei für den Server ein Namensservereintrag hinzugefügt werden. Für AIX würde ein solcher Namensservereintrag etwa wie folgt aussehen:

```
siteload.firma.com. IN NS siteselector.firma.com.
```

Hier ist **siteselector.firma.com** der Host-Name der Site-Selector-Maschine. In allen anderen benannten Datendateien für DNS-Server sind äquivalente Einträge erforderlich.

Ein Client fordert die Auflösung eines Domännennamens bei einem Namensserver innerhalb seines Netzes an. Der Namensserver leitet die Anforderung an die Site-Selector-Maschine weiter. Site Selector löst den Domännennamen dann in die IP-Adresse eines der Server auf, die unter dem Sitenamen konfiguriert wurden. Anschließend gibt Site Selector die IP-Adresse des ausgewählten Servers an den Namensserver zurück. Der Namensserver liefert die IP-Adresse an den Client. (Site Selector arbeitet als nicht rekursiver Namensserver (Blattknotenserver) und meldet einen Fehler, wenn die Domännennamensanforderung nicht aufgelöst werden kann.)

Abb. 11 auf Seite 44 veranschaulicht eine Site, bei der Site Selector zusammen mit einem DNS-System die Last auf lokale und ferne Server verteilt.

Site Selector stellt die folgenden Funktionen bereit:

- Der **sss**server bearbeitet Anforderungen von der Befehlszeile an den Namensserver, den Manager und die Advisor-Funktionen.
- Die **Namensserver**-Funktion unterstützt die Verteilung eingehender Namensserveranforderungen. Eine DNS-Auflösung ist erst möglich, wenn Sie die Namensserverfunktion für Site Selector gestartet haben. Site Selector ist am Port 53 bereit, eingehende DNS-Anforderungen zu empfangen. Wenn der Name der anfragenden Site konfiguriert ist, gibt Site Selector eine Serveradresse (aus einer Gruppe von Serveradressen) zurück, die dem Site-namen zugeordnet ist.
- Der **Manager** definiert Wertigkeiten, die vom Namensserver benutzt werden und auf folgenden Kriterien basieren:
 - von den Advisor-Funktionen bereitgestellte Rückmeldungen von den Servern
 - Rückmeldungen von einem Systemüberwachungsprogramm wie Metric Server.

Die Benutzung des Managers ist optional. Ohne den Manager wird der Lastausgleich nach einer gewichteten RoundRobin-Zeitplanung und ausgehend von den aktuellen Serverwertigkeiten durchgeführt. Es stehen keine Advisor-Funktionen zur Verfügung.

- **Metric Server** ist eine Network-Dispatcher-Komponente zur Systemüberwachung, die auf der Back-End-Servermaschine installiert wird. (Wenn Sie Network Dispatcher mit einer Servermaschine verknüpfen, für die ein Lastausgleich durchgeführt wird, müssen Sie Metric Server auf der Maschine mit Network Dispatcher installieren.)

Mit Metric Server kann Site Selector den Grad der Aktivität eines Servers überwachen, den Server mit der geringsten Auslastung feststellen und einen ausgefallenen Server erkennen. Die Last ist ein Maß für das Arbeitsaufkommen eines Server. Der Administrator des Systems mit Site Selector steuert die Art der Lastmessung. Sie können Site Selector an die Anforderungen der eigenen Umgebung anpassen und dabei Faktoren wie die Zugriffshäufigkeit, die Gesamtzahl der Benutzer und die Zugriffsarten (beispielsweise kurze Abfragen, lange Abfragen, Transaktionen mit hoher CPU-Belastung) berücksichtigen.

Der Lastausgleich wird auf der Basis von Serverwertigkeiten vorgenommen. Für Site Selector gibt es vier Proportionen, die der Manager zur Ermittlung der Wertigkeiten verwendet:

- CPU
- Speicher
- Port
- System

Alle CPU- und Speicherwerte werden von Metric Server bereitgestellt. Wenn Sie mit Site Selector arbeiten, sollten Sie demzufolge auch Metric Server verwenden.

Weitere Informationen hierzu finden Sie im Abschnitt „Metric Server“ auf Seite 161.

- Die **Advisor-Funktionen** richten Abfragen an die Server und analysieren die Ergebnisse nach Protokoll, bevor sie den Manager zum Festlegen der entsprechenden Wertigkeiten aufrufen. Es ist nicht immer sinnvoll, einige dieser Advisor-Funktionen in einer typischen Konfiguration zu verwenden. Sie können auch eigene Advisor-Funktionen schreiben. Die Benutzung der Advisor-Funktionen ist optional, wird jedoch empfohlen. Weitere Informationen hierzu finden Sie im Abschnitt „Advisor-Funktionen“ auf Seite 149.
- Zum Konfigurieren und Verwalten des Namensservers, der Advisor-Funktionen, von Metric Server und des Managers können Sie die Befehlszeile (**sscontrol**) oder die grafische Benutzerschnittstelle (**ndadmin**) verwenden.

Die vier wichtigsten Funktionen von Site Selector (Namensserver, Manager, Metric Server und Advisor-Funktionen) interagieren, um die eingehenden Anforderungen auf die Server zu verteilen und aufzulösen.

Hinweise zu TTL

Der DNS-gestützte Lastausgleich erfordert, dass Namensauflösungen zwischengespeichert werden können. Der TTL-Wert (Time To Live) bestimmt die Effizienz des DNS-gestützten Lastausgleichs. TTL legt fest, wie lange ein anderer Namensserver die aufgelöste Antwort zwischenspeichert. Bei einem kleinen TTL-Wert können geringfügige Änderungen der Server- oder Netzlast schneller realisiert werden. Wird die Zwischenspeicherung inaktiviert, müssen die Clients sich mit jeder Namensauflösungsanforderung an den maßgeblichen Namensserver wenden, was potenziell die Latenzzeit erhöht. Bei der Auswahl eines TTL-Wertes sollte sorgfältig abgewogen werden, welchen Einfluss das Inaktivieren der Zwischenspeicherung auf eine Umgebung hat. Es ist auch zu bedenken, dass der DNS-gestützte Lastausgleich potenziell von der Zwischenspeicherung von Namensauflösungen auf dem Client eingeschränkt werden kann.

TTL kann mit dem Befehl **sscontrol sitename [add | set]** konfiguriert werden. Weitere Informationen hierzu finden Sie im Abschnitt „sscontrol sitename — Sitenamen konfigurieren“ auf Seite 358.

Netzproximität verwenden

Die Netzproximität ist die Berechnung der Nähe jedes einzelnen Servers zum anfordernden Client. Zum Bestimmen der Netzproximität sendet der Agent Metric Server (der auf jedem Server mit Lastausgleich installiert sein muss) ein "ping" an die Client-IP-Adresse und meldet Site Selector die Antwortzeit. Site Selector bezieht die Proximitätsantwort in die Lastausgleichsentscheidung ein. Site Selector kombiniert den Wert der Netzproximitätsantwort mit der Wertigkeit vom Manager und ermittelt so die endgültige Wertigkeit für den Server. Die Verwendung der Netzproximität mit Site Selector ist optional.

Site Selector stellt die folgenden Netzproximitätsoptionen bereit, die pro Site-namen festgelegt werden können:

- Cache-Lebensdauer: Die Zeitperiode, während der eine Proximitätsantwort gültig und im Cache gespeichert bleibt.
- Prozentsatz für Proximität: Die Bedeutung der Proximitätsantwort, gemessen am Zustand des Servers (vom Manager vorgegebene Wertigkeit).
- Auf alle warten: Legt fest, ob vor der Beantwortung der Client-Anfrage auf alle Proximitätsantworten (ping-Antworten) der Server gewartet werden soll.

Ist dieser Wert auf **ja** gesetzt, sendet Metric Server ein "ping" an den Client, um die Zeit für die Proximitätsantwort zu ermitteln. Der Namensserver wartet auf die Antworten aller Metric-Server oder das Eintreten einer Zeitlimitüberschreitung. Anschließend erstellt der Namensserver für jeden Server aus der Zeit für die Proximitätsantwort und der vom Manager berechneten Wertigkeit eine kombinierte Wertigkeit. Site Selector teilt dem Client die Server-IP-Adresse mit der besten kombinierten Wertigkeit mit. (Es wird davon ausgegangen, dass die meisten Client-Namensserver ein Zeitlimit von 5 Sekunden haben. Site Selector versucht, vor Ablauf dieses Zeitlimits zu antworten.)

Ist dieser Wert auf **nein** gesetzt, erfolgt die Namensauflösung für den Client auf der Basis der aktuellen Wertigkeiten vom Manager. Anschließend sendet Metric Server ein "ping" an den Client, um die Zeit für die Proximitätsantwort zu ermitteln. Der Namensserver stellt die von Metric Server empfangene Antwortzeit in den Cache. Wenn der Client eine zweite Anforderung stellt, erstellt der Namensserver für jeden Server aus der aktuellen Wertigkeit vom Manager und dem zwischengespeicherten Wert der ping-Antwort eine kombinierte Wertigkeit. Site Selector gibt auf die zweite Anforderung des Clients die IP-Adresse des Servers mit der besten kombinierten Wertigkeit zurück.

Optionen für die Netzproximität können mit dem Befehl **sscontrol sitename [add | set]** gesetzt werden. Weitere Informationen hierzu finden Sie in „Anhang D. Befehlsreferenz für Site Selector“ auf Seite 335.

Kapitel 11. Site Selector konfigurieren

Lesen Sie vor Ausführung der in diesem Kapitel beschriebenen Schritte „Kapitel 10. Planung für Site Selector“ auf Seite 113. Dieses Kapitel erläutert das Erstellen einer Basiskonfiguration für die Komponente Site Selector von Network Dispatcher.

- Komplexere Konfigurationen für Network Dispatcher finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Konfigurations-Tasks im Überblick

Anmerkung: Vergewissern Sie sich vor Ausführung der Konfigurationsschritte in dieser Tabelle, dass die Site Selector-Maschine und alle Servermaschinen mit dem Netz verbunden sind, gültige IP-Adressen haben und sich gegenseitig mit ping-Aufrufen erreichen können.

Tabelle 9. Konfigurations-Tasks für Site Selector

Task	Beschreibung	Referenzinformationen
Maschine mit Site Selector konfigurieren	Stellen Sie fest, welche Voraussetzungen zu erfüllen sind.	„Maschine mit Site Selector konfigurieren“ auf Seite 123
Am Lastausgleich beteiligte Maschinen konfigurieren	Definieren Sie Ihre Lastausgleichskonfiguration.	„Schritt 4. Am Lastausgleich beteiligte Servermaschinen definieren“ auf Seite 124

Konfigurationsmethoden

Es gibt im Wesentlichen vier Methoden für das Erstellen einer Basisconfiguration für die Komponente Site Selector von Network Dispatcher:

- Befehlszeile
- Scripts
- Grafische Benutzerschnittstelle (GUI)
- Konfigurationsassistent

Befehlszeile

Dies ist die direkte Methode für die Konfiguration von Site Selector. Die Werte der Befehlsparameter müssen in englischen Zeichen eingegeben werden. Die einzige Ausnahme hiervon bilden Host-Namen (die z. B. in den Befehlen "site-name" und "server" verwendet werden) und Dateinamen.

Starten Sie Site Selector wie folgt von der Befehlszeile aus:

- Setzen Sie an der Eingabeaufforderung den Befehl **ssserver** ab.

Anmerkung: Mit dem Befehl **ssserver stop** können Sie den Dienst stoppen.

- Setzen Sie anschließend die gewünschten Steuerbefehle für Site Selector ab, um die Konfiguration einzurichten. Bei den in diesem Handbuch beschriebenen Prozeduren wird von der Verwendung der Befehlszeile ausgegangen. Der Befehl lautet **sscontrol**. Weitere Informationen zu Befehlen finden Sie in „Anhang D. Befehlsreferenz für Site Selector“ auf Seite 335.

Sie können eine Minimalversion der Parameter für den Befehl "sscontrol" eingeben. Sie müssen nur die eindeutigen Buchstaben der Parameter eingeben. Beispiel: Wenn Sie Hilfe für den Befehl zum Speichern von Dateien aufrufen möchten, können Sie **sscontrol he f** anstelle von **sscontrol help file** eingeben.

Wenn Sie die Befehlszeilenschnittstelle starten möchten, setzen Sie den Befehl **sscontrol** ab, um die Eingabeaufforderung "sscontrol" aufzurufen.

Sie können die Befehlszeilenschnittstelle verlassen, indem Sie den Befehl **exit** oder **quit** absetzen.

Anmerkung: Unter Windows 2000 wird ndserver für die Dispatcher-Komponente automatisch gestartet. Falls Sie nur mit Site Selector und nicht mit der Dispatcher-Komponente arbeiten, können Sie den automatischen Start von ndserver wie folgt unterbinden:

1. Klicken Sie im Fenster "Dienste" von Windows 2000 mit der rechten Maustaste auf "IBM Dispatcher".
2. Wählen Sie den Menüeintrag "Eigenschaften" aus.
3. Wählen Sie im Feld **Starttyp** die Option "Manuell" aus.
4. Klicken Sie auf OK und schließen Sie das Fenster "Dienste".

Scripts

Die Befehle zum Konfigurieren von Site Selector können in eine Konfigurations-Script-Datei eingegeben und dann zusammen ausgeführt werden.

Anmerkung: Falls Sie den Inhalt einer Script-Datei (z. B. meinScript) schnell ausführen möchten, verwenden Sie einen der folgenden Befehle:

- Führen Sie zum Aktualisieren der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:
sscontrol file appendload *meinScript*
- Führen Sie zum vollständigen Ersetzen der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:
sscontrol file newload *meinScript*

GUI

Ein Beispiel für die GUI zeigt Abb. 2 auf Seite 6.

Gehen Sie zum Starten der GUI wie folgt vor:

1. Vergewissern Sie sich, dass ssserver aktiv ist. Setzen Sie an einer Eingabeaufforderung als Benutzer "root" oder Administrator den Befehl **ssserver** ab.
2. Führen Sie anschließend einen der folgenden Schritte aus:
 - Geben Sie unter AIX, Linux oder Solaris **ndadmin** ein.
 - Klicken Sie unter Windows 2000 nacheinander auf **Start, Programme, IBM WebSphere, Edge Server, IBM Network Dispatcher** und **Network Dispatcher**.

Zum Konfigurieren von Site Selector auf der GUI müssen Sie zunächst in der Baumstruktur **Site Selector** auswählen. Sie können den Manager starten, sobald Sie eine Verbindung zu einem Host hergestellt haben. Sie können auch Sitenamen mit Ports und Servern erstellen sowie Advisor-Funktionen für den Manager starten.

Von der GUI aus können Sie die gleichen Schritte wie mit dem Befehl **sscontrol** ausführen. Wenn Sie beispielsweise einen Sitenamen von der Befehlszeile aus definieren möchten, müssen Sie den Befehl **sscontrol sitename add Site-name** eingeben. Zum Definieren eines Sitenamens von der GUI aus müssen Sie mit der rechten Maustaste auf "Namensserver" klicken und in dem daraufhin angezeigten Popup-Menü mit der linken Maustaste auf **Sitenamen hinzufügen**. Geben Sie im Dialogfenster den Sitenamen ein und klicken Sie auf **OK**.

Bereits vorhandene Site-Selector-Konfigurationsdateien können Sie mit der im Popup-Menü **Host** angezeigten Option **Neue Konfiguration laden** (zum vollständigen Ersetzen der derzeitigen Konfiguration) oder **An aktuelle Konfiguration anfügen** (zum Aktualisieren der derzeitigen Konfiguration) laden. Sie sollten Ihre Site-Selector-Konfiguration von Zeit zu Zeit mit der Option **Konfigurationsdatei sichern unter** in einer Datei sichern. Diese Option ist ebenfalls im Popup-Menü **Host** enthalten. Über das Menü **Datei** oben auf der GUI können Sie Ihre aktuellen Host-Verbindungen in einer Datei speichern oder Verbindungen aus vorhandenen Dateien aller Network-Dispatcher-Komponenten wiederherstellen.

Sie können auf **Hilfe** zugreifen, indem Sie auf das Fragezeichen in der oberen rechten Ecke des Fensters von Network Dispatcher klicken.

- **Hilfe für Feld** — beschreibt jedes Feld und gibt die Standardwerte an.
- **Vorgehensweise** — listet Tasks auf, die von dieser Anzeige aus ausgeführt werden können.
- **Inhaltsverzeichnis** — zeigt ein Inhaltsverzeichnis mit allen Hilfetexten an.
- **Index** — zeigt einen alphabetischen Index der Hilfethemen an.

Weitere Informationen zur Verwendung der GUI finden Sie im Abschnitt „Allgemeine Anweisungen zur Verwendung der GUI“ auf Seite 7.

Konfigurationsassistent

Führen Sie folgende Schritte aus, wenn Sie den Konfigurationsassistenten verwenden:

1. Starten Sie den `ssserver` von Site Selector, indem Sie an der Eingabeaufforderung als Benutzer `"root"` oder Administrator den Befehl **`ssserver`** absetzen.
2. Starten Sie die Assistentenfunktion von Site Selector, **`sswizard`**.
Sie können den Assistenten von der Eingabeaufforderung aus starten, indem Sie den Befehl **`sswizard`** absetzen. Sie können den Konfigurationsassistenten aber auch auf der GUI unter der Komponente Site Selector auswählen.

Der Site-Selector-Assistent führt Sie schrittweise durch den Prozess zum Erstellen einer Basiskonfiguration für die Komponente Site Selector. Er stellt Ihnen Fragen zu Ihrem Netz und leitet Sie beim Konfigurieren eines Sitenamens an, mit dem Site Selector den Datenverkehr auf eine Gruppe von Servern verteilen kann.

Bei Verwendung des Konfigurationsassistenten für Site Selector erscheinen die folgenden Anzeigen:

- Einführung in den Assistenten
- Was Sie erwarten können
- Vor dem Beginn
- Auswahl eines Hosts für die Konfiguration (falls erforderlich)
- Sitenamen definieren
- Server hinzufügen
- Advisor starten
- Netzproximität konfigurieren

Maschine mit Site Selector konfigurieren

Vor dem Konfigurieren der Maschine mit Site Selector müssen Sie (unter AIX, Linux oder Solaris) als Benutzer "root" oder (unter Windows 2000) als Administrator registriert sein.

Für eine Gruppe von Servern, die Sie konfigurieren, benötigen Sie einen nicht auflösbaren DNS-Host-Namen als Sitenamen. Der Sitename ist der Name, mit dem Clients auf Ihre Site zugreifen (z. B. `www.IhreFirma.com`). Site Selector verteilt mit dem DNS den Datenverkehr für die Site auf die Server der Gruppe.

Schritt 1. Serverfunktion starten

AIX, Linux und Solaris: Geben Sie zum Starten der Serverfunktion `ssserver` ein.

Anmerkung: Beim Starten von `ssserver` wird automatisch eine Standard-konfigurationsdatei (`default.cfg`) geladen. Wenn Sie die Konfiguration in `default.cfg` sichern, werden alle in dieser Datei gesicherten Angaben beim nächsten Starten von `ssserver` automatisch geladen.

Schritt 2. Namensserver starten

Geben Sie zum Starten des Namensservers den Befehl `sscontrol nameserver start` ein.

Optional können Sie den Namensserver starten, indem Sie ihn mit dem Schlüsselwort "bindaddress" ausschließlich an die angegebene Adresse binden.

Schritt 3. Sitenamen definieren und Optionen für Sitenamen festlegen

Site Selector verteilt die an den Sitenamen gesendeten Anforderungen auf die entsprechenden Server, die für die Site konfiguriert sind.

Der Sitename ist ein nicht auflösbarer Host-Name, den der Client anfordert. Der Sitename muss ein vollständig qualifizierter Domänenname sein (z. B. `www.dnsdownload.com`). Wenn ein Client diesen Sitenamen anfordert, wird eine der dem Sitenamen zugeordneten Server-IP-Adressen zurückgegeben.

Setzen Sie zum Definieren eines Sitenamens den folgenden Befehl ab:

```
sscontrol sitename add Sitename
```

Wenn Sie Optionen für den Sitenamen festlegen möchten, setzen Sie den folgenden Befehl ab:

```
sscontrol sitename  
set Wert_der_Sitenamenoption
```

Weitere Informationen hierzu finden Sie in „Anhang D. Befehlsreferenz für Site Selector“ auf Seite 335.

Schritt 4. Am Lastausgleich beteiligte Servermaschinen definieren

Die Servermaschinen sind die Maschinen, auf denen die Anwendungen ausgeführt werden, deren Last verteilt werden soll. Für den *Server* wird der symbolische Name der Servermaschine oder deren Adresse in Schreibweise mit Trennzeichen angegeben. Setzen Sie den folgenden Befehl ab, um für den Sitenamen von Schritt 3 einen Server zu definieren:

```
sscontrol server add Sitename:Server
```

Für einen Sitenamen müssen Sie mehrere Server definieren, um einen Lastausgleich durchführen zu können.

Schritt 5. Manager-Funktion starten (optional)

Die Manager-Funktion verbessert den Lastausgleich. Vergewissern Sie sich vor dem Starten der Manager-Funktion, dass auf allen am Lastausgleich beteiligten Maschinen Metric Server installiert ist.

Setzen Sie zum Starten des Managers den folgenden Befehl ab:

```
sscontrol manager start
```

Schritt 6. Advisor-Funktion starten (optional)

Die Advisor-Funktionen liefern dem Manager weitere Informationen über die Fähigkeit der am Lastausgleich beteiligten Servermaschinen, auf Anforderungen zu antworten. Advisor-Funktionen sind protokollspezifisch. Network Dispatcher stellt zahlreiche Advisor-Funktionen bereit. Wenn Sie beispielsweise die HTTP-Advisor-Funktion für einen bestimmten Sitenamen starten möchten, setzen Sie den folgenden Befehl ab:

```
sscontrol advisor start http Sitename:Port
```

Schritt 7. Systemmesswert definieren (optional)

Informationen zur Verwendung von Systemmesswerten und Metric Server finden Sie im Abschnitt „Metric Server“ auf Seite 161.

Schritt 8. Proportionen für den Sitenamen festlegen

Wenn Sie Advisor-Funktionen starten, können Sie die Wichtigkeit ändern, die in Entscheidungen für den Lastausgleich einfließenden Informationen von Advisor-Funktionen (Port-Informationen) beigemessen wird. Setzen Sie zum Festlegen der Proportionen für den Sitenamen den Befehl **sscontrol sitename set *Sitename* proportions** ab. Weitere Informationen hierzu finden Sie im Abschnitt „Proportionale Bedeutung von Statusinformationen“ auf Seite 145.

Servermaschinen für Lastausgleich konfigurieren

Sie sollten Metric Server zusammen mit der Komponente Site Selector verwenden. Informationen zum Konfigurieren von Metric Server auf allen Maschinen, für die Site Selector einen Lastausgleich durchführt, finden Sie im Abschnitt „Metric Server“ auf Seite 161.

Kapitel 12. Planung für Consultant für Cisco CSS Switches

In diesem Kapitel wird beschrieben, was die für die Planung des Netzes zuständige Person vor der Installation und Konfiguration der Komponente Consultant für Cisco CSS Switches berücksichtigen muss.

- Informationen zum Konfigurieren der Lastausgleichparameter von Consultant für Cisco CSS Switches finden Sie in „Kapitel 13. Consultant für Cisco CSS Switches konfigurieren“ auf Seite 133.
- Informationen zum Konfigurieren von Network Dispatcher für erweiterte Funktionen finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Dieses Kapitel umfasst:

- „Hardware- und Softwarevoraussetzungen“
- „Überlegungen bei der Planung“

Hardware- und Softwarevoraussetzungen

- für AIX finden Sie im Abschnitt „Voraussetzungen für AIX“ auf Seite 12.
- für Linux finden Sie im Abschnitt „Voraussetzungen für Red Hat Linux oder SuSE Linux“ auf Seite 17.
- für Solaris finden Sie im Abschnitt „Voraussetzungen für Solaris“ auf Seite 21.
- für Windows 2000 finden Sie im Abschnitt „Voraussetzungen für Windows 2000“ auf Seite 23.

Überlegungen bei der Planung

Die Konfiguration für Cisco Consultant ist von der Konfiguration des Cisco CSS Switch abhängig (siehe Tabelle 10 auf Seite 129). Nachdem Sie die Planung und Konfiguration für den Cisco CSS Switch abgeschlossen haben, können Sie Cisco Consultant konfigurieren und verwenden. Planungs- und Konfigurationsanweisungen für den Cisco CSS Switch finden Sie in der zugehörigen Dokumentation.

Consultant umfasst Folgendes:

- Der **lbcs**erver enthält die Konfigurationsdaten und interagiert mit dem Cisco CSS Switch. Der Präfix "lbc" steht für load-balancing consultant. Der lbcs-erver setzt sich aus folgenden Funktionen zusammen:
 - Der **Executor** enthält die Konfigurationsdaten und die für das Herstellen einer Verbindung zum Cisco CSS Switch erforderlichen Informationen.
 - Der **Manager** generiert anhand erfasster Informationen Wertigkeiten und sendet diese an den Cisco CSS Switch. Der Manager sammelt Daten von folgenden Komponenten:
 - Cisco CSS Switch
 - Server (mit Hilfe der Advisor-Funktionen)

Die Advisor-Funktionen fragen die Server ab und analysieren die Ergebnisse nach Protokoll, bevor sie den Manager zum Festlegen der entsprechenden Wertigkeiten aufrufen. Derzeit stellt Cisco Consultant Advisor-Funktionen für HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3 (und andere) bereit. Sie können auch eigene Advisor-Funktionen schreiben. (Lesen Sie hierzu die Informationen im Abschnitt „Kundenspezifische (anpassbare) Advisor-Funktion erstellen“ auf Seite 155.) Die Verwendung der Advisor-Funktionen ist optional, wird jedoch empfohlen.
 - Server (mit Hilfe von Metric Server)

Metric Server gibt an Consultant Informationen zur Serverauslastung in Form systemspezifischer Messwerte weiter, die Aufschluss über den Zustand der Server geben. Der Manager fragt Metric Server auf den einzelnen Servern ab. Dabei verwendet er die Messwerte der Agenten, um die Zuordnung von Wertigkeiten für den Prozess des Lastausgleichs zu unterstützen. Die Ergebnisse werden auch in den Manager-Bericht gestellt.
- Sie können den Executor, die Advisor-Funktionen und den Manager sowohl von einer Befehlszeile als auch von einer grafischen Benutzerschnittstelle aus konfigurieren und verwalten.
 - **lbcc**ontrol ist die Befehlszeilenschnittstelle zu Consultant.
 - **ndad**min ist die grafische Benutzerschnittstelle, die verwendet wird, um Consultant zu konfigurieren und seinen Status zu überwachen.

Der Manager sammelt Informationen vom Cisco CSS Switch, von den Advisor-Funktionen und von Metric Server. Der Manager passt anhand der erhaltenen Informationen die Wertigkeit der Servermaschinen an den einzelnen Ports an und teilt dem Cisco CSS Switch die neue Wertigkeit mit, die dieser dann beim Lastausgleich für neue Verbindungen verwendet. Wenn der Manager feststellt, dass ein Server inaktiv ist, ordnet er diesem Server die Wertigkeit null zu und setzt den Serverbetrieb aus. Der Cisco CSS Switch stellt daraufhin die Weiterleitung von Datenverkehr an diesen Server ein.

Die Advisor-Funktionen überwachen jeden Server am zugeordneten Port, um die Antwortzeit und die Verfügbarkeit der einzelnen Server zu ermitteln.

Diese Informationen werden dann an den Manager weitergegeben. Die Advisor-Funktionen überwachen zudem, ob ein Server aktiv oder inaktiv ist.

Eine ordnungsgemäße Consultant-Konfiguration muss die Konfiguration des Cisco CSS Switch spiegeln. Lesen Sie zunächst die Informationen in der Veröffentlichung *Cisco Services Switch Getting Started Guide* zum Konfigurieren des Cisco CSS Switch. Konfigurieren Sie Consultant erst, wenn der Switch fehlerfrei funktioniert.

Die Konfiguration des Cisco CSS Switch umfasst Eigner, content-Regeln und Dienste, die einer Consultant-Konfiguration wie folgt zugeordnet werden:

Tabelle 10. Begriffe für die Konfiguration von Consultant und des Cisco CSS Switch

Cisco CSS Switch	Consultant
Virtuelle IP-Adresse (VIP) der content-Regeln von einem oder mehreren der Eigner	Cluster
In der content-Regel enthaltener Port	Port
Dienst	Server

Die Consultant-Konfiguration umfasst Folgendes:

- *Cluster* ist ein auflösbarer Name oder eine Adresse in Schreibweise mit Trennzeichen.
- *Port* ist die Nummer des Ports, der für dieses Protokoll verwendet wird.
- *Server*.

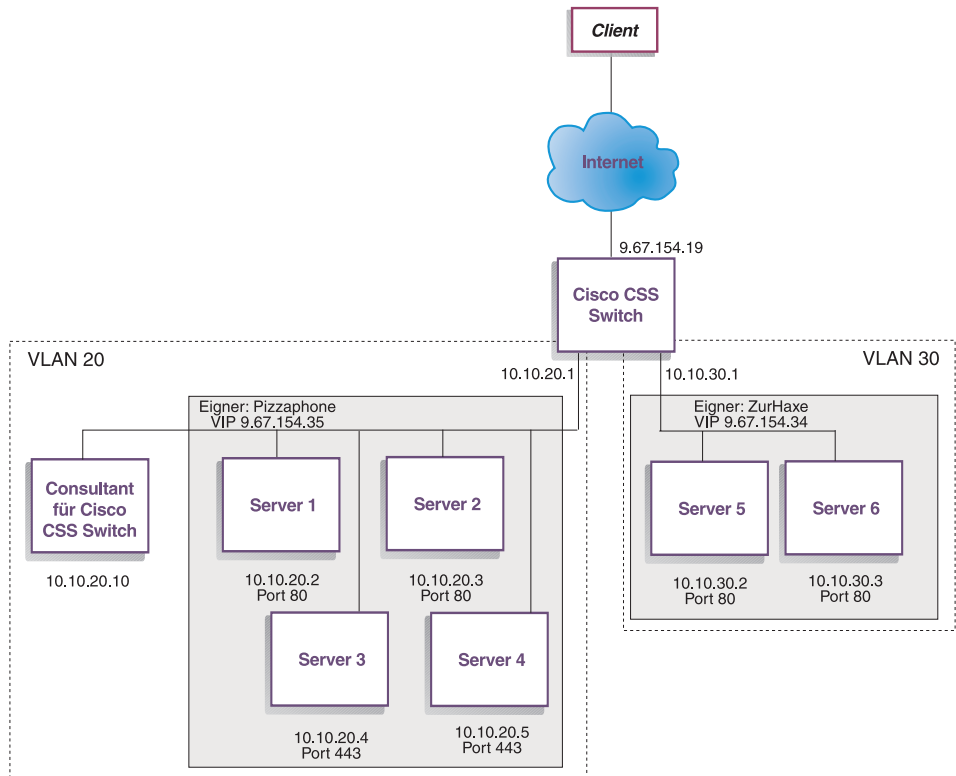


Abbildung 21. Konfigurationsbeispiel für Consultant mit 2 Clustern mit jeweils 3 Ports

Abb. 21:

- 9.67.154.19 ist die Netzverbindung zum Internet.
- Es sind zwei VLAN (20 und 30) konfiguriert.

Für den Executor müssen Sie eine Adresse und einen Namen der SNMP-Benutzergemeinschaft konfigurieren, die mit den entsprechenden Attributen des Cisco CSS Switch übereinstimmen. Informationen zum Konfigurieren des Executors finden Sie im Abschnitt „lbcontrol executor — Executor steuern“ auf Seite 371.

Tabelle 11. Beispiel für eine in der Consultant-Konfiguration abgebildete Konfiguration des Cisco CSS Switch

Cisco CSS SwitchKonfiguration	ConsultantKonfiguration
username admin superuser snmp community <i>Benutzergemeinschaft</i> private read-write	lbcccontrol executor set address 10.10.20.1 lbcccontrol executor set communityname <i>Benutzergemeinschaft</i>
content-Regel 1 port <i>80</i> balance weightedrr add service <i>Server1</i> add service <i>Server2</i> vip address <i>9.67.154.35</i> active	lbcccontrol cluster add <i>9.67.154.35</i> lbcccontrol port add 9.67.154.35: <i>80</i>
content-Regel 2 protocol tcp port <i>443</i> balance weightedrr add service Server3 add service Server4 vip address 9.67.154.35 active	lbcccontrol port add 9.67.154.35: <i>443</i>
service Server1 ip address <i>10.10.20.2</i> port <i>80</i> weight 4 active	lbcccontrol server add 9.67.154.35: <i>80</i> :Server1 address <i>10.10.20.2</i>
service Server3 ip address <i>10.10.20.4</i> port <i>443</i> weight 4 active	lbcccontrol server add 9.67.154.35: <i>443</i> :Server3 address <i>10.10.20.4</i>

Kapitel 13. Consultant für Cisco CSS Switches konfigurieren

Lesen Sie vor Ausführung der in diesem Kapitel beschriebenen Schritte „Kapitel 12. Planung für Consultant für Cisco CSS Switches“ auf Seite 127. Dieses Kapitel erläutert das Erstellen einer Basiskonfiguration für die Komponente Consultant für Cisco CSS Switches von Network Dispatcher.

- Komplexere Konfigurationen für Network Dispatcher finden Sie in „Kapitel 14. Erweiterte Funktionen von Network Dispatcher“ auf Seite 141.
- Informationen zur Fernverwaltung mit Authentifizierung, zu den Protokollen von Network Dispatcher sowie zur Verwendung der Komponenten von Network Dispatcher finden Sie in „Kapitel 15. Betrieb und Verwaltung von Network Dispatcher“ auf Seite 219.

Übersicht über die Konfigurations-Tasks

Vor Ausführung einer der in diesem Kapitel beschriebenen Konfigurationsmethoden müssen Sie die folgenden Schritte ausführen:

1. Vergewissern Sie sich, dass der Cisco CSS Switch und alle Servermaschinen richtig konfiguriert sind.
2. Konfigurieren Sie Cisco Consultant so, dass die Adresse des Executors und der Name der SNMP-Benutzergemeinschaft mit den entsprechenden Attributen des Cisco CSS Switch übereinstimmen. Informationen zum Konfigurieren des Executors finden Sie im Abschnitt „lbcontrol executor — Executor steuern“ auf Seite 371.

Tabelle 12. Konfigurations-Tasks für Consultant für Cisco CSS Switches

Task	Beschreibung	Referenzinformationen
Konfigurieren der Maschine mit Consultant für Cisco CSS Switches	Ermitteln Sie die Voraussetzungen.	„Maschine mit Consultant für Cisco CSS Switches konfigurieren“ auf Seite 136
Testen der Konfiguration	Überprüfen Sie, ob die Konfiguration funktioniert.	„Konfiguration testen“ auf Seite 139

Konfigurationsmethoden

Es gibt im Wesentlichen drei Methoden für das Erstellen einer Basis-konfiguration für die Komponente Consultant für Cisco CSS Switches von Network Dispatcher:

- Befehlszeile
- Scripts
- Grafische Benutzerschnittstelle (GUI)

Befehlszeile

Dies ist die direkte Methode für die Konfiguration von Cisco Consultant. Bei den in diesem Handbuch beschriebenen Prozeduren wird von der Verwendung der Befehlszeile ausgegangen. Die Werte der Befehlsparameter müssen in englischen Zeichen eingegeben werden. Die einzige Ausnahme hiervon bilden Host-Namen (die z. B. in den Befehlen "cluster" und "server" verwendet werden) und Dateinamen.

Starten Sie Cisco Consultant wie folgt von der Befehlszeile aus:

- Setzen Sie an der Eingabeaufforderung den Befehl **lbserver** ab.

Anmerkung: Mit dem Befehl **lbserver stop** können Sie den Dienst stoppen.

- Setzen Sie anschließend die gewünschten Steuerbefehle für Cisco Consultant ab, um die Konfiguration einzurichten. Der Befehl lautet **lbcontrol**. Weitere Informationen zu Befehlen finden Sie in „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265.

Sie können eine gekürzte Version der Parameter für den Befehl "lbcontrol" eingeben. Sie müssen nur die eindeutigen Buchstaben der Parameter eingeben. Beispiel: Wenn Sie Hilfe für den Befehl zum Speichern von Dateien aufrufen möchten, können Sie **lbcontrol h e f** anstelle von **lbcontrol help file** angeben.

Wenn Sie die Befehlszeilenschnittstelle starten möchten, setzen Sie den Befehl **lbcontrol** ab, um die Eingabeaufforderung "lbcontrol" aufzurufen.

Sie können die Befehlszeilenschnittstelle verlassen, indem Sie den Befehl **exit** oder **quit** absetzen.

Anmerkung: Unter Windows 2000 wird ndserver für die Dispatcher-Komponente automatisch gestartet. Falls Sie nur mit Cisco Consultant und nicht mit der Dispatcher-Komponente arbeiten, können Sie den automatischen Start von ndserver wie folgt unterbinden:

1. Klicken Sie im Fenster "Dienste" von Windows 2000 mit der rechten Maustaste auf "IBM Dispatcher".

2. Wählen Sie den Menüeintrag "Eigenschaften" aus.
3. Wählen Sie im Feld **Starttyp** die Option "Manuell" aus.
4. Klicken Sie auf OK und schließen Sie das Fenster "Dienste".

Scripts

Die Befehle zum Konfigurieren von Consultant für Cisco CSS Switches können in eine Konfigurations-Script-Datei eingegeben und dann zusammen ausgeführt werden.

Anmerkung: Falls Sie den Inhalt einer Script-Datei (z. B. meinScript) schnell ausführen möchten, verwenden Sie einen der folgenden Befehle:

- Führen Sie zum Aktualisieren der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:
lbccontrol file appendload meinScript
- Führen Sie zum vollständigen Ersetzen der derzeitigen Konfiguration die ausführbaren Befehle Ihrer Script-Datei mit folgendem Befehl aus:
lbccontrol file newload meinScript

GUI

Abb. 2 auf Seite 6 zeigt ein Beispiel für die grafische Benutzerschnittstelle (GUI).

Gehen Sie zum Starten der GUI wie folgt vor:

1. Wenn lbcservice noch nicht aktiv ist, starten Sie den Dienst jetzt, indem Sie als Root den folgenden Befehl absetzen:
lbcservice
2. Führen Sie anschließend einen der folgenden Schritte aus:
 - Geben Sie unter AIX, Linux oder Solaris **ndadmin** ein.
 - Klicken Sie unter Windows 2000 nacheinander auf **Start, Programme, IBM WebSphere, Edge Server, IBM Network Dispatcher** und **Network Dispatcher**.

Gehen Sie zum Konfigurieren von Cisco Consultant von der GUI aus wie folgt vor:

1. Klicken Sie in der Baumstruktur mit der rechten Maustaste auf "Cisco Consultant".
2. Stellen Sie eine Verbindung zu einem Host her.
3. Erstellen Sie Cluster mit Ports und Servern.
4. Starten Sie den Manager.
5. Starten Sie Advisor-Funktionen für den Manager.

Von der GUI aus können Sie alle mit dem Befehl **lbcontrol** ausführbaren Schritte ausführen. Wenn Sie beispielsweise einen Cluster von der Befehlszeile aus konfigurieren möchten, müssten Sie den Befehl **lbcontrol cluster add Cluster** eingeben. Zum Definieren eines Clusters von der GUI aus müssen Sie mit der rechten Maustaste auf "Executor" und dann mit der linken Maustaste auf **Cluster hinzufügen** klicken. Geben Sie die Cluster-Adresse in das Dialogfenster ein und klicken Sie dann auf **OK**.

Bereits vorhandene Konfigurationsdateien für Cisco Consultant können Sie mit der im Popup-Menü **Host** angezeigten Option **Neue Konfiguration laden** (zum vollständigen Ersetzen der derzeitigen Konfiguration) oder **An aktuelle Konfiguration anfügen** (zum Aktualisieren der derzeitigen Konfiguration) laden. Wählen Sie regelmäßig die Option **Konfigurationsdatei sichern als** aus, um Ihre Konfiguration für Cisco Consultant in einer Datei zu speichern. Wenn Sie in der Menüleiste auf **Datei** klicken, können Sie Ihre aktuellen Host-Verbindungen in einer Datei speichern oder Verbindungen aus vorhandenen Dateien aller Network-Dispatcher-Komponenten wiederherstellen.

Falls Sie **Hilfe** benötigen, klicken Sie oben rechts im Network-Dispatcher-Fenster auf das Fragezeichen.

- **Hilfe für Feld** — beschreibt jedes Feld und gibt die Standardwerte an.
- **Vorgehensweise** — listet Tasks auf, die von dieser Anzeige aus ausgeführt werden können.
- **Inhaltsverzeichnis** — zeigt ein Inhaltsverzeichnis mit allen Hilfetexten an.
- **Index** — zeigt einen alphabetischen Index der Hilfethemen an.

Weitere Informationen zur Verwendung der GUI finden Sie im Abschnitt „Allgemeine Anweisungen zur Verwendung der GUI“ auf Seite 7.

Maschine mit Consultant für Cisco CSS Switches konfigurieren

Vor dem Konfigurieren der Maschine mit Consultant für Cisco CSS Switches müssen Sie (unter AIX, Linux oder Solaris) als Benutzer "root" oder (unter Windows 2000) als Administrator registriert sein.

Consultant muss eine Verbindung zum Cisco CSS Switch als Cisco-CSS-Switch-Administrator herstellen können.

Wenn Sie den Executor konfigurieren, müssen die Adresse und der Name der SNMP-Benutzergemeinschaft mit den entsprechenden Attributen des Cisco CSS Switch übereinstimmen.

Hilfe zu den in dieser Prozedur verwendeten Befehlen finden Sie in „Anhang E. Befehlsreferenz für Consultant für Cisco CSS Switches“ auf Seite 363.

Schritt 1. Serverfunktion starten

Wenn `lbcservice` noch nicht aktiv ist, starten Sie den Dienst jetzt, indem Sie als Root den folgenden Befehl absetzen:

```
lbcservice
```

Schritt 2. Executor-Funktion konfigurieren

Sie müssen eine Adresse und einen Namen für die SNMP-Benutzergemeinschaft konfigurieren. Diese Werte müssen mit den entsprechenden Attributen des Cisco CSS Switch übereinstimmen.

Schritt 3. Cluster definieren und Cluster-Optionen festlegen

Cluster ist entweder ein auflösbarer Name oder eine Adresse in Schreibweise mit Trennzeichen. Der Cluster entspricht der virtuellen IP-Adresse des Cisco CSS Switch für die content-Regel eines Eigners.

Geben Sie zum Definieren eines Clusters **lbcontrol cluster add** *Cluster* ein. Zum Festlegen von Cluster-Optionen müssen Sie **lbcontrol cluster set** eingeben.

Schritt 4. Ports definieren und Port-Optionen festlegen

Geben Sie zum Definieren eines Ports **lbcontrol port add** *Cluster:Port* ein. Der Port entspricht dem Port, der in der content-Regel des Cisco CSS Switch für den Eigner konfiguriert ist.

Port ist die Nummer des Ports, den Sie für dieses Protokoll verwenden und die in der content-Regel des Eigners für den Cisco CSS Switch angegeben ist. Weitere Informationen hierzu finden Sie im Abschnitt „*lbcontrol port* — Ports konfigurieren“ auf Seite 386.

Schritt 5. Am Lastausgleich beteiligte Servermaschinen definieren

Sie können für jede Cluster-Port-Kombination mehrere Instanzen eines Servers konfigurieren. (Denken Sie daran, dass die Adresse und der Name der SNMP-Benutzergemeinschaft mit den entsprechenden Attributen des Cisco CSS Switch übereinstimmen muss.) Wenn Sie mehrere Instanzen eines Servers konfigurieren, können Sie zwischen verschiedenen Anwendungsservern unterscheiden, die sich auf einer physischen Maschine befinden und am selben Port auf dieselbe IP-Adresse reagieren.

Geben Sie zum Definieren einer am Lastausgleich beteiligten Servermaschine Folgendes ein:

```
lbcontrol server add Cluster:Port:Server address x.x.x.x | Host-Name
```

Der *Server* entspricht dem Dienstenamen des Cisco CSS Switch.

Für einen Cluster müssen Sie pro Port mehrere Server definieren, um einen Lastausgleich durchführen zu können. Andernfalls muss der gesamte Datenverkehr von einem Server verarbeitet werden. Lesen Sie hierzu die Informationen im Abschnitt „Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)“ auf Seite 163.

Weitere Informationen zur Syntax des Befehls `lbcccontrol server` finden Sie im Abschnitt „lbcccontrol server — Server konfigurieren“ auf Seite 388.

Schritt 6. Manager-Funktion starten

Geben Sie zum Starten des Managers den Befehl **lbcccontrol manager start** ein. Weitere Informationen hierzu finden Sie im Abschnitt „lbcccontrol manager — Manager steuern“ auf Seite 378.

Schritt 7. Advisor-Funktion starten (optional)

Die Advisor-Funktionen liefern dem Manager weitere Informationen über die Fähigkeit der am Lastausgleich beteiligten Servermaschinen, auf Anforderungen zu antworten. Advisor-Funktionen sind protokollspezifisch. Soll beispielsweise die HTTP-Advisor-Funktion gestartet werden, setzen Sie den folgenden Befehl ab:

```
lbcccontrol advisor start http Port
```

Eine Liste der Advisor-Funktionen mit den zugehörigen Standard-Ports finden Sie im Abschnitt „lbcccontrol advisor — Advisor steuern“ auf Seite 364. Eine Beschreibung der einzelnen Advisor-Funktionen können Sie dem Abschnitt „Liste der Advisor-Funktionen“ auf Seite 153 entnehmen.

Schritt 8. Cluster-Proportionen festlegen

Wenn Sie Advisor-Funktionen starten, müssen Sie die Cluster-Proportionen so ändern, dass die Informationen der Advisor-Funktionen in die Entscheidungen zum Lastausgleich einbezogen werden. Verwenden Sie den Befehl **lbcccontrol cluster proportions**. Lesen Sie hierzu die Informationen im Abschnitt „Proportionale Bedeutung von Statusinformationen“ auf Seite 145.

Anmerkung: Wenn Sie eine Advisor-Funktion starten und **Proportion für Systemmetrik** gleich 0 ist, wird dieser Wert auf 1 erhöht. Da die Cluster-Proportionen in der Summe 100 ergeben müssen, wird die Proportion mit dem höchsten Wert in diesem Fall um 1 verringert.

Schritt 9. Metric Server starten (optional)

Informationen zur Verwendung von Metric Server finden Sie im Abschnitt „Metric Server“ auf Seite 161.

Konfiguration testen

Testen Sie, ob die Konfiguration korrekt ist.

1. Setzen Sie den Manager "loglevel" auf 4.
2. Trennen Sie einen Server für eine Minute vom Cisco CSS Switch *oder* fahren Sie den Anwendungsserver für eine Minute herunter.
3. Stellen Sie die Verbindung des Servers zum Switch wieder her oder führen Sie einen Neustart für den Anwendungsserver aus.
4. Setzen Sie den Manager "loglevel" auf den gewünschten Wert (1) zurück.
5. Zeigen Sie die Datei manager.log im Verzeichnis .../nd/servers/logs/lbc an und suchen Sie nach dem Eintrag **setServerWeights setting service**.

Kapitel 14. Erweiterte Funktionen von Network Dispatcher

In diesem Kapitel wird erklärt, wie die Lastausgleichparameter von Network Dispatcher konfiguriert werden und Network Dispatcher für die Verwendung der erweiterten Funktionen eingerichtet wird.

Anmerkung: Falls Sie die Dispatcher-Komponente *nicht* verwenden, ersetzen Sie beim Lesen dieses Kapitels "ndcontrol" durch Folgendes:

- Für CBR: **cbrcontrol**
- Für Mailbox Locator: **mlcontrol**
- Für Site Selector: **sscontrol** (lesen Sie hierzu die Informationen in „Anhang D. Befehlsreferenz für Site Selector“ auf Seite 335)
- Für Cisco Consultant: **lbcontrol** (lesen Sie hierzu die Informationen in „Anhang E. Befehlsreferenz für Consultant für Cisco CSS Switches“ auf Seite 363)

Tabelle 13. Erweiterte Konfigurations-Tasks für Network Dispatcher

Task	Beschreibung	Referenzinformationen
Ändern der Einstellungen für den Lastausgleich (optional)	<p>Sie können die folgenden Einstellungen für den Lastausgleich ändern:</p> <ul style="list-style-type: none">• Die proportionale Bedeutung der Statusinformationen. <p>Das Standardverhältnis ist 50-50-0-0. Wenn Sie den Standardwert verwenden, werden die Informationen von den Advisor-Funktionen und von Metric Server nicht benutzt.</p> <ul style="list-style-type: none">• Wertigkeiten• Feste Wertigkeiten vom Manager• Manager-Intervalle• Sensitivitätsschwelle• Glättungsfaktor	„Lastausgleich mit Network Dispatcher optimieren“ auf Seite 144
Verwendung von Scripts, um einen Alert zu generieren oder Serverausfälle zu protokollieren, wenn der Manager Server als inaktiv/aktiv markiert	Network Dispatcher stellt Benutzer-Exits bereit, die Scripts aktivieren, wenn der Manager Server als inaktiv/aktiv markiert.	„Scripts zum Generieren eines Alerts oder Protokollieren eines Serverausfalls verwenden“ auf Seite 149

Tabelle 13. Erweiterte Konfigurations-Tasks für Network Dispatcher (Forts.)

Task	Beschreibung	Referenzinformationen
Verwendung von Advisor-Funktionen und Erstellen angepasster Advisor-Funktionen	Beschreibt die Advisor-Funktionen und das Schreiben eigener angepasster Advisor-Funktionen zum protokollieren spezifischer Serverstatus	„Advisor-Funktionen“ auf Seite 149 „Kundenspezifische (anpassbare) Advisor-Funktion erstellen“ auf Seite 155
Verwendung der WLM-Advisor-Funktion (Workload Manager)	Die WLM-Advisor-Funktion stellt Informationen zur Systembelastung für Network Dispatcher bereit.	„Advisor-Funktion Workload Manager“ auf Seite 159
Verwendung des Agenten Metric Server	Metric Server stellt Informationen zur Systembelastung für Network Dispatcher bereit.	„Metric Server“ auf Seite 161
Verwendung der Serverpartitionierung	Definieren Sie logische Server zur Verteilung der Last ausgehend von den verfügbaren Diensten.	„Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)“ auf Seite 163
Option "Advisor-Anforderung/ Antwort (URL)"	Definieren Sie eine eindeutige HTTP-URL-Zeichenfolge für einen spezifischen Dienst, der auf der Maschine abgefragt werden soll.	„Option 'Anforderung/ Antwort (URL)' der HTTP-Advisor-Funktion“ auf Seite 165
Verknüpfung von Network Dispatcher mit einer am Lastausgleich beteiligten Maschine	Konfigurieren Sie eine verknüpfte Network-Dispatcher-Maschine.	„Verknüpfte Server verwenden“ auf Seite 166
Konfigurieren der Weitverkehrsunterstützung von Dispatcher	Konfigurieren Sie einen fernen Dispatcher für den Lastausgleich in einem WAN. Der Lastausgleich in einem WAN kann auch (ohne fernen Dispatcher) mit einer Serverplattform durchgeführt werden, die GRE unterstützt.	„Dispatcher-WAN-Unterstützung konfigurieren“ auf Seite 168
Konfigurieren der hohen Verfügbarkeit oder der gegenseitigen hohen Verfügbarkeit	Konfigurieren Sie eine zweite Dispatcher-Maschine, um eine Ausweichmaschine zu haben.	„Hohe Verfügbarkeit“ auf Seite 177
Konfigurieren des regelbasierten Lastausgleichs	Definieren Sie Bedingungen, unter denen eine Untergruppe Ihrer Server verwendet wird.	„Regelbasierten Lastausgleich konfigurieren“ auf Seite 185
Verwendung expliziter Verbindungen	Vermeiden Sie es, den Dispatcher in Verbindungen zu umgehen.	„Explizite Verbindungen benutzen“ auf Seite 197
Verwendung eines privaten Netzes	Konfigurieren Sie den Dispatcher für den Lastausgleich bei Servern in einem privaten Netz.	„Konfiguration für ein privates Netz verwenden“ auf Seite 198

Tabelle 13. Erweiterte Konfigurations-Tasks für Network Dispatcher (Forts.)

Task	Beschreibung	Referenzinformationen
Zusammenfassung allgemeiner Serverkonfigurationen durch einen Platzhalter-Cluster	Adressen, die nicht explizit konfiguriert sind, verwenden den Platzhalter-Cluster für die Verteilung des Datenverkehrs.	„Platzhalter-Cluster verwenden, um Serverkonfigurationen zusammenzufassen“ auf Seite 199
Verwendung eines Platzhalter-Clusters für den Lastausgleich bei Firewalls	Es erfolgt ein Lastausgleich des gesamten Datenverkehrs für Firewalls.	„Platzhalter-Cluster für den Lastausgleich von Firewalls verwenden“ auf Seite 200
Verwendung eines Platzhalter-Clusters mit Caching Proxy für transparente Weiterleitung	Der Dispatcher kann zum Aktivieren einer transparenten Weiterleitung verwendet werden.	„Platzhalter-Cluster mit Caching Proxy für transparente Weiterleitung verwenden“ auf Seite 201
Verwendung eines Platzhalter-Ports für die Übertragung von Datenverkehr mit nicht konfiguriertem Port	Ermöglicht die Bearbeitung von Datenverkehr, der für keinen bestimmten Port konfiguriert ist.	„Platzhalter-Port für die Übertragung von Datenverkehr mit nicht konfiguriertem Port verwenden“ auf Seite 201
Verwendung der Affinitätsfunktion zum Konfigurieren einer Haltezeit für einen Cluster-Port	Ermöglicht das Übertragen von Client-Anforderungen an denselben Server.	„Funktionsweise der Affinität für Network Dispatcher“ auf Seite 202
Verwendung der SDA-API (Server Directed Affinity)	Stellt eine API zur Verfügung, mit der ein externer Agent das Affinitätsverhalten des Dispatchers beeinflussen kann.	„SDA-API zur Steuerung der Client-/Serveraffinität“ auf Seite 202
Verwendung der Port-übergreifenden Affinität, um die Affinität an allen Ports zu nutzen	Ermöglicht den Empfang von Client-Anforderungen von verschiedenen Ports und deren Übertragung an einen Server.	„Port-übergreifende Affinität“ auf Seite 204
Verwendung der Affinitätsadressmaske zum Festlegen einer gemeinsamen IP-Teilnetzadresse	Ermöglicht das Übertragen von Client-Anforderungen, die aus demselben Teilnetz empfangen werden, an denselben Server.	„Affinitätsadressmaske“ auf Seite 204
Außerkräftsetzung der Regelaaffinität, damit ein Server die Port-Affinität außer Kraft setzen kann	Ermöglicht einem Server, die Einstellung für stickytime an seinem Port zu überschreiben.	„Überschreibung der Regelaaffinität“ auf Seite 205
Verwendung der aktiven Cookie-Affinität um die Last von Servern für CBR auszugleichen	Diese Regeloption ermöglicht die Bindung einer Sitzung an einen bestimmten Server.	„Aktive Cookie-Affinität“ auf Seite 207

Tabelle 13. Erweiterte Konfigurations-Tasks für Network Dispatcher (Forts.)

Task	Beschreibung	Referenzinformationen
Verwendung der passiven Cookie-Affinität, um die Last von Servern für die inhaltsabhängige Weiterleitung und die CBR-Komponente auszugleichen.	Mit dieser Regeloption kann eine Sitzung ausgehend vom Cookie-Namen/Wert an einen bestimmten Server gebunden werden.	„Passive Cookie-Affinität“ auf Seite 209
Verwendung der URI-Affinität für den Lastausgleich bei Caching-Proxy-Servern mit Zwischenspeicherung spezifischer Inhalte auf jedem einzelnen Server	Mit dieser Regeloption kann eine Sitzung ausgehend vom URI an einen bestimmten Server gebunden werden.	„URI-Affinität“ auf Seite 210
Verwendung der DoS-Erkennung für die Benachrichtigung von Administratoren über potenzielle Attacken (per Alert)	Der Dispatcher analysiert eingehende Anforderungen auf eine verdächtige Anzahl halboffener TCP-Verbindungen auf Servern.	„Erkennung von DoS-Attacken“ auf Seite 211
Binäre Protokollierung zur Analyse der Serverstatistik	Ermöglicht das Speichern von Serverinformationen in Binärdateien und das Abrufen dieser Informationen aus Binärdateien.	„Binäres Protokollieren verwenden, um Serverstatistiken zu analysieren“ auf Seite 213
Verwendung von Cisco Consultant (zusätzliche Informationen)	Interaktion von Cisco Consultant und dem Cisco CSS Switch sowie zusätzliche Informationen zum Konfigurieren von Wertigkeiten	„Zusätzliche Informationen zu den erweiterten Funktionen von Cisco Consultant“ auf Seite 215

Lastausgleich mit Network Dispatcher optimieren

Die Manager-Funktion von Network Dispatcher führt den Lastausgleich ausgehend von den folgenden Einstellungen durch:

- „Proportionale Bedeutung von Statusinformationen“ auf Seite 145
- „Wertigkeiten“ auf Seite 146
- „Manager-Intervalle“ auf Seite 147
- „Advisor-Intervalle“ auf Seite 151
- „Berichtszeitlimit für Advisor-Funktion“ auf Seite 152
- „Sensitivitätsschwelle“ auf Seite 148
- „Glättungsfaktor“ auf Seite 148

Zur Optimierung des Lastausgleichs für Ihr Netz können Sie diese Einstellungen ändern.

Proportionale Bedeutung von Statusinformationen

Der Manager kann in seine Gewichtungsentscheidung alle oder einige der nachfolgend genannten externen Faktoren einfließen lassen:

- *Aktive Verbindungen*: Die (vom Executor protokollierte) Anzahl aktiver Verbindungen auf jeder am Lastausgleich beteiligten Servermaschine. Diese Proportion gilt nicht für Site Selector.

Oder —

CPU: Prozentsatz der auf jeder am Lastausgleich beteiligten Servermaschine genutzten CPU (Vorgabe vom Metric Server Agent). Für Site Selector wird diese Proportion anstelle der Spalte für aktive Verbindungen angezeigt.

- *Neue Verbindungen*: Die (vom Executor protokollierte) Anzahl neuer Verbindungen auf jeder am Lastausgleich beteiligten Servermaschine. Diese Proportion gilt nicht für Site Selector.

Oder —

Speicher: Prozentsatz des auf jeder am Lastausgleich beteiligten Servermaschine genutzten Speichers (Vorgabe vom Metric Server Agent). Für Site Selector wird diese Proportion anstelle der Spalte für neue Verbindungen angezeigt.

- *Port-spezifisch*: Vorgaben von den Advisor-Funktionen, die am Port empfangsbereit sind.
- *Systemmesswert*: Vorgabe von den Systemüberwachungs-Tools wie Metric Server oder WLM.

Der Manager erhält die beiden ersten Werte (aktive und neue Verbindungen) neben der aktuellen Wertigkeit jedes Servers und anderen für die Berechnungen erforderlichen Informationen vom Executor. Diese Werte basieren auf Informationen, die intern vom Executor generiert und gespeichert werden.

Anmerkung: Für Site Selector erhält der Manager die beiden ersten Werte (CPU und Speicher) von Metric Server. Die beiden ersten Werte für Cisco Consultant (aktive und neue Verbindungen) erhält der Manager vom Cisco CSS Switch.

Sie können die relative Bedeutung der vier Werte pro Cluster (oder Sitename) ändern. Die Proportionen sind vergleichbar mit Prozentsätzen. Die Summe der relativen Proportionen muss 100 % ergeben. Das Standardverhältnis ist 50/50/0/0, wobei die Advisor- und Systeminformationen ignoriert werden. In Ihrer Umgebung sollten Sie andere Proportionen ausprobieren, um die Kombination mit der besten Leistung zu finden.

Anmerkung: Wenn Sie eine Advisor-Funktion (mit Ausnahme von WLM) hinzufügen und die **Port-Proportion** null ist, erhöht der Manager diesen Wert auf 1. Da die Summe der relativen Proportionen immer 100 ist, muss der höchste Wert um 1 vermindert werden.

Wenn Sie die Advisor-Funktion WLM hinzufügen und die **Proportion der Systemmesswerte** null ist, erhöht der Manager diesen Wert auf 1. Da die Summe der relativen Proportionen immer 100 ist, muss der höchste Wert um 1 vermindert werden.

Die Anzahl aktiver Verbindungen hängt sowohl von der Anzahl der Clients als auch von der Zeit ab, die für die Nutzung der von den am Lastausgleich beteiligten Servermaschinen bereitgestellten Dienste erforderlich ist. Sind die Client-Verbindungen schnell (wie bei kleinen Webseiten, die mit HTTP GET bedient werden), ist die Anzahl aktiver Verbindungen ziemlich klein. Wenn die Client-Verbindungen langsamer sind (z. B. bei einer Datenbankabfrage), wird die Anzahl aktiver Verbindungen höher sein.

Sie sollten eine zu niedrige Proportionseinstellung für aktive und neue Verbindungen vermeiden. Wenn Sie diese beiden ersten Werte nicht jeweils auf mindestens 20 gesetzt haben, werden der Lastausgleich und die Glättungsfunktion von Network Dispatcher inaktiviert.

Verwenden Sie zum Festlegen der proportionalen Bedeutung den Befehl **ndcontrol cluster set Cluster proportions**. Weitere Informationen hierzu finden Sie im Abschnitt „ndcontrol cluster — Cluster konfigurieren“ auf Seite 274.

Wertigkeiten

Anmerkung: Wenn Sie die Komponente Cisco Consultant verwenden, finden Sie weitere Informationen im Abschnitt „Wertigkeiten von Cisco Consultant“ auf Seite 216.

Die Manager-Funktion legt Wertigkeiten ausgehend von internen Zählern des Executors, vom Feedback der Advisor-Funktionen und vom Feedback eines Systemüberwachungsprogramms wie Metric Server fest. Falls Sie Wertigkeiten bei Ausführung des Managers manuell festlegen möchten, geben Sie den Befehl "ndcontrol server" mit der Option "fixedweight" an. Eine Beschreibung der Option "fixedweight" finden Sie im Abschnitt „Feste Wertigkeiten vom Manager“ auf Seite 147.

Wertigkeiten gelten für alle Server an einem Port. An einem bestimmten Port werden die Anforderungen entsprechend ihrer relativen Wertigkeit verteilt. Hat beispielsweise ein Server die Wertigkeit 10 und der andere Server die Wertigkeit 5, erhält der Server mit der Wertigkeit 10 doppelt so viele Anforderungen wie der Server mit der Wertigkeit 5.

Für die Wertigkeit, die ein Server haben kann, können Sie einen oberen Grenzwert angeben. Verwenden Sie dazu den Befehl **ndcontrol port set weightbound**. Mit diesem Befehl wird die Differenz festgelegt, die für die einzelnen Server hinsichtlich der Anzahl der Anforderungen gelten soll. Wird die

maximale Wertigkeit auf 1 gesetzt, können alle Server die Wertigkeit 1 haben. Stillgelegte Server haben die Wertigkeit 0 und inaktive Server die Wertigkeit -1. Wenn Sie diese Zahl erhöhen, vergrößern sich die Unterschiede bei der Gewichtung von Servern. Bei einer maximalen Wertigkeit von 2 kann ein Server doppelt so viele Anforderungen wie ein anderer Server erhalten. Bei einer maximalen Wertigkeit von 10 kann ein Server zehn Mal so viele Anforderungen wie ein anderer Server erhalten. Der Standardwert für die maximale Wertigkeit ist 20.

Stellt eine Advisor-Funktion fest, dass ein Server inaktiviert wurde, informiert er den Manager, der die Wertigkeit für den Server auf null setzt. Der Executor sendet in diesem Fall keine weiteren Verbindungen an diesen Server, solange die Wertigkeit bei null liegt. Falls es vor Änderung der Wertigkeit aktive Verbindungen zum Server gab, können diese normal beendet werden.

Feste Wertigkeiten vom Manager

Ohne den Manager können Advisor-Funktionen nicht ausgeführt werden und nicht erkennen, ob ein Server inaktiv ist. Wenn Sie die Advisor-Funktionen ausführen möchten, der Manager jedoch *nicht* die von Ihnen für einen bestimmten Server festgelegte Wertigkeit aktualisieren soll, verwenden Sie den Befehl `"ndcontrol server"` mit der Option **fixedweight**. Beispiel:

```
ndcontrol server set Cluster:Port:Server fixedweight yes
```

Nachdem Sie `"fixedweight"` auf `"yes"` gesetzt haben, können Sie die Wertigkeit mit dem Befehl **ndcontrol server set weight** auf den gewünschten Wert setzen. Der Wert für die Serverwertigkeit bleibt während der Ausführung des Managers unverändert erhalten, bis Sie einen weiteren Befehl `"ndcontrol server"` absetzen, bei dem `"fixedweight"` auf `"no"` gesetzt ist. Weitere Informationen hierzu finden Sie im Abschnitt „ndcontrol server — Server konfigurieren“ auf Seite 320.

Manager-Intervalle

Um den Gesamtdurchsatz zu optimieren, wird die Interaktion von Manager und Executor in ihrer Häufigkeit eingeschränkt. Sie können dieses Intervall mit den Befehlen **ndcontrol manager interval** und **ndcontrol manager refresh** ändern.

Mit dem Manager-Intervall wird angegeben, wie oft der Manager die Serverwertigkeiten aktualisiert, die der Executor für die Weiterleitung von Verbindungen benutzt. Ein zu niedriges Manager-Intervall kann sich negativ auf die Leistung auswirken, da der Manager den Executor permanent unterbricht. Ein zu hohes Manager-Intervall kann bedeuten, dass die Weiterleitung von Anforderungen durch den Executor nicht auf genauen, auf dem neuesten Stand befindlichen Informationen basiert.

Wollen Sie beispielsweise das Manager-Intervall auf 1 Sekunde setzen, geben Sie den folgenden Befehl ein:

```
ndcontrol manager interval 1
```

Der Manager-Aktualisierungszyklus (Refresh) gibt an, wie oft der Manager Statusinformationen vom Executor anfordert. Der Aktualisierungszyklus basiert auf der Intervallzeit.

Wollen Sie beispielsweise den Manager-Aktualisierungszyklus auf 3 setzen, geben Sie den folgenden Befehl ein:

```
ndcontrol manager refresh 3
```

In diesem Fall wartet der Manager 3 Intervalle ab, bevor er Statusinformationen vom Executor anfordert.

Sensitivitätsschwelle

Network Dispatcher bietet noch weitere Methoden der Optimierung des Lastausgleichs für Ihre Server. Im Interesse einer hohen Übertragungsgeschwindigkeit werden die Wertigkeiten der Server nur aktualisiert, wenn sich signifikante Änderungen der Wertigkeit ergeben. Das permanente Aktualisieren der Wertigkeiten bei geringfügigen oder nicht vorhandenen Änderungen des Serverstatus würde zu einem unnötigen Systemaufwand führen. Wenn die prozentuale Änderung der Wertigkeit innerhalb der summierten Wertigkeit für alle Server an einem Port über der Sensitivitätsschwelle liegt, aktualisiert der Manager die vom Executor für die Verteilung der Verbindungen verwendeten Wertigkeiten. Nehmen wir beispielsweise an, die Gesamtwertigkeit ändert sich von 100 % auf 105 %. Die Änderung beträgt also 5 %. Beim standardmäßigen Sensitivitätsschwellenwert von 5 aktualisiert der Manager nicht die vom Executor verwendeten Wertigkeiten, da die prozentuale Änderung nicht **über** dem Schwellenwert liegt. Ändert sich die Gesamtwertigkeit jedoch von 100 % auf 106 %, aktualisiert der Manager die Wertigkeiten. Wollen Sie beispielsweise die Sensitivitätsschwelle des Managers auf einen anderen Wert als den Standardwert setzen (zum Beispiel 6), geben Sie den folgenden Befehl ein:

```
ndcontrol manager sensitivity 6
```

In den meisten Fällen müssen Sie diesen Wert nicht ändern.

Glättungsfaktor

Der Manager berechnet die Serverwertigkeiten dynamisch. Daher kann eine aktualisierte Wertigkeit erheblich von der vorherigen Wertigkeit abweichen. In den meisten Fällen stellt dies kein Problem dar. Gelegentlich kann dies jedoch zu erheblichen Schwankungen bei der Verteilung von Anforderungen führen. So kann beispielsweise ein Server aufgrund seiner hohen Wertigkeit den größten Teil der Anforderungen erhalten. Der Manager stellt fest, dass der Server über eine hohe Anzahl von aktiven Verbindungen verfügt und sehr langsam

antwortet. Der Manager verschiebt die Wertigkeit dann auf die freien Server, so dass dort derselbe Effekt auftritt und Ressourcen folglich ineffizient genutzt werden.

Um die Auswirkungen dieses Problems zu verringern, benutzt der Manager einen Glättungsfaktor. Der Glättungsfaktor begrenzt das Maß, in dem sich die Wertigkeit eines Servers ändern kann, und dämpft so die Änderung bei der Verteilung von Anforderungen. Ein höherer Glättungsfaktor führt zu einer weniger drastischen Änderung der Serverwertigkeiten. Ein geringerer Glättungsfaktor führt zu einer drastischeren Änderung der Serverwertigkeiten. Der Standardwert für den Glättungsfaktor ist 1,5. Bei einem Wert von 1,5 können Serverwertigkeiten sehr dynamisch sein. Bei einem Faktor von 4 oder 5 sind die Wertigkeiten stabiler. Wenn Sie den Glättungsfaktor beispielsweise auf 4 setzen möchten, geben Sie den folgenden Befehl ein:

```
ndcontrol manager smoothing 4
```

In den meisten Fällen müssen Sie diesen Wert nicht ändern.

Scripts zum Generieren eines Alerts oder Protokollieren eines Serverausfalls verwenden

Network Dispatcher stellt Benutzer-Exits bereit, die Scripts aktivieren, die von Ihnen angepasst werden können. Sie können Scripts für die Ausführung automatisierter Aktionen erstellen. Eine solche Aktion wäre beispielsweise das Informieren eines Administrators über inaktive Server per Alert oder das Registrieren eines Ausfalls. Scripts, die Sie anpassen können, finden Sie im Installationsverzeichnis **...nd/servers/samples**. Zum Ausführen der Dateien müssen Sie sie in das Verzeichnis **...nd/servers/bin** verschieben und die Erweiterung **".sample"** löschen. Es stehen die folgenden Beispiel-Scripts bereit:

- **serverDown** — Ein Server wird vom Manager als inaktiv markiert.
- **serverUp** — Ein Server wird vom Manager als aktiv markiert.
- **managerAlert** — Alle Server für einen bestimmten Port werden als inaktiv markiert.
- **managerClear** — Mindestens ein Server ist aktiv, nachdem alle Server für einen bestimmten Port als inaktiv markiert wurden.

Advisor-Funktionen

Advisor-Funktionen sind Agenten von Network Dispatcher. Ihr Zweck ist es, den Zustand und die Belastung der Servermaschinen zu beurteilen. Dies erfolgt durch einen proaktiven Austausch mit den Servern, der dem von Clients vergleichbar ist. Advisor können als transportable Clients der Anwendungsserver betrachtet werden.

Das Produkt stellt mehrere protokollspezifische Advisor-Funktionen für die am häufigsten verwendeten Protokolle zur Verfügung. Es ist jedoch nicht

sinnvoll, alle verfügbaren Advisor-Funktionen mit jeder Komponente von Network Dispatcher zu verwenden. (Die Telnet-Advisor-Funktion wird beispielsweise nicht mit der CBR-Komponente verwendet.) Network Dispatcher unterstützt auch das Konzept der „angepassten Advisor-Funktion“, so dass Benutzer eigene Advisor-Funktionen schreiben können.

Einschränkung für bindungsspezifische Serveranwendungen unter Linux:

Unter Linux bietet Network Dispatcher keine Unterstützung für die Verwendung von Advisor-Funktionen beim Lastausgleich für Server mit bindungsspezifischen Serveranwendungen (einschließlich anderer Komponenten von Network Dispatcher wie Mailbox Locator oder Site Selector), wenn die Bindung an die Cluster-IP-Adresse erfolgt.

Arbeitsweise der Advisor-Funktionen

Advisor-Funktionen öffnen regelmäßig eine TCP-Verbindung zu jedem Server und senden eine Anforderungsnachricht an den Server. Der Inhalt der Nachricht ist spezifisch für das Protokoll, das auf dem Server ausgeführt wird. Die HTTP-Advisor-Funktion sendet beispielsweise eine HTTP-Anfrage „HEAD“ an den Server.

Die Advisor-Funktionen warten dann auf den Empfang einer Antwort vom Server. Nach Empfang der Antwort beurteilt die Advisor-Funktion den Server. Um diesen „Lastwert“ zu ermitteln, messen die meisten Advisor-Funktionen die Zeit, bis der Server antwortet, und verwenden dann diesen Wert (in Millisekunden) als Lastwert.

Die Advisor-Funktionen übergeben dann den Lastwert an die Manager-Funktion, die ihn im Manager-Bericht in der Spalte „Port“ angibt. Der Manager addiert anschließend die Wertigkeiten für alle Quellen entsprechend ihren Proportionen und übergibt diese Werte an die Executor-Funktion. Der Executor benutzt diese Wertigkeiten dann für den Lastausgleich neuer ankommender Client-Verbindungen.

Stellt die Advisor-Funktion fest, dass ein Server aktiv ist und ordnungsgemäß arbeitet, meldet er einen positiven Lastwert ungleich null an den Manager. Stellt die Advisor-Funktion fest, dass ein Server inaktiv ist, gibt er den speziellen Lastwert -1 zurück. Der Manager und der Executor leiten in diesem Fall keine weiteren Verbindungen an diesen Server weiter.

Advisor-Funktion starten und stoppen

Sie können eine Advisor-Funktion Cluster-übergreifend für einen bestimmten Port starten (Gruppen-Advisor-Funktion). Sie können aber auch an einem Port verschiedene Advisor-Funktionen für verschiedene Cluster ausführen (Cluster-/sitespezifische Advisor-Funktion). Wenn Sie Network Dispatcher beispielsweise mit drei Clustern (*ClusterA*, *ClusterB*, *ClusterC*), jeweils mit Port 80, konfiguriert haben, können Sie folgende Schritte ausführen:

- Cluster-/sitespezifische Advisor-Funktion: Geben Sie zum Starten einer Advisor-Funktion am Port 80 für *ClusterA* wie folgt den Cluster und den Port an:

```
ndcontrol advisor start
http ClusterA:80
```

Dieser Befehl startet die Advisor-Funktion "http" am Port 80 für *ClusterA*. Die Advisor-Funktion "http" wird für alle Port 80 von *ClusterA* zugeordneten Server ausgeführt.

- Gruppen-Advisor-Funktion: Geben Sie zum Starten einer angepassten Advisor-Funktion am Port 80 für alle anderen Cluster wie folgt den Port an:

```
ndcontrol advisor start angepasster_Advisor 80
```

Dieser Befehl startet die Advisor-Funktion *angepasster_Advisor* am Port 80 von *ClusterB* und *ClusterC*. Die angepasste Advisor-Funktion wird für alle Port 80 von *ClusterB* und *ClusterC* zugeordneten Server ausgeführt. (Weitere Informationen zu angepassten Advisor-Funktionen finden Sie im Abschnitt „Kundenspezifische (anpassbare) Advisor-Funktion erstellen“ auf Seite 155.)

Anmerkung: Die Gruppen-Advisor-Funktion wird für alle Cluster/Sites ausgeführt, für die es derzeit keine Cluster-/sitespezifische Advisor-Funktion gibt.

Wenn Sie das obige Konfigurationsbeispiel für die Gruppen-Advisor-Funktion verwenden, können Sie bei Bedarf die angepasste Advisor-Funktion *angepasster_Advisor* am Port 80 für einen oder beide Cluster (*ClusterB* und *ClusterC*) stoppen.

- Geben Sie zum Stoppen der angepassten Advisor-Funktion am Port 80 von *ClusterB* wie folgt Cluster und Port an:

```
ndcontrol advisor stop angepasster_Advisor ClusterB:80
```

- Zum Stoppen der angepassten Advisor-Funktion am Port 80 von *ClusterB* und *ClusterC* müssen Sie wie folgt nur den Port angeben:

```
ndcontrol advisor stop angepasster_Advisor 80
```

Advisor-Intervalle

Anmerkung: Die Advisor-Standardwerte funktionieren in den meisten Fällen effizient. Gehen Sie mit Vorsicht vor, wenn Sie andere Werte als die Standardwerte verwenden.

Das Advisor-Intervall legt fest, wie oft eine Advisor-Funktion den Status der Server an dem von ihr überwachten Port abfragt und die Ergebnisse dann an den Manager übergibt. Ein zu niedriges Advisor-Intervall kann sich negativ auf die Leistung auswirken, da der Advisor die Server permanent unterbricht.

Ist das Advisor-Intervall zu hoch, basieren die Entscheidungen des Managers hinsichtlich der Gewichtung unter Umständen nicht auf exakten aktuellen Informationen.

Wenn Sie das Intervall der HTTP-Advisor-Funktion am Port 80 beispielsweise auf 3 Sekunden setzen möchten, geben Sie den folgenden Befehl ein:

```
ndcontrol advisor interval http 80 3
```

Es ist nicht sinnvoll, ein Advisor-Intervall anzugeben, das kleiner als das Manager-Intervall ist. Das Standard-Advisor-Intervall liegt bei sieben Sekunden.

Berichtszeitlimit für Advisor-Funktion

Der Manager verwendet keine Informationen einer Advisor-Funktion, deren Zeitmarke älter als die für das Berichtszeitlimit der Advisor-Funktion festgelegte Zeit ist, um sicherzustellen, dass keine veralteten Informationen verwendet werden. Das Berichtszeitlimit der Advisor-Funktion muss größer als das Sendeaufrufintervall der Advisor-Funktion sein. Ist das Zeitlimit kleiner, ignoriert der Manager Berichte, die logisch betrachtet verwendet werden müssten. Für Berichte der Advisor-Funktion gilt standardmäßig kein Zeitlimit, so dass der Standardwert "unlimited" ist.

Wenn Sie das Berichtszeitlimit für die HTTP-Advisor-Funktion am Port 80 beispielsweise auf 30 Sekunden setzen möchten, geben Sie den folgenden Befehl ein:

```
ndcontrol advisor timeout http 80 30
```

Weitere Informationen zum Festlegen des Berichtszeitlimits für die Advisor-Funktion finden Sie im Abschnitt „ndcontrol advisor — Advisor steuern“ auf Seite 268.

Serververbindungs- und -empfangszeitlimit der Advisor-Funktion

Für Network Dispatcher können Sie die Zeitlimits der Advisor-Funktion festlegen, innerhalb derer der Ausfall eines Servers festgestellt werden soll. Die Zeitlimits für ausgefallene Server ("connecttimeout" und "receivetimeout") bestimmen, wie lange eine Advisor-Funktion wartet, bis sie einen gescheiterten Sende- oder Empfangsvorgang meldet.

Für eine schnellstmögliche Erkennung ausgefallener Server müssen Sie das Verbindungs- und Empfangszeitlimit der Advisor-Funktion auf den kleinsten Wert (eine Sekunde) sowie das Intervall für Advisor-Funktion und Manager auf den kleinsten Wert (eine Sekunde) setzen.

Anmerkung: Falls es in Ihrer Umgebung ein mittleres bis hohes Datenverkehrsaufkommen gibt, so dass sich die Serverantwortzeit erhöht, sollten Sie die Werte "connecttimeout" und "receivetimeout"

out" nicht zu niedrig festlegen. Andernfalls könnte die Advisor-Funktion einen ausgelasteten Server vorschnell als ausgefallenen Server markieren.

Wenn Sie "connecttimeout" und "receivetimeout" für die HTTP-Advisor-Funktion am Port 80 beispielsweise auf 9 Sekunden setzen möchten, geben Sie den folgenden Befehl ein:

```
ndcontrol advisor connecttimeout http 80 9
ndcontrol advisor receivetimeout http 80 9
```

Der Standardwert für das Verbindungs- und Empfangszeitlimit liegt beim Dreifachen des Wertes, der für das Intervall der Advisor-Funktion angegeben wurde.

Liste der Advisor-Funktionen

- Die Advisor-Funktion **http** öffnet eine Verbindung, sendet standardmäßig eine HEAD-Anfrage, wartet auf eine Antwortverbindung und gibt die verstrichene Zeit als Arbeitslast zurück. Im Abschnitt „Option 'Anforderung/ Antwort (URL)' der HTTP-Advisor-Funktion" auf Seite 165 können Sie nachlesen, wie Sie die Art der Anfrage ändern können, die von der HTTP-Advisor-Funktion gesendet wird.
- Die Advisor-Funktion **ftp** öffnet eine Verbindung, sendet eine SYST-Anfrage, wartet auf eine Antwort, beendet die Verbindung und gibt die verstrichene Zeit als Arbeitslast zurück.
- Die Advisor-Funktion **telnet** öffnet eine Verbindung, wartet auf die erste Nachricht vom Server, beendet die Verbindung und gibt die verstrichene Zeit als Arbeitslast zurück.
- Die Advisor-Funktion **nntp** öffnet eine Verbindung, wartet auf die erste Nachricht vom Server, sendet einen quit-Befehl, beendet die Verbindung und gibt die verstrichene Zeit als Arbeitslast zurück.
- Die Advisor-Funktion **imap** öffnet eine Verbindung, wartet auf die erste Nachricht vom Server, sendet einen quit-Befehl, beendet die Verbindung und gibt die verstrichene Zeit als Arbeitslast zurück.
- Die Advisor-Funktion **pop3** öffnet eine Verbindung, wartet auf die erste Nachricht vom Server, sendet einen quit-Befehl, beendet die Verbindung und gibt die verstrichene Zeit als Arbeitslast zurück.
- Die Advisor-Funktion **smtp** öffnet eine Verbindung, wartet auf die erste Nachricht vom Server, sendet einen quit-Befehl, beendet die Verbindung und gibt die verstrichene Zeit als Arbeitslast zurück.
- Die Advisor-Funktion **ssl** öffnet eine Verbindung, sendet eine CLIENT-HELLO-Anfrage, wartet auf eine Antwort, beendet die Verbindung und gibt die verstrichene Zeit als Arbeitslast zurück.

Anmerkung: Die SSL-Advisor-Funktion ist nicht von der Schlüsselverwaltung oder von Zertifikaten abhängig.

- Die Advisor-Funktion **ssl2http** wird für die unter Port 443 aufgelisteten Server gestartet und ausgeführt, öffnet jedoch einen Socket zum "mapport" für HTTP-Anforderungen. Wenden Sie die Advisor-Funktion "ssl2http" nur für CBR an, wenn vom Client zum Proxy das Protokoll SSL und vom Proxy zum Server das Protokoll HTTP verwendet wird. Weitere Informationen hierzu finden Sie im Abschnitt „SSL-Datenverkehr vom Client zum Proxy und HTTP-Datenverkehr vom Proxy zum Server verteilen“ auf Seite 85.
- Die Caching-Proxy-Advisor-Funktion (**ibmproxy**) öffnet eine Verbindung, sendet eine für Caching Proxy spezifische HTTP-GET-Anfrage und interpretiert die Antwort als eine Caching-Proxy-Arbeitslast.

Anmerkung: Wenn Sie die Advisor-Funktion **ibmproxy** verwenden möchten, muss Caching Proxy auf allen Servern mit Lastausgleich aktiv sein. Auf der Maschine mit Network Dispatcher muss Caching Proxy nur installiert werden, wenn es sich um die Maschine handelt, für die gleichzeitig der Lastausgleich durchgeführt wird.

- Die Advisor-Funktion **dns** öffnet eine Verbindung, sendet eine Zeigeranfrage für DNS, wartet auf eine Antwort, beendet die Verbindung und gibt die verstrichene Zeit als Arbeitslast zurück.
- Die Advisor-Funktion **connect** tauscht keine protokollspezifischen Daten mit dem Server aus. Er misst nur die Zeit, die benötigt wird, um eine TCP-Verbindung zu dem Server zu öffnen und zu schließen. Dieser Advisor ist für Serveranwendungen nützlich, die TCP verwenden, jedoch mit einem Protokoll höherer Ebene, für das keine von IBM gelieferte oder anpassbare Advisor-Funktion verfügbar ist.
- Die Advisor-Funktion **ping** öffnet keine TCP-Verbindung zu Servern und meldet stattdessen, ob der Server auf ein "ping" antwortet. Die Advisor-Funktion "ping" kann für jeden Port verwendet werden, ist jedoch speziell für Konfigurationen mit einem Platzhalter-Port konzipiert, über den Datenverkehr mit verschiedenen Protokollen fließen kann. Er ist außerdem für Konfigurationen mit Servern nützlich, die andere als die TCP-Protokolle verwenden, z. B. UDP.
- Die Advisor-Funktion **reach** sendet ein "ping" an die zugehörigen Zielmaschinen. Dieser Advisor wurde für die Dispatcher-Komponenten für hohe Verfügbarkeit entwickelt, um die Erreichbarkeit der „reach-Ziele“ zu bestimmen. Die Ergebnisse werden an die Komponente für hohe Verfügbarkeit übergeben und erscheinen nicht im Manager-Bericht. Im Gegensatz zu anderen Advisor-Funktionen wird "reach" *automatisch* von der Manager-Funktion der Dispatcher-Komponente gestartet.
- Die Advisor-Funktion **db2** arbeitet mit den DB2-Servern zusammen. Der Dispatcher verfügt über die Fähigkeit, den Status von DB2-Servern zu über-

prüfen, ohne dass Kunden eigene angepasste Advisor-Funktionen schreiben müssen. Die DB2-Advisor-Funktion kommuniziert nur mit dem Port für DB2-Verbindungen, nicht mit dem Port für Java-Verbindungen.

- Die Advisor-Funktion **wlm** (Workload Manager) ist für Server auf OS/390-Großrechnern bestimmt, die die Komponente MVS Workload Manager (WLM) ausführen. Weitere Informationen hierzu finden Sie im Abschnitt „Advisor-Funktion Workload Manager“ auf Seite 159.
- Die Advisor-Funktion **self** sammelt Informationen zum Auslastungsstatus von Back-End-Servern. Sie können die Advisor-Funktion "self" anwenden, wenn Sie den Dispatcher in einer Client-/Serverkonfiguration verwenden, so dass der Dispatcher Informationen von der Advisor-Funktion "self" an den übergeordneten Network Dispatcher liefert. Die Advisor-Funktion "self" misst insbesondere die Verbindungen pro Sekunde für die Back-End-Server des Dispatchers auf Executor-Ebene. Weitere Informationen hierzu finden Sie im Abschnitt „Advisor-Funktion 'self' in einer Client/Server-WAND-Konfiguration“ auf Seite 176.
- Der Dispatcher bietet einem Kunden die Möglichkeit, eine *angepasste* (anpassbare) Advisor-Funktion zu schreiben. Damit werden persönliche Protokolle unterstützt (zusätzlich zu TCP), für die IBM keinen spezifischen Advisor entwickelt hat. Weitere Informationen hierzu finden Sie im Abschnitt „Kundenspezifische (anpassbare) Advisor-Funktion erstellen“.
- Die Advisor-Funktion **was** (WebSphere Application Server) arbeitet mit den WebSphere-Application-Servern zusammen. Anpassbare Beispieldateien für die Advisor-Funktion finden Sie im Installationsverzeichnis. Der Abschnitt „WAS-Advisor-Funktion“ auf Seite 156 enthält weitere Informationen zu diesem Thema.

Kundenspezifische (anpassbare) Advisor-Funktion erstellen

Die kundenspezifische (anpassbare) Advisor-Funktion ist ein kurzer Java-Code, den Sie als Klassendatei bereitstellen, die vom Basiscode aufgerufen wird. Der Basiscode gewährleistet alle Verwaltungsdienste wie das Starten und Stoppen einer Instanz der angepassten Advisor-Funktion, das Bereitstellen von Status und Berichten sowie das Aufzeichnen von Protokolldaten in einer Protokolldatei. Er übergibt auch die Ergebnisse an die Manager-Funktion. Der Basiscode führt regelmäßig einen Advisor-Zyklus aus, wobei alle Server in der Konfiguration individuell ausgewertet werden. Dieser beginnt mit dem Öffnen einer Verbindung zu einer Servermaschine. Wenn das Socket geöffnet wird, ruft der Basiscode die Methode (Funktion) „getLoad“ der angepassten Advisor-Funktion auf. Die angepasste Advisor-Funktion führt dann alle für die Auswertung des Serverstatus erforderlichen Schritte aus. Normalerweise sendet er eine benutzerdefinierte Nachricht an den Server und wartet dann auf eine Antwort. (Die angepasste Advisor-Funktion erhält Zugriff auf den geöffneten Socket.) Der Basiscode schließt dann den Socket zu dem Server und übergibt die Lastinformationen an den Manager.

Der Basiscode und die angepasste Advisor-Funktion können im normalen Modus oder im Ersetzungsmodus arbeiten. Die Auswahl der Betriebsart wird in der Datei der angepassten Advisor-Funktion als Parameter der Methode "constructor" angegeben. Im normalen Modus tauscht die angepasste Advisor-Funktion Daten mit dem Server aus. Der Basiscode der Advisor-Funktion misst die Zeit für den Austausch und berechnet den Lastwert. Der Basiscode übergibt dann diesen Lastwert an den Manager. Die angepasste Advisor-Funktion muss nur null (bei Erfolg) oder -1 (bei einem Fehler) zurückgeben. Zur Angabe des normalen Modus wird die Markierung "replace" der Methode "constructor" auf "false" (falsch) gesetzt.

Im Ersetzungsmodus führt der Basiscode keine Zeitmessungen aus. Der Code der angepassten Advisor-Funktion führt alle für die funktionsspezifischen Anforderungen erforderlichen Operationen aus und gibt dann einen tatsächlichen Lastwert zurück. Der Basiscode akzeptiert diesen Wert und übergibt ihn an den Manager. Um bestmögliche Ergebnisse zu erzielen, sollten Sie den Lastwert zwischen 10 und 1000 normalisieren, wobei 10 einen schnellen Server und 1000 einen langsamen Server angibt. Zur Angabe des Ersetzungsmodus muss die Markierung "replace" der Methode "constructor" auf "true" gesetzt werden.

Auf diese Weise können Sie eigene Advisor-Funktionen schreiben, die die benötigten präzisen Informationen über Server zur Verfügung stellen. Zu Network Dispatcher wird ein Beispiel für eine angepasste Advisor-Funktion, **ADV_sample.java**, geliefert. Nach der Installation von Network Dispatcher finden Sie den Beispielcode im Installationsverzeichnis **...nd/servers/samples/CustomAdvisors**.

Die Standardinstallationsverzeichnisse sind:

- AIX: /usr/lpp/nd
- Linux: /opt/nd
- Sun: /opt/nd
- Windows 2000: c:\Programme\IBM\nd

WAS-Advisor-Funktion

Das Installationsverzeichnis von Network Dispatcher enthält Beispieldateien für angepasste Advisor-Funktionen, insbesondere für die WAS-Advisor-Funktion (WebSphere Application Server).

- ADV_was.java ist die Datei, die kompiliert und auf der Network Dispatcher-Maschine ausgeführt werden muss.
- Die Datei NDAdvisor.java.servlet muss kompiliert und auf der WAS-Maschine ausgeführt werden (nachdem sie in NDAdvisor.java umbenannt wurde).

Die Beispieldateien für die WAS-Advisor-Funktion befinden sich in demselben Verzeichnis wie die Datei ADV_sample.java.

Namenskonvention

Der Dateiname für Ihre angepasste Advisor-Funktion muss das Format „ADV_*meinAdvisor*.java“ haben. Er muss mit dem Präfix „ADV_“ in Großbuchstaben beginnen. Alle nachfolgenden Zeichen müssen Kleinbuchstaben sein.

Aufgrund von Java-Konventionen muss der Name der in der Datei definierten Klasse mit dem Namen der Datei übereinstimmen. Wenn Sie den Beispielcode kopieren, stellen Sie sicher, dass alle Exemplare von „ADV_sample“ in der Datei in den neuen Klassennamen geändert werden.

Kompilierung

Angepasste Advisor-Funktionen werden in der Sprache Java geschrieben. Sie müssen deshalb einen Java-1.3-Compiler für Ihre Maschine erwerben und installieren. Während der Kompilierung wird auf die folgenden Dateien Bezug genommen:

- die Datei der angepassten Advisor-Funktion
- die Basisklassendatei `ibmnd.jar` im Unterverzeichnis `...nd/servers/lib` des Installationsverzeichnisses von Network Dispatcher.

Der Klassenpfad muss während der Kompilierung auf die Datei der angepassten Advisor-Funktion und die Datei mit den Basisklassen zeigen.

Ein Kompilierungsbeefehl für Windows 2000 könnte wie folgt aussehen:

```
javac -classpath <Installationsverzeichnis>\nd\servers\lib\ibmnd.jar  
ADV_fred.java
```

Für diesen Befehl gilt Folgendes:

- Ihre Advisor-Datei hat den Namen `ADV_fred.java`.
- Ihre Advisor-Datei ist im aktuellen Verzeichnis gespeichert.

Die Ausgabe der Kompilierung ist eine Klassendatei, zum Beispiel `ADV_fred.class`

Kopieren Sie vor dem Starten der Advisor-Funktion die Klassendatei in das Unterverzeichnis `...nd/servers/lib/CustomAdvisors` des Installationsverzeichnisses von Network Dispatcher.

Anmerkung: Bei Bedarf können angepasste Advisor-Funktionen unter einem Betriebssystem kompiliert und unter einem anderen Betriebssystem ausgeführt werden. Sie können beispielsweise Ihre Advisor-Funktion unter Windows 2000 kompilieren, die Klassendatei (im Binärformat) auf eine AIX-Maschine kopieren und die Advisor-Funktion dort ausführen.

Für AIX, Linux und Sun ist die Syntax ähnlich.

Ausführung

Bevor Sie die angepasste Advisor-Funktion ausführen, müssen Sie die Klassendatei in das richtige Unterverzeichnis von Network Dispatcher kopieren:

```
.../nd/servers/lib/CustomAdvisors/ADV_fred.class
```

Konfigurieren Sie die Komponente, starten Sie die zugehörige Manager-Funktion und setzen Sie wie folgt den Befehl zum Starten der angepassten Advisor-Funktion ab:

```
ndcontrol advisor start fred 123
```

Für diesen Befehl gilt Folgendes:

- Der Name Ihrer Advisor-Funktion ist "fred", wie in ADV_fred.java.
- Der Port, an dem Ihre Advisor-Funktion ausgeführt wird, ist 123.

Erforderliche Routinen

Eine angepasste Advisor-Funktion erweitert wie alle anderen Advisor-Funktionen den Advisor-Basiscode ADV_Base. Es ist der Advisor-Basiscode, der die meisten Funktionen ausführt. Dazu gehört das Zurückmelden von Belastungen an den Manager, die für den Wertigkeitsalgorithmus des Managers verwendet werden. Darüber hinaus stellt der Advisor-Basiscode Socket-Verbindungen her, schließt Sockets und stellt Send- und Empfangsmethoden für die Advisor-Funktion bereit. Die Advisor-Funktion selbst wird nur zum Senden von Daten an den Port bzw. Empfangen von Daten vom Port des empfohlenen Servers verwendet. Die TCP-Methoden innerhalb des Advisor-Basiscodes sind zeitlich gesteuert, um die Last zu berechnen. Mit einer Markierung der Methode "constructor" in ADV_base kann bei Bedarf die vorhandene Last mit der neuen, von der Advisor-Funktion zurückgegebenen Last überschrieben werden.

Anmerkung: Der Advisor-Basiscode stellt in angegebenen Intervallen die Last ausgehend von einem in der Methode "constructor" gesetzten Wert für den Wertigkeitsalgorithmus bereit. Wenn die eigentliche Advisor-Funktion noch keine gültige Last zurückgeben kann, verwendet der Advisor-Basiscode die vorherige Last.

Basisklassenmethoden sind:

- Eine Routine **constructor**. Die constructor-Routine ruft die constructor-Methode "base class" auf (siehe Advisor-Beispieldatei).
- Eine Methode **ADV_AdvisorInitialize**. Diese Methode stellt einen Hook für den Fall zur Verfügung, dass zusätzliche Schritte ausgeführt werden müssen, nachdem die Basisklasse ihre Initialisierung beendet hat.

- Eine Routine **getload**. Die Basis-Advisor-Klasse führt das Öffnen des Sockets aus. Daher muss getload nur die entsprechenden Sende- und Empfangsanforderungen absetzen, um den Advisor-Zyklus zu beenden.

Suchreihenfolge

Network Dispatcher durchsucht zunächst die Liste der eigenen Advisor-Funktionen. Wenn eine bestimmte Advisor-Funktion dort nicht aufgeführt ist, durchsucht Network Dispatcher die Kundenliste der angepassten Advisor-Funktionen.

Benennung und Pfad

- Die Klasse der angepassten Advisor-Funktion muss sich im Unterverzeichnis **...nd/servers/lib/CustomAdvisors/** des Basisverzeichnisses von Network Dispatcher befinden. Die Standardwerte für dieses Verzeichnis hängen vom verwendeten Betriebssystem ab:
 - AIX
/usr/lpp/nd/servers/lib/CustomAdvisors/
 - Linux
/opt/nd/servers/lib/CustomAdvisors/
 - Solaris
/opt/nd/servers/lib/CustomAdvisors/
 - Windows 2000
Allgemeiner Installationsverzeichnispfad:
C:\Programme\IBM\edge\nd\servers\lib\CustomAdvisors

Interner Installationsverzeichnispfad:
C:\Programme\IBM\nd\servers\lib\CustomAdvisors
- Es sind nur alphabetische Zeichen in Kleinschreibung zulässig. Ein Bediener muss somit bei der Eingabe von Befehlen in der Befehlszeile nicht auf die Groß-/Kleinschreibung achten. Der Advisor-Name muss den Präfix **ADV_** haben.

Beispiel-Advisor-Funktion

Die Programmliste für eine Beispiel-Advisor-Funktion finden Sie im Abschnitt „Beispiel-Advisor-Funktion“ auf Seite 400. Nach der Installation befindet sich diese Beispiel-Advisor-Funktion im Verzeichnis **...nd/servers/samples/CustomAdvisors**.

Advisor-Funktion Workload Manager

WLM ist Code, der auf MVS-Großrechnern ausgeführt wird. Er kann abgefragt werden, um die Belastung auf der MVS-Maschine zu bestimmen.

Wurde MVS Workload Management auf Ihrem OS/390-System konfiguriert, kann der Dispatcher Kapazitätsinformationen von WLM akzeptieren und die Informationen für den Lastausgleich verwenden. Mit der Advisor-Funktion WLM öffnet der Dispatcher regelmäßig Verbindungen über den WLM-Port der einzelnen Server in der Dispatcher-Host-Tabelle und akzeptiert die zurückgegebenen ganzzahligen Kapazitätswerte. Da diese ganzen Zahlen die noch verfügbare Kapazität darstellen und der Dispatcher Werte erwartet, die die Belastung auf jeder Maschine angeben, werden die ganzzahligen Kapazitätswerte vom Advisor in Lastwerte umgekehrt und normalisiert (d. h., ein hoher ganzzahliger Kapazitätswert und ein niedriger Lastwert geben beide einen akzeptablen Zustand eines Servers an). Die daraus resultierenden Belastungen werden in die Spalte 'System' des Manager-Berichts gestellt.

Es gibt mehrere wichtige Unterschiede zwischen dem WLM-Advisor und anderen Advisor-Funktionen des Dispatchers:

1. Andere Advisor-Funktionen öffnen Verbindungen zu den Servern unter Verwendung des Ports, über den der normale Client-Datenverkehr fließt. Die WLM-Advisor-Funktion benutzt für das Öffnen von Verbindungen zu den Servern nicht den für normalen Datenverkehr verwendeten Port. Der WLM-Agent muss auf den einzelnen Servermaschinen so konfiguriert werden, dass er an dem Port empfangsbereit ist, an dem die WLM-Advisor-Funktion des Dispatchers gestartet wurde. Der Standard-WLM-Port ist 10007.
2. Andere Advisor-Funktionen bewerten nur die in der Konfiguration Cluster:Port:Server des Dispatchers definierten Server, deren Server-Port mit dem Port der Advisor-Funktion übereinstimmt. Die WLM-Advisor-Funktion wird für alle Server in der Konfiguration Cluster:Port:Server des Dispatchers ausgeführt. Daher dürfen Sie bei Verwendung der WLM-Advisor-Funktion nur WLM-Server definieren.
3. Andere Advisor-Funktionen stellen ihre Lastinformationen in die Spalte „Port“ des Manager-Berichts. Die Advisor-Funktion WLM stellt ihre Lastinformationen in die Spalte 'System' des Manager-Berichts.
4. Es ist möglich, protokollspezifische Advisor-Funktionen zusammen mit der Advisor-Funktion WLM zu verwenden. Die protokollspezifischen Advisor-Funktionen fragen die Server an den regulären Ports für Datenverkehr ab. Die WLM-Advisor-Funktion fragt die Systembelastung dagegen am WLM-Port ab.

Einschränkung für Metric Server

Der WLM-Agent gibt wie der Agent Metric Server Berichte zu kompletten Serversystemen aus und nicht zu einzelnen protokollspezifischen Serverdämonen. Metric Server und WLM stellen ihre Ergebnisse in die Spalte "System" des Manager-Berichts. Deshalb wird die gleichzeitige Ausführung der Advisor-Funktionen WLM und Metric Server nicht unterstützt.

Metric Server

Diese Funktion ist für alle Komponenten von Network Dispatcher verfügbar.

Metric Server gibt Network Dispatcher Informationen zur Serverauslastung. Diese Informationen werden in Form systemspezifischer Messwerte für den Serverzustand bereitgestellt. Der Manager von Network Dispatcher richtet Anfragen an den Agenten Metric Server, der sich auf jedem der Server befindet, und legt anhand der Messwerte, die er von den Agenten erhalten hat, Wertigkeiten für den Lastausgleich fest. Die Ergebnisse werden auch in den Manager-Bericht gestellt.

Anmerkung: Wenn für jeden Server zwei oder mehr Messwerte ermittelt und in einen Systemauslastungswert normalisiert werden, kann es zu Rundungsfehlern kommen.

Ein Konfigurationsbeispiel ist in Abb. 11 auf Seite 44 dargestellt.

WLM-Einschränkung

Wie die Advisor-Funktion WLM gibt Metric Server Berichte zu kompletten Serversystemen aus und nicht zu einzelnen protokollspezifischen Serverdämonen. WLM und Metric Server stellen ihre Ergebnisse in die Spalte "System" des Manager-Berichts. Deshalb wird die gleichzeitige Ausführung der Advisor-Funktionen WLM und Metric Server nicht unterstützt.

Vorbedingungen

Der Agent Metric Server muss auf Servern installiert und ausgeführt werden, für die Network Dispatcher einen Lastausgleich durchführt.

Metric Server verwenden

Nachfolgend sind die Schritte aufgeführt, mit denen Sie Metric Server für den Dispatcher konfigurieren. Wenn Sie Metric Server für andere Komponenten von Network Dispatcher konfigurieren möchten, sind ähnliche Schritte auszuführen.

- Network Dispatcher Manager (Network-Dispatcher-Seite)
 1. Starten Sie **ndserver**.
 2. Setzen Sie den Befehl **ndcontrol manager start *manager.log Port*** ab.
Port ist hier der ausgewählte RMI-Port für alle Metric-Server-Agenten. Der in der Datei `metricserver.cmd` festgelegte Standard-RMI-Port ist 10004.
 3. Setzen Sie den Befehl **ndcontrol metric add *Cluster:Systemmesswert*** ab.
Systemmesswert ist hier der Name des Scripts (auf dem Back-End-Server), das für jeden Server, der unter dem angegebenen Cluster (oder Sitenamen) in der Konfiguration enthalten ist, ausgeführt werden soll. Für den Kunden stehen die beiden Scripts **cpuload** und **memload** bereit. Sie können auch angepasste Scripts für Systemmesswerte erstellen. Das

Script enthält einen Befehl, der einen numerischen Wert im Bereich von 0-100 zurückgeben sollte. Dieser numerische Wert sollte eine Lastmessung und keinen Verfügbarkeitswert darstellen.

Anmerkung: Für Site Selector werden "cpuload" und "memload" automatisch ausgeführt.

Einschränkung: Wenn der Name Ihres Scripts für Systemmesswerte unter Windows 2000 eine andere Erweiterung als ".exe" hat, müssen Sie den vollständigen Namen der Datei (z. B. "meinsystemscript.bat") angeben. Dies ergibt sich aus einer Java-Einschränkung.

4. Fügen Sie zur Konfiguration nur Server hinzu, die einen Metric-Server-Agenten enthalten, der für den in der Datei metricserver.cmd angegebenen Port ausgeführt wird. Der Port sollte mit dem im Befehl **manager start** angegebenen Port-Wert übereinstimmen.

Anmerkung: Gewährleisten Sie wie folgt die Sicherheit:

- Erstellen Sie auf der Network-Dispatcher-Maschine einen Schlüsselring für die Komponente, die ausgeführt wird. (Verwenden Sie dazu den Befehl **ndkeys create**.) Weitere Informationen zu "ndkeys" finden Sie im Abschnitt „Authentifizierte Fernverwaltung“ auf Seite 219.
 - Kopieren Sie den resultierenden Schlüsselring auf der Servermaschine in das Verzeichnis **.../nd/admin/key**. Stellen Sie sicher, dass die Berechtigungen für den Schlüsselring dem Benutzer "root" den Lesezugriff ermöglichen.
- Agent Metric Server (Seite der Servermaschine)
 1. Installieren Sie das Metric-Server-Paket aus dem Installationsverzeichnis von Network Dispatcher.
 2. Überprüfen Sie anhand des Scripts **metricserver** im Verzeichnis **/usr/bin**, ob der gewünschte RMI-Port verwendet wird. (Für Windows 2000 lautet das Verzeichnis C:\WINNT\SYSTEM32.) Der Standard-RMI-Port ist 10004.

Anmerkung: Der für den RMI-Port angegebene Wert muss mit dem RMI-Port-Wert für Metric Server auf der Network-Dispatcher-Maschine übereinstimmen.

3. Die beiden folgenden Scripts werden dem Kunden bereits zur Verfügung gestellt: **cpuload** (gibt den Prozentsatz der verwendeten CPU im Bereich von 0-100 zurück) und **memload** (gibt den Prozentsatz des belegten Speichers im Bereich von 0-100 zurück). Diese Scripts befinden sich im Verzeichnis **...nd/ms/script**.

Optional können Kunden ihre eigenen angepassten Script-Dateien für Messwerte schreiben, in denen definiert ist, welchen Befehl Metric Ser-

ver auf den Servermaschinen absetzen soll. Vergewissern Sie sich, dass alle angepassten Scripts ausführbar sind und sich im Verzeichnis **...nd/ms/script** befinden. Angepasste Scripts **müssen** einen numerischen Lastwert im Bereich von 0 bis 100 zurückgeben.

Anmerkung: Ein angepasstes Script für Messwerte muss ein gültiges Programm oder Script mit der Erweiterung **".bat"** oder **".cmd"** sein. Auf UNIX-Plattformen müssen Scripts mit der Shell-Deklaration beginnen, da sie sonst möglicherweise nicht richtig ausgeführt werden.

4. Starten Sie den Agenten durch Absetzen des Befehls **metricserver**.
5. Zum Stoppen des Agenten Metric Server müssen Sie den Befehl **metric-server stop** absetzen.

Wenn Metric Server für eine vom lokalen Host abweichende Adresse ausgeführt werden soll, müssen Sie die Datei "metricserver" auf der am Lastausgleich beteiligten Servermaschine editieren. Fügen Sie in der Datei "metricserver" nach dem Eintrag "java" Folgendes ein:

```
-Djava.rmi.server.hostname=andere_Adresse
```

Fügen Sie außerdem vor den Anweisungen "if" die folgende Zeile zur Datei "metricserver" hinzu: `hostname andere_Adresse`.

Unter Windows 2000 müssen Sie außerdem in Microsoft Stack den Aliasnamen für *andere_Adresse* angeben. Informationen zum Angeben eines Aliasnamens für eine Adresse in Microsoft Stack finden Sie auf Seite 185.

Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)

Wenn Sie einen Server in der Network-Dispatcher-Konfiguration angeben, können Sie die Last ausgehend vom Status des gesamten Servers (mit dem Agenten Metric Server) und/oder vom Status einer Port-spezifischen Anwendung (mit der Advisor-Funktion) verteilen.

Bei Anwendung der Serverpartitionierung können Sie darüber hinaus zwischen URLs und ihren spezifischen Anwendungen unterscheiden. Ein Webserver kann beispielsweise JSPs und HTML-Seiten bereitstellen, Datenbankabfragen bedienen usw. Network Dispatcher bietet jetzt die Möglichkeit, einen Cluster- und Port-spezifischen Server in mehrere logische Server zu partitionieren. Dadurch können Sie einen bestimmten Dienst auf der Maschine anweisen festzustellen, ob eine Servlet-Steuerkomponente oder eine Datenbankabfrage schneller oder gar nicht ausgeführt wird.

Mit der Serverpartitionierung kann Network Dispatcher z. B. erkennen, dass der HTML-Dienst Seiten schnell bereitstellt, die Datenbankverbindung jedoch nicht mehr aktiv ist. Dadurch können Sie die Last mit größerer Detaillierung und dienstspezifisch verteilen und müssen sich nicht auf die Wertigkeit des Gesamtserverns verlassen.

Innerhalb der Network-Dispatcher-Konfiguration können Sie einen physischen oder logischen Server mit der Hierarchie *Cluster:Port:Server* darstellen. Der Server kann eine eindeutige IP-Adresse der Maschine (physischer Server) sein, die als symbolischer Name oder in Schreibweise mit Trennzeichen angegeben wird. Wenn Sie den Server als partitionierten Server konfigurieren, müssen Sie den Befehl **ndcontrol server add** mit einer auflösbaren Serveradresse des physischen Servers für den Parameter **address** angeben. Weitere Informationen hierzu finden Sie im Abschnitt „ndcontrol server — Server konfigurieren“ auf Seite 320.

Nachfolgend sehen Sie ein Beispiel für die Partitionierung physischer Server in logische Server zur Bearbeitung von Anforderungen verschiedenen Typs.

```
Cluster: 1.1.1.1
  Port: 80
    Server: A (IP address 1.1.1.2)
             html server
    Server: B (IP address 1.1.1.2)
             gif server
    Server: C (IP address 1.1.1.3)
             html server
    Server: D (IP address 1.1.1.3)
             jsp server
    Server: E (IP address 1.1.1.4)
             gif server
    Server: F (IP address 1.1.1.4)
             jsp server
  Rule1: \*.htm
        Server: A
        Server: C
  Rule2: \*.jsp
        Server: D
        Server: F
  Rule3: \*.gif
        Server: B
        Server: E
```

In diesem Beispiel wird der Server 1.1.1.2 in zwei logische Server partitioniert, A (zur Bearbeitung von HTML-Anforderungen) und B (zur Bearbeitung von GIF-Anforderungen). Server 1.1.1.3 wird in zwei logische Server partitioniert, C (zur Bearbeitung von HTML-Anforderungen) und D (zur Bearbeitung von JSP-Anforderungen). Server 1.1.1.4 wird in zwei logische Server partitioniert, E (zur Bearbeitung von GIF-Anforderungen) und F (zur Bearbeitung von JSP-Anforderungen).

Anmerkung: Es gilt die Einschränkung, dass SDA (Server Directed Affinity) nicht zusammen mit der Serverpartitionierung angewendet werden kann, da SDA für Suchfunktionen eindeutige Serveradressen in der Konfiguration erfordert. Weitere Informationen hierzu finden Sie im Abschnitt „SDA-API zur Steuerung der Client-/Serveraffinität“ auf Seite 202.

Option 'Anforderung/Antwort (URL)' der HTTP-Advisor-Funktion

Die URL-Option der HTTP-Advisor-Funktion ist für die Komponenten Dispatcher und CBR verfügbar.

Nach dem Starten einer HTTP-Advisor-Funktion können Sie für den Dienst, den Sie vom Server anfordern möchten, eine eindeutige Client-HTTP-URL-Zeichenfolge definieren. Mit dieser Zeichenfolge kann die HTTP-Advisor-Funktion den Status einzelner Dienste auf einem Server bewerten.

Dies können Sie erreichen, indem Sie logische Server, die dieselbe physische IP-Adresse haben, mit eindeutigen Servernamen definieren. Weitere Informationen hierzu finden Sie im Abschnitt „Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)“ auf Seite 163.

Für jeden unter dem HTTP-Port definierten logischen Server können Sie eine für den Dienst, den Sie vom Server anfordern möchten, eine eindeutige Client-HTTP-URL-Zeichenfolge angeben. Die HTTP-Advisor-Funktion verwendet die Zeichenfolge **advisorrequest**, um den Status der Server abzufragen. Der Standardwert ist HEAD / HTTP/1.0. Die Zeichenfolge **advisorresponse** ist die Antwort der Advisor-Funktion, nach der die HTTP-Advisor-Funktion die HTTP-Antwort durchsucht. Die HTTP-Advisor-Funktion vergleicht die Zeichenfolge **advisorresponse** mit der tatsächlich vom Server empfangenen Antwort. Der Standardwert ist null.

Wichtiger Hinweis: Wenn die HTTP-URL-Zeichenfolge ein Leerzeichen enthält, gilt Folgendes:

- Bei Absetzen des Befehls von der Shell-Eingabeaufforderung **ndcontrol>>** müssen Sie die Zeichenfolge in Anführungszeichen setzen. Beispiel:

```
server set Cluster:Port:Server advisorrequest "head / http/2.0"  
server set Cluster:Port:Server advisorresponse "HTTP 200 OK"
```
- Beim Absetzen des Befehls **ndcontrol** an der Eingabeaufforderung des Betriebssystems müssen Sie dem Text die Zeichen "\" voranstellen und den Text mit den Zeichen \"" beenden. Beispiel:

```
ndcontrol server set Cluster:Port:Server advisorrequest  
\"head / http/2.0\"  
ndcontrol server set Cluster:Port:Server advisorresponse \"HTTP 200 OK\"
```

Anmerkung: Nach dem Start einer HTTP-Advisor-Funktion für eine angegebene HTTP-Port-Nummer, wird für Server an diesem HTTP-Port der Abfrage-/Antwortwert der Advisor-Funktion aktiviert. Weitere Informationen hierzu finden Sie im Abschnitt „ndcontrol server — Server konfigurieren“ auf Seite 320.

Verknüpfte Server verwenden

Network Dispatcher kann sich auf derselben Maschine befinden wie ein Server, für dessen Anforderungen er einen Lastausgleich durchführt. Dies wird als *Verknüpfen* eines Servers bezeichnet. Die Verknüpfung gilt für die Komponenten Dispatcher, Site Selector, Mailbox Locator und Cisco Consultant. Für CBR wird die Verknüpfung auch unterstützt. Dies gilt jedoch nur bei Verwendung bindungsspezifischer Webserver und Caching-Proxy-Server.

Anmerkung: In Zeiten hohen Datenverkehrs konkurriert ein zusammengeführter Server mit dem Network Dispatcher um Ressourcen. Sind jedoch keine überlasteten Maschinen vorhanden, kann mit einem zusammengeführten Server die Gesamtzahl der Maschinen reduziert werden, die für das Einrichten einer Site für den Lastausgleich erforderlich sind.

Für Dispatcher

Red Hat Linux Version 7.1 (Linux-Kernel-Version 2.4.2-2) oder SuSE Linux Version 7.1 (Linux-Kernel-Version 2.4.0 - 4 GB): Wenn Sie bei Ausführung der Dispatcher-Komponente mit der Weiterleitungsmethode "mac" sowohl die Verknüpfung als auch die hohe Verfügbarkeit konfigurieren möchten, müssen Sie einen Patch-Code für den Linux-Kernel installieren. Weitere Informationen zum Installieren des Patch-Codes finden Sie im Abschnitt „Patch-Code für Linux-Kernel (zum Unterdrücken von ARP-Antworten an der Loopback-Schnittstelle) installieren“ auf Seite 77. Wenn Sie diese Anweisungen ausführen, übergehen Sie den Schritt zum Angeben des Aliasnamens für den Loopback-Adapter. Fügen Sie die Anweisung "ifconfig" zur Script-Datei für hohe Verfügbarkeit (goStandby) hinzu, um einen Aliasnamen für den Loopback-Adapter anzugeben. Die genannte Script-Datei wird ausgeführt, wenn ein Dispatcher in den Bereitschaftsstatus wechselt.

Solaris: Sie können keine WAND-Advisor-Funktionen konfigurieren, wenn der Eingangspunkt-Dispatcher verknüpft ist. Weitere Informationen hierzu finden Sie im Abschnitt „Ferne Advisor mit der Weitverkehrsunterstützung verwenden“ auf Seite 170.

In früheren Releases mussten die Adresse des verknüpften Servers und die NFA (Non-Forwarding Address) in der Konfiguration übereinstimmen. Diese Einschränkung wurde aufgehoben.

Für das Konfigurieren eines verknüpften Servers bietet der Befehl **ndcontrol server** eine Option mit dem Namen **collocated** an, die auf *yes* oder *no* gesetzt werden kann. Die Standardeinstellung ist "no". Die Adresse des Servers muss eine gültige IP-Adresse einer Netzschnittstellenkarte in der Maschine sein.

Anmerkung: Für **Windows 2000**: Sie können Dispatcher verknüpfen, jedoch *nicht* das Schlüsselwort "collocated" verwenden. Die Verknüpfung wird bei Verwendung der Dispatcher-Weiterleitungsmethoden "nat" und "cbr", nicht jedoch bei Verwendung der Weiterleitungsmethode "mac" unterstützt. Weitere Informationen zu den Weiterleitungsmethoden von Dispatcher finden Sie in den Abschnitten „NAT/NAPT-Weiterleitungsmethode (nat) des Dispatchers“ auf Seite 55, „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)“ auf Seite 57 und „MAC-Weiterleitungsmethode (mac) des Dispatchers“ auf Seite 54.

Einen verknüpften Server können Sie auf eine der folgenden Arten konfigurieren:

- Wenn Sie die NFA als Adresse des verknüpften Servers verwenden: Legen Sie die NFA mit dem Befehl **ndcontrol executor set nfa IP-Adresse** fest. Fügen Sie den Server, der die NFA verwendet, mit dem Befehl **ndcontrol server add Cluster:Port:Server** hinzu.
- Wenn Sie eine andere Adresse als die NFA verwenden: Fügen Sie den Server mit der gewünschten IP-Adresse hinzu, indem Sie den Parameter "collocated" wie folgt auf "yes" setzen: **ndcontrol server add Cluster:Port:Server collocated yes**.

Weitere Informationen über die Syntax für den Befehl **ndcontrol server** enthält „ndcontrol server — Server konfigurieren“ auf Seite 320.

Für CBR

CBR unterstützt die Verknüpfung auf allen Plattformen, ohne zusätzliche Konfigurationsschritte zu erfordern. Die verwendeten Webserver und der verwendete Caching Proxy müssen jedoch bindungsspezifisch sein.

Für Mailbox Locator

Mailbox Locator unterstützt die Verknüpfung auf allen Plattformen. Der Server muss allerdings an eine andere Adresse als Network Dispatcher gebunden werden. Wenn Sie einen POP3- oder IMAP-Server auf derselben Maschine verknüpfen möchten, muss dieser an eine IP-Adresse gebunden werden, die sich von der Cluster-Adresse unterscheidet. Dies können Sie durch Verwendung der Loopback-Adresse erreichen.

Für Site Selector

Site Selector unterstützt die Verknüpfung auf allen Plattformen, ohne zusätzliche Konfigurationsschritte zu erfordern.

Für Cisco Consultant

Cisco Consultant unterstützt die Verknüpfung auf allen Plattformen, ohne zusätzliche Konfigurationsschritte zu erfordern.

Dispatcher-WAN-Unterstützung konfigurieren

Diese Funktion ist nur für die Dispatcher-Komponente verfügbar.

Wenn Sie die WAN-Unterstützung und die Weiterleitungsmethode "nat" von Dispatcher nicht verwenden, erfordert die Dispatcher-Konfiguration, dass die Dispatcher-Maschine und die zugehörigen Server demselben LAN-Segment zugeordnet sind (siehe Abb. 22). Das Paket eines Clients wird auf der ND-Maschine empfangen und an den Server gesendet und dann wieder von dem Server direkt an den Client gesendet.

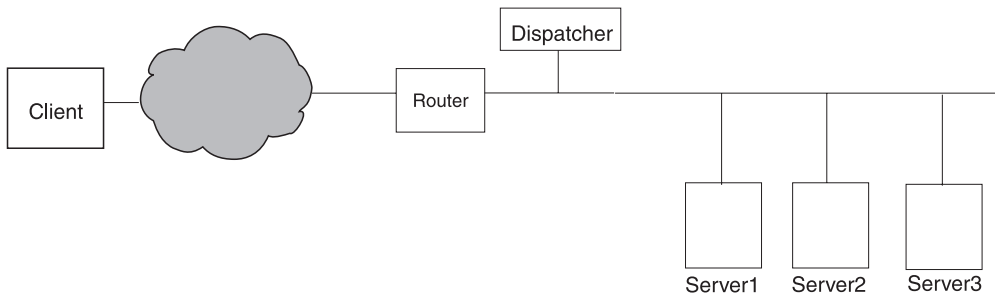


Abbildung 22. Beispiel einer Konfiguration mit einem LAN-Segment

Durch die WAN-Erweiterung von Dispatcher werden Server an anderen Standorten, die als *ferne Server* bezeichnet werden, unterstützt (siehe Abb. 23 auf Seite 169). Wenn GRE am fernen Standort nicht unterstützt wird und Sie nicht die Dispatcher-Weiterleitungsmethode "nat" verwenden, muss der ferne Standort aus einer Dispatcher-Maschine (Dispatcher 2) und den lokal angeschlossenen Servern (ServerG, ServerH und ServerI) bestehen. Alle Dispatcher-Maschinen müssen unter demselben Betriebssystem ausgeführt werden. Das Paket eines Clients kann jetzt vom Internet an eine Dispatcher-Maschine und von dort an eine Dispatcher-Maschine an einem anderen geografischen Standort sowie an einen der dort lokal angeschlossenen Server gesendet werden.

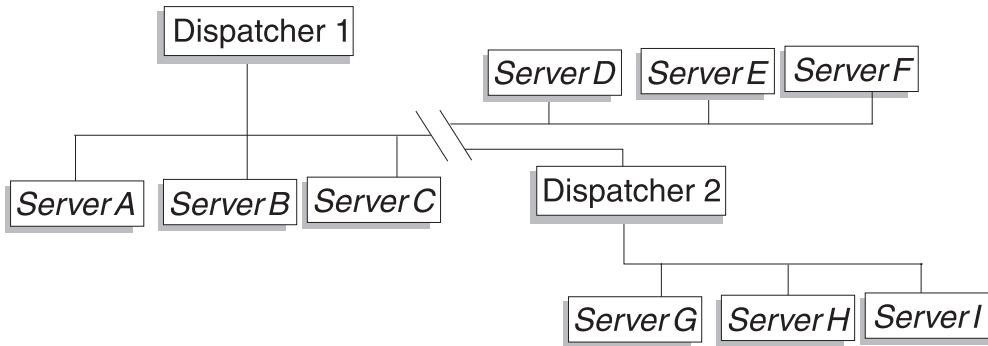


Abbildung 23. Beispiel einer Konfiguration mit lokalen und fernen Servern

Damit kann eine Cluster-Adresse weltweit alle Client-Anforderungen unterstützen und die Last auf Server auf der ganzen Welt verteilen.

An der Dispatcher-Maschine, die das Paket anfänglich empfängt, können weiterhin lokale Server angeschlossen sein, und die Dispatcher-Maschine kann die Last auf ihre lokalen Server und auf die fernen Server verteilen.

Befehlssyntax

Weitverkehrsbefehle sind nicht komplex. Führen Sie folgende Schritte aus, um die Weitverkehrsunterstützung zu konfigurieren:

1. Fügen Sie die Server hinzu. Wird einem Dispatcher ein Server hinzugefügt, müssen Sie definieren, ob es sich bei dem Server um einen lokalen Server oder einen fernen Server handelt (siehe oben). Soll ein Server hinzugefügt und der Server als lokaler Server definiert werden, geben Sie den Befehl **ndcontrol server add** ohne Angabe eines Routers ein. Dieser Wert ist der Standardwert. Soll der Server als ferner Server definiert werden, müssen Sie den Router angeben, über den der Dispatcher das Paket senden muss, um den fernen Server zu erreichen. Der Server muss ein anderer Dispatcher sein, und die Adresse des Servers muss die NFA des Dispatchers sein. Wird beispielsweise in Abb. 24 auf Seite 172 *ND 2* als ferner Server unter *ND 1* hinzugefügt, müssen Sie *Router 1* als Router-Adresse definieren. Allgemeine Syntax:

```
ndcontrol server add Cluster:Port:Server router Adresse
```

Weitere Informationen zum Schlüsselwort "router" finden Sie im Abschnitt „ndcontrol server — Server konfigurieren“ auf Seite 320.

2. Konfigurieren Sie Aliasnamen. Auf der ersten Dispatcher-Maschine (auf der die Client-Anforderung aus dem Internet empfangen wird) müssen für die Cluster-Adresse wie bisher mit Hilfe von **cluster configure**, **ifconfig** oder **ndconfig** Aliasnamen erstellt werden. Auf den fernen Dispatcher-Maschinen werden jedoch für die Cluster-Adresse **keine** Aliasnamen auf der Netzschnittstellenkarte erstellt.

Ferne Advisor mit der Weitverkehrsunterstützung verwenden

Auf Eingangspunkt-Dispatchern der meisten Plattformen funktionieren die Advisor-Funktionen ohne spezielle Konfiguration.

Linux: Es gibt eine Einschränkung für die Verwendung von fernen Advisor-Funktionen in Konfigurationen mit WAN-Unterstützung. Protokollspezifische Advisor-Funktionen wie die HTTP-Advisor-Funktion, die auf der Eingangspunkt-Dispatcher-Maschine ausgeführt werden, können den Status der Servermaschinen am fernen Standort nicht richtig bewerten. Sie können dieses Problem minimieren, indem Sie einen der folgenden Schritte ausführen:

- Führen Sie auf der Eingangspunkt-Dispatcher-Maschine die protokollunabhängige Advisor-Funktion "ping" aus.
- Führen Sie auf der Eingangspunkt-Dispatcher-Maschine eine protokollspezifische Advisor-Funktion und auf der fernen Dispatcher-Maschine einen passenden protokollspezifischen Serverdämon (z. B. einen Webserver) aus.

Beide genannten Optionen ermöglichen der Advisor-Funktion auf der Eingangspunkt-Dispatcher-Maschine, den Status der fernen Dispatcher-Maschine zu bewerten.

Solaris: Auf Eingangspunkt-Dispatcher-Maschinen müssen Sie (anstelle von "ifconfig" oder Cluster-Konfigurationsmethoden) die Konfigurationsmethode "arp" verwenden. Beispiel:

```
arp -s <meine_Cluster-Adresse> <meine_MAC-Adresse> pub
```

Anmerkung: Für Solaris gelten die folgenden Einschränkungen:

- WAND-Advisor-Funktionen können nur mit der Cluster-Konfigurationsmethode "arp" ausgeführt werden.
- Advisor-Funktionen für bindungsspezifische Server können nur mit der Cluster-Konfigurationsmethode "arp" ausgeführt werden.
- Die Verknüpfung ist nur bei Verwendung der Cluster-Konfigurationsmethode "ifconfig" möglich.

Auf fernen Dispatchern müssen Sie für jede ferne Cluster-Adresse die folgenden Konfigurationsschritte ausführen. Für eine Konfiguration mit hoher Verfügbarkeit am fernen Network-Dispatcher-Standort müssen Sie diese Schritte auf beiden Maschinen ausführen.

AIX

- Geben Sie für den Loopback-Adapter die Cluster-Adresse als Aliasnamen an. Der Wert von "netmask" muss auf 255.255.255.255 gesetzt sein. Beispiel:
ifconfig lo0 alias 9.67.34.123 netmask 255.255.255.255

Anmerkung: Advisor, die sowohl auf der lokalen als auch auf der fernen Dispatcher-Maschine ausgeführt werden, sind erforderlich.

Linux

- Geben Sie für den Loopback-Adapter die Cluster-Adresse als Aliasnamen an. Beispiel:

ifconfig lo:1 9.67.34.123 netmask 255.255.255.255 up

Anmerkung: Advisor, die sowohl auf der lokalen als auch auf der fernen Dispatcher-Maschine ausgeführt werden, sind erforderlich.

Solaris

- Es sind keine zusätzlichen Konfigurationsschritte erforderlich.

Windows 2000

1. Der Dispatcher erfordert zwei IP-Adressen: eine Adresse für den Microsoft-TCP/IP-Stack und eine Adresse für den Network-Dispatcher-Stack. Konfigurieren Sie die NFA unter Verwendung der IP-Adresse des Network-Dispatcher-Stack. Beispiel:

ndconfig en0 alias 9.55.30.45 netmask 255.255.240.0

2. Konfigurieren Sie den Loopback-Adapter mit der fernen Cluster-Adresse als Aliasname. Der Wert von "netmask" muss auf 255.255.255.255 gesetzt sein. Beispiel:

ndconfig lo0 alias 9.67.34.123 netmask 255.255.255.255

3. Löschen Sie alle Einträge in der arp-Tabelle für die ferne Cluster-Adresse.
 - a. Geben Sie folgendes ein, um den Inhalt der arp-Tabelle anzuzeigen:
arp -a
 - b. Geben Sie folgendes ein, um einen vorhandenen Eintrag zu löschen:
arp -d 9.67.34.123

Anmerkung: Geben Sie folgendes ein, um die MAC-Adresse Ihrer Schnittstelle zu bestimmen:

1) **ping** *Host-Name*

2) **arp -a**

und suchen Sie nach der Adresse Ihrer Maschine.

4. Fügen Sie unter Verwendung der NFA (IP-Adresse des Network-Dispatcher-Stack) eine Route zum fernen Cluster (9.67.34.123) hinzu. Der Wert von "mask" muss auf 255.255.255.255 gesetzt sein. Beispiel:

route add 9.67.34.123 mask 255.255.255.255 9.55.30.45

Konfigurationsbeispiel

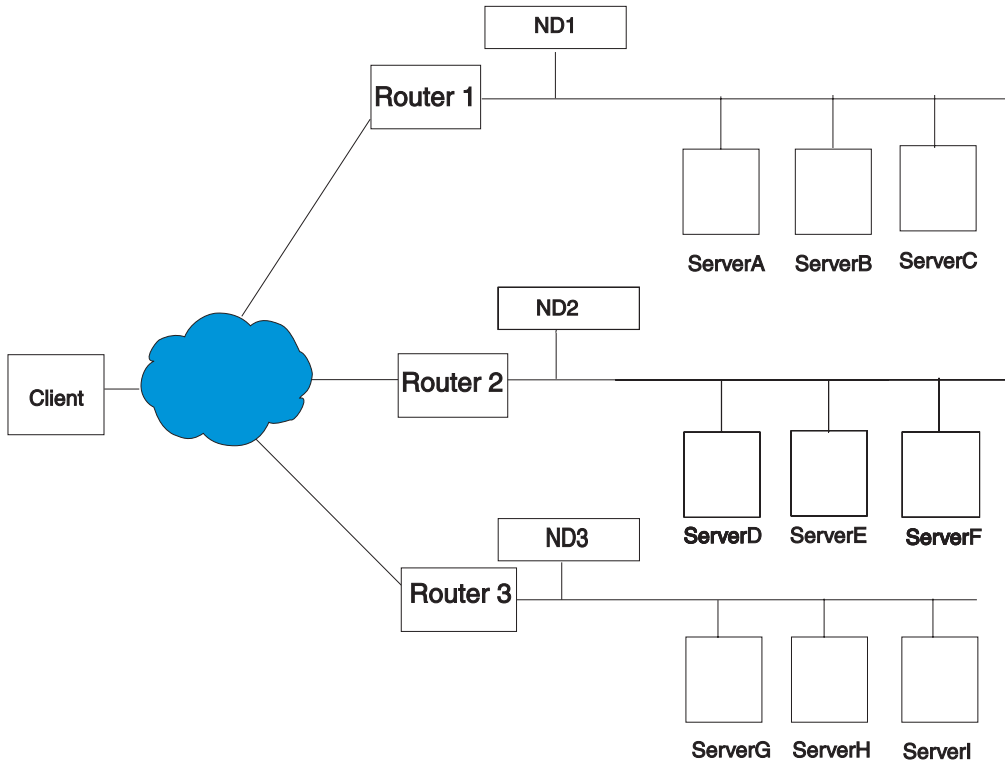


Abbildung 24. WAN-Beispielkonfiguration mit fernen Network-Dispatcher-Maschinen

Dieses Beispiel bezieht sich auf die in Abb. 24 gezeigte Konfiguration.

Nachfolgend wird beschrieben, wie die Dispatcher-Maschinen für die Unterstützung der Cluster-Adresse xebec am Port 80 konfiguriert werden. ND1 ist als „Eingangspunkt“ definiert. Es wird eine Ethernet-Verbindung vorausgesetzt. Für ND1 sind fünf Server definiert, drei lokale (ServerA, ServerB, ServerC) und zwei ferne (ND2 und ND3). Für die fernen Dispatcher ND2 und ND3 sind jeweils drei lokale Server definiert.

An der Konsole des ersten Dispatchers (ND1) folgende Schritte ausführen:

1. Den Executor starten.
ndcontrol executor start
2. Definieren Sie die NFA der Dispatcher-Maschine.
ndcontrol executor set nfa ND1

3. Definieren Sie den Cluster.
ndcontrol cluster add xebec
4. Definieren Sie den Port.
ndcontrol port add xebec:80
5. Definieren Sie die Server.
 - a. **ndcontrol server add xebec:80:ServerA**
 - b. **ndcontrol server add xebec:80:ServerB**
 - c. **ndcontrol server add xebec:80:ServerC**
 - d. **ndcontrol server add xebec:80:ND2 router Router1**
 - e. **ndcontrol server add xebec:80:ND3 router Router1**
6. Konfigurieren Sie unter Windows 2000 die NFA des Dispatcher-LAN-Adapters.
ndcontrol cluster configure ND1. konfigurieren Sie außerdem xebec als Cluster-Adresse.
7. Konfigurieren Sie die Cluster-Adresse.
ndcontrol cluster configure xebec

An der Konsole des zweiten Dispatchers (ND2) folgende Schritte ausführen:

1. Den Executor starten.
ndcontrol executor start
2. Definieren Sie die NFA der Dispatcher-Maschine.
ndcontrol executor set nfa ND2
3. Definieren Sie den Cluster.
ndcontrol cluster add xebec
4. Definieren Sie den Port.
ndcontrol port add xebec:80
5. Definieren Sie die Server.
 - a. **ndcontrol server add xebec:80:ServerD**
 - b. **ndcontrol server add xebec:80:ServerE**
 - c. **ndcontrol server add xebec:80:ServerF**
6. Konfigurieren Sie unter Windows 2000 die NFA des Dispatcher-LAN-Adapters.
ndcontrol cluster configure ND2

An der Konsole des dritten Dispatchers (ND3) folgende Schritte ausführen:

1. Den Executor starten.
ndcontrol executor start
2. Definieren Sie die NFA der Dispatcher-Maschine.
ndcontrol executor set nfa ND3
3. Definieren Sie den Cluster.
ndcontrol cluster add xebec
4. Definieren Sie den Port.
ndcontrol port add xebec:80
5. Definieren Sie die Server.
 - a. **ndcontrol server add xebec:80:ServerG**
 - b. **ndcontrol server add xebec:80:ServerH**
 - c. **ndcontrol server add xebec:80:ServerI**
6. Konfigurieren Sie unter Windows 2000 die NFA des Dispatcher-LAN-Adapters.
ndcontrol cluster configure ND3

Anmerkungen

1. Geben auf allen Servern (A-I) für die Loopback-Einheit die Cluster-Adresse als Aliasnamen an.
2. Cluster und Ports werden mit `ndcontrol` auf allen beteiligten Dispatcher-Maschinen hinzugefügt. Dies gilt für den Dispatcher, der als Eingangspunkt definiert ist, und für alle fernen Dispatcher.
3. Der Abschnitt „Ferne Advisor mit der Weitverkehrsunterstützung verwenden“ auf Seite 170 enthält Informationen über die Verwendung ferner Advisor mit der Weitverkehrsunterstützung.
4. Die Weitverkehrsunterstützung verbietet unendliche Route-Schleifen. (Wenn eine Dispatcher-Maschine ein Paket von einem anderen Dispatcher empfängt, wird das Paket nicht an einen dritten Dispatcher weitergeleitet.) Mit der Weitverkehrsunterstützung wird nur eine Ebene von fernen Dispatchern unterstützt.
5. Das Weitverkehrsnetz unterstützt UDP und TCP.
6. Die Weitverkehrsunterstützung kann zusammen mit der Funktion für hohe Verfügbarkeit verwendet werden. Jedem Dispatcher kann eine benachbarte Partnermaschine in Bereitschaft (an demselben LAN-Segment) zugeordnet werden.
7. Der Manager und die Advisor können zusammen mit der Weitverkehrsunterstützung verwendet werden. In diesem Fall sollten sie auf allen teilnehmenden Dispatcher-Maschinen gestartet werden.
8. Network Dispatcher unterstützt WAND nur auf ähnlichen Betriebssystemen.

Unterstützung für GRE (Generic Routing Encapsulation)

Generic Routing Encapsulation (GRE) ist ein Internet-Protokoll, das in RFC 1701 und RFC 1702 spezifiziert ist. Bei Verwendung von GRE kann Network Dispatcher Client-IP-Pakete in IP/GRE-Pakete integrieren und an Serverplattformen mit GRE-Unterstützung wie OS/390 weiterleiten. Mit der GRE-Unterstützung kann die Dispatcher-Komponente die Arbeitslast von Paketen auf mehrere Serveradressen verteilen, die einer MAC-Adresse zugeordnet sind.

Network Dispatcher implementiert GRE als Teil der WAND-Funktion (Wide Area Network Dispatcher). Auf diese Weise stellt Network Dispatcher WAN-Lastausgleich direkt für alle Serversysteme zur Verfügung, die GRE-Pakete entpacken können. Network Dispatcher muss nicht auf einem fernen System installiert sein, wenn die fernen Server eingebundene GRE-Pakete unterstützen. Network Dispatcher integriert WAND-Pakete, deren GRE-Feld auf den Dezimalwert 3735928559 gesetzt ist.

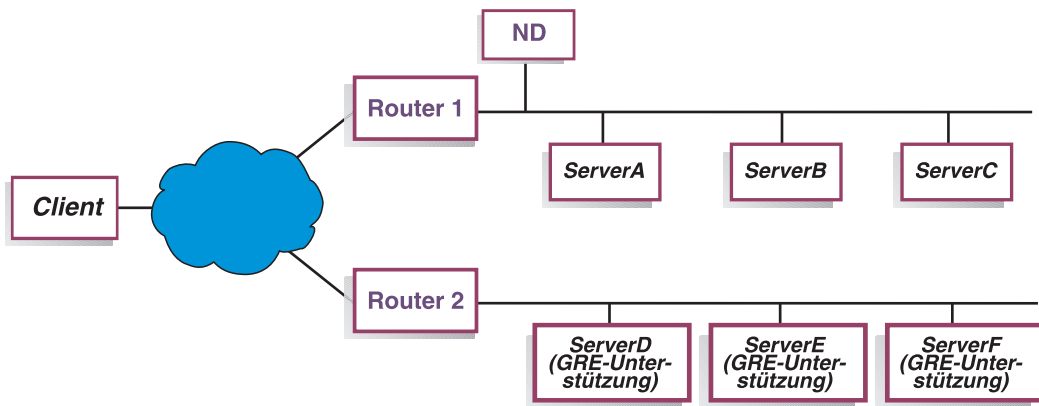


Abbildung 25. WAN-Beispielkonfiguration mit einer Serverplattform, die GRE unterstützt

Wenn Sie für dieses Beispiel (Abb. 25) einen fernen ServerD mit GRE-Unterstützung hinzufügen möchten, müssen Sie ihn in Ihrer Network-Dispatcher-Konfiguration definieren, wie Sie einen WAND-Server in der Hierarchie Cluster:Port:Server definieren würden:

```
ndcontrol server add Cluster:Port:ServerD router Router1
```

Advisor-Funktion 'self' in einer Client/Server-WAND-Konfiguration

Die Advisor-Funktion "self" ist für die Dispatcher-Komponente verfügbar.

Wenn Network Dispatcher in einer Client/Server-WAND-Konfiguration (Wide Area Network Dispatcher) installiert ist, stellt der Dispatcher eine *self*-Advisor-Funktion bereit, die Informationen zum Auslastungsstatus von Back-End-Servern sammelt.

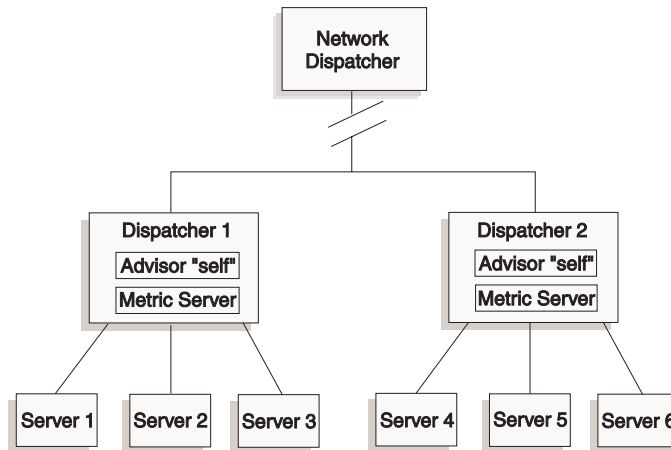


Abbildung 26. Beispiel für eine Client/Server-WAND-Konfiguration mit Advisor-Funktion "self"

In diesem Beispiel befinden sich die Advisor-Funktion "self" und Metric Server auf den beiden Dispatcher-Maschinen, deren Lastausgleich vom übergeordneten Network Dispatcher durchgeführt wird. Die Advisor-Funktion "self" misst insbesondere die Verbindungen pro Sekunde für die Back-End-Server des Dispatchers auf Executor-Ebene.

Der Selbst-Advisor schreibt die Ergebnisse in die Datei `ndloadstat`. Network Dispatcher stellt außerdem den externen Messwert "ndload" bereit. Bei Ausführung der Konfiguration des Agenten Metric Server auf den Dispatcher-Maschinen wird der externe Messwert "ndload" aufgerufen. Das `ndload`-Script extrahiert eine Zeichenfolge aus der Datei "ndloadstat" und gibt sie an den Agenten Metric Server zurück. Anschließend geben die Metric-Server-Agenten (von den einzelnen Dispatcher-Maschinen) den Wert für den Auslastungsstatus an den übergeordneten Network Dispatcher zurück, damit dieser bestimmen kann, welcher Dispatcher Client-Anforderungen weiterleiten soll.

Die ausführbare Datei "ndload" befindet sich im Network-Dispatcher-Verzeichnis `.../nd/ms/script`.

Hohe Verfügbarkeit

Die Funktion der hohen Verfügbarkeit ist nur für die Dispatcher-Komponente verfügbar. Um die Verfügbarkeit des Dispatchers zu verbessern, benutzt die Dispatcher-Funktion für hohe Verfügbarkeit die folgenden Mechanismen:

- Zwei Dispatcher, die mit denselben Clients und demselben Cluster von Servern sowie untereinander verbunden sind. Beide Dispatcher müssen dasselbe Betriebssystem benutzen.
- Ein Mechanismus mit Überwachungssignalen zwischen den beiden Dispatcher-Maschinen, um einen Dispatcher-Ausfall zu erkennen. Für mindestens ein Überwachungssignale austauschendes Paar müssen die NFAs als Quellen- und Zieladresse definiert sein.

Nach Möglichkeit sollte mindestens eines der Paare die Überwachungssignale über ein anderes als das für den regulären Cluster-Datenverkehr vorgesehene Teilnetz austauschen. Durch Abgrenzung des durch die Überwachungssignale verursachten Datenverkehrs können in Spitzenbelastungszeiten Fehler bei der Übernahme vermieden werden. Außerdem kann so die Zeit verkürzt werden, die nach einer Überbrückung für eine vollständige Wiederherstellung benötigt wird.

- Eine Liste mit Erreichbarkeitszielen. Beide Dispatcher-Maschinen müssen diese Adressen ansprechen können, damit ein normaler Lastausgleich des Datenverkehrs stattfinden kann. Weitere Informationen hierzu finden Sie im Abschnitt „Fehlererkennung mit Hilfe von Überwachungssignal und Erreichbarkeitsziel“ auf Seite 181.
- Synchronisation der Dispatcher-Informationen (d. h. der Verbindungstabellen, der Erreichbarkeitstabellen und anderer Informationen).
- Logik zur Auswahl des aktiven Dispatchers, der für einen bestimmten Cluster von Servern zuständig ist, und des Dispatchers in Bereitschaft, der permanent für diesen Cluster von Servern synchronisiert wird.
- Ein Mechanismus zur Ausführung der IP-Übernahme, wenn die Logik oder ein Bediener entscheidet, dass der aktive Dispatcher und der Dispatcher in Bereitschaft ihren Status tauschen sollen.

Anmerkung: Eine Abbildung und Beschreibung einer Konfiguration mit *gegenseitiger hoher Verfügbarkeit*, in der sich zwei Dispatcher-Maschinen, die zwei Cluster-Gruppen gemeinsam benutzen, gegenseitig als Ausweichmaschine verwenden, finden Sie im Abschnitt „Gegenseitige hohe Verfügbarkeit“ auf Seite 53. Die beiderseitige Hochverfügbarkeit ähnelt der hohen Verfügbarkeit, basiert jedoch speziell auf einer Cluster-Adresse und nicht auf einer Dispatcher-Maschine als Ganzes. Auf beiden Maschinen müssen die gemeinsam benutzten Cluster-Gruppen identisch konfiguriert werden.

Hohe Verfügbarkeit konfigurieren

Die vollständige Syntax des Befehls **ndcontrol highavailability** steht in „ndcontrol highavailability — Hohe Verfügbarkeit steuern“ auf Seite 289.

In „Dispatcher-Maschine konfigurieren“ auf Seite 64 sind die meisten der nachfolgend aufgeführten Taskst genauer beschrieben.

1. Starten Sie den Server auf beiden Dispatcher-Servermaschinen.
2. Starten Sie den Executor auf beiden Maschinen.
3. Vergewissern Sie sich, dass die NFA jeder Dispatcher-Maschine konfiguriert und eine fpr das Teilnetz der Dispatcher-Maschinen gültige IP-Adresse ist.

Nur für Windows 2000: Konfigurieren Sie zusätzlich jede NFA (nicht für Weiterleitung bestimmte Adresse) mit dem Befehl **ndconfig**. Beispiel:

```
ndconfig en0 NFA netmask Netzmaske
```

4. Konfigurieren Sie auf beiden Maschinen die Cluster-, Port- und Serverinformationen.

Anmerkung: Für die Konfiguration der beiderseitigen Hochverfügbarkeit (Abb. 14 auf Seite 53) konfigurieren Sie beispielsweise die Cluster-Gruppen, die von den beiden Dispatchern gemeinsam benutzt werden, wie folgt:

- Geben Sie für Dispatcher 1 folgendes aus:

```
ndcontrol cluster set ClusterA primaryhost NFAdispatcher1  
ndcontrol cluster set ClusterB primaryhost NFAdispatcher2
```

- Geben Sie für Dispatcher 2 folgendes aus:

```
ndcontrol cluster set ClusterB primaryhost NFAdispatcher2  
ndcontrol cluster set ClusterA primaryhost NFAdispatcher1
```

5. Starten Sie auf beiden Maschinen den Manager und die Advisor. Die Advisor-Funktion "reach" wird automatisch von der Manager-Funktion gestartet.
6. Erstellen Sie auf beiden Dispatcher-Maschinen Alias-Script-Dateien. Weitere Informationen hierzu finden Sie im Abschnitt „Scripts verwenden“ auf Seite 182.
7. Fügen Sie auf beiden Maschinen Überwachungssignalinformationen hinzu:

```
ndcontrol highavailability heartbeat add Quellenadresse Zieladresse
```

Anmerkung: Quellenadresse und Zieladresse sind die IP-Adressen (entweder DNS-Namen oder Adressen in Schreibweise mit Trennzeichen) der Dispatcher-Maschinen. Die Werte auf den beiden Maschinen werden umgedreht. Beispiel:

```
Primäre Maschine - highavailability heartbeat
add 9.67.111.3 9.67.186.8
Partnermaschine - highavailability heartbeat
add 9.67.186.8 9.67.111.3
```

Für mindestens ein Überwachungssignale austauschendes Paar müssen die NFAs als Quellen- und Zieladresse definiert sein.

Nach Möglichkeit sollte mindestens eines der Paare die Überwachungssignale über ein anderes als das für den regulären Cluster-Datenverkehr vorgesehene Teilnetz austauschen. Durch Abgrenzung des durch die Überwachungssignale verursachten Datenverkehrs können in Spitzenbelastungszeiten Fehler bei der Übernahme vermieden werden. Außerdem kann so die Zeit verkürzt werden, die nach einer Überbrückung für eine vollständige Wiederherstellung benötigt wird.

8. Konfigurieren Sie auf beiden Maschinen über den Befehl **reach add** die Liste der IP-Adressen, die der Dispatcher erreichen muss, um einen vollständigen Service zu gewährleisten. Beispiel:
`ndcontrol highavailability reach add 9.67.125.18`

Erreichbarkeitsziele werden empfohlen, sind aber nicht erforderlich. „Fehlererkennung mit Hilfe von Überwachungssignal und Erreichbarkeitsziel“ auf Seite 181 enthält weitere Informationen.

9. Fügen Sie jeder Maschine die Informationen über die Wiederherstellungsstrategie hinzu:
 - Für die **primäre** Maschine:
`ndcontrol highavailability backup add primary [auto | manual] Port`
 - Für die **Partnermaschine**:
`ndcontrol highavailability backup
add backup [auto | manual] Port`
 - Bei der beiderseitigen Hochverfügbarkeit verfügt jede Dispatcher-Maschine über **beide** Rollen (primäre Maschine und Partnermaschine):
`ndcontrol highavailability backup add both [auto | manual] Port`

Anmerkung: Wählen Sie als *Port* einen nicht verwendeten Port Ihrer Maschinen aus. Die beiden Maschinen kommunizieren über diesen Port.

10. Überprüfen Sie den Status der hohen Verfügbarkeit auf den beiden Maschinen:

```
ndcontrol highavailability status
```

Die Maschinen sollten jeweils die korrekte Rolle (Partnermaschine und/oder primäre Maschine), die korrekten Status und die korrekten untergeordneten Status aufweisen. Die primäre Maschine sollte aktiv und synchronisiert sein. Die Ausweichmaschine sollte sich im Bereitschaftsmodus befinden und innerhalb kurzer Zeit synchronisiert werden. Der Parameter für die Strategie muss für beide Maschinen auf denselben Wert gesetzt sein.

Anmerkungen:

1. Wollen Sie eine einzelne Dispatcher-Maschine ohne eine Partnermaschine konfigurieren, um Pakete weiterzuleiten, benutzen Sie beim Start keine Befehle für hohe Verfügbarkeit.
2. Wollen Sie eine für die hohe Verfügbarkeit erstellte Konfiguration mit zwei Dispatcher-Maschinen in eine Konfiguration mit einer einzigen Maschine ändern, beenden Sie den Executor auf einer der Maschinen und löschen Sie dann die Funktionen für hohe Verfügbarkeit (Überwachungssignale, Erreichbarkeit und Partnermaschine) auf der anderen Maschine.
3. In beiden oben geschilderten Fällen müssen Sie ggf. Cluster-Adressen als Aliasnamen für die Netzschnittstellenkarte angeben.
4. Wenn zwei Dispatcher-Maschinen in einer Konfiguration mit hoher Verfügbarkeit synchronisiert werden, sollten Sie zunächst alle ndcontrol-Befehle (zum Aktualisieren der Konfiguration auf der Bereitschaftsmaschine und dann auf der aktiven Maschine ausführen.
5. Wenn Sie zwei Dispatcher-Maschinen in einer Umgebung mit hoher Verfügbarkeit verwenden, können unerwartete Ergebnisse auftreten, wenn einer der Parameter für Executor, Cluster, Port oder Server (z. B. port stickytime) auf beiden Maschinen auf verschiedene Werte gesetzt ist.
6. Berücksichtigen Sie bei der beiderseitigen Hochverfügbarkeit den Fall, in dem einer der Dispatcher aktiv Pakete für seinen primären Cluster weiterleiten muss und außerdem das Weiterleiten von Paketen für den Partner-Cluster übernehmen muss. Stellen Sie sicher, dass damit die Kapazität für den Durchsatz auf dieser Maschine nicht überschritten wird.
7. Wenn Sie unter Linux bei Verwendung der MAC-Port-Weiterleitungsmethode von Dispatcher gleichzeitig hohe Verfügbarkeit und Verknüpfung konfigurieren, müssen Sie einen Patch-Code für den Linux-Kernel installieren. Weitere Informationen zum Installieren des Patch-Codes finden Sie im Abschnitt „Patch-Code für Linux-Kernel (zum Unterdrücken von ARP-Antworten an der Loopback-Schnittstelle) installieren“ auf Seite 77.

Fehlererkennung mit Hilfe von Überwachungssignal und Erreichbarkeitsziel

Neben den Basiskriterien der Fehlererkennung (durch Überwachungssignale erkannter Verlust der Konnektivität zwischen aktivem Dispatcher und Bereitschafts-Dispatcher) gibt es einen weiteren Fehlererkennungsmechanismus, der als *Erreichbarkeitskriterien* bezeichnet wird. Wenn Sie den Dispatcher konfigurieren, können Sie eine Liste von Hosts angeben, die für jeden der Dispatcher erreichbar sein sollten, damit die Dispatcher fehlerfrei arbeiten können.

Sie müssen mindestens einen Host für jedes Teilnetz auswählen, das die Dispatcher-Maschine verwendet. Die Hosts können Router, IP-Server oder andere Arten von Hosts sein. Die Erreichbarkeit von Hosts wird über Ping-Aufrufe durch den Erreichbarkeits-Advisor abgefragt. Es findet eine Übernahme statt, wenn keine Überwachungssignalnachrichten durchkommen oder wenn die Erreichbarkeitskriterien von dem Dispatcher in Bereitschaft eher erfüllt werden als von dem primären Dispatcher. Damit die Entscheidung anhand aller verfügbaren Informationen getroffen wird, sendet der aktive Dispatcher regelmäßig Informationen über seine Erreichbarkeit an den Dispatcher in Bereitschaft. Der Dispatcher in Bereitschaft vergleicht dann diese Informationen mit seinen eigenen Erreichbarkeitsinformationen und entscheidet, ob eine Übernahme vorgenommen werden soll oder nicht.

Anmerkung: Wenn Sie das Erreichbarkeitsziel konfigurieren, müssen Sie die Advisor-Funktion *reach* starten. Die Advisor-Funktion "reach" wird automatisch von der Manager-Funktion gestartet. Weitere Informationen zur Advisor-Funktion "reach" finden Sie auf Seite 154.

Wiederherstellungsstrategie

Es werden zwei Dispatcher-Maschinen konfiguriert, die primäre Maschine und eine zweite Maschine, die so genannte *Partnermaschine*. Wird die primäre Maschine gestartet, leitet sie die gesamten Verbindungsdaten so lange an die Partnermaschine weiter, bis die beiden Maschinen synchronisiert sind. Die primäre Maschine wird *aktiv*, d. h., sie beginnt mit dem Lastausgleich. Die Partnermaschine überwacht in der Zwischenzeit den Status der primären Maschine und befindet sich in *Bereitschaft*.

Stellt die Partnermaschine an einem beliebigen Punkt fest, dass die primäre Maschine ausgefallen ist, *übernimmt* sie die Lastausgleichsfunktionen der primären Maschine und wird zur aktiven Maschine. Ist die primäre Maschine wieder betriebsbereit, gehen die Maschinen anhand der vom Benutzer konfigurierten *Wiederherstellungsstrategie* vor.

Es gibt zwei Arten von Strategie:

Auto Die primäre Maschine nimmt das Weiterleiten von Paketen automatisch wieder auf, sobald sie wieder betriebsbereit ist.

Manual

Die Partnermaschine setzt das Weiterleiten von Paketen fort, auch wenn die primäre Maschine wieder betriebsbereit ist. Soll die primäre Maschine wieder in den Status der aktiven Maschine und die Partnermaschine wieder in den Bereitschaftsstatus zurückgesetzt werden, ist ein manueller Eingriff erforderlich.

Der Parameter für die Strategie muss für beide Maschinen auf denselben Wert gesetzt werden.

Bei der Strategie der manuellen Wiederherstellung können Sie über den Befehl **takeover** das Weiterleiten von Paketen durch eine bestimmte Maschine erzwingen. Die manuelle Wiederherstellung ist nützlich, wenn die andere Maschine gewartet wird. Die automatische Wiederherstellung ist für den normalen, nichtüberwachten Betrieb konzipiert.

In einer Konfiguration mit gegenseitiger hoher Verfügbarkeit gibt es keinen Fehler auf Cluster-Basis. Tritt ein Fehler bei einer Maschine auf, übernimmt die andere Maschine die Rolle für beide Cluster, auch wenn der Fehler nur einen Cluster betrifft.

Anmerkung: In einer Übernahmesituation können einige Verbindungsaktualisierungen verloren gehen. Vorhandene Verbindungen, die längere Zeit bestehen (z. B. telnet-Verbindungen), auf die zum Zeitpunkt der Übernahme zugegriffen wird, können dadurch beendet werden.

Scripts verwenden

Damit der Dispatcher Pakete weiterleiten kann, müssen auf einer Netzschnittstelleneinheit Aliasnamen für jede Cluster-Adresse erstellt werden.

- In einer Standalone-Dispatcher-Konfiguration müssen auf einer Netzschnittstellenkarte Aliasnamen für jede Cluster-Adresse erstellt werden (beispielsweise en0, tr0).
- In einer Konfiguration mit hoher Verfügbarkeit
 - muss auf der aktiven Maschine auf einer Netzschnittstellenkarte ein Aliasname für jede Cluster-Adresse erstellt werden (beispielsweise en0, tr0).
 - Auf der Bereitschaftsmaschine muss jede Cluster-Adresse als Aliasname einer Loopback-Einheit (z. B. lo0) angegeben werden.

- In allen Maschinen, in denen der Executor beendet wurde, müssen alle Aliasnamen entfernt werden, um Konflikte mit einer anderen Maschine zu vermeiden, die möglicherweise gestartet wird.

Da die Dispatcher-Maschinen bei einem erkannten Fehler ihren Status tauschen, müssen die oben angegebenen Befehle automatisch abgesetzt werden. Dazu führt der Dispatcher vom Benutzer erstellte Scripts aus. Beispiel-Scripts finden Sie im Verzeichnis **...nd/servers/samples**. Zum Ausführen *müssen* Sie diese in das Verzeichnis **...nd/servers/bin** verschieben.

Anmerkung: In einer Konfiguration mit gegenseitiger hoher Verfügbarkeit wird jedes "go"-Script vom Dispatcher mit einem Parameter aufgerufen, der die Adresse des primären Dispatchers angibt. Das Script muss diesen Parameter abfragen und die **ifconfig**-Befehle (bzw. unter Windows 2000 die **ndconfig**-Befehle) für die Cluster-Adressen ausführen, die diesem primären Dispatcher zugeordnet sind.

Sie können die folgenden Beispiel-Scripts verwenden:

goActive

Das Script goActive wird ausgeführt, wenn ein Dispatcher in den aktiven Status wechselt und mit dem Weiterleiten von Paketen beginnt.

- Wenn Sie den Dispatcher in einer Konfiguration mit hoher Verfügbarkeit verwenden, müssen Sie dieses Script erstellen. Dieses Script löscht die Aliasnamen von Loopback-Einheiten und fügt Einheitenaliasnamen hinzu.
- Wird der Dispatcher in einer Standalone-Konfiguration ausgeführt, benötigen Sie dieses Script nicht.

goStandby

Das Script goStandby wird ausgeführt, wenn ein Dispatcher in den Bereitschaftsstatus wechselt, in dem der Status der aktiven Maschine überwacht wird, jedoch keine Pakete weitergeleitet werden.

- Wenn Sie den Dispatcher in einer Konfiguration mit hoher Verfügbarkeit verwenden, müssen Sie dieses Script erstellen. Dieses Script sollte Einheitenaliasnamen löschen und Aliasnamen von Loopback-Einheiten hinzufügen.
- Wird der Dispatcher in einer Standalone-Konfiguration ausgeführt, benötigen Sie dieses Script nicht.

goInOp

Das Script goInOp wird beim Stoppen und beim ersten Starten eines Dispatcher-Executors ausgeführt.

- Wenn Sie den Dispatcher normalerweise in einer Konfiguration mit hoher Verfügbarkeit verwenden, können Sie dieses Script erstellen. Dieses Script löscht alle Aliasnamen von Einheiten und Loopback-Einheiten.
- Wird der Dispatcher normalerweise in einer Standalone-Konfiguration ausgeführt, ist dieses Script optional. Sie können das Script erstellen und zum Löschen von Aliasnamen für Einheiten benutzen oder Aliasnamen manuell löschen.

goIdle Das Script goIdle wird ausgeführt, wenn ein Dispatcher in den Freizu-stand wechselt und mit dem Weiterleiten von Paketen beginnt. Dieser Fall tritt ein, wenn die hohe Verfügbarkeit nicht hinzugefügt wurde, wie es in einer Standalone-Konfiguration der Fall ist. In einer Konfiguration mit hoher Verfügbarkeit geschieht dies auch vor dem Hinzufügen bzw. nach dem Entfernen der Merkmale für hohe Verfügbarkeit.

- Wenn der Dispatcher normalerweise in einer Konfiguration mit hoher Verfügbarkeit verwendet wird, sollten Sie dieses Script **nicht** erstellen.
- Wird der Dispatcher normalerweise in einer Standalone-Konfiguration ausgeführt, ist dieses Script optional. Sie können dieses Script erstellen und zum Hinzufügen von Aliasnamen für Einheiten benutzen oder Aliasnamen manuell hinzufügen. Wenn Sie dieses Script nicht für Ihre Standalone-Konfiguration erstellen, müssen Sie den Befehl **ndcontrol cluster configure** verwenden oder bei jedem Start des Executors die Aliasnamen manuell konfigurieren.

highavailChange

Das Script highavailChange wird ausgeführt, wenn sich der Status der hohen Verfügbarkeit auf einer Dispatcher-Maschine so ändert, dass eines der "go"-Scripts aufgerufen wird. Der einzige an dieses Script übergebene Parameter ist der Name des gerade vom Dispatcher ausgeführten "go"-Scripts. Sie können dieses Script beispielsweise so schreiben, dass Informationen zu Statusänderungen verwendet werden, um Alerts an einen Administrator zu senden, oder derartige Ereignisse einfach erfasst werden.

Anmerkung: Für Windows 2000: Wenn Sie Ihre Konfiguration so eingerichtet haben, dass Site Selector den Lastausgleich für zwei Dispatcher-Maschinen in einer Umgebung mit hoher Verfügbarkeit durchführt, müssen Sie im Microsoft Stack einen Aliasnamen für die Messwertserver hinzufügen. Dieser Aliasname sollte auch zum Script goActive hinzugefügt werden. Beispiel:

```
call netsh interface ip add address "Local Area Connection"  
    addr=9.37.51.28 mask=255.255.240.0
```

In den Scripts goStandby und GoInOp muss der Aliasname entfernt werden. Beispiel:

```
call netsh interface ip delete address "Local Area Connection"  
    addr=9.37.51.28
```

Wenn die Maschine mehrere NICs enthält, überprüfen Sie zunächst, welche Schnittstelle verwendet werden sollte. Setzen Sie dazu an der Eingabeaufforderung den Befehl `netsh interface ip show address` ab. Dieser Befehl gibt eine Liste der zur Zeit konfigurierten Schnittstellen zurück und versieht die Angabe "Local Area Connection" mit einer Nummer (z. B. "Local Area Connection 2"), so dass Sie bestimmen, welche Schnittstelle Sie verwenden sollten.

Regelbasierten Lastausgleich konfigurieren

Mit einem auf Regeln basierenden Lastausgleich kann genau abgestimmt werden, wann und warum Pakete an welche Server gesendet werden. Network Dispatcher überprüft alle hinzugefügten Regeln von der ersten Priorität bis zur letzten Priorität, stoppt bei der ersten Regel, die wahr ist, und führt dann den Lastausgleich zwischen allen Servern aus, die mit der Regel verbunden sind. Die Last wird bereits ausgehend von Ziel und Port ausgeglichen, jedoch unter Verwendung von Regeln, die erweiterte Möglichkeiten für die Verteilung von Verbindungen bieten.

In den meisten Fällen sollten Sie beim Konfigurieren von Regeln eine **immer gültige** Standardregel konfigurieren, um auch Anforderungen zu registrieren, die von den anderen Regeln höherer Priorität nicht erfasst werden. Dies könnte beispielsweise die Antwort "Die Site ist derzeit leider nicht verfügbar, versuchen Sie es später erneut" sein, wenn alle anderen Server nicht für die Client-Anforderung verwendet werden können.

Sie sollten den regelbasierten Lastausgleich für Dispatcher und Site Selector verwenden, wenn Sie aus bestimmten Gründen nur einen Teil Ihrer Server nutzen möchten. Für die CBR-Komponente *müssen* Sie in jedem Fall Regeln verwenden.

Anmerkung: Eine Konfiguration mit Regeln gilt *nicht* für Mailbox Locator (diese Komponente leitet IMAP- oder POP3-Anforderungen ausgehend von Benutzer-ID und Kennwort an bestimmte Server weiter) und für Cisco Consultant (diese Komponente nutzt die Manager-Funktion und die Advisor-Funktionen, um Informationen zum Lastausgleich für den Cisco CSS Switch bereitzustellen).

Es sind folgende Arten von Regeln verfügbar:

- Für Dispatcher:
 - Client-IP-Adresse
 - Uhrzeit
 - Verbindungen/Sekunde pro Port
 - Summe der aktiven Verbindungen pro Port
 - Client-Port
 - Diensttyp (TOS, Type of Service)
 - Reservierte Bandbreite
 - Gemeinsame Bandbreite
 - Immer wahr
 - Inhalt einer Anforderung
- Für CBR:
 - Client-IP-Adresse
 - Uhrzeit
 - Verbindungen/Sekunde pro Port
 - Summe der aktiven Verbindungen pro Port
 - Immer wahr
 - Inhalt einer Anforderung
- Für Site Selector:
 - Client-IP-Adresse
 - Uhrzeit
 - Messwert für alle
 - Durchschnitt der Messwerte
 - Immer wahr

Es wird empfohlen, einen Plan der Logik zu erstellen, die von den Regeln befolgt werden soll, bevor der Konfiguration Regeln hinzugefügt werden.

Wie werden Regeln ausgewertet?

Jede Regel hat einen Namen, einen Typ und eine Priorität und kann neben einer Servergruppe auch einen Anfangs- und Endbereich haben. Dem Regeltyp "content" für die CBR-Komponente ist ein regulärer Ausdruck (pattern) für den Abgleich zugeordnet. (Beispiele und Szenarien für die Verwendung der content-Regel sowie eine gültige pattern-Syntax für die content-Regel finden Sie in „Anhang C. Syntax der content-Regel“ auf Seite 331.)

Regeln werden in der Reihenfolge ihrer Priorität ausgewertet. Eine Regel mit der Priorität 1 (kleinere Nummer) wird vor einer Regel mit der Priorität 2 (größere Nummer) ausgewertet. Die erste Regel, die erfüllt ist, wird verwendet. Sobald eine Regel erfüllt ist, werden keine weiteren Regeln ausgewertet.

Eine Regel ist erfüllt, wenn die beiden folgenden Bedingungen zutreffen:

1. Das Prädikat der Regel muss wahr sein. Das heißt, dass der Wert, der ausgewertet wird, zwischen dem Anfangs- und dem Endbereich liegen muss, oder der Inhalt mit dem regulären Ausdruck übereinstimmen muss, der für "pattern" in der content-Regel angegeben wurde. Für Regeln des Typs "true" stimmt das Prädikat unabhängig vom Anfangs- und Endbereich immer überein.
2. Sind der Regel Server zugeordnet, muss mindestens ein Server verfügbar sein, an den Pakete weitergeleitet werden.

Sind einer Regel keine Server zugeordnet, muss für die Regel nur die erste Bedingung zutreffen, um erfüllt zu sein. In diesem Fall löscht der Dispatcher die Verbindungsanforderung. Site Selector gibt die Namensserveranforderung mit einem Fehler zurück und CBR veranlasst Caching Proxy, eine Fehlerseite auszugeben.

Wird keine der Regeln erfüllt, wählt Dispatcher aus allen für den Port verfügbaren Servern einen Server aus. Site Selector wählt aus allen für den Sitenamen verfügbaren Servern einen Server aus, und CBR veranlasst Caching Proxy, eine Fehlerseite auszugeben.

Regeln verwenden, die auf der Client-IP-Adresse basieren

Dieser Regeltyp ist für die Komponenten Dispatcher, CBR und Site Selector verfügbar.

Möglicherweise sollen Regeln auf der Basis der Client-IP-Adresse verwendet werden, wenn Kunden auf der Basis ihrer IP-Adresse berücksichtigt und Ressourcen zugeordnet werden sollen.

Beispielsweise haben Sie festgestellt, dass in Ihrem Netz in großem Umfang ein unbezahlter und deshalb unerwünschter Datenaustausch von Clients mit bestimmten IP-Adressen stattfindet. Sie erstellen eine Regel mit dem Befehl **ndcontrol rule**. Beispiel:

```
ndcontrol rule add 9.67.131.153:80:ni type ip beginrange 9.0.0.0  
endrange 9.255.255.255
```

Diese "ni"-Regel blendet alle Verbindungen für IBM Clients aus. Anschließend fügen Sie die Server zur Regel hinzu, auf die IBM Mitarbeiter Zugriff haben sollen. Werden keine Server zur Regel hinzugefügt, werden Anforderungen von den Adressen 9.x.x.x von keinem Ihrer Server bedient.

Regeln verwenden, die auf der Uhrzeit basieren

Dieser Regeltyp ist für die Komponenten Dispatcher, CBR und Site Selector verfügbar.

Möglicherweise sollen aus Gründen der Kapazitätsplanung Regeln verwendet werden, die auf der Uhrzeit basieren. Ist beispielsweise Ihre Website täglich zu bestimmten Zeiten besonders stark frequentiert, können Sie HTTP während der gesamten Zeit fünf Server zuordnen und dann während der Spitzenzeit weitere fünf Server hinzufügen.

Ein anderer Grund für die Verwendung einer Regel, die auf der Uhrzeit basiert, kann vorliegen, wenn Sie jede Nacht um Mitternacht einige der Server zur Wartung herunterfahren möchten. In diesem Fall würden Sie eine Regel erstellen, mit der die Server während der benötigten Wartungszeit ausgeschlossen werden.

Regeln auf der Basis der Verbindungen pro Sekunde an einem Port verwenden

Dieser Regeltyp ist für die Komponenten Dispatcher und CBR verfügbar.

Anmerkung: Der Manager muss aktiv sein, damit die folgenden Regeln ausgeführt werden können.

Vielleicht möchten Sie Regeln verwenden, die auf den Verbindungen pro Sekunde an einem Port basieren, wenn einige Ihrer Server auch von anderen Anwendungen benutzt werden sollen.

Sie können beispielsweise zwei Regeln erstellen:

1. Wenn Verbindungen pro Sekunde am Port 80 > 100, dann diese 2 Server verwenden
2. Wenn Verbindungen pro Sekunde am Port 80 > 2000, dann diese 10 Server verwenden

Möglicherweise verwenden Sie Telnet und möchten Sie zwei Ihrer fünf Server für Telnet reservieren, es sei denn, die Verbindungen pro Sekunde überschreiten eine bestimmte Stufe. In diesem Fall würde der Dispatcher zu Spitzenzeiten die Last auf alle fünf Server verteilen.

Regeln auf der Grundlage der an einem Port insgesamt aktiven Verbindungen verwenden

Dieser Regeltyp ist für die Komponenten Dispatcher und CBR verfügbar.

Anmerkung: Der Manager muss aktiv sein, damit die folgenden Regeln ausgeführt werden können.

Wenn Ihre Server überlastet sind und beginnen, Pakete zu verwerfen, möchten Sie vielleicht Regeln anwenden, die auf der Gesamtanzahl der an einem Port aktiven Verbindungen basieren. Von bestimmten Webservern werden weiterhin Verbindungen akzeptiert, auch wenn sie nicht über genügend Threads verfügen, um auf die Anforderung zu antworten. Von dem Client wird daraufhin eine Zeitlimitüberschreitung angefordert, und der Kunde, der Ihre Website aufruft, erhält keinen Service. Sie können Regeln verwenden, die auf den aktiven Verbindungen basieren, um die Kapazität innerhalb eines Pools mit Servern auszugleichen.

Sie wissen beispielsweise aus Erfahrung, dass Ihre Server den Service einstellen, nachdem sie 250 Verbindungen akzeptiert haben. Sie können eine Regel mit dem Befehl **ndcontrol rule** oder mit dem Befehl **cbrcontrol rule** erstellen. Beispiel:

```
ndcontrol rule add 130.40.52.153:80:pool2 type aktiv  
beginrange 250 endrange 500
```

oder

```
cbrcontrol rule add 130.40.52.153:80:pool2 type active  
beginrange 250 endrange 500
```

Sie würden dann der Regel Ihre aktuellen Server plus einige zusätzliche Server hinzufügen, die andernfalls für eine andere Verarbeitung verwendet werden.

Auf dem Client-Port basierende Regeln verwenden

Dieser Regeltyp ist nur in der Dispatcher-Komponente verfügbar.

Wenn Ihre Clients eine Software verwenden, die für Anforderungen von TCP/IP einen bestimmten Port anfordert, möchten Sie vielleicht Regeln auf der Basis des Client-Ports verwenden.

Sie könnten beispielsweise eine Regel erstellen, die angibt, dass für alle Anforderungen mit einem Client-Port von 10002 eine Gruppe besonders schneller Server bereitgestellt wird, da bekannt ist, dass alle Client-Anforderungen mit diesem Port von einer besonders wichtigen Kundengruppe stammen.

Regeln verwenden, die auf der Service-Art (Type of Service = TOS) basieren

Dieser Regeltyp ist nur in der Dispatcher-Komponente verfügbar.

Möglicherweise sollen Regeln verwendet werden, die auf dem Inhalt des Felds "Type of Service" (TOS) im IP-Header basieren. Wird beispielsweise eine Client-Anforderung mit einem TOS-Wert empfangen, der einen normalen Service angibt, kann die Anforderung an eine Servergruppe weitergeleitet werden. Wird eine andere Client-Anforderung mit einem anderen TOS-Wert empfangen, der einen Service mit höherer Priorität angibt, kann die Anforderung an eine andere Servergruppe weitergeleitet werden.

Die TOS-Regel ermöglicht die vollständige Konfiguration jedes Bits im TOS-Byte unter Verwendung des Befehls **ndcontrol rule**. Für signifikante Bits, die im TOS-Byte abgeglichen werden sollen, verwenden Sie 0 oder 1. Andernfalls wird der Wert x verwendet. Das folgende Beispiel zeigt das Hinzufügen einer TOS-Regel:

```
ndcontrol rule add 9.67.131.153:80:tsr type Service tos 0xx1010x
```

Regeln auf der Basis der reservierten und gemeinsam benutzten Bandbreite verwenden

Regeln für Kapazitätsauslastung und Bandbreite sind nur für die Dispatcher-Komponente verfügbar.

Bei Verwendung der Kapazitätsauslastungsfunktion misst der Dispatcher die Menge an Daten, die von jedem seiner Server übertragen wird. Dispatcher protokolliert die Kapazität auf Server-, Regel-, Port-, Cluster- und Executor-Ebene. Für jede dieser Ebenen existiert ein neuer Byte-Zählerwert: übertragene Kilobytes pro Sekunde. Der Wert (übertragene Kilobytes pro Sekunde) wird über ein Intervall von 60 Sekunden ermittelt. Sie können diese Kapazitätswerte in der grafischen Benutzerschnittstelle (GUI) oder in der Ausgabe eines Befehlszeilenberichts anzeigen.

Dispatcher gibt Ihnen die Möglichkeit, mit der Regel *Reservierte Bandbreite* Gruppen von Servern in Ihrer Konfiguration eine angegebene Bandbreite zuzuordnen. Überschreitet der Datenverkehr die Schwelle der reservierten Bandbreite können Sie wie folgt vorgehen:

- Senden Sie den Datenverkehr unter Verwendung einer immer gültigen Regel, die mit einer Antwort vom Typ "Site ausgelastet" reagiert, an einen anderen Server.
- Oder verwenden Sie die Regel *Gemeinsam genutzte Bandbreite*, um auf Cluster- oder Executor-Ebene eine bestimmte Bandbreite zur gemeinsamen Nutzung festzulegen. Wenn die Obergrenze für die gemeinsam genutzte Bandbreite annähernd erreicht ist, können Sie den direkten Datenverkehr mit einer immer gültigen Regel, die mit einer Antwort des Typs "Site ausgelastet" reagiert, zu einem anderen Server umleiten.

Wenn Sie wie oben beschrieben die Regel "Gemeinsam genutzte Bandbreite" zusammen mit der Regel "Reservierte Bandbreite" anwenden, können Sie für bevorzugte Clients einen besseren Serverzugang gewährleisten und so den Durchsatz für Transaktionen dieser Clients optimieren. Beispiel: Durch Anwendung der Regel "Gemeinsame Bandbreite" zur Verwendung ungenutzter Bandbreite können Sie denjenigen Kunden, die Onlinehandel auf Server-Clustern betreiben, einen höheren Serverzugriff ermöglichen als den Kunden, die die Server-Cluster zur Investitionssuche verwenden.

Beachten Sie folgende Überlegungen, um festzustellen, inwieweit Ihnen die Regeln zur Verwendung der Bandbreite Unterstützung bieten können beim Verwalten des Antwortdatenverkehrs, der von den Servern an die Clients fließt:

- Bandbreitenregeln können Sie bei der Verwaltung des Antwortdatenverkehrs einer Gruppe von Servermaschinen unterstützen, der durch Client-Anforderungen entsteht, die über Network Dispatcher fließen. Gelangt ein Teil des Client-Datenverkehrs an Network Dispatcher vorbei direkt zu den Servermaschinen, sind die Ergebnisse nicht vorhersehbar.
- Regeln zur Verwendung der Bandbreite können Sie beim Steuern des Antwortdatenverkehrs unterstützen, der über eine Verbindung von einer Gruppe von Servermaschinen an das Netz übertragen wird, wenn alle Server dieselbe Verbindung zum Netz verwenden. Verwenden Server für den Zugang zum Netz verschiedene oder mehrere Verbindungen, sind die Ergebnisse für die einzelnen Verbindungen nicht vorhersehbar.
- Bandbreitenregeln sind nur sinnvoll, wenn sich alle Server in demselben lokalen Netz wie die Network-Dispatcher-Maschine befinden. Sind ferne Server vorhanden, dann bestehen unterschiedliche Pfade zum Netz, und die Ergebnisse können unvorhersehbar sein.

Regel "Reservierte Bandbreite"

Dieser Regeltyp ist nur in der Dispatcher-Komponente verfügbar.

Mit der Regel "Reservierte Bandbreite" können Sie einen Lastausgleich auf der Basis der von einer Servergruppe gelieferten Datenmenge in Kilobytes pro Sekunde durchführen. Durch Festlegen eines Schwellenwertes (Zuordnen eines bestimmten Bandbreitenbereichs) für jede Gruppe von Servern in der Konfiguration können Sie die von jeder Cluster-Port-Kombination genutzte Bandbreite steuern und gewährleisten. Nachfolgend sehen Sie ein Beispiel für das Hinzufügen einer `reservedbandwidth`-Regel:

```
ndcontrol rule add 9.67.131.153:80:rbw type reservedbandwidth  
beginrange 0 endrange 300
```

Der Anfangs- und Endbereich werden in Kilobytes pro Sekunde angegeben.

Regel "Gemeinsame Bandbreite"

Dieser Regeltyp ist nur in der Dispatcher-Komponente verfügbar.

Wenn die übertragene Datenmenge die Begrenzung für die Regel "Reservierte Bandbreite" überschreitet, können Sie mit der Regel "Gemeinsam genutzte Bandbreite" nicht genutzte Bandbreite der Site verfügbar machen. Sie können diese Regel so definieren, dass die Bandbreite auf Cluster-Ebene oder auf Executor-Ebene gemeinsam genutzt wird. Durch gemeinsame Nutzung der Bandbreite auf Cluster-Ebene kann innerhalb desselben Clusters eine maximale Bandbreite über mehrere Ports (Anwendungen/Protokolle) hinweg von einem oder mehreren Ports genutzt werden. Durch gemeinsame Nutzung der Bandbreite auf Executor-Ebene kann innerhalb der gesamten Dispatcher-Konfiguration eine maximale Bandbreite von einem oder mehreren Clustern genutzt werden.

Vor der Konfiguration der Regel "Gemeinsame Bandbreite" müssen Sie die maximale Bandbreite (Kilobytes pro Sekunde) angeben, die auf Executor- oder Cluster-Ebene gemeinsam genutzt werden kann, indem Sie den Befehl **ndcontrol executor** oder **ndcontrol cluster** mit der Option `"sharedbandwidth"` verwenden. Nachfolgend sind Beispiele für die Befehlssyntax aufgeführt:

```
ndcontrol executor set sharedbandwidth Größe  
ndcontrol cluster [add | set] 9.12.32.9 sharedbandwidth Größe
```

Größe ist für `"sharedbandwidth"` ein ganzzahliger Wert (in Kilobytes pro Sekunde). Der Standardwert ist Null. Ist der Wert gleich Null, kann die Bandbreite nicht gemeinsam benutzt werden. Das Maximum, das Sie für `"sharedbandwidth"` angeben, darf nicht größer als der Wert für die gesamte verfügbare Bandbreite (gesamte Serverkapazität) sein.

Nachfolgend einige Beispiele für das Hinzufügen oder Definieren einer `sharedbandwidth`-Regel:

```
ndcontrol rule add 9.20.30.4:80:shbw type sharedbandwidth sharelevel  
Wertndcontrol rule set 9.20.34.11:80:shrule sharelevel Wert
```

Der *Wert* für "sharelevel" ist "executor" oder "cluster". Der Parameter "sharelevel" ist für die Regel "sharebandwidth" erforderlich.

Regel 'Messwert für alle'

Dieser Regeltyp ist nur in der Komponente Site Selector verfügbar.

Für die Regel "Messwert für alle" wählen Sie einen Systemmesswert (cpuload, memload oder ein eigenes angepasstes Script für Systemmesswerte) aus. Site Selector vergleicht den Systemmesswert (der vom Agenten Metric Server auf jedem Server mit Lastausgleich zurückgegeben wird) mit dem von Ihnen für die Regel festgelegten Anfangs- und Endbereich. Die Regel ist erst erfüllt, wenn der aktuelle Messwert für alle Server der Gruppe innerhalb des für die Regel festgelegten Bereichs liegt.

Anmerkung: Das von Ihnen gewählte Script für Systemmesswerte muss sich auf jedem der Server mit Lastausgleich befinden.

Nachfolgend sehen Sie ein Beispiel für das Hinzufügen einer Regel "Messwert für alle" zu Ihrer Konfiguration:

```
sscontrol rule add dnsload.com:allrule1 type metricall  
metricname cpuload beginrange 0 endrange 100
```

Regel "Durchschnitt der Messwerte"

Dieser Regeltyp ist nur in der Komponente Site Selector verfügbar.

Für die Regel "Durchschnitt der Messwerte" wählen Sie einen Systemmesswert (cpuload, memload oder ein eigenes angepasstes Script für Systemmesswerte) aus. Site Selector vergleicht den Systemmesswert (der vom Agenten Metric Server auf jedem Server mit Lastausgleich zurückgegeben wird) mit dem von Ihnen für die Regel festgelegten Anfangs- und Endbereich. Die Regel ist erst erfüllt, wenn der *Durchschnitt* der aktuellen Messwerte auf allen Servern der Gruppe innerhalb des für die Regel festgelegten Bereichs liegt.

Anmerkung: Das von Ihnen gewählte Script für Systemmesswerte muss sich auf jedem der Server mit Lastausgleich befinden.

Nachfolgend sehen Sie ein Beispiel für das Hinzufügen einer Regel "Durchschnitt der Messwerte" zu Ihrer Konfiguration:

```
sscontrol rule add dnsload.com:avgrule1 type metricavg  
metricname cpuload beginrange 0 endrange 100
```

Regeln verwenden, die immer wahr sind

Dieser Regeltyp ist für die Komponenten Dispatcher, CBR und Site Selector verfügbar.

Es kann eine Regel erstellt werden, die "immer wahr" ist. Eine solche Regel wird immer ausgewählt, es sei denn, alle ihr zugeordneten Server sind inaktiv. Aus diesem Grund sollte sie eine niedrigere Priorität als andere Regeln haben.

Sie können sogar mehrere Regeln haben, die "immer wahr" sind. Jeder Regel kann eine Gruppe mit Servern zugeordnet sein. Die erste wahre Regel mit einem verfügbaren Server wird ausgewählt. Angenommen, Sie haben sechs Server. Zwei dieser Server sollen unter allen Umständen den Datenaustausch steuern, es sei denn, beide Server sind inaktiv. Sind die ersten beiden Server inaktiv, soll eine zweite Gruppe mit Servern den Datenaustausch steuern. Sind alle vier dieser Server inaktiv, sollen die letzten zwei Server den Datenaustausch steuern. Sie könnten drei Regeln erstellen, die "immer wahr" sind. Die erste Gruppe mit Servern wird dann immer ausgewählt, wenn mindestens ein Server aktiv ist. Sind beide inaktiv, wird ein Server aus der zweiten Gruppe ausgewählt, usw.

Als weiteres Beispiel können Sie mit einer Regel, die "immer wahr" ist, sicherstellen, daß eingehende Clients keinen Service erhalten, wenn sie nicht den festgelegten Regeln entsprechen. Mit Hilfe des Befehls **ndcontrol rule** würden Sie die folgende Regel erstellen:

```
ndcontrol rule add 130.40.52.153:80:jamais type true priority 100
```

Wenn Sie anschließend keine Server zur Regel hinzufügen, werden die Client-Pakete ohne Antwort gelöscht.

Anmerkung: Beim Erstellen einer immer gültigen Regel müssen Sie keinen Anfangs- oder Endbereich festlegen.

Sie können mehrere Regeln definieren, die "immer wahr" sind, und dann durch Ändern der Prioritätsebene festlegen, welche Regel ausgeführt werden soll.

Regeln verwenden, die auf dem Inhalt der Anforderung basieren

Dieser Regeltyp ist für die Komponenten Dispatcher und CBR verfügbar.

Dieser Regeltyp wird verwendet, wenn Anforderungen an Gruppen von Servern gesendet werden sollen, die speziell für die Bearbeitung eines bestimmten Teils des Sitedatenverkehrs konfiguriert wurden. Beispielsweise wollen Sie eine Gruppe von Servern für die Bearbeitung aller *cgi-bin*-Anforderungen, eine andere Gruppe für die Bearbeitung aller Audiodatenstromanforderungen und eine dritte Gruppe für die Bearbeitung aller anderen Anforderungen verwenden. Sie würden eine Regel mit einem *pattern*-Wert hinzufügen, der mit dem Pfad zu Ihrem *cgi-bin*-Verzeichnis übereinstimmt, eine zweite Regel, die mit dem *Dateityp* Ihrer Audio-Streaming-Dateien übereinstimmt, und eine dritte Regel, die immer wahr ist, um den restlichen Datenverkehr zu bearbeiten. Sie würden dann jeder Regel die entsprechenden Server hinzufügen.

Wichtiger Hinweis: Beispiele und Szenarien für die Verwendung der *content*-Regel sowie eine gültige *pattern*-Syntax für die *content*-Regel finden Sie in „Anhang C. Syntax der *content*-Regel“ auf Seite 331.

Regeln zur Konfiguration hinzufügen

Zum Hinzufügen von Regeln können Sie den Befehl **ndcontrol rule add** verwenden, die Beispielkonfigurationsdatei editieren oder die grafische Benutzeroberfläche (GUI) benutzen. Sie können für jeden definierten Port eine oder mehrere Regel(n) hinzufügen.

Der Prozess besteht aus zwei Schritten: Hinzufügen der Regel und Definieren der Server, die verwendet werden sollen, wenn die Regel wahr ist. Beispielsweise möchte der Systemadministrator die Auslastung der Proxy-Server durch die einzelnen Unternehmensbereiche verfolgen. Dem Systemadministrator sind die IP-Adressen bekannt, die jedem Unternehmensbereich zugeordnet sind. Der Systemadministrator würde die erste Gruppe mit Regeln auf der Basis der Client-IP-Adressen erstellen, um zwischen den Lasten der einzelnen Unternehmensbereiche unterscheiden zu können.

```
ndcontrol rule add 130.40.52.153:80:Ber1 type ip b 9.1.0.0 e 9.1.255.255
ndcontrol rule add 130.40.52.153:80:Ber2 type ip b 9.2.0.0 e 9.2.255.255
ndcontrol rule add 130.40.52.153:80:Ber3 type ip b 9.3.0.0 e 9.3.255.255
```

Anschließend würde der Systemadministrator jeder Regel einen anderen Server hinzufügen und dann die Last auf jedem der Server messen, um dem Unternehmensbereich die verwendeten Services korrekt in Rechnung zu stellen. Beispiel:

```
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 useserver 130.40.52.153:80:div3 207.72.33.47
```

Regeloption für Serverauswertung

Die Option für Serverauswertung ist nur in der Dispatcher-Komponente verfügbar.

Der Befehl **ndcontrol rule** bietet eine Serverauswertungsoption für Regeln an. Mit der Option *evaluate* können Sie die Regelbedingungen für alle Server an einem Port oder für die in der Regel angegebenen Server auswerten. (In früheren Versionen von Network Dispatcher konnten nur die Regelbedingungen für alle Server an einem Port erfasst werden.)

Anmerkung: Die Option für Serverauswertung ist nur für Regeln gültig, die ihre Entscheidungen ausgehend von den Kenndaten der Server treffen. Dazu gehören die Regel "Summe Verbindungen (pro Sekunde)", die Regel "Aktive Verbindungen" und die Regel "Reservierte Bandbreite".

Nachfolgend einige Beispiele für das Hinzufügen oder Definieren der Auswertungsoption für eine Regel "Reservierte Bandbreite":

```
ndcontrol rule add 9.22.21.3:80:rbweval type reservedbandwidth evaluate Ebene
ndcontrol rule set 9.22.21.3:80:rbweval evaluate Ebene
```

Die *Ebene* für die Option "evaluate" kann auf "port" oder "rule" gesetzt werden. Der Standardwert ist "port".

In der Regel angegebene Server auswerten

Mit der Option zum Erfassen der Regelbedingungen für die in der Regel definierten Server können Sie zwei Regeln mit den folgenden Kenndaten konfigurieren:

- Die erste auszuwertende Regel enthält alle Server, die den Inhalt der Website verwalten. Die Option "evaluate" wird auf *rule* gesetzt (damit die Regelbedingungen für die in der Regel definierten Server ausgewertet werden).
- Die zweite Regel ist eine immer gültige Regel, in der nur ein Server definiert ist, der mit einer Antwort des Typs "Site ausgelastet" reagiert.

Wenn der Datenverkehr den Schwellenwert für die in der ersten Regel angegebenen Server überschreitet, wird er an den in der zweiten Regel definierten Server ("Site ausgelastet") gesendet. Sinkt die Zahl der Datenübertragungen unter den Schwellenwert, der für die Server in der ersten Regel definiert ist, werden die nachfolgenden Datenübertragungen erneut an die Server in der ersten Regel gesendet.

Server am Port auswerten

Wenn Sie bei den für das vorherige Beispiel beschriebenen Regeln den Wert der Option "evaluate" für die erste Regel auf *port* setzen (damit die Regelbedingungen für alle Server am Port ausgewertet werden) und der Datenverkehr den Schwellenwert für diese Regel überschreitet, wird er an den der zweiten Regel zugeordneten Server ("Site ausgelastet") gesendet.

Die erste Regel misst den Datenverkehr aller Server (einschließlich des Verkehrs für den Server "Site ausgelastet") am Port, um festzustellen, ob der Schwellenwert überschritten wird. Geht die Überlastung der ersten Regel zugeordneten Server zurück, kann der Datenverkehr entgegen der Absicht weiterhin an den Server "Site ausgelastet" gesendet werden, sofern der Datenverkehr am Port weiterhin den Schwellenwert für die erste Regel überschreitet.

Explizite Verbindungen benutzen

Normalerweise sind die Lastausgleichsfunktionen des Dispatchers unabhängig vom Inhalt der Sites, auf denen das Produkt benutzt wird. In einem bestimmten Bereich kann der Inhalt der Site jedoch von Bedeutung sein und können Entscheidungen über den Inhalt erhebliche Auswirkungen auf die Effektivität des Dispatchers haben. Dies ist der Bereich der Verbindungsadressierung.

Wenn Ihre Seiten Links enthalten, die auf einzelne Server für Ihre Site zeigen, zwingen Sie einen Client, auf eine bestimmte Maschine zuzugreifen und so die sonst wirksame Lastausgleichsfunktion zu umgehen.

Aus diesem Grund wird empfohlen, dass Sie in allen auf Ihren Seiten enthaltenen Verbindungen (Links) immer die Adresse des Dispatchers benutzen. Berücksichtigen Sie, dass die Art der benutzten Adressierung nicht immer offensichtlich ist, wenn Ihre Site eine automatisierte Programmierung benutzt, bei der HTML dynamisch erstellt wird. Um den Lastausgleich zu optimieren, sollten Sie auf alle expliziten Adressierungen achten und sie, falls möglich, vermeiden.

Konfiguration für ein privates Netz verwenden

Sie können den Dispatcher und die TCP-Servermaschinen für ein privates Netz konfigurieren. Durch diese Konfiguration können Konkurrenzsituationen auf dem öffentlichen oder externen Netz, die sich auf die Leistung auswirken, verringert werden.

Unter AIX hat diese Konfiguration auch den Vorteil, dass der schnelle SP High Performance Switch genutzt werden kann, wenn der Dispatcher und die TCP-Servermaschinen auf Knoten in einem SP Frame ausgeführt werden.

Um ein privates Netz zu erstellen, muss jede Maschine über mindestens zwei LAN-Karten verfügen, wobei eine der Karten mit dem privaten Netz verbunden wird. Zudem muss die zweite LAN-Karte auf einem anderen Teilnetz konfiguriert werden, damit die Dispatcher-Maschine die Client-Anforderungen über das private Netz an die TCP-Servermaschinen sendet.

Windows 2000: Führen Sie den folgenden Befehl aus:

```
ndconfig en1 10.0.0.x netmask 255.255.255.0
```

Hier ist en1 der Name der zweiten Schnittstellenkarte in der Dispatcher-Maschine, 10.0.0.x die Netzadresse der zweiten Schnittstellenkarte und 255.255.255.0 die Netzmaske des privaten Netzes.

Die über den Befehl **ndcontrol server add** hinzugefügten Server müssen mit den Adressen des privaten Netzes hinzugefügt werden. Beispielsweise muss bei dem Beispiel für den Server Apple in Abb. 27 auf Seite 199 der Befehl wie folgt aussehen:

```
ndcontrol server add Cluster-Adresse:80:10.0.0.1
```

Er darf nicht wie folgt aussehen:

```
ndcontrol server add Cluster-Adresse :80:9.67.131.18
```

Wenn mit Site Selector Lastinformationen für den Dispatcher bereitstellen, muss Site Selector so konfiguriert werden, dass die Last an den privaten Adressen gemeldet wird.

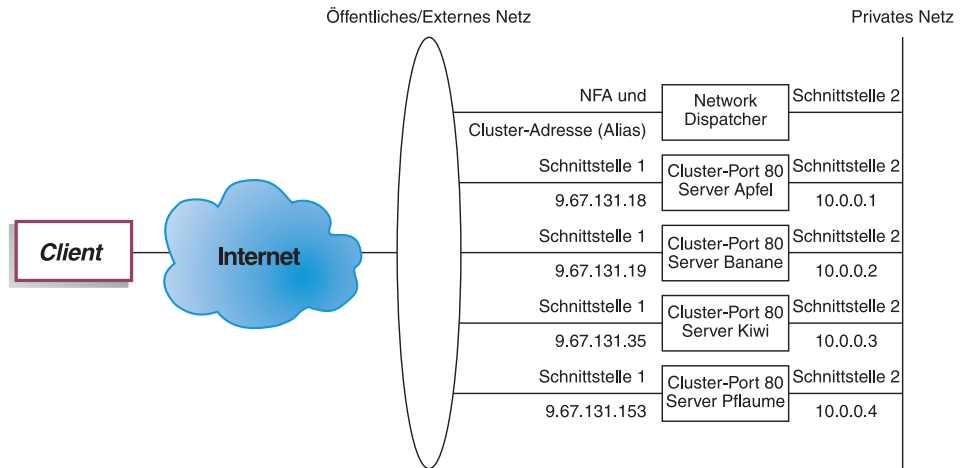


Abbildung 27. Beispiel für ein privates Netz mit dem Dispatcher

Die Verwendung der Konfiguration für ein privates Netz ist nur in der Dispatcher-Komponente gültig.

Platzhalter-Cluster verwenden, um Serverkonfigurationen zusammenzufassen

Das Wort "Platzhalter" bezieht sich auf die Fähigkeit des Clusters, mehreren IP-Adressen zu entsprechen (d. h. agiert als Platzhalter). Cluster-Adresse 0.0.0.0 wird verwendet, um einen Platzhalter-Cluster anzugeben.

Wenn Sie für viele Cluster-Adressen einen Lastausgleich durchführen müssen und die Port-/Serverkonfigurationen für alle Cluster identisch sind, können Sie die Cluster in einer Sternkonfiguration zusammenfassen.

Sie müssen dennoch jede Cluster-Adresse explizit auf einem der Netzwerkadapter Ihrer Dispatcher-Workstation konfigurieren. Sie sollten jedoch keine der Cluster-Adressen mit dem Befehl `ndcontrol cluster add` zur Dispatcher-Konfiguration hinzufügen.

Fügen Sie nur den Platzhalter-Cluster (Adresse 0.0.0.0) hinzu und konfigurieren Sie die Ports und Server wie für den Lastausgleich erforderlich. Für den Datenverkehr an jede der auf dem Adapter konfigurierten Adressen erfolgt ein Lastausgleich unter Verwendung der Platzhalter-Cluster-Konfiguration.

Ein Vorteil dieser Methode besteht darin, dass der Datenverkehr an alle Cluster-Adressen bei der Bestimmung des besten Servers berücksichtigt wird. Ist der Datenverkehr bei einem Cluster besonders hoch, und hat der Cluster viele

aktive Verbindungen auf einem der Server erstellt, findet für den Datenverkehr an andere Cluster-Adressen ein Lastausgleich unter Verwendung dieser Informationen statt.

Sie können den Platzhalter-Cluster mit tatsächlichen Clustern kombinieren, wenn Sie einige Cluster-Adressen mit eindeutiger Port-/Serverkonfiguration und einige Cluster-Adressen mit gemeinsamer Konfigurationen haben. Die eindeutigen Konfigurationen müssen jeweils einer tatsächlichen Cluster-Adresse zugeordnet werden. Alle gemeinsamen Konfigurationen können dem Platzhalter-Cluster zugeordnet werden.

Die Verwendung eines Platzhalter-Clusters für die Zusammenfassung von Serverkonfigurationen ist nur in der Dispatcher-Komponente gültig.

Platzhalter-Cluster für den Lastausgleich von Firewalls verwenden

Die Verwendung eines Platzhalter-Clusters für den Lastausgleich von Firewalls ist nur in der Dispatcher-Komponente gültig. Cluster-Adresse 0.0.0.0 wird verwendet, um einen Platzhalter-Cluster anzugeben.

Der Platzhalter-Cluster kann für den Lastausgleich von Datenverkehr an Adressen verwendet werden, die nicht explizit auf einem Netzwerkadapter der Dispatcher-Workstation konfiguriert sind. Dazu muss der Dispatcher mindestens den gesamten Datenverkehr sehen können, für den ein Lastausgleich erfolgen soll. Die Dispatcher-Workstation erkennt keinen Datenverkehr an Adressen, die nicht explizit auf einem ihrer Netzwerkadapter konfiguriert wurden. Eine Ausnahme hiervon bilden Adressen, die für bestimmten Datenverkehr als Standard-Route konfiguriert sind.

Wurde der Dispatcher als Standard-Route konfiguriert, erfolgt der Lastausgleich für den TCP- oder UDP-Datenverkehr, der über die Dispatcher-Maschine transportiert wird, unter Verwendung der Platzhalter-Cluster-Konfiguration.

Diese Methode kann für den Lastausgleich von Firewalls verwendet werden. Da Firewalls Pakete für jede Zieladresse und jeden Ziel-Port verarbeiten können, müssen Sie den Lastausgleich für den Datenverkehr unabhängig von der Zieladresse und dem Ziel-Port durchführen können.

Firewalls werden verwendet, um den Datenverkehr von nicht gesicherten Clients zu gesicherten Servern zu steuern und die Antworten von den gesicherten Servern zu bearbeiten sowie den Datenverkehr von Clients auf der gesicherten Seite zu Servern auf der nicht gesicherten Seite zu steuern und die Antworten zu bearbeiten.

Sie müssen zwei Dispatcher-Maschinen konfigurieren, eine für den Lastausgleich des nicht gesicherten Datenverkehrs an die nicht gesicherten Firewall-Adressen und eine für den Lastausgleich des gesicherten Datenverkehrs an die gesicherten Firewall-Adressen. Da beide Dispatcher den Platzhalter-Cluster und den Platzhalter-Port mit verschiedenen Gruppen von Serveradressen verwenden müssen, ist es erforderlich, dass sich die beiden Dispatcher auf zwei separaten Workstations befinden.

Platzhalter-Cluster mit Caching Proxy für transparente Weiterleitung verwenden

Die Verwendung eines Platzhalter-Clusters mit Caching Proxy für transparente Weiterleitung ist nur für die Dispatcher-Komponente möglich. Cluster-Adresse 0.0.0.0 wird verwendet, um einen Platzhalter-Cluster anzugeben.

Bei Verwendung der Platzhalter-Cluster-Funktion kann der Dispatcher eine transparente Weiterleitung für einen Caching-Proxy-Server aktivieren, der sich auf derselben Maschine wie der Dispatcher befindet. Dies ist nur eine AIX-Funktion, da zwischen der Dispatcher-Komponente und der TCP-Komponente des Betriebssystems eine Kommunikation stattfinden muss.

Zum Aktivieren dieses Merkmals müssen Sie Caching Proxy für den Empfang von Client-Anforderungen am Port 80 starten. Anschließend konfigurieren Sie einen Platzhalter-Cluster. Konfigurieren Sie im Platzhalter-Cluster den Port 80. Für Port 80 konfigurieren Sie die NFA der Dispatcher-Maschine als einzigen Server. Der gesamte Client-Datenverkehr an Adressen des Ports 80 wird nun an den Caching-Proxy-Server auf der Dispatcher-Workstation gesendet. Anschließend wird die Client-Anforderung wie üblich weitergeleitet. Die Antwort wird von Caching Proxy an den Client zurückgesendet. In diesem Modus führt die Dispatcher-Komponente keinen Lastausgleich durch.

Platzhalter-Port für die Übertragung von Datenverkehr mit nicht konfiguriertem Port verwenden

Der Platzhalter-Port kann für Datenverkehr verwendet werden, der nicht für einen explizit konfigurierten Port bestimmt ist. Eine solche Verwendung wäre der Lastausgleich für Firewalls. Zum anderen kann mit einem Platzhalter-Port sichergestellt werden, dass an einen nicht konfigurierten Port gerichteter Datenverkehr entsprechend bearbeitet wird. Durch Definieren eines Platzhalter-Ports ohne Server stellen Sie sicher, dass alle Anforderungen an einen nicht konfigurierten Port gelöscht und nicht an das Betriebssystem zurückgesendet werden. Ein Platzhalter-Port wird mit der Port-Nummer 0 (null) angegeben. Beispiel:

```
ndcontrol port add Cluster:0
```

Anmerkung: Der mit Platzhalterzeichen angegebene Port kann nicht für FTP-Datenverkehr verwendet werden.

Funktionsweise der Affinität für Network Dispatcher

Wenn Sie den Port eines Clusters als "sticky" konfigurieren, aktivieren Sie die Affinitätsfunktion. Wird der Port eines Clusters als sticky konfiguriert, können nachfolgende Client-Anforderungen an denselben Server übertragen werden. Dies geschieht, indem für die Option "Haltezeit für Port" einige Sekunden angegeben werden. Sie können die Funktion inaktivieren, indem Sie sticky-time auf null setzen.

Interaktion mit Port-übergreifender Affinität: Wird die Port-übergreifende Affinität aktiviert, müssen die Werte für "stickytime" der gemeinsam benutzten Ports identisch (und ungleich null) sein. Weitere Informationen befinden sich unter „Port-übergreifende Affinität“ auf Seite 204.

Verhalten bei Inaktivierung der Affinität

Wird bei inaktiverter Funktion eine neue TCP-Verbindung von einem Client empfangen, verwendet der Dispatcher den zu diesem Zeitpunkt richtigen Server und leitet die Pakete an diesen Server weiter. Wird eine weitere Verbindung von demselben Client empfangen, behandelt der Dispatcher diese Verbindung als eine neue Verbindung und wählt wieder den zu diesem Zeitpunkt richtigen Server aus.

Verhalten bei Aktivierung der Affinität

Bei Aktivierung der Funktion wird eine nachfolgende Anforderung von demselben Client an denselben Server geleitet.

Nach einer gewissen Zeit hört der Client auf, Transaktionen zu senden, so dass der Affinitätseintrag entfernt wird. Jeder Affinitätseintrag bleibt nur für die für "stickytime" festgelegte Zeit in Sekunden erhalten. Werden innerhalb der Haltezeit (stickytime) weitere Verbindungen empfangen, ist der Affinitätseintrag noch gültig, so dass die Anforderung an denselben Server weitergeleitet wird. Wenn eine Verbindung nicht innerhalb der Haltezeit empfangen wird, wird der Eintrag gelöscht. Für eine nach Ablauf der Haltezeit empfangene Verbindung wird ein neuer Server ausgewählt.

SDA-API zur Steuerung der Client-/Serveraffinität

Die Verwendung der Server Directed Affinity (SDA) API ist nur in der Dispatcher-Komponente gültig.

Die SDA-Funktion stellt eine API zur Verfügung, die es einem externen Agenten ermöglicht, das Dispatcher-Affinitätsverhalten zu beeinflussen.

Anmerkung: Es gilt die Einschränkung, dass SDA (Server Directed Affinity) nicht zusammen mit der Serverpartitionierung angewendet werden kann, da SDA für Suchfunktionen eindeutige Serveradressen in der Konfiguration erfordert.

SDA kann auch nicht zusammen mit der SSL-ID-Affinität verwendet werden, weil Server mit SDA die Affinitätstabelle steuern.

SDA-Funktionen

Ihre Anwendung hat möglicherweise angezeigt, dass die Serversysteme in der Lage sind, Client-Anforderungen an bestimmte Servermaschinen zu übertragen, und die Serversysteme dies besser können als der Dispatcher. Sie möchten, dass der Client mit dem Server Ihrer Wahl "kommuniziert" und nicht mit dem Server, der von der Lastausgleichsfunktion des Dispatchers ausgewählt wurde. Die SDA-Funktion stellt diese API zur Verfügung. Sie können jetzt Ihre eigene Software schreiben, um einen SDA-Agenten zu implementieren, der mit einem Empfangsprogramm im Dispatcher kommuniziert. Er kann dann die Dispatcher-Affinitätstabellen bearbeiten, um

- den Inhalt abzufragen.
- neue Sätze einzufügen.
- Sätze zu entfernen.

Sätze, die von einem SDA-Agenten in eine Affinitätstabelle eingefügt wurden, bleiben für unbegrenzte Zeit in der Tabelle. Sie verlieren nicht ihre Gültigkeit durch Zeitlimitüberschreitung. Sie werden nur entfernt, wenn sie von dem SDA-Agenten gelöscht werden oder wenn ein Dispatcher-Advisor feststellt, dass der Server inaktiv ist.

SDA-Komponenten des Dispatchers

Der Dispatcher implementiert ein neues Socket-Empfangsprogramm, um Anforderungen von einem SDA-Agenten zu akzeptieren und zu bearbeiten. Öffnet ein SDA-Agent eine Verbindung mit dem Dispatcher, akzeptiert das Empfangsprogramm die Verbindung und lässt die Verbindung geöffnet. Mehrere Anforderungen und Antworten können über diese anhaltende Verbindung fließen. Der Socket schließt, wenn er vom SDA-Agenten geschlossen wird oder wenn der Dispatcher einen nicht behebbaren Fehler erkennt. Innerhalb des Dispatchers nimmt das Empfangsprogramm jede Anforderung von dem SDA-Agenten entgegen, kommuniziert mit der entsprechenden Affinitätstabelle in dem Dispatcher-Executor-Kernel und bereitet eine Antwort für den SDA-Agenten vor.

Weitere Informationen hierzu finden Sie in den folgenden Dateien im Installationsverzeichnis von Network Dispatcher:

- API: `...nd/servers/samples/SDA/SDA_API.htm`
- Mustercode für einen SDA-Agenten:
`...nd/servers/samples/SDA/SDA_SampleAgent.java`

Port-übergreifende Affinität

Die Port-übergreifende Affinität gilt nur für die Dispatcher-Komponente.

Die Port-übergreifende Affinität ist Ausdehnung der Haltefunktion auf mehrere Ports. Wird beispielsweise eine Client-Anforderung zuerst an einem Port und die nächste Anforderung an einem anderen Port empfangen, kann der Dispatcher die Client-Anforderungen bei Port-übergreifender Affinität an denselben Server senden. Für die Verwendung dieser Funktion müssen die Ports folgende Bedingungen erfüllen:

- sie müssen dieselbe Cluster-Adresse benutzen
- sie müssen denselben Server benutzen
- sie müssen denselben Wert (ungleich null) für **stickytime** haben
- sie müssen denselben Wert für **stickymask** haben.

Mehrere Ports können eine Verbindung zu einem **crossport** herstellen. Wenn vom selben Client weitere Verbindungen an demselben Port oder einem gemeinsam benutzten Port ankommen, wird auf denselben Server zugegriffen. Nachfolgend sehen Sie eine Beispielkonfiguration für mehrere Ports mit einer Port-übergreifenden Affinität für Port 10:

```
ndcontrol port set Cluster:20 crossport 10
ndcontrol port set Cluster:30 crossport 10
ndcontrol port set Cluster:40 crossport 10
```

Nachdem Sie die Port-übergreifende Affinität konfiguriert haben, können Sie den Wert für stickytime des Ports flexibel ändern. Sie sollten "stickytime" jedoch für alle gemeinsam benutzten Ports auf denselben Wert setzen, da andernfalls unerwartete Ergebnisse auftreten können.

Wenn Sie die Port-übergreifende Affinität aufheben möchten, setzen Sie den Wert für crossport auf seine eigene Port-Nummer zurück. „ndcontrol port — Ports konfigurieren“ auf Seite 305 enthält ausführliche Informationen über die Befehlssyntax für die Option **crossport**.

Affinitätsadressmaske

Die Affinitätsadressmaske gilt nur für die Dispatcher-Komponente.

Die Affinitätsadressmaske ist eine Erweiterung der Sticky-Funktion, mit der Clients auf der Basis gemeinsamer Teilnetzadressen zusammengefasst werden. Die Angabe von **stickymask** im Befehl **ndcontrol port** ermöglicht es Ihnen, die höherwertigen Bits der 32-Bit-IP-Adresse zu maskieren. Wenn diese Funktion aktiviert ist und eine Client-Anforderung zum ersten Mal eine Verbindung zu dem Port herstellt, werden alle nachfolgenden Anforderungen von Clients mit derselben Teilnetzadresse (repräsentiert vom maskierten Abschnitt der Adresse) an denselben Server übertragen.

Wenn Sie beispielsweise alle eingehenden Client-Anforderungen mit derselben Netzadresse der Klasse A an einen Server übergeben möchten, setzen Sie den stickymask-Wert für den Port auf 8 (Bits). Sollen Client-Anforderungen mit derselben Netzadresse der Klasse B zusammengefasst werden, setzen Sie den Wert für stickymask auf 16 (Bits). Sollen Client-Anforderungen mit derselben Netzadresse der Klasse C zusammengefasst werden, setzen Sie den Wert für stickymask auf 24 (Bits).

Die besten Ergebnisse werden erzielt, wenn Sie den Wert für stickymask beim erstmaligen Starten von Network Dispatcher definieren. Wird der Wert für stickymask dynamisch geändert, können unvorhersehbare Ergebnisse auftreten.

Interaktion mit Port-übergreifender Affinität: Wenn Sie die Port-übergreifende Affinität aktivieren, müssen die Werte für "stickymask" der gemeinsam benutzten Ports identisch sein. Weitere Informationen befinden sich unter „Port-übergreifende Affinität“ auf Seite 204.

Um die Affinitätsadressmaske zu aktivieren, geben Sie einen ähnlichen Befehl `ndcontrol port` wie den folgenden aus:

```
ndcontrol port set Cluster:Port stickymask 8
```

Gültige Werte für stickymask sind 8, 16, 24 und 32. Der Wert 8 gibt an, dass die ersten 8 höherwertigen Bits der IP-Adresse (Netzadresse der Klasse A) maskiert werden. Der Wert 16 gibt an, dass die ersten 16 höherwertigen Bits der IP-Adresse (Netzadresse der Klasse B) maskiert werden. Der Wert 24 gibt an, dass die ersten 24 höherwertigen Bits der IP-Adresse (Netzadresse der Klasse C) maskiert werden. Wird der Wert 32 angegeben, wird die gesamte IP-Adresse maskiert, wodurch die Affinitätsadressmaskenfunktion inaktiviert wird. Der Standardwert für stickymask ist 32.

„`ndcontrol port` — Ports konfigurieren“ auf Seite 305 enthält ausführliche Informationen über die Befehlssyntax für stickymask (Affinitätsadressmaskenfunktion).

Überschreibung der Regelaaffinität

Mit der Außerkraftsetzung der Regelaaffinität können Sie Affinität eines Ports für einen Bestimmten Server außer Kraft setzen. Angenommen, Sie verwenden eine Regel, um die Anzahl der Verbindungen mit jedem Anwendungsserver zu begrenzen, und haben einen Überlaufserver mit einer Regel 'immer wahr', die "Bitte später erneut versuchen" für diese Anwendung angibt. Der Port hat einen stickytime-Wert von 25 Minuten. Sie möchten also nicht, dass der Client an diesen Server gebunden wird. Durch Außerkraftsetzung der Regelaaffinität können Sie bewirken, dass der Überlaufserver die diesem Port normalerweise zugeordnete Affinität außer Kraft setzt. Fordert der Client das nächste Mal

den Cluster an, erfolgt ein Lastausgleich auf der Basis des besten verfügbaren Anwendungsservers und nicht des Überlaufservers.

„`ndcontrol server` — Server konfigurieren“ auf Seite 320 enthält ausführliche Informationen über die Befehlssyntax beim Überschreiben der Regelaaffinität mit der Option **sticky** im Befehl `server`.

Stilllegung gehaltener Verbindungen

Die Stilllegung gehaltener Verbindungen gilt für die Komponenten Dispatcher und CBR. Wenn Sie aus bestimmten Gründen (Aktualisierungen, Upgrades, Wartung usw.) einen Server aus der Network-Dispatcher-Konfiguration entfernen müssen, können Sie den Befehl **`ndcontrol manager quiesce`** verwenden. Mit dem Unterbefehl `quiesce` können vorhandene Verbindungen beendet werden (ohne weiter bedient zu werden). Nachfolgende neue Verbindungen vom Client zum stillgelegten Server werden nur weitergeleitet, wenn die Verbindung als gehaltene Verbindung (sticky) bezeichnet ist und die Haltezeit (stickytime) nicht abgelaufen ist. Alle anderen neuen Verbindungen zum Server werden vom Unterbefehl `quiesce` unterbunden.

Verwenden Sie `quiesce "now"` nur, wenn Sie die Haltezeit definiert haben und vor Ablauf der Haltezeit neue Verbindungen an einen anderen als den stillgelegten Server gesendet werden sollen. Im folgenden Beispiel wird die Option `"now"` für die Stilllegung des Servers 9.40.25.67 verwendet:

```
ndcontrol manager quiesce 9.40.25.67 now
```

Die Option `"now"` bestimmt wie folgt, was mit gehaltenen Verbindungen geschehen soll:

- Wenn Sie *nicht* die Option `"now"` angeben, können vorhandene Verbindungen beendet werden. Nachfolgende neue Verbindungen zum stillgelegten Server werden weitergeleitet, sofern sie von Clients mit vorhanden und als gehaltene Verbindungen bezeichneten stammen und der stillgelegte Server die neue Anforderung vor Ablauf der Haltezeit empfängt. (Falls Sie das Merkmal "Haltezeit" (Affinität) jedoch nicht aktiviert haben, kann der stillgelegte Server keine neuen Verbindungen empfangen.) Auf diese Weise können Server schrittweise stillgelegt werden. Sie können einen Server beispielsweise nach und nach stilllegen und dann auf den Zeitpunkt des geringsten Datenverkehrsaufkommen warten (vielleicht am frühen Morgen), um den Server vollständig aus der Konfiguration zu entfernen.
- Durch Angabe von `"now"` legen Sie den Server so still, dass vorhandene Verbindungen beendet werden können, alle neuen Verbindungen, einschließlich der nachfolgenden Verbindungen von Clients mit bereits vorhandenen gehaltenen Verbindungen, jedoch unterbunden werden. Diese abrupte Methode der Serverstilllegung war in früheren Versionen von Network Dispatcher die einzig mögliche Methode.

Affinitätsoption für Regeln

Mit dem Befehl **ndcontrol rule** können Sie die folgenden Arten der Affinität angeben:

- **Aktive Cookie-Affinität** — Aktiviert die Verteilung von Webdatenverkehr mit Affinität zu einem Server ausgehend von den von Network Dispatcher generierten Cookies.
- **Passive Cookie-Affinität** — Aktiviert die Verteilung von Webdatenverkehr mit Affinität zu einem Server, ausgehend von den Identifizierungs-Cookies, die von den Servern generiert werden. Bei Verwendung der passiven Cookie-Affinität müssen Sie den Befehl "rule" mit dem Parameter "cookie-name" angeben.
- **URI-Affinität** — aktiviert den Lastausgleich für Webdatenverkehr auf Caching-Proxy-Servern mit effektiver Vergrößerung des Cache.

Der Standardwert für die Option "affinity" ist "none". Die Option **stickytime** für den Port-Befehl (port) muss auf null gesetzt (inaktiviert) sein, damit die Option **affinity** des Regelbefehls (rule) auf die aktive oder passive Cookie-Affinität bzw. auf die URI-Affinität gesetzt werden kann. Ist für die Regel eine Affinität definiert, kann keine Haltezeit für den Port aktiviert werden.

Die aktive Cookie-Affinität gilt nur für die Komponente CBR. Die passive Cookie-Affinität und die URI-Affinität gelten für die Komponente CBR sowie für die Weiterleitungsmethode "cbr" der Dispatcher-Komponente.

Aktive Cookie-Affinität

Die aktive Cookie-Affinität gilt nur für die CBR-Komponente. Sie bietet eine Möglichkeit, Clients an einen bestimmten Server zu "binden". Diese Funktion wird aktiviert, indem der Wert **stickytime** einer Regel auf eine positive Zahl und die Affinität auf "activecookie" gesetzt wird. Dies kann beim Hinzufügen der Regel oder mit dem Befehl "rule set" geschehen. Ausführliche Informationen zur Befehlssyntax finden Sie im Abschnitt „ndcontrol rule — Regeln konfigurieren“ auf Seite 312.

Wenn eine Regel für aktive Cookie-Affinität aktiviert wurde, wird der Lastausgleich für neue Client-Anforderungen mit Standard-CBR-Algorithmen durchgeführt. Aufeinanderfolgende Anforderungen eines Clients werden dabei an den zu Beginn ausgewählten Server gesendet. Der ausgewählte Server ist als Cookie in der Antwort an den Client gespeichert. Solange die zukünftigen Anforderungen des Clients das Cookie enthalten und jede Anforderung innerhalb der Haltezeit empfangen wird, bleibt der Client an den anfänglichen Server gebunden.

Mit der aktiven Cookie-Affinität wird sichergestellt, dass die Arbeitslast eines Clients über einen bestimmten Zeitraum hinweg an denselben Server weitergeleitet wird. Dies wird erreicht, indem ein Cookie gesendet wird, das von dem Client-Browser gespeichert wird. Das Cookie enthält die Kombination Cluster:Port, auf deren Grundlage die Entscheidung getroffen wurde, den Server, an den die Arbeitslast weitergeleitet wurde, und eine Zeitmarke für das Zeitlimit, bei dessen Erreichung die Affinität ungültig wird. Bei Erfüllung einer Regel mit gesetzter aktiver Cookie-Affinität wird das vom Client gesendete Cookie überprüft. Wenn ein Cookie mit der Kennung für die Cluster:Port-Kombination gefunden wird, die die Regel erfüllt, werden der Server, an den die Arbeitslast weitergeleitet werden soll, und die Zeitmarke für das Zeitlimit aus dem Cookie extrahiert. Wenn der Server noch zu der von der Regel verwendeten Gruppe gehört, seine Wertigkeit größer als null ist und die Zeitmarke für den Verfall einen späteren Zeitpunkt als die aktuelle Zeit angibt, wird der Server in dem Cookie für den Lastausgleich ausgewählt. Ist eine der vorhergehenden drei Bedingungen nicht erfüllt, wird ein Server unter Verwendung des normalen Algorithmus ausgewählt. Nach Auswahl eines Servers (mit einer der beiden Methoden) wird ein neues Cookie erstellt, das IBM CBR, die Angabe Cluster:Port:ausgewählterServer und eine Zeitmarke enthält. Die Zeitmarke gibt die Uhrzeit an, zu der die Affinität ungültig wird. Die Angabe "Cluster:Port:ausgewählterServer" wird codiert, so dass keine Informationen zur CBR-Konfiguration erkennbar sind. Ein "Verfalls"parameter wird auch in das Cookie eingefügt. Dieser Parameter hat ein Format, das der Browser verstehen kann, und bewirkt, dass das Cookie zwei Stunden nach Erreichen der Zeitmarke für den Verfall ungültig wird. Damit soll vermieden werden, dass die Cookie-Datenbank des Clients zu sehr anwächst.

Dieses neue Cookie wird dann in die Kopfzeilen eingefügt, die an den Client gesendet werden. Ist der Browser des Clients so konfiguriert, dass er Cookies akzeptiert, sendet er nachfolgende Anforderungen zurück.

Die Option für aktive Cookie-Affinität für den Regelbefehl (rule) kann nur auf "activecookie" gesetzt werden, wenn die Haltezeit (stickytime) für den Port gleich null (inaktiviert) ist. Ist die aktive Cookie-Affinität für eine Regel aktiviert, kann keine Haltezeit für den Port aktiviert werden.

Aktive Cookie-Affinität aktivieren

Verwenden Sie zum Aktivieren der aktiven Cookie-Affinität für eine bestimmte Regel wie folgt den Befehl "rule set":

```
rule set Cluster:Port:Regel stickytime 60  
rule set Cluster:Port:Regel affinity activecookie
```

Grund für die Verwendung der aktiven Cookie-Affinität

Die Haltezeit wird in der Regel für CGI oder Servlets verwendet, die den Client-Status auf dem Server speichern. Der Status wird durch eine Cookie-ID identifiziert (dies sind Server-Cookies).

Der Client-Status ist nur auf dem ausgewählten Server gespeichert. Der Client benötigt also das Cookie von diesem Server, um diesen Status zwischen Anforderungen zu wahren.

Passive Cookie-Affinität

Die passive Cookie-Affinität gilt für die inhaltsabhängige Weiterleitung (cbr) durch die Dispatcher-Komponente und die CBR-Komponente. Informationen zum Konfigurieren der Dispatcher-Weiterleitungsmethode "cbr" finden Sie im Abschnitt „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)" auf Seite 57.

Die passive Cookie-Affinität bietet eine Möglichkeit, Clients an einen bestimmten Server zu binden. Wenn Sie für eine Regel die Affinität auf "passivecookie" setzen, können Sie den Webdatenverkehr mit Affinität zu einem Server verteilen. Die Affinität basiert auf den von den Servern generierten Identifizierungs-Cookies. Die passive Cookie-Affinität wird auf Regelebene konfiguriert. Wird eine Regel mit aktivierter passiver Cookie-Affinität erfüllt, wählt Network Dispatcher den Server ausgehend von dem im HTTP-Header der Client-Anforderung enthaltenen Cookie-Namen aus. Die Server, an die Network Dispatcher neue eingehende Anforderungen sendet, werden anhand der Cookies, die während der bisherigen Verbindungen von den Servern generiert wurden, ausgewählt. Wenn in der Client-Anforderung kein Cookie-Wert gefunden wird oder dieser nicht mit einem der Server-Cookie-Werte übereinstimmt, wird der Server mit Hilfe der gewichteten RoundRobin-Methode ausgewählt.

Gehen Sie zum Konfigurieren der **passiven Cookie-Affinität** wie folgt vor:

- Für den Dispatcher müssen Sie zunächst die Weiterleitungsmethode "cbr" konfigurieren. (Informationen hierzu finden Sie im Abschnitt „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)" auf Seite 57.) Für die CBR-Komponente ist dieser Schritt nicht erforderlich.
- Setzen Sie den Parameter **affinity** des Befehls **ndcontrol rule [add | set]** auf "passivecookie". Der Parameter **cookieName** muss auf den Namen des Cookies gesetzt werden, nach dem Network Dispatcher im HTTP-Header der Client-Anforderung suchen soll.
- Legen Sie für jeden in der Regel definierten Server den Parameter **cookievalue** des Befehls **ndcontrol server [add | set]** fest.

Die Option für passive Cookie-Affinität für den Regelbefehl (rule) kann nur auf "passivecookie" gesetzt werden, wenn die Haltezeit (stickytime) für den Port gleich null (inaktiviert) ist. Ist die passive Cookie-Affinität für eine Regel aktiviert, kann keine Haltezeit für den Port aktiviert werden.

URI-Affinität

Die URI-Affinität gilt für die Weiterleitungsmethode "cbr" von Dispatcher und die CBR-Komponente. Informationen zum Konfigurieren der Weiterleitungsmethode "cbr" finden Sie im Abschnitt „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)“ auf Seite 57.

Bei Verwendung der URI-Affinität kann die Arbeitslast des Webdatenverkehrs so auf Caching-Proxy-Server verteilt werden, dass auf den einzelnen Servern unterschiedlicher Inhalt im Cache gespeichert werden kann. Auf diese Weise vergrößern Sie effektiv den Cache Ihrer Site, da eine redundante Zwischenspeicherung von Inhalten auf mehreren Maschinen vermieden wird. Konfigurieren Sie die URI-Affinität auf Regelebene. Wenn eine Regel mit aktivierter URI-Affinität erfüllt ist und die entsprechende Gruppe von Servern verfügbar und aktiv ist, leitet Network Dispatcher neue eingehende Client-Anforderungen mit demselben URI an einen Server weiter.

Normalerweise verteilt Network Dispatcher Anforderungen auf mehrere Server, die identische Inhalte bereitstellen. Wenn Sie Network Dispatcher mit einer Gruppe von Caching-Servern verwenden, wird häufig abgerufener Inhalt unter Umständen auf allen Servern zwischengespeichert. Daraus ergibt sich eine sehr hohe Client-Belastung, wenn auf mehreren Maschinen zwischengespeicherte identische Inhalte repliziert werden. Diese Vorgehensweise ist besonders für Websites mit großem Datenvolumen sinnvoll.

Wenn Ihre Website jedoch nur ein mittleres Client-Datenvolumen mit den verschiedensten Inhalten unterstützt und Sie einen großen, auf mehrere Server verteilten Cache bevorzugen, ist der Durchsatz Ihrer Site besser, wenn jeder Caching Server eindeutige Inhalte enthält und Network Dispatcher die Anforderungen nur an den Caching Server mit den entsprechenden Inhalten weiterleitet.

Bei Verwendung der URI-Affinität können Sie mit Network Dispatcher den zwischengespeicherten Inhalt auf einzelne Server verteilen und so eine redundante Zwischenspeicherung von Inhalten auf mehreren Maschinen vermeiden. Durch diese Erweiterung kann der Durchsatz von Serversites mit vielfältigen Inhalten, die Caching-Proxy-Server verwenden, verbessert werden. Identische Anforderungen werden an einen Server gesendet, so dass der Inhalt nur auf einem Server zwischengespeichert wird. Mit jeder zum Pool hinzugefügten Servermaschine vergrößert sich der effektive Cache.

Gehen Sie zum Konfigurieren der **URI-Affinität** wie folgt vor:

- Für den Dispatcher müssen Sie zunächst die Weiterleitungsmethode "cbr" konfigurieren. (Informationen hierzu finden Sie im Abschnitt „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)" auf Seite 57.) Für die CBR-Komponente ist dieser Schritt nicht erforderlich.
- Setzen Sie den Parameter **affinity** des Befehls **ndcontrol rule [add|set]** oder **cbrcontrol rule [add|set]** auf "uri".

Die Option für URI-Affinität für den Regelbefehl (rule) kann nur auf URI gesetzt werden, wenn die Haltezeit (stickytime) für den Port gleich null (inaktiviert) ist. Ist die URI-Affinität für eine Regel aktiviert, kann keine Haltezeit für den Port aktiviert werden.

Erkennung von DoS-Attacken

Diese Funktion ist nur für die Dispatcher-Komponente verfügbar.

Der Dispatcher ist in der Lage, potenzielle DoS-Attacken zu erkennen und Administratoren durch einen Alert zu benachrichtigen. Dazu analysiert der Dispatcher eingehende Anforderungen auf eine verdächtige Anzahl halboffener TCP-Verbindungen von Servern, die ein allgemeines Kennzeichen einfacher DoS-Attacken sind. Bei einer DoS-Attacke empfängt eine Site eine große Anzahl fabrizierter SYN-Pakete von einer Vielzahl von Quellen-IP-Adressen und Quellen-Port-Nummern. Folgepakete für diese TCP-Verbindungen werden jedoch nicht empfangen. Dies führt zu einer großen Anzahl halboffener TCP-Verbindungen auf den Servern, so dass diese mit der Zeit sehr langsam werden und keine neuen ankommenden Verbindungen mehr akzeptieren können.

Network Dispatcher stellt Benutzer-Exits, die Scripts aufrufen. Diese Scripts können so angepasst werden, dass der Administrator per Alert von einer möglichen DoS-Attacke informiert wird. Dispatcher stellt im Verzeichnis **...nd/servers/samples** das folgende Beispiel-Script bereit:

- halfOpenAlert — es wurde eine mögliche DoS-Attacke (Denial of Service) festgestellt
- halfOpenAlertDone — die DoS-Attacke ist beendet

Zum Ausführen der Dateien müssen Sie sie in das Verzeichnis **...nd/servers/bin** verschieben und die Erweiterung ".sample" löschen.

Zum Implementieren der Erkennung von DoS-Attacken müssen Sie wie folgt den Parameter **maxhalfopen** des Befehls **ndcontrol port** setzen:

```
ndcontrol port set 127.40.56.1:80 maxhalfopen 1000
```

Im obigen Beispiel vergleicht der Dispatcher die aktuelle Gesamtanzahl halboffener Verbindungen (für alle Server des Clusters 127.40.56.1 am Port 80) mit dem Schwellenwert 1000 (der vom Parameter "maxhalfopen" angegeben ist). Übersteigt die Anzahl der aktuellen halboffenen Verbindungen den Schwellenwert, wird ein Alert-Script (halfOpenAlert) aufgerufen. Fällt die Anzahl halboffener Verbindungen unter den Schwellenwert, wird ein anderes Alert-Script aufgerufen, um das Ende der Attacke anzuzeigen.

Bestimmen Sie wie folgt den Wert, den Sie für "maxhalfopen" definieren sollten: Wenn auf Ihrer Site ein mäßiger bis starker Datenverkehr zu verzeichnen ist, erstellen Sie in regelmäßigen Abständen (vielleicht alle 10 Minuten) mit **ndcontrol port halfopenaddressreport Cluster:Port** einen Bericht zu halboffenen Verbindungen. Der Bericht gibt die aktuelle Gesamtanzahl der empfangenen halboffenen Verbindungen an. Setzen Sie "maxhalfopen" auf einen Wert, der 50 % bis 200 % über der höchsten Anzahl halboffener Verbindungen liegt, die auf Ihrer Site aufgetreten sind.

Neben statistischen Daten generiert "halfopenaddressreport" für alle Client-Adressen (maximal 8000 Adresspaare), deren Serverzugriff halboffene Verbindungen zur Folge hatten, Einträge im Protokoll (`..nd/servers/logs/dispatcher/halfOpen.log`).

Anmerkung: Es gibt SNMP-Alarmnachrichten, die den Scripts halfOpenAlert und halfOpenAlertDone entsprechen. Wenn der SNMP-Subagent konfiguriert und aktiv ist, werden unter den Bedingungen, die die Scripts aufrufen, die entsprechenden Alarmnachrichten gesendet. Weitere Informationen zum SNMP-Subagenten finden Sie im Abschnitt „Simple Network Management Protocol mit Dispatcher verwenden“ auf Seite 225.

Back-End-Server können Sie zusätzlich vor DoS-Attacken schützen, indem Sie Platzhalter-Cluster und -Ports konfigurieren. Fügen Sie unter jedem konfigurierten Cluster einen Platzhalter-Port ohne Server hinzu. Fügen Sie außerdem einen Platzhalter-Cluster mit einem Platzhalter-Port und ohne Server hinzu. Dies hat zur Folge, dass alle Pakete, die an einen Platzhalter-Cluster oder -Port gesendet werden, gelöscht werden. Informationen zu Platzhalter-Clustern und -Ports finden Sie in den Abschnitten „Platzhalter-Cluster verwenden, um Serverkonfigurationen zusammenzufassen“ auf Seite 199 und „Platzhalter-Port für die Übertragung von Datenverkehr mit nicht konfiguriertem Port verwenden“ auf Seite 201.

Binäres Protokollieren verwenden, um Serverstatistiken zu analysieren

Anmerkung: Die binäre Protokollierung gibt nicht für die Komponente Site Selector.

Die binäre Protokollierung ermöglicht das Speichern von Serverdaten in Binärdateien. Diese Dateien können dann verarbeitet werden, um die Serverinformationen zu analysieren, die über einen bestimmten Zeitraum gesammelt wurden.

Die folgenden Informationen werden für jeden in der Konfiguration definierten Server in dem binären Protokoll gespeichert:

- Cluster-Adresse
- Port-Nummer
- Server-ID
- Serveradresse
- Serverwertigkeit
- Summe Verbindungen für Server
- Aktive Verbindungen für Server
- Last am Server-Port
- Serversystembelastung

Einige dieser Informationen werden im Rahmen des Manager-Zyklus aus dem Executor abgerufen. Der Manager muss daher aktiv sein, damit die Informationen in den binären Protokollen aufgezeichnet werden können.

Verwenden Sie den Befehl **ndcontrol log set**, um das binäre Protokollieren zu konfigurieren.

- log start
- log stop
- log set interval <Sekunde>
- log set retention <Stunden>
- log status

Mit der Option 'start' wird die Protokollierung von Serverinformationen in binären Protokollen im Protokollverzeichnis gestartet. Ein Protokoll wird zu Beginn jeder Stunde mit dem Datum und der Uhrzeit als Name der Datei erstellt.

Mit der Option 'stop' wird die Protokollierung von Serverinformationen in binären Protokollen gestoppt. Der Protokolldienst wird standardmäßig gestoppt.

Mit der Option 'set interval' wird gesteuert, wie oft Informationen in die Protokolle geschrieben werden. Der Manager sendet in jedem Manager-Intervall Serverdaten an den Protokollserver. Die Daten werden nur in die Protokolle geschrieben, wenn seit dem Schreiben des letzten Protokolleintrags die für das Protokollintervall angegebene Zeit in Sekunden verstrichen ist. Standardmäßig wird das Protokollierungsintervall auf 60 Sekunden gesetzt. Zwischen den Einstellungen für das Manager-Intervall und das Protokollierungsintervall gibt es eine gewisse Interaktion. Da dem Protokollserver Informationen nicht schneller zur Verfügung gestellt werden als dies im Manager-Intervall (in Sekunden) angegeben ist, wird durch Angabe eines Protokollierungsintervalls, das kleiner als das Manager-Intervall ist, das Protokollierungsintervall de facto auf denselben Wert wie das Manager-Intervall gesetzt. Mit dieser Protokollierungstechnik können Sie Serverinformationen mit größerer Detaillierung erfassen. Sie können alle vom Manager festgestellten Änderungen der Serverinformationen für die Berechnung von Serverwertigkeiten erfassen. Dieser Informationsumfang ist jedoch wahrscheinlich nicht erforderlich, um die Serverauslastung und Trends zu analysieren. Werden Serverinformationen alle 60 Sekunden protokolliert, erhalten Sie Momentaufnahmen von Serverinformationen in Abhängigkeit vom zeitlichen Verlauf. Wird das Protokollierungsintervall auf einen sehr niedrigen Wert gesetzt, kann dies zu großen Datenmengen führen.

Mit der Option 'set retention' wird gesteuert, wie lange Protokolldateien aufbewahrt werden. Protokolldateien, die älter als die angegebene Verweildauer (Stunden) sind, werden von dem Protokollserver gelöscht. Dies geschieht nur, wenn der Protokollserver von dem Manager aufgerufen wird, d. h., wird der Manager gestoppt, werden alte Protokolldateien nicht gelöscht.

Mit der Option 'status' werden die aktuellen Einstellungen des Protokolldienstes zurückgegeben. Diese Einstellungen geben an, ob der Service gestartet ist und welche Werte für das Intervall und die Verweildauer angegeben sind.

Im Verzeichnis `...nd/servers/samples/BinaryLog` stehen ein Beispiel-Java-Programm und eine Beispielbefehlsdatei zur Verfügung. Dieses Beispiel zeigt, wie alle Informationen aus den Protokolldateien abgerufen und angezeigt werden können. Es kann für jede Art von Datenanalyse angepasst werden. Beispiel unter Verwendung des bereitgestellten Scripts und Programms für Dispatcher:

ndlogreport 2001/05/01 8:00 2001/05/01 17:00

Dieser Befehl liefert einen Bericht mit den Serverdaten der Dispatcher-Komponente vom 1. Mai 2001 in der Zeit von 8.00 Uhr bis 17.00 Uhr. (Verwenden Sie für CBR **cbrlogreport**. Für Mailbox Locator müssen Sie **mllogreport** verwenden. Verwenden Sie für Cisco Consultant **lbclogreport**.)

Zusätzliche Informationen zu den erweiterten Funktionen von Cisco Consultant

Für Cisco Consultant führt der Cisco CSS Switch die Tasks aus, die der Executor bei der Dispatcher-Komponente übernimmt. Neben der aktuellen Wertigkeit der einzelnen Server und einigen anderen für Berechnungen erforderlichen Informationen erhält der Manager vom Cisco CSS Switch die Werte für aktive und neue Verbindungen. Diese Werte basieren auf Informationen, die intern im Cisco CSS Switch generiert und gespeichert werden.

Cisco Consultant fragt die MIB (Verwaltungsinformationsdatenbank) des Cisco CSS Switch ab, um Informationen zu den aktiven und neuen Verbindungen zu erhalten, und empfängt folgendes:

- **Für aktive Verbindungen** empfängt Cisco Consultant den Wert `apSvcConnections` aus der Datenbank `svcExtMIB`. Diese Variable ist nach Dienstnamen indexiert und wird direkt aktiven Verbindungen zugeordnet, wie sie im Manager eingetragen sind. Der MIB-Eintrag "`apSvcConnections`" sieht wie folgt aus:

```
apSvcConnections OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Aktuelle Anzahl der TCP-Verbindungen für diesen Dienst"
DEFVAL { 0 }
--DEFAULT ap-display-name Service Connections
::= {apSvcEntry 20}
```

Die Objektkennung für `apSvcConnections` lautet wie folgt:

1.3.6.1.4.1.2467.1.15.2.1.20

Die Anzahl der aktiven Verbindungen hängt von der Anzahl der Clients sowie von der Zeit ab, die für die Nutzung der von den am Lastausgleich beteiligten Servermaschinen bereitgestellten Dienste erforderlich ist. Bei schnellen Client-Verbindungen (wie sie für kleine Webseiten, die mit HTTP GET bedient werden, typisch sind), ist die Anzahl der aktiven Verbindungen ziemlich klein. Wenn die Client-Verbindungen langsamer sind (z. B. bei einer Datenbankabfrage), ist die Anzahl aktiver Verbindungen größer.

- **Für neue Verbindungen** setzt Cisco Consultant die MIB-Variable "apCntsvcHits" in der Datenbank cntSvcExtMib des Cisco CSS Switch. Cisco Consultant führt für jeden Dienst die folgenden Schritte aus:
 - Berechnen der Summe aller apCntsvcHits mit diesem Dienst im Index
 - Aufzeichnen der Gesamtanzahl empfangener apCntsvcHits
 - Berechnen der Differenz.

Der Index für diese Variable sieht wie folgt aus:

```
INDEX { apCntsvcOwnName, apCntsvcCntName, apCntsvcSvcName }
```

Der MIB-Eintrag sieht wie folgt aus:

```
apCntsvcHits OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Gesamtanzahl der Abläufe, die diesem Dienst für diese content-Regel
    zugeordnet wurden"
DEFVAL { 0 }
--DEFAULT ap-display-name Hits
--DEFAULT apjam-popup-ref apCntSvcInst, Statistics
--DEFAULT apjam-chart-def cntSvcHitsChart, pie, apCntInst,
    "Hit Information Per Service:
--DEFAULT apjam-chart-item cntSvcHitsChart, getnext, apCntsvcSvcName
::= {apSvcEntry 20}
```

Die Objektkennung für apCntsvcHits lautet wie folgt:

```
1.3.6.1.4.1.2467.1.18.2.1.4
```

Wertigkeiten von Cisco Consultant

Der Cisco CSS Switch muss für den Lastausgleich mit der gewichteten Round-Robin-Methode konfiguriert werden. Informationen hierzu finden Sie im Abschnitt "Configuring Weight" der Veröffentlichung *Content Services Switch Basic Configuration Guide*.

Die Manager-Funktion legt Wertigkeiten auf der Grundlage von internen Zählern des Cisco CSS Switch und von Feedback der Advisor-Funktionen und von Metric Server fest. Falls Sie Wertigkeiten bei Ausführung des Managers manuell festlegen möchten, geben Sie den Befehl **lbcontrol server** mit der Option **fixedweight** an.

Ist keiner der Server verfügbar, sind alle Wertigkeiten gleich null. Wenn keiner der Server Anforderungen verarbeitet und alle Wertigkeiten gleich null sind, werden die Wertigkeiten auf die Hälfte der Wertigkeitsgrenze gesetzt, um für Server, die in der Lage sind, Anforderungen zu verarbeiten, eine Chancengleichheit zu gewährleisten. Das Überwachungsprogramm zeigt die Nullwertigkeiten als gültig an. An allen anderen Stellen zeigt Cisco Consultant jedoch eine Wertigkeit an, die der Hälfte der Wertigkeitsgrenze entspricht.

Wertigkeiten werden mit SNMP an den Cisco CSS Switch gesendet. Cisco Consultant setzt apSvcWeight in der Datenbank svcExt.mib. Der MIB-Eintrag apSvcWeight sieht wie folgt aus:

```
apSvcWeight OBJECT-TYPE
SYNTAX Integer32(1..10)
MAX-ACCESS read-create
STATUS current
DESCRIPTION
    "Dienstwertigkeit, die zusammen mit Messwerten für die Arbeitslast
    bei Entscheidungen bezüglich der Lastzuordnung verwendet wird.
    Anhand der Wertigkeit können Abläufe einem bestimmten Dienst
    zugeteilt werden."
DEFVAL { 1 }
--DEFAULT ap-display-name Service Weight
--DEFAULT apjam-popup-ref apServicesGroupInst, Properties, Advanced
--DEFAULT apjam-wizard-field 2, normal
::= {apSvcEntry 16}
```

Die Objektkennung für apSvcWeight lautet wie folgt:

1.3.6.1.4.1.2467.1.15.2.1.12

Wertigkeiten gelten für alle Server an einem Port. An einem bestimmten Port werden die Anfragen ausgehend von einem Vergleich der Wertigkeiten der einzelnen Server verteilt. Hat beispielsweise ein Server die Wertigkeit 10 und der andere Server die Wertigkeit 5, erhält der Server mit der Wertigkeit 10 doppelt so viele Anforderungen wie der Server mit der Wertigkeit 5.

Für die Wertigkeit, die ein Server haben kann, können Sie einen oberen Grenzwert angeben. Verwenden Sie dazu den Befehl **lbcontrol port set weightbound**. Dieser Befehl gibt die Unterschiede für die Anzahl der Anforderungen an, die jeder Server erhält. Wenn Sie die maximale Wertigkeit auf 1 setzen, können alle Server die Wertigkeit 1 haben. Zurückgestellte Server erhalten die Wertigkeit 0 und inaktive Server die Wertigkeit -1. Wenn Sie diese Zahl erhöhen, vergrößern sich die Unterschiede bei der Gewichtung von Servern. Wird die maximale Wertigkeit auf 2 gesetzt, kann ein Server doppelt so viele Anforderungen wie ein anderer Server erhalten.

Wenn ein Server offline ist...

Erkennt eine Advisor-Funktion, dass ein Server offline ist, teilt sie dies dem Manager mit. Der Manager setzt dann die Wertigkeit des Servers auf null. Ist die Wertigkeit eines Servers größer als null, wird sie an den Cisco CSS Switch gesendet. Der Server wird aktiviert. Wenn die Serverwertigkeit jedoch kleiner als null oder gleich null ist, wird der Server zurückgestellt. Zum Aktivieren und Aussetzen von Diensten wird die MIB-Variable apSvcEnable in der svcExt.mib des Cisco CSS Switch gesetzt.

Der MIB-Eintrag apSvcEnable sieht wie folgt aus:

```
apSvcEnable OBJECT-TYPE
SYNTAX  Integer
         disable(0)
         enable(1)
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "Status des Dienstes - aktiviert oder inaktiviert"
DEFVAL { disable }
--DEFAULT ap-display-name Status
--DEFAULT apjam-popup-ref apServicesGroupInst, Properties
--DEFAULT apjam-wizard-field 2, normal
::= {apSvcEntry 12}
```

Die Objektkennung für apSvcEnable lautet wie folgt:

1.3.6.1.4.1.2467.1.15.2.1.16

Kapitel 15. Betrieb und Verwaltung von Network Dispatcher

Anmerkung: Falls Sie die Dispatcher-Komponente *nicht* verwenden, ersetzen Sie beim Lesen der allgemeinen Abschnitte dieses Kapitels, die sich nicht auf eine bestimmte Komponente beziehen, "ndcontrol" und "ndserver" durch Folgendes:

- Für CBR: **cbrcontrol** und **cbrserver**
- Für Mailbox Locator: **mlcontrol** und **mlserver**
- Für Site Selector: **cbrcontrol** und **ssserver**
- Für Cisco Consultant: **lbcontrol** und **lbserver**

Dieses Kapitel erläutert die Verwendung und Verwaltung von Network Dispatcher und ist in folgende Abschnitte untergliedert:

- „Authentifizierte Fernverwaltung“
- „Protokolle von Network Dispatcher verwenden“ auf Seite 221
- „Dispatcher-Komponente verwenden“ auf Seite 223
 - „Simple Network Management Protocol mit Dispatcher verwenden“ auf Seite 225
- „Komponente Content Based Routing verwenden“ auf Seite 231
- „Mailbox Locator verwenden“ auf Seite 232
- „Site Selector verwenden“ auf Seite 233
- „Cisco Consultant verwenden“ auf Seite 233

Authentifizierte Fernverwaltung

Network Dispatcher stellt eine Option zur Verfügung, mit der die Konfigurationsprogramme auf einer anderen Maschine als der Maschine ausgeführt werden können, auf der die Network-Dispatcher-Server ausgeführt werden.

Die Kommunikation zwischen den Konfigurationsprogrammen (ndcontrol, cbrcontrol, mlcontrol, sscontrol, lbcontrol, ndwizard, cbrwizard, mlwizard, sswizard, ndadmin) wird mit Java Remote Method Invocation (RMI) durchgeführt. Der Befehl, mit dem die Verbindung zu einer Network Dispatcher-Maschine für die Fernverwaltung hergestellt wird, lautet **ndcontrol host:ferner-Host**. Stammt der RMI-Aufruf von einer anderen Maschine als der lokalen Maschine, muss eine Authentifizierung mit allgemeinem Schlüssel und privatem Schlüssel stattfinden, bevor der Konfigurationsbefehl akzeptiert wird.

Die Kommunikation zwischen den Steuerprogrammen, die auf derselben Maschine wie die Komponentenserver ausgeführt werden, wird nicht authentifiziert.

Verwenden Sie den folgenden Befehl, um öffentliche und private Schlüssel für die ferne Authentifizierung zu generieren:

ndkeys [create | delete]

Dieser Befehl muss auf derselben Maschine wie Network Dispatcher ausgeführt werden.

Bei Verwendung der Option **create** wird im Schlüsselverzeichnis des Servers (**...nd/servers/key/**) ein öffentlicher Schlüssel erstellt. Im Verwaltungsverzeichnis für Schlüssel (**...nd/admin/keys/**) der einzelnen Network-Dispatcher-Komponenten werden private Schlüssel erstellt. Der Dateiname für den privaten Schlüssel ist *Komponente-Serveradresse-RMI-Port*. Diese privaten Schlüssel müssen anschließend zu den fernen Clients transportiert und in das Verwaltungsverzeichnis für Schlüssel gestellt werden.

Auf einer Network-Dispatcher-Maschine mit der Adresse 10.0.0.25 (hostname), die für jede Komponente den Standard-RMI-Port verwendet, generiert der Befehl **ndkeys create** die folgenden Dateien:

- Öffentlicher Schlüssel: **.../nd/servers/key/authorization.key**
- Private Schlüssel:
 - **.../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**

Die Verwaltungsdateigruppe wurde auf einer anderen Maschine installiert. Die Dateien der privaten Schlüssel müssen auf der fernen Client-Maschine in das Verzeichnis **.../nd/admin/keys** gestellt werden.

Jetzt ist der ferne Client berechtigt, Network Dispatcher auf der Maschine 10.0.0.25 zu konfigurieren.

Dieselben Schlüssel müssen Sie auf allen fernen Clients verwenden, die berechtigt sein sollen, Network Dispatcher auf der Maschine 10.0.0.25 zu konfigurieren.

Würde der Befehl **ndkeys create** erneut ausgeführt, hätte dies die Generierung einer neuen Gruppe von allgemeinen/privaten Schlüsseln zur Folge. Dies

würde bedeuten, dass alle fernen Clients, die unter Verwendung der vorherigen Schlüssel die Herstellung einer Verbindung versuchen, nicht berechtigt wären. Der neue Schlüssel müsste in das korrekte Verzeichnis auf den Clients gestellt werden, die erneut berechtigt werden sollen.

Mit dem Befehl **ndkeys delete** werden die öffentlichen und privaten Schlüssel von der Servermaschine gelöscht. Werden diese Schlüssel gelöscht, sind keine fernen Clients mehr berechtigt, eine Verbindung zu den Servern herzustellen.

Für "ndkeys create" und "ndkeys delete" gibt es die Option **force**. Die Option **force** unterdrückt die Eingabeaufforderungen, die von Ihnen eine Bestätigung für das Überschreiben oder Löschen der vorhandenen Schlüssel anfordern.

Protokolle von Network Dispatcher verwenden

Network Dispatcher sendet Einträge an ein Serverprotokoll, ein Manager-Protokoll, an das Protokoll eines Messwertüberwachungsprogramms (protokollbezogene Kommunikation mit Metric-Server-Agenten) und an das Protokoll jeder von Ihnen verwendeten Advisor-Funktion.

Anmerkung: Zusätzlich können Einträge in ein Subagentenprotokoll (SNMP) gestellt werden. Dies gilt allerdings nur für die Dispatcher-Komponente.

Sie können die Protokollstufe festlegen, um den Umfang der Nachrichten zu definieren, die in das Protokoll geschrieben werden. Bei Stufe 0 werden Fehler protokolliert. Network Dispatcher protokolliert außerdem Header und Datensätze von Ereignissen, die nur einmal eintreten. (Beim Starten einer Advisor-Funktion wird beispielsweise eine Nachricht in das Manager-Protokoll geschrieben.) Bei Stufe 1 werden weitere Informationen aufgenommen. Bis Stufe 5 nimmt die Ausführlichkeit kontinuierlich zu. Bei Stufe 5 werden alle generierten Nachrichten aufgenommen, damit sie im Falle eines Fehlers für das Debugging verwendet werden können. Die Standardeinstellung für das Serverprotokoll ist 0. Für das Manager-Protokoll, das Protokoll der Advisor-Funktionen sowie das Protokoll der Subagenten ist die Standardeinstellung 1.

Zudem können Sie die maximale Größe eines Protokolls festlegen. Wenn Sie eine maximale Größe für die Protokolldatei festlegen, findet ein Dateiumbruch statt. Hat die Datei die angegebene Größe erreicht, werden alle weiteren Einträge wieder an den Anfang der Datei geschrieben und die dort befindlichen Einträge überschrieben. Sie können für die Protokollgröße keinen Wert angeben, der kleiner als der aktuelle Wert für die Protokollgröße ist. Protokolleinträge werden mit einer Zeitmarke versehen, so dass Sie erkennen können, in welcher Reihenfolge sie geschrieben wurden.

Je höher Sie die Protokollstufe setzen, desto vorsichtiger müssen Sie die Protokollgröße auswählen, da die Protokolldatei sehr schnell voll ist, wenn Sie eine Protokollierung auf einer höheren Stufe wählen. Bei Stufe 0 ist es wahrscheinlich sicher, die Standardprotokollgröße von 1 MB zu verwenden. Ab Stufe 3 sollten Sie die Größe jedoch begrenzen. Bedenken Sie aber, dass bei einem zu kleinen Wert die Protokollierung nicht mehr sinnvoll ist.

- Konfigurieren Sie die Protokollstufe oder die maximale Größe eines Serverprotokolls mit dem Befehl **ndcontrol set**.
- Für ein Manager-Protokoll können Sie die Protokollstufe oder die maximale Größe mit dem Befehl **ndcontrol manager** konfigurieren. Dieser Befehl steuert auch die Protokollstufe für das Protokoll des Messwertüberwachungsprogramms, in dem die Kommunikation mit den Metric-Server-Agenten aufgezeichnet wird.
- Für das Protokoll einer Advisor-Funktion können Sie die Protokollstufe oder die maximale Größe mit dem Befehl **ndcontrol advisor** konfigurieren.
- Konfigurieren Sie die Protokollstufe oder die maximale Größe eines Subagentenprotokolls mit dem Befehl **ndcontrol subagent**. (Der SNMP-Subagent wird nur von der Dispatcher-Komponente verwendet.)

Pfade für die Protokolldatei ändern

Die von Network Dispatcher generierten Protokolle werden standardmäßig im Unterverzeichnis logs des Installationsverzeichnisses von Network Dispatcher gespeichert. Wenn Sie diesen Pfad ändern möchten, setzen Sie die Variable *nd_logdir* im ndserver-Script entsprechend.

AIX, Linux und Solaris: Sie finden das ndserver-Script im Verzeichnis /usr/bin. In diesem Script ist die Variable *nd_logdir* auf das Standardverzeichnis gesetzt. Sie können diese Variable ändern, um Ihr Protokollverzeichnis anzugeben. Beispiel:

ND_LOGDIR=/Pfad/für/meine/Protokolle/

Windows 2000: Sie finden die ndserver-Datei im Systemverzeichnis von Windows 2000 (in der Regel c:\WINNT\SYSTEM32). In der ndserver-Datei ist die Variable *nd_logdir* auf das Standardverzeichnis gesetzt. Sie können diese Variable ändern, um Ihr Protokollverzeichnis anzugeben. Beispiel:

set ND_LOGDIR=c:\Pfad\für\meine\Protokolle

Für alle Betriebssysteme ist sicherzustellen, dass sich rechts und links vom Gleichheitszeichen keine Leerzeichen befinden und dass der Pfad mit einem Schrägstrich endet ("/" bzw. "\").

Binäres Protokollieren

Anmerkung: Die binäre Protokollierung ist für die Komponente Site Selector nicht möglich.

Für die binäre Protokollierung von Network Dispatcher wird dasselbe Verzeichnis (log) wie für die übrigen Protokolldateien verwendet. Weitere Informationen hierzu finden Sie in „Binäres Protokollieren verwenden, um Serverstatistiken zu analysieren“ auf Seite 213.

Dispatcher-Komponente verwenden

Dieser Abschnitt erläutert die Verwendung und Verwaltung der Dispatcher-Komponente.

Dispatcher starten und stoppen

- Geben Sie zum Starten des Dispatchers in einer Befehlszeile **ndserver** ein.
- Geben Sie zum Stoppen des Dispatchers in einer Befehlszeile **ndserver stop** ein.

Inaktivitätszeitlimit verwenden

Network Dispatcher betrachtet Verbindungen als veraltet, wenn sie die durch das Inaktivitätszeitlimit angegebene Zeit (Sekunden) lang inaktiv waren. Wird das Inaktivitätszeitlimit überschritten, entfernt Network Dispatcher den Eintrag für diese Verbindung aus seinen Tabellen und löscht den nachfolgenden Datenverkehr für diese Verbindung. Auf Port-Ebene können Sie das Inaktivitätszeitlimit beispielsweise mit dem Befehl **ndcontrol port set staletime-out** angeben.

Das Inaktivitätszeitlimit kann auf Executor-, Cluster- und Port-Ebene gesetzt werden. Auf Executor- und Cluster-Ebene liegt der Standardwert bei 300 Sekunden. Es wird bis hinunter zum Port gefiltert. Auf Port-Ebene ist der Standardwert vom jeweiligen Port abhängig. Einige herkömmliche Ports haben unterschiedliche Inaktivitätszeitlimits. Der Telnet-Port 23 hat beispielsweise ein Standardlimit von 32.000.000 Sekunden.

Dienste können auch eigene Inaktivitätszeitlimits haben. Für LDAP (Lightweight Directory Access Protocol) gibt es z. B. den Konfigurationsparameter `idletimeout`. Bei Überschreitung der von `idletimeout` angegebenen Zeit in Sekunden wird die Beendigung einer inaktiven Client-Verbindung erzwungen. Das Inaktivitätszeitlimit (`idletimeout`) kann auch auf 0 gesetzt werden, so dass Verbindungen nicht zwangsweise beendet werden können.

Wenn das Inaktivitätszeitlimit von Network Dispatcher kleiner als das des Dienstes ist, können Konnektivitätsprobleme auftreten. Im Falle von LDAP liegt das Inaktivitätslimit von Network Dispatcher (`staletimeout`) standardmäßig bei 300 Sekunden. Ist die Verbindung 300 Sekunden inaktiv, entfernt

Network Dispatcher den Eintrag für die Verbindung aus seinen Tabellen. Wenn das Inaktivitätszeitlimit (idletimeout) über 300 Sekunden liegt (oder auf 0 gesetzt ist), könnte der Client davon ausgehen, dass er weiterhin mit dem Server verbunden ist. Wenn der Client Pakete sendet, werden diese von Network Dispatcher gelöscht. Das hat zur Folge, dass LDAP blockiert, wenn eine Anfrage an den Server gesendet wird. Sie können dieses Problem vermeiden, indem Sie das Inaktivitätszeitlimit von LDAP (idletimeout) auf einen Wert ungleich null setzen, der genauso groß wie das Inaktivitätszeitlimit von Network Dispatcher (staletimeout) oder kleiner als dieses ist.

Über Anzahl beendeter Verbindungen die Speicherbereinigungsfunktion steuern

Ein Client sendet ein FIN-Paket, nachdem er alle Pakete gesendet hat, um dem Server mitzuteilen, dass die Transaktion beendet ist. Wenn der Dispatcher das FIN-Paket erhält, kennzeichnet er die Transaktion nicht mehr als AKTIV, sondern als BEENDET. Wenn eine Transaktion als BEENDET gekennzeichnet ist, kann der für die Verbindung reservierte Speicher von der Speicherbereinigungsfunktion, die in den Executor integriert ist, bereinigt werden.

Über die Schlüsselwörter **fintimeout** und **fincount** können Sie festlegen, wie oft der Executor eine Speicherbereinigung durchführt und wie viel Speicher bereinigt wird. Der Executor prüft regelmäßig die Liste der von ihm zugeordneten Verbindungen. Wenn die Anzahl der Verbindungen mit dem Status BEENDET größer-gleich der im Schlüsselwort **fincount** festgelegten Anzahl der beendeten Verbindungen ist, versucht der Executor, den Speicher freizugeben, der für diese Verbindungsdaten benutzt wird. Die Standardanzahl beendeter Verbindungen kann durch Eingabe des Befehls **ndcontrol executor set fincount** geändert werden.

Die Speicherbereinigungsfunktion gibt den Speicher für alle Verbindungen mit dem Status BEENDET frei, die älter sind als die im Schlüsselwort **fintimeout** als Zeitlimit für die Beendigung inaktiver Verbindungen angegebene Anzahl von Sekunden. Das Zeitlimit für die Beendigung inaktiver Verbindungen kann durch Eingabe des Befehls **ndcontrol executor set fintimeout** geändert werden.

Das Inaktivitätszeitlimit gibt die Zeit der Inaktivität einer Verbindung in Sekunden an, nach der die Verbindung entfernt wird. Weitere Informationen hierzu finden Sie im Abschnitt „Inaktivitätszeitlimit verwenden“ auf Seite 223. Die Anzahl beendeter Verbindungen hat auch Auswirkungen darauf, wie oft „lange inaktive“ Verbindungen entfernt werden. Wenn Ihre Dispatcher-Maschine keine hohe Speicherkapazität hat, sollten Sie Anzahl beendeter Verbindungen (FIN-Zähler) auf einen niedrigeren Wert setzen. Bei einer stark frequentierten Website sollten Sie den FIN-Zähler auf einen höheren Wert setzen.

Berichte der GUI — Menüoption 'Überwachen'

Ausgehend von den Informationen des Executors können mehrere Diagramme angezeigt und an den Manager übergeben werden. (Die Menüoption "Überwachen" der GUI erfordert, dass die Manager-Funktion aktiviert ist):

- Verbindungen pro Sekunde je Server (mehrere Server können in demselben Diagramm angezeigt werden)
- Relative Wertigkeiten pro Server an einem bestimmten Port
- Durchschnittliche Verbindungsdauer pro Server an einem bestimmten Port

Simple Network Management Protocol mit Dispatcher verwenden

Anmerkung: Unter Linux wird SNMP nicht von Network Dispatcher unterstützt.

Ein Netzverwaltungssystem ist ein Programm, das ständig ausgeführt und verwendet wird, um ein Netz zu überwachen, den Status eines Netzes wiederzugeben und ein Netz zu steuern. Simple Network Management Protocol (SNMP), ein häufig verwendetes Protokoll für die Kommunikation mit Einheiten in einem Netz, ist der aktuelle Netzverwaltungsstandard. Die Netzeinheiten verfügen normalerweise über einen *SNMP-Agenten* und einen oder mehrere Subagenten. Der SNMP-Agent kommuniziert mit der *Netzverwaltungsstation* oder antwortet auf SNMP-Befehlszeilenanforderungen. Der *SNMP-Subagent* ruft Daten ab und aktualisiert die Daten und übergibt diese Daten an den SNMP-Agenten, der sie an den Requester weiterleitet.

Der Dispatcher stellt eine *SNMP-Verwaltungsinformationsbasis* (ibmNetDispatcherMIB) und einen SNMP-Subagenten zur Verfügung. Damit wird Ihnen die Verwendung jedes Netzverwaltungssystems ermöglicht, wie beispielsweise Tivoli NetView, Tivoli Distributed Monitoring oder HP OpenView, um den Zustand, die Leistung und die Aktivität des Dispatchers zu überwachen. Die MIB-Daten beschreiben den Dispatcher, der verwaltet wird, und geben den aktuellen Status des Dispatchers wieder. Die MIB wird im Unterverzeichnis **..nd/admin/MIB** installiert.

Anmerkung: Die MIB *ibmNetDispatcherMIB.02* wird nicht mit dem Tivoli NetView-Programm *xnmloadmib2* geladen. Um den Fehler zu beheben, müssen Sie den Bereich NOTIFICATION-GROUP der MIB auf Kommentar setzen. Geben Sie dazu am Beginn der Zeile "indMibNotifications Group NOTIFICATION-GROUP" sowie der sechs darauf folgenden Zeilen "- -" ein.

Das Netzverwaltungssystem verwendet SNMP-Befehle GET, um MIB-Werte auf anderen Maschinen zu überprüfen. Es kann dann den Benutzer benachrichtigen, wenn angegebene Schwellenwerte überschritten werden. Sie können anschließend die Leistung des Dispatchers beeinflussen, indem Sie Konfigu-

rationsdaten für den Dispatcher so ändern, dass Dispatcher-Probleme im voraus bestimmt oder berichtigt werden, bevor sie den Ausfall des Dispatchers oder Webservers zur Folge haben.

SNMP-Befehle und -Protokoll

Das System stellt normalerweise einen SNMP-Agenten für jede Netzverwaltungsstation zur Verfügung. Der Benutzer sendet einen Befehl GET an den SNMP-Agenten. Dieser SNMP-Agent sendet dann einen Befehl GET, um die angegebenen MIB-Variablenwerte von einem Subagenten abzurufen, der für diese MIB-Variablen zuständig ist.

Der Dispatcher stellt einen Subagenten zur Verfügung, der MIB-Daten aktualisiert und abrufen. Der Subagent antwortet mit den entsprechenden MIB-Daten, wenn der SNMP-Agent einen Befehl GET sendet. Der SNMP-Agent überträgt die Daten an die Netzverwaltungsstation. Die Netzverwaltungsstation kann Sie benachrichtigen, wenn angegebene Schwellenwerte überschritten werden.

Die Dispatcher-SNMP-Unterstützung beinhaltet einen SNMP-Subagenten, der DPI-Funktionalität verwendet (DPI = Distributed Protocol Interface). DPI ist eine Schnittstelle zwischen einem SNMP-Agenten und seinen Subagenten.

SNMP unter AIX und Solaris aktivieren

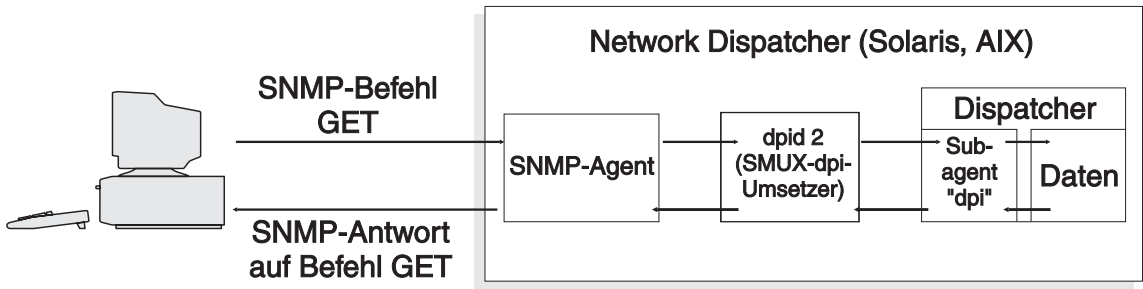


Abbildung 28. SNMP-Befehle für AIX und Solaris

AIX stellt einen SNMP-Agenten bereit, der das SNMP-Multiplexer-Protokoll (SMUX) verwendet und die zusätzliche ausführbare Datei DPID2 anbietet, die als Umsetzer zwischen DPI und SMUX fungiert.

Für Solaris müssen Sie einen SMUX-fähigen SNMP-Agenten erwerben, da dieses Betriebssystem keinen solchen bereitstellt. Network Dispatcher stellt DPID2 für Solaris im Verzeichnis /opt/nd/servers/samples/SNMP bereit.

Den DPI-Agenten müssen Sie als Benutzer "root" ausführen. Bevor Sie den DPID2-Dämon ausführen, aktualisieren Sie die Dateien /etc/snmpd.peers und /etc/snmpd.conf wie folgt:

- Fügen Sie in der Datei /etc/snmpd.peers den folgenden Eintrag für dpid hinzu:

```
"dpid2"          1.3.6.1.4.1.2.3.1.2.2.1.1.2          "dpid_password"
```
- Fügen Sie in der Datei /etc/snmpd.conf den folgenden Eintrag für dpid hinzu:

```
smux          1.3.6.1.4.1.2.3.1.2.2.1.1.2          dpid_password          #dpid
```

Aktualisieren Sie snmpd, damit die Datei /etc/snmpd.conf erneut gelesen wird:

```
refresh -s snmpd
```

Starten Sie den DPID-SMUX-Peer:

```
dpid2
```

Die Dämonen müssen in der folgenden Reihenfolge gestartet werden:

1. SNMP-Agent
2. DPI-Umsetzungsprogramm
3. Dispatcher-Subagent

SNMP unter Windows 2000 aktivieren

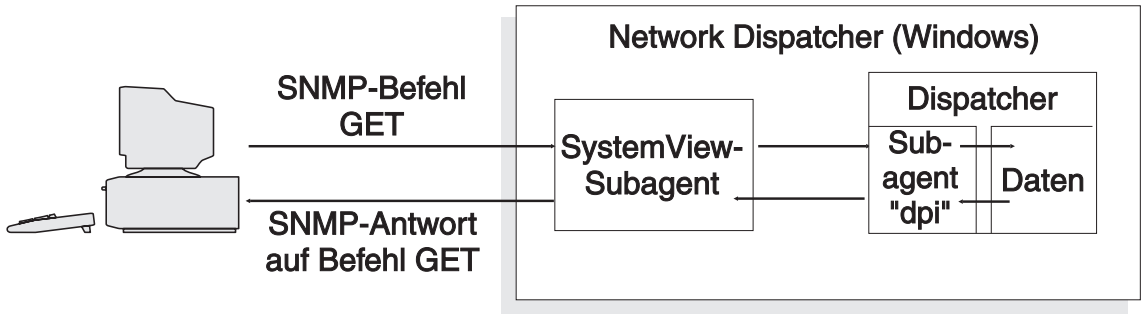


Abbildung 29. SNMP-Befehle für Windows 2000

Wenn Sie einen DPI-fähigen SNMP-Agenten für Windows 2000 benötigen, installieren Sie die Windows-NT-Version aus dem IBM SystemView Agent Toolkit von <http://www.tivoli.com/support/sva>.

Bevor Sie den SystemView-SNMPD-Prozess starten, müssen Sie die SNMP-Unterstützung von Microsoft Windows inaktivieren. Der snmp-Prozess von SystemView unterstützt DPI-Subagenten und Microsoft-kompatible Agenten.

Sie können die Windows-SNMP-Unterstützung wie folgt inaktivieren:

1. Klicken Sie auf Start -> Programme -> Verwaltung -> Dienste.

2. Klicken Sie mit der rechten Maustaste auf **SNMP** und wählen Sie **Eigenschaften** aus.
3. Ändern Sie den **Starttyp** in "Deaktiviert".

Anmerkung: Wird die SNMP-Unterstützung von Microsoft Windows nicht inaktiviert, kann der Dispatcher-SNMP-Subagent keine Verbindung zum snmpd-Agenten herstellen.

Befolgen Sie die Anweisungen im Abschnitt „Namen einer Benutzergemeinschaft für SNMP angeben“, um den SystemView-SNMP-Agenten zu konfigurieren.

Namen einer Benutzergemeinschaft für SNMP angeben

Sie sollten den Namen der SNMP-Benutzergemeinschaft konfigurieren. Der standardmäßige SNMP-Benutzergemeinschaftsname lautet `public`. Auf UNIX-Systemen wird der Name in einer Datei mit dem Namen `/etc/snmpd.conf` festgelegt.

Der Name der Benutzergemeinschaft muss auf allen Systemen konsistent konfiguriert und verwendet werden. Wenn der Name der Benutzergemeinschaft für Network Dispatcher in der Konfiguration des SNMP-Agenten auf "Unsere-Gemeinschaft" gesetzt wurde, muss er in der Konfiguration des Subagenten ebenfalls auf "UnsereGemeinschaft" gesetzt werden.

Unter Windows 2000 müssen Sie vor dem Erstellen des Namens für die Benutzergemeinschaft den IBM SystemView SNMP Agent konfigurieren.

1. Klicken Sie auf dem Desktop auf das Symbol **IBM SystemView Agent**.
2. Klicken Sie auf **snmpcfg**.
3. Fügen Sie im Dialogfenster "SNMP-Konfiguration" den Namen der Benutzergemeinschaft hinzu. Geben Sie zu Testzwecken **public** als Namen der Benutzergemeinschaft ein.

Dieser Schritt ermöglicht es jedem Host in jedem Netz, auf die SNMP-MIB-Variablen zuzugreifen. Wenn Sie überprüft haben, dass diese Werte funktionieren, können Sie sie entsprechend Ihren Anforderungen ändern.

4. Überprüfen Sie, ob in der Datei `\sva\dm\bin\svastart.bat` die Option **-dpi** angegeben ist.
5. Starten Sie den SNMP-Dämon mit der Datei `svastart.bat` im Unterverzeichnis `\sva\dm\bin`.

Verwenden Sie bei aktivem Executor den Befehl **ndcontrol subagent start [Name_der_Benutzergemeinschaft]**, um den Namen der Benutzergemeinschaft zu definieren, der zwischen dem DPI-Subagenten des Dispatchers und dem SNMP-Agenten verwendet wird. Standardmäßig lautet der Name der Benutzergemeinschaft `public`. Wenn Sie diesen Wert ändern, müssen Sie auch den

neuen Namen der Benutzergemeinschaft zum SystemView-Agenten hinzufügen. Verwenden Sie dazu wie oben angegeben "snmpcfg".

Nachrichten

Die Kommunikation von SNMP erfolgt über das Senden und Empfangen von *Nachrichten*, die von verwalteten Einheiten gesendet werden, um Ausnahmesituationen oder das Auftreten besonderer Ereignisse, wie beispielsweise das Erreichen eines Schwellenwerts, zu melden.

Der Subagent verwendet die folgenden Alarmnachrichten:

- indHighAvailStatus
- indSrvrGoneDown
- indDOSAttack
- indDOSAttackDone

Die Nachricht **indHighAvailStatus** gibt an, dass sich der Wert der Statusvariablen (hasState) des Hochverfügbarkeitsstatus geändert hat. Die gültigen Werte von hasState sind:

-Ruhend

Diese Maschine führt einen Lastausgleich durch und versucht nicht, Kontakt mit der Dispatcher-Partnermaschine aufzunehmen.

-Empfangsbereit

Die Funktion für hohe Verfügbarkeit wurde gerade gestartet und der Dispatcher ist für die Partnermaschine empfangsbereit.

-Aktiv Diese Maschine führt einen Lastausgleich durch.

-Bereitschaft

Diese Maschine überwacht die aktive Maschine.

-Vorwegnehmen

Diese Maschine befindet sich während des Wechsels von primärer Maschine zu Partnermaschine in einem Übergangszustand.

-Auswählen

Der Dispatcher wählt aus, welche die primäre Maschine und welche die Partnermaschine ist.

-Executor nicht aktiv

Der Executor ist nicht aktiv.

Die Alarmnachricht **indSrvrGoneDown** gibt an, dass die Wertigkeit des vom Abschnitt csAddr, psNum, ssAddr der Objektkennung angegebenen Servers gleich null ist. Die letzte bekannte Anzahl aktiver Verbindungen für den Server wird in der Nachricht gesendet. Diese Alarmnachricht gibt an, dass der angegebene Server inaktiviert ist, soweit Dispatcher dies feststellen konnte.

Die Alarmnachricht **indDOSAttack** gibt an, dass der Wert für "numhalfopen" (die Anzahl halboffener Verbindungen, die nur SYN-Pakete enthalten) an dem vom Abschnitt csAddr psNum der Objektkennung angegebenen Port den Schwellenwert "maxhalfopen" überschritten hat. Die Anzahl der für den Port konfigurierten Server wird in der Alarmnachricht gesendet. Diese Alarmnachricht zeigt an, dass bei Network Dispatcher möglicherweise eine DoS-Attacke aufgetreten ist.

Die Alarmnachricht **indDOSAttackDone** gibt an, dass der Wert für "numhalfopen" (die Anzahl halboffener Verbindungen, die nur SYN-Pakete enthalten) an dem vom Abschnitt csAddr psNum der Objektkennung angegebenen Port unter den Schwellenwert "maxhalfopen" gefallen ist. Die Anzahl der für den Port konfigurierten Server wird in der Alarmnachricht gesendet. Wenn Network Dispatcher nach dem Senden einer indDOSAttack-Alarmnachricht feststellt, dass die mögliche DoS-Attacke vorüber ist, wird diese Alarmnachricht gesendet.

Aufgrund einer Einschränkung in der SMUX-API kann es sich bei der Unternehmenskennung, die in Nachrichten von dem ibmNetDispatcher-Subagenten gemeldet wird, um die Unternehmenskennung von dpid2 und nicht um die Unternehmenskennung von ibmNetDispatcher, 1.3.6.1.4.1.2.6.144, handeln. Die SNMP-Verwaltungsdienstprogramme können jedoch die Quelle der Nachricht bestimmen, da die Daten eine Objektkennung aus der ibmNetDispatcher-MIB enthalten.

SNMP-Unterstützung über den Befehl ndcontrol aktivieren und inaktivieren

Mit dem Befehl **ndcontrol subagent start** wird die SNMP-Unterstützung aktiviert. Mit dem Befehl **ndcontrol subagent stop** wird die SNMP-Unterstützung inaktiviert.

Weitere Informationen über den Befehl ndcontrol befinden sich unter „ndcontrol subagent — SNMP-Subagenten konfigurieren“ auf Seite 329.

Gesamten Datenverkehr zur Sicherheit der Network-Dispatcher-Maschine mit ipchains oder iptables zurückweise (unter Linux)

In den Linux-Kernel ist das Firewall-Tool ipchains integriert. Wenn Network Dispatcher und ipchains gleichzeitig ausgeführt werden, sieht Network Dispatcher die Pakete zuerst. Erst danach werden sie von ipchains gesehen. Deshalb kann ipchains verwendet werden, um die Sicherheit einer Linux-Maschine mit Network Dispatcher zu erhöhen. Bei einer solchen Maschine könnte es sich beispielsweise um einen Rechner mit Network Dispatcher handeln, der einen Lastausgleich für Firewalls durchführt.

Wenn ipchains oder iptables für eine vollständige Einschränkung konfiguriert ist (so dass kein ein- oder ausgehender Datenverkehr zulässig ist), arbeitet die Paketweiterleitungsfunktion von Network Dispatcher normal weiter.

ipchains und iptables *können nicht* zum Filtern von eingehendem Datenverkehr verwendet werden, für den noch kein Lastausgleich durchgeführt wurde.

Ein gewisses Maß an Datenverkehr muss erlaubt sein, da Network Dispatcher sonst nicht fehlerfrei arbeiten kann. Nachfolgend sind einige Beispiele für eine solche Kommunikation aufgelistet:

- Die Advisor-Funktionen auf der Maschine mit Network Dispatcher und auf den Back-End-Servern kommunizieren miteinander.
- Network Dispatcher sendet ping-Aufrufe an Back-End-Server, reach-Ziele und Network-Dispatcher-Partnermaschinen für hohe Verfügbarkeit.
- Die Benutzerschnittstellen (grafische Benutzerschnittstelle, Befehlszeile und Assistenten) verwenden RMI.
- Die Back-End-Server müssen auf die ping-Aufrufe der Network-Dispatcher-Maschine reagieren.

Eine angemessene ipchains-Strategie für die Network-Dispatcher-Maschinen wäre, den gesamten Datenverkehr mit Ausnahme des Verkehrs von oder zu den Back-End-Servern, den Partnermaschinen für hohe Verfügbarkeit, allen reach-Zielen oder Konfigurations-Hosts zu unterbinden.

Komponente Content Based Routing verwenden

Dieser Abschnitt erläutert die Verwendung und Verwaltung der CBR-Komponente von Network Dispatcher.

CBR starten und stoppen

- Geben Sie zum Starten von CBR in einer Befehlszeile **cbrserver** ein.
- Geben Sie zum Stoppen von CBR in einer Befehlszeile **cbrserver stop** ein.

CBR und Caching Proxy kooperieren über die API des Caching-Proxy-Plug-In bei der Bearbeitung von HTTP- und HTTPS-Anfragen (SSL). CBR kann erst mit dem Lastausgleich für die Server beginnen, wenn Caching Proxy auf derselben Maschine ausgeführt wird. Konfigurieren Sie CBR und Caching Proxy wie im Abschnitt „CBR-Konfigurationsbeispiel“ auf Seite 100 beschrieben.

CBR steuern

Nachdem Sie CBR gestartet haben, können Sie die Komponente mit einer der folgenden Methoden steuern:

- Konfigurieren Sie CBR mit dem Befehl **cbrcontrol**. Die vollständige Syntax dieses Befehls ist „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265 beschrieben. Einige Verwendungsbeispiele sind an dieser Stelle aufgeführt.
- Konfigurieren Sie CBR auf der grafischen Benutzerschnittstelle (GUI). Geben Sie in der Befehlszeile **ndadmin** ein, um die GUI zu öffnen. Weitere Informationen zum Konfigurieren von CBR auf der GUI finden Sie im Abschnitt „GUI“ auf Seite 90.

CBR-Protokolle verwenden

Die von CBR verwendeten Protokolle ähneln den Protokollen, die im Dispatcher verwendet werden. Weitere Informationen hierzu finden Sie im Abschnitt „Protokolle von Network Dispatcher verwenden“ auf Seite 221.

Anmerkung:

In früheren Releases konnten Sie den Protokollverzeichnispfad für CBR in der Caching-Proxy-Konfigurationsdatei ändern. Jetzt können Sie den Verzeichnispfad, in dem das Protokoll gespeichert wird, in der cbrserver-Datei ändern. Lesen Sie hierzu die Informationen im Abschnitt „Pfade für die Protokolldatei ändern“ auf Seite 222.

Mailbox Locator verwenden

Mailbox Locator starten und stoppen

- Geben Sie zum Starten von Mailbox Locator in einer Befehlszeile **mlserver** ein.
- Geben Sie zum Stoppen von Mailbox Locator in einer Befehlszeile **mlserver stop** ein.

Mailbox Locator steuern

Nachdem Sie Mailbox Locator gestartet haben, können Sie die Komponente mit einer der folgenden Methoden steuern:

- Konfigurieren Sie Mailbox Locator mit dem Befehl **mlcontrol**. Die vollständige Syntax dieses Befehls ist „Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator“ auf Seite 265 beschrieben. Einige Verwendungsbeispiele sind an dieser Stelle aufgeführt.
- Konfigurieren Sie Mailbox Locator auf der grafischen Benutzerschnittstelle (GUI). Geben Sie in der Befehlszeile **ndadmin** ein, um die GUI zu öffnen. Weitere Informationen zum Konfigurieren von Mailbox Locator auf der GUI finden Sie im Abschnitt „GUI“ auf Seite 107.

Protokolle von Mailbox Locator verwenden

Die von Mailbox Locator verwendeten Protokolle ähneln den Protokollen des Dispatchers. Weitere Informationen befinden sich unter „Protokolle von Network Dispatcher verwenden“ auf Seite 221.

Site Selector verwenden

Site Selector starten und stoppen

- Geben Sie zum Starten von Site Selector in einer Befehlszeile **sssserver** ein.
- Geben Sie zum Stoppen von Site Selector in einer Befehlszeile **sssserver stop** ein.

Site Selector steuern

Nachdem Sie Site Selector gestartet haben, können Sie die Komponente mit einer der folgenden Methoden steuern:

- Konfigurieren Sie Site Selector mit dem Befehl **sscontrol**. Die vollständige Syntax dieses Befehls ist in „Anhang D. Befehlsreferenz für Site Selector“ auf Seite 335 beschrieben. Einige Verwendungsbeispiele sind an dieser Stelle aufgeführt.
- Konfigurieren Sie Site Selector auf der grafischen Benutzerschnittstelle (GUI). Geben Sie in der Befehlszeile **ndadmin** ein, um die GUI zu öffnen. Weitere Informationen zum Konfigurieren von Site Selector auf der GUI finden Sie im Abschnitt „GUI“ auf Seite 121.

Protokolle von Site Selector verwenden

Die von Site Selector verwendeten Protokolle ähneln den Protokollen des Dispatchers. Weitere Informationen befinden sich unter „Protokolle von Network Dispatcher verwenden“ auf Seite 221.

Cisco Consultant verwenden

Cisco Consultant starten und stoppen

1. Geben Sie zum Starten von Cisco Consultant in einer Befehlszeile **lbcserver** ein.
2. Geben Sie zum Stoppen von Cisco Consultant in einer Befehlszeile **lbcserver stop** ein.

Cisco Consultant steuern

Nachdem Sie Cisco Consultant gestartet haben, können Sie die Komponente mit einer der folgenden Methoden steuern:

- Konfigurieren Sie Cisco Consultant mit dem Befehl **lbccontrol**. Die vollständige Syntax dieses Befehls ist in „Anhang E. Befehlsreferenz für Consultant für Cisco CSS Switches“ auf Seite 363 beschrieben. Einige Verwendungsbeispiele sind an dieser Stelle aufgeführt.
- Konfigurieren Sie Cisco Consultant auf der grafischen Benutzerschnittstelle (GUI). Geben Sie in der Befehlszeile **ndadmin** ein, um die GUI zu öffnen. Weitere Informationen zum Konfigurieren von Cisco Consultant auf der GUI finden Sie im Abschnitt „GUI“ auf Seite 121.

Protokolle von Cisco Consultant verwenden

Die von Cisco Consultant verwendeten Protokolle ähneln den Protokollen des Dispatchers. Weitere Informationen befinden sich unter „Protokolle von Network Dispatcher verwenden“ auf Seite 221.

Metric Server verwenden

Metric Server starten und stoppen

Metric Server stellt Informationen zur Serverauslastung für Network Dispatcher bereit. Metric Server befindet sich auf jedem Server, der in den Lastausgleich einbezogen ist.

- Geben Sie auf jeder Maschine mit Metric Server in einer Befehlszeile **metric-server start** ein, um Metric Server zu starten.
- Geben Sie auf jeder Maschine mit Metric Server in einer Befehlszeile **metric-server stop** ein, um Metric Server zu stoppen.

Protokolle von Metric Server verwenden

Ändern Sie die Protokollstufe im Start-Script für Metric Server. Sie können eine Protokollstufe von 0 bis 5 angeben. Die Stufen sind denen für die Network-Dispatcher-Protokolle vergleichbar. Daraufhin wird im Verzeichnis **...ms/logs** ein Agentenprotokoll erstellt.

Kapitel 16. Fehlerbehebung

Anhand der Informationen in diesem Kapitel können Fehler erkannt und behoben werden, die sich auf Network Dispatcher beziehen. Suchen Sie nach dem Fehler, den Sie erkannt haben, in „Fehlerbehebungstabellen“.

Fehlerbehebungstabellen

Die nachfolgenden Tabellen sind zur Fehlerbehebung für Dispatcher, CBR, Mailbox Locator, Site Selector und Consultant für Cisco CSS Switches bestimmt.

Tabelle 14. Tabelle zur Fehlerbehebung für Dispatcher

Fehler	Mögliche Ursache	Siehe...
Dispatcher wird nicht korrekt ausgeführt	In Konflikt stehende Port-Nummern	„Port-Nummern für Dispatcher überprüfen“ auf Seite 242
Ein auf der Dispatcher-Maschine konfigurierter Server antwortet nicht auf Lastausgleichsanforderungen	Falsche oder sich widersprechende Adresse	„Problem: Dispatcher und Server antworten nicht“ auf Seite 245
Kein Service für Verbindungen von Client-Maschinen oder Zeitlimitüberschreitung bei Verbindungen	<ul style="list-style-type: none">• Falsche Konfiguration für Weiterleitung• Kein Aliasname auf NIC für die Cluster-Adresse• Für den Server wurde die Cluster-Adresse nicht als Aliasname der Loopback-Einheit festgelegt• Zusätzliche Route nicht gelöscht• Port nicht für jeden Cluster definiert• Server sind inaktiv oder haben die Wertigkeit null	„Problem: Dispatcher-Anforderungen werden nicht verteilt“ auf Seite 246
Client-Maschinen erhalten keinen Service oder überschreiten das Zeitlimit	Funktion für hohe Verfügbarkeit arbeitet nicht	„Problem: Die Dispatcher-Funktion für hohe Verfügbarkeit arbeitet nicht“ auf Seite 246

Tabelle 14. Tabelle zur Fehlerbehebung für Dispatcher (Forts.)

Fehler	Mögliche Ursache	Siehe...
Es kann kein Überwachungssignal hinzugefügt werden (Windows 2000)	Die Quellenadresse ist auf keinem Adapter konfiguriert	„Problem: Es kann kein Überwachungssignal hinzugefügt werden (Windows 2000)“ auf Seite 246
Server verarbeitet keine Anforderungen (Windows)	Es wurde eine zusätzliche Route in der Route-Tabelle erstellt.	„Problem: Zusätzliche Routes (Windows 2000)“ auf Seite 247
Advisor arbeiten nicht korrekt mit der Weitverkehrsunterstützung	Advisor werden auf fernen Maschinen nicht ausgeführt	„Problem: Advisor arbeiten nicht korrekt“ auf Seite 247
SNMPD kann nicht gestartet oder weiter ausgeführt werden (Windows 2000).	Der in den SNMP-Befehlen übergebene Name der Benutzergemeinschaft stimmt nicht mit dem Namen der Benutzergemeinschaft überein, der zum Starten des Subagenten verwendet wurde.	„Problem: SNMPD wird nicht korrekt ausgeführt (Windows 2000)“ auf Seite 247
Dispatcher, Microsoft IIS und SSL arbeiten nicht oder setzen die Arbeit nicht fort	Protokollübergreifend können keine verschlüsselten Daten gesendet werden.	„Problem: Dispatcher, Microsoft IIS und SSL funktionieren nicht (Windows 2000)“ auf Seite 247
Verbindung zur fernen Maschine zurückgewiesen	Es wird noch eine ältere Version der Schlüssel verwendet.	„Problem: Dispatcher-Verbindung zu einer fernen Maschine“ auf Seite 247
Der Befehl ndcontrol oder ndadmin schlägt mit der Nachricht ‘Server antwortet nicht’ oder ‘Zugriff auf RMI-Server nicht möglich’ fehl	<ol style="list-style-type: none"> 1. Befehle können nicht ausgeführt werden, weil der Stack SOCKSifiziert ist oder ndserver nicht gestartet wurde. 2. Die RMI-Ports sind nicht richtig definiert. 	„Problem: Befehl ndcontrol oder ndadmin schlägt fehl“ auf Seite 248
Wenn Netscape als Standardbrowser zum Anzeigen der Onlinehilfe verwendet wird, erscheint die Fehlernachricht “Datei ... nicht gefunden” (Windows 2000).	Falsche Einstellung für die HTML-Dateizuordnung	„Problem: Fehlernachricht “Datei nicht gefunden...” beim Anzeigen der Onlinehilfe (Windows 2000)“ auf Seite 248

Tabelle 14. Tabelle zur Fehlerbehebung für Dispatcher (Forts.)

Fehler	Mögliche Ursache	Siehe...
Beim Starten von ndserver unter Solaris 2.7 erscheint die Fehlernachricht "stty: : No such device or address".	Diese Fehlernachricht können Sie ignorieren. Es liegt kein Fehler vor. "ndserver" wird ordnungsgemäß ausgeführt.	„Problem: Irrelevante Fehlernachricht beim Starten von ndserver unter Solaris 2.7“ auf Seite 249
Die grafische Benutzerschnittstelle wird nicht richtig gestartet.	Unzureichender Paging-Bereich.	„Problem: Die grafische Benutzerschnittstelle (GUI) wird nicht richtig gestartet“ auf Seite 249
Fehler bei der Ausführung von Dispatcher mit installiertem Caching Proxy	Caching-Proxy-Datei-abhängigkeit	„Problem: Fehler bei der Ausführung von Dispatcher mit installiertem Caching Proxy“ auf Seite 249
Die grafische Benutzerschnittstelle wird nicht richtig angezeigt.	Die Auflösung ist nicht korrekt.	„Problem: Die grafische Benutzerschnittstelle (GUI) wird nicht richtig angezeigt“ auf Seite 250
Die Hilfetextanzeigen werden manchmal von anderen Fenstern verdeckt.	Java-Einschränkung	„Problem: Unter 2000 sind die Hilfefenster manchmal von anderen offenen Fenstern verdeckt“ auf Seite 250
Network Dispatcher kann Rahmen nicht verarbeiten und weiterleiten.	Für jede NIC ist eine eindeutige MAC-Adresse erforderlich.	„Problem: Network Dispatcher kann Rahmen nicht verarbeiten und weiterleiten“ auf Seite 250
Die Anzeige ist blau.	Es ist keine Netzwerkkarte installiert/konfiguriert.	„Problem: Beim Starten des Executors von Network Dispatcher erscheint eine blaue Anzeige“ auf Seite 250
Automatische Pfaderkennung verhindert Datenrückfluss	Die Loopback-Adresse wird als Aliasname für den Cluster verwendet.	„Problem: Automatische Pfaderkennung verhindert Datenrückfluss mit Network Dispatcher“ auf Seite 251
Die Advisor-Funktionen zeigen alle Server als inaktiv an.	Die TCP-Kontrollsumme wurde falsch berechnet.	„Problem: Die Advisor-Funktionen zeigen alle Server als inaktiv an“ auf Seite 252

Tabelle 14. Tabelle zur Fehlerbehebung für Dispatcher (Forts.)

Fehler	Mögliche Ursache	Siehe...
Keine hohe Verfügbarkeit im Weitverkehrsmodus von Network Dispatcher	Der ferne Dispatcher muss auf dem lokalen Dispatcher als Server eines Clusters definiert werden.	„Problem: Keine hohe Verfügbarkeit im Weitverkehrsmodus von Network Dispatcher“ auf Seite 252
Die GUI Blockiert oder verhält sich nicht erwartungsgemäß, wenn versucht wird, eine große Konfigurationsdatei zu laden.	Java kann nicht auf so viel Speicher zugreifen, wie für die Bearbeitung einer so großen Änderung der GUI erforderlich ist.	„Problem: Beim Laden einer großen Konfigurationsdatei blockiert die GUI oder verhält sich nicht erwartungsgemäß“ auf Seite 253

Tabelle 15. Tabelle zur Fehlerbehebung für CBR

Fehler	Mögliche Ursache	Siehe...
CBR wird nicht korrekt ausgeführt	In Konflikt stehende Port-Nummern	„Port-Nummern für CBR überprüfen“ auf Seite 243
Der Befehl cbrcontrol oder ndadmin scheitert mit der Nachricht ‘Server antwortet nicht’ oder ‘Zugriff auf RMI-Server nicht möglich’.	Befehle können nicht ausgeführt werden, weil der Stack SOCKSifiziert ist oder cbrserver nicht gestartet wurde.	„Problem: Der Befehl cbrcontrol oder ndadmin scheitert“ auf Seite 254
Die Last von Anforderungen wird nicht verteilt.	Caching Proxy wurde vor dem Executor gestartet.	„Problem: Anforderungen werden nicht verteilt“ auf Seite 254
Unter Solaris scheitert der Befehl "cbrcontrol executor start" mit der Nachricht ‘Fehler: Executor wurde nicht gestartet’.	Unter Umständen müssen die IPC-Standardwerte geändert werden, um den Befehl ordnungsgemäß ausführen zu können.	„Problem: Unter Solaris scheitert der Befehl cbrcontrol executor start“ auf Seite 255
URL-Regel arbeitet nicht	Syntax- oder Konfigurationsfehler	„Problem: Syntax- oder Konfigurationsfehler“ auf Seite 255

Tabelle 16. Tabelle zur Fehlerbehebung für Mailbox Locator

Fehler	Mögliche Ursache	Siehe...
Mailbox Locator wird nicht korrekt ausgeführt	In Konflikt stehende Port-Nummern	„Port-Nummern für Mailbox Locator überprüfen“ auf Seite 243
Der Befehl "mlserver" gibt die Ausnahmebedingung "java.rmi.RMI Security Exception: security.fd.read" zurück.	Die Systembegrenzung für Dateideskriptoren ist für die Anzahl der Anforderungen, die "mlserver" zu bedienen versucht, zu klein.	„Problem: Der Befehl mlserver wird gestoppt“ auf Seite 255
Der Befehl "mlcontrol" oder "ndadmin" scheitert mit der Nachricht 'Server antwortet nicht' oder 'Zugriff auf RMI-Server nicht möglich'.	Befehle können nicht ausgeführt werden, weil der Stack SOCKSifiziert ist oder "mlserver" nicht gestartet wurde.	„Problem: Der Befehl mlcontrol oder ndadmin scheitert“ auf Seite 256
Ein Port kann nicht hinzugefügt werden.	An diesem Port ist bereits eine andere Anwendung empfangsbereit.	„Problem: Ein Port kann nicht hinzugefügt werden“ auf Seite 256
Bei dem Versuch, einen Port hinzuzufügen, wird ein Weiterleitungsfehler empfangen.	Die Cluster-Adresse wurde nicht vor dem Start des Proxy auf einer NIC konfiguriert, oder an diesem Port wird eine andere Anwendung ausgeführt.	„Problem: Empfang eines Proxy-Fehlers beim Hinzufügen eines Ports“ auf Seite 256

Tabelle 17. Tabelle zur Fehlerbehebung für Site Selector

Fehler	Mögliche Ursache	Siehe...
Site Selector wird nicht korrekt ausgeführt	Konflikt verursachende Port-Nummer	„Port-Nummern für Site Selector überprüfen“ auf Seite 244
Site Selector gewichtet vom Solaris-Client eingehende Anforderungen nicht nach der RoundRobin-Methode.	Solaris-Systeme führen einen Namensservice-Cache-Dämon aus.	„Problem: Site Selector verteilt den Datenverkehr von Solaris-Clients nicht nach der RoundRobin-Methode“ auf Seite 257
Der Befehl "sscontrol" oder "ndadmin" scheitert mit der Nachricht 'Server antwortet nicht' oder 'Zugriff auf RMI-Server nicht möglich'.	Befehle können nicht ausgeführt werden, weil der Stack SOCKSifiziert ist oder "ssserver" nicht gestartet wurde.	„Problem: Der Befehl sscontrol oder ndadmin scheitert“ auf Seite 257

Tabelle 17. Tabelle zur Fehlerbehebung für Site Selector (Forts.)

Fehler	Mögliche Ursache	Siehe...
"ssserver" kann unter Windows 2000 nicht gestartet werden.	Unter Windows muss der Host-Name nicht im DNS enthalten sein.	„Problem: sserver wird unter Windows 2000 nicht gestartet“ auf Seite 257
Für eine Maschine mit duplizierten Routes wird der Lastausgleich nicht richtig durchgeführt. Die Namensauflösung scheint nicht zu funktionieren.	Eine Site-Selector-Maschine enthält mehrere Adapter, die mit demselben Teilnetz verbunden sind.	„Problem: Site Selector führt bei duplizierten Routes den Lastausgleich nicht korrekt durch“ auf Seite 258

Tabelle 18. Tabelle zur Fehlerbehebung für Consultant für Cisco CSS Switches

Fehler	Mögliche Ursache	Siehe...
"lbcserver" wird nicht gestartet.	In Konflikt stehende Port-Nummern	„Port-Nummern für Cisco Consultant überprüfen“ auf Seite 245
Der Befehl "lbcontrol" oder "ndadmin" scheitert mit der Nachricht 'Server antwortet nicht' oder 'Zugriff auf RMI-Server nicht möglich'.	Befehle können nicht ausgeführt werden, weil der Stack SOCKSifiziert ist oder "lbcserver" nicht gestartet wurde.	„Problem: Der Befehl lbcontrol oder ndadmin scheitert“ auf Seite 258
Empfangener Fehler: Für Port 14099 kann kein Eintrag in der Registrierungsdatenbank erstellt werden.	Abgelaufene Produktlizenz	„Problem: Für Port 14099 kann kein Eintrag in der Registrierungsdatenbank erstellt werden“ auf Seite 259

Tabelle 19. Tabelle zur Fehlerbehebung für Metric Server

Fehler	Mögliche Ursache	Siehe...
IOException für Metric Server unter Windows 2000 bei Ausführung von benutzerdefinierten Messwertdateien mit der Erweiterung .bat oder .cmd	Es ist ein vollständiger Messwertname erforderlich.	„Problem: IOException für Metric Server unter Windows 2000 bei Ausführung von benutzerdefinierten Messwertdateien mit der Erweiterung .bat oder .cmd“ auf Seite 259
Metric Server meldet die Lastinformationen nicht an die Network-Dispatcher-Maschine	Mögliche Ursachen sind unter anderem: <ul style="list-style-type: none"> • Auf der Metric-Server-Maschine gibt es keine Schlüsselringe. • Der Host-Name der Metric-Server-Maschine ist nicht im lokalen Namensserver registriert. 	„Problem: Metric Server meldet die Last nicht an die Network-Dispatcher-Maschine“ auf Seite 259
Beim Übertragen von Schlüsselringen zum Server enthält das Metric-Server-Protokoll den Eintrag "Für den Zugriff auf den Agenten ist eine Kennung erforderlich".	Der Schlüsselring ist beschädigt und kann deshalb nicht autorisiert werden.	„Problem: Metric-Server-Protokoll meldet, dass für den Zugriff auf den Agenten eine Kennung erforderlich ist“ auf Seite 260

Port-Nummern für Dispatcher überprüfen

Falls beim Ausführen des Dispatchers Probleme auftreten, verwendet unter Umständen eine Ihrer Anwendungen eine Port-Nummer, die normalerweise vom Dispatcher benutzt wird. Der Dispatcher-Server benutzt die folgenden Port-Nummern.

- 10099 zum Empfangen der Befehle von ndcontrol
- 10004 zum Senden von Messwertabfragen an Metric Server
- 10005 zum Empfangen von Informationen von einem SDA-Agenten

Wenn eine andere Anwendung eine der Dispatcher-Port-Nummern benutzt, können Sie die Port-Nummer für Dispatcher wie folgt ändern:

- Den zum Empfang von Befehlen verwendeten Port können Sie wie folgt ändern:
 - Setzen Sie die Variable ND_RMIPORT am Anfang der Datei "ndserver" auf den Port, an dem Dispatcher Befehle empfangen soll.
- Den zum Empfang der Messwerte von Metric Server verwendeten Port können Sie wie folgt ändern:
 - Setzen Sie die Variable RMI_PORT in der Datei "metricserver" auf den Port, über den Dispatcher mit Metric Server kommunizieren soll.
 - Geben Sie beim Starten des Managers das Argument metric_port an. Eine Beschreibung der Befehlssyntax für **ndcontrol manager start** finden Sie im Abschnitt „ndcontrol manager — Manager steuern“ auf Seite 296.
- Wenn Sie den zum Empfang von SDA-Informationen verwendeten Port ändern möchten, setzen Sie die Variable ND_AFFINITY_PORT in der Datei "ndserver" auf den Port, an dem der Dispatcher SDA-Informationen empfangen soll.

Anmerkung: Unter Windows 2000 befinden sich die Dateien "ndserver" und "metricserver" im Verzeichnis c:\winnt\system32. Auf anderen Plattformen sind diese Dateien im Verzeichnis /usr/bin/ enthalten.

Port-Nummern für CBR überprüfen

Wenn beim Ausführen von CBR Fehler auftreten, verwendet unter Umständen eine Ihrer Anwendungen eine Port-Nummer, die normalerweise von CBR benutzt wird. CBR benutzt die folgenden Port-Nummern:

- 11099 zum Empfangen der Befehle von cbrcontrol
- 10004 zum Senden von Messwertabfragen an Metric Server

Wenn eine andere Anwendung eine der CBR-Port-Nummern verwendet, können Sie die CBR-Port-Nummern wie folgt ändern:

- Den zum Empfang von Befehlen verwendeten Port können Sie wie folgt ändern:
 - Setzen Sie die Variable ND_RMIPORT am Anfang der Datei "cbrserver" auf den Port, an dem CBR Befehle empfangen soll.
- Den zum Empfang der Messwerte von Metric Server verwendeten Port können Sie wie folgt ändern:
 - Setzen Sie die Variable RMI_PORT in der Datei "metricserver" auf den Port, über den CBR mit Metric Server kommunizieren soll.
 - Geben Sie beim Starten des Managers das Argument metric_port an. Eine Beschreibung der Befehlssyntax für **manager start** finden Sie im Abschnitt „ndcontrol manager — Manager steuern“ auf Seite 296.

Anmerkung: Unter Windows 2000 befinden sich die Dateien "cbrserver" und "metricserver" im Verzeichnis c:\winnt\system32. Auf anderen Plattformen sind diese Dateien im Verzeichnis /usr/bin/ enthalten.

Port-Nummern für Mailbox Locator überprüfen

Wenn bei Ausführung von Mailbox Locator Fehler auftreten, verwendet unter Umständen eine Ihrer Anwendungen eine Port-Nummer, die normalerweise von Mailbox Locator benutzt wird. Mailbox Locator benutzt die folgenden Port-Nummern:

- 13099 zum Empfangen der Befehle von mlcontrol
- 10004 zum Senden von Messwertabfragen an Metric Server

Wenn eine andere Anwendung eine der Port-Nummern für Mailbox Locator verwendet, können Sie die Port-Nummern für Mailbox Locator wie folgt ändern:

- Den zum Empfang von Befehlen verwendeten Port können Sie wie folgt ändern:
 - Setzen Sie die Variable ND_RMIPORT am Anfang der Datei "mlserver" auf den Port, an dem Mailbox Locator Befehle empfangen soll.

- Den zum Empfang der Messwerte von Metric Server verwendeten Port können Sie wie folgt ändern:
 - Setzen Sie die Variable `RMI_PORT` in der Datei `"metricserver"` auf den Port, über den Mailbox Locator mit Metric Server kommunizieren soll.
 - Geben Sie beim Starten des Managers das Argument `metric_port` an. Eine Beschreibung der Befehlssyntax für **manager start** finden Sie im Abschnitt „ndcontrol manager — Manager steuern“ auf Seite 296.

Anmerkung: Unter Windows 2000 befinden sich die Dateien `"mlserver"` und `"metricserver"` im Verzeichnis `c:\winnt\system32`. Auf anderen Plattformen sind diese Dateien im Verzeichnis `/usr/bin` enthalten.

Port-Nummern für Site Selector überprüfen

Wenn bei Ausführung der Komponente Site Selector Fehler auftreten, verwendet unter Umständen eine Ihrer Anwendungen eine Port-Nummer, die normalerweise von Site Selector benutzt wird. Site Selector benutzt die folgenden Port-Nummern:

- 12099 zum Empfangen der Befehle von `sscontrol`
- 10004 zum Senden von Messwertabfragen an Metric Server

Wenn eine andere Anwendung eine der Port-Nummern für Site Selector verwendet, können Sie die Port-Nummern für Site Selector wie folgt ändern:

- Den zum Empfang von Befehlen verwendeten Port können Sie wie folgt ändern:
 - Setzen Sie die Variable `ND_RMIPORT` am Anfang der Datei `"ssserver"` auf den Port, an dem Site Selector Befehle empfangen soll.
- Den zum Empfang der Messwerte von Metric Server verwendeten Port können Sie wie folgt ändern:
 - Setzen Sie die Variable `RMI_PORT` in der Datei `"metricserver"` auf den Port, über den Site Selector mit Metric Server kommunizieren soll.
 - Geben Sie beim Starten des Managers das Argument `metric_port` an. Eine Beschreibung der Befehlssyntax für **manager start** finden Sie im Abschnitt „sscontrol manager — Manager steuern“ auf Seite 344.

Anmerkung: Unter Windows 2000 befinden sich die Dateien `"ssserver"` und `"metricserver"` im Verzeichnis `c:\winnt\system32`. Auf anderen Plattformen sind diese Dateien im Verzeichnis `/usr/bin/` enthalten.

Port-Nummern für Cisco Consultant überprüfen

Wenn bei Ausführung von Cisco Consultant Fehler auftreten, verwendet unter Umständen eine andere Anwendung eine Port-Nummer, die normalerweise vom lserver der Komponente Cisco Consultant benutzt wird. Cisco Consultant benutzt die folgenden Port-Nummern:

14099 zum Empfang der Befehle von lbcontrol

10004 zum Senden von Messwertabfragen an Metric Server

Wenn eine andere Anwendung eine der Port-Nummern für Consultant verwendet, können Sie die Port-Nummern für Consultant wie folgt ändern:

- Zum Ändern des für den Empfang der Befehle von lbcontrol verwendeten Ports müssen Sie die Variable ND_RMIPORT in der Datei "lbserver" ändern. Ersetzen Sie den Wert 14099 durch die Nummer des Ports, an dem Consultant lbcontrol-Befehle empfangen soll.
- Den zum Empfang der Messwerte von Metric Server verwendeten Port können Sie wie folgt ändern:
 1. Ändern Sie die Variable RMI_PORT in der Datei "metricserver". Ersetzen Sie den Wert 10004 durch die Nummer des Ports, über den Consultant mit Metric Server kommunizieren soll.
 2. Geben Sie beim Starten des Managers das Argument metric_port an. Eine Beschreibung der Befehlssyntax für "lbcontrol manager start" finden Sie im Abschnitt „lbcontrol manager — Manager steuern“ auf Seite 378.

Anmerkung: Unter Windows 2000 befinden sich die Dateien "lbserver" und "metricserver" im Verzeichnis c:\winnt\system32. Auf anderen Plattformen sind diese Dateien im Verzeichnis /usr/bin enthalten.

Allgemeine Probleme lösen — Dispatcher

Problem: Dispatcher wird nicht ausgeführt

Dieses Problem kann auftreten, wenn eine andere Anwendung einen der Ports benutzt, die normalerweise vom Dispatcher verwendet werden. Weitere Informationen enthält „Port-Nummern für Dispatcher überprüfen“ auf Seite 242.

Problem: Dispatcher und Server antworten nicht

Dieses Problem tritt auf, wenn eine andere Adresse als die angegebene Adresse verwendet wird. Stellen Sie bei Verknüpfung von Dispatcher und Server sicher, dass die in der Konfiguration verwendete Serveradresse die NFA ist oder als verknüpft konfiguriert ist.

Problem: Dispatcher-Anforderungen werden nicht verteilt

Bei diesem Problem erfolgt beispielsweise kein Service für Verbindungen von Client-Maschinen, oder es treten Zeitsperren für Verbindungen auf. Überprüfen Sie folgendes, um den Fehler zu bestimmen:

1. Haben Sie die NFA, Cluster, Ports und Server für die Weiterleitung konfiguriert? Überprüfen Sie die Konfigurationsdatei.
2. Wurde auf der Netzschnittstellenkarte ein Aliasname für die Cluster-Adresse erstellt? Überprüfen Sie dies mit `netstat -ni`.
3. Ist auf jedem Server der Aliasname für die Loopback-Einheit auf die Cluster-Adresse gesetzt? Überprüfen Sie dies mit `netstat -ni`.
4. Wurde die zusätzliche Route gelöscht? Überprüfen Sie dies mit dem Befehl `netstat -nr`.
5. Benutzen Sie den Befehl **ndcontrol cluster status**, um die Informationen für die einzelnen definierten Cluster zu überprüfen. Vergewissern Sie sich, dass Sie für jeden Cluster einen Port definiert haben.
6. Stellen Sie mit dem Befehl **ndcontrol server report::** sicher, dass Ihre Server nicht inaktiv sind und nicht die Wertigkeit null haben.

Problem: Die Dispatcher-Funktion für hohe Verfügbarkeit arbeitet nicht

Dieses Problem tritt auf, wenn eine Dispatcher-Umgebung mit hoher Verfügbarkeit konfiguriert ist und bei Verbindungen der Client-Maschinen kein Service erfolgt oder Zeitlimits abgelaufen sind. Überprüfen Sie folgendes, um den Fehler zu korrigieren oder zu bestimmen:

- Überprüfen Sie, ob Sie die Scripts `goActive`, `goStandby` und `goInOp` erstellt haben, und stellen Sie sie in das Unterverzeichnis `bin` des Installationsverzeichnis von Dispatcher. Weitere Informationen zu diesen Scripts finden Sie im Abschnitt „Scripts verwenden“ auf Seite 182.
- Vergewissern Sie sich unter **AIX**, **Linux** und **Solaris**, dass in den Scripts `goActive`, `goStandby` und `goInOp` die Option `execute permission` gesetzt ist.
- Unter **Windows 2000** müssen Sie die NFA konfigurieren.

Problem: Es kann kein Überwachungssignal hinzugefügt werden (Windows 2000)

Dieser Fehler tritt unter Windows 2000 auf, wenn die Quellenadresse nicht auf einem Adapter konfiguriert wurde. Überprüfen Sie folgendes, um den Fehler zu korrigieren oder zu bestimmen:

- Unter **Windows 2000** müssen Sie die NFA mit der Token-Ring- oder Ethernet-Schnittstelle konfigurieren und einen der folgenden Befehle absetzen:

```
ndconfig  
tr0 <IP-Adresse> netmask <Netzmaske> oder ndcontrol  
cluster configure
```


Problem: Zusätzliche Routes (Windows 2000)

Nach dem Konfigurieren von Servermaschinen stellen Sie unter Umständen fest, dass Sie unbeabsichtigt eine oder mehrere zusätzliche Routes erstellt haben. Werden diese zusätzlichen Routes nicht entfernt, kann der Dispatcher nicht ordnungsgemäß arbeiten. Informationen zum Feststellen und Löschen zusätzlicher Routes finden Sie im Abschnitt „Servermaschinen für Lastausgleich konfigurieren“ auf Seite 71.

Problem: Advisor arbeiten nicht korrekt

Wird die Weitverkehrsunterstützung verwendet und scheinen die Advisor nicht korrekt zu arbeiten, müssen Sie sicherstellen, dass sie sowohl auf den lokalen als auch auf den fernen Dispatchern gestartet wurden. Lesen Sie hierzu die Informationen im Abschnitt „Ferne Advisor mit der Weitverkehrsunterstützung verwenden“ auf Seite 170.

Problem: SNMPD wird nicht korrekt ausgeführt (Windows 2000)

Wird bei Verwendung von SNMP-Subagenten der DNMP-Dämon von System-View Agent nicht gestartet oder nicht weiter ausgeführt, vergewissern Sie sich, dass die SNMP-Benutzergemeinschaft mit dem Programm `snmpcfg` konfiguriert wurde. Für den Zugriff auf SNMP-Daten von dem Dispatcher-Subagenten muss der in den SNMP-Befehlen übergebene Benutzergemeinschaftsname mit dem Benutzergemeinschaftsnamen übereinstimmen, mit dem der Subagent gestartet wurde.

Problem: Dispatcher, Microsoft IIS und SSL funktionieren nicht (Windows 2000)

Werden Dispatcher, Microsoft IIS und SSL verwendet und arbeiten diese nicht zusammen, kann dies auf ein Problem mit der Aktivierung der SSL-Sicherheit zurückzuführen sein. Weitere Informationen dazu, wie Sie ein Schlüsselpaar generieren, ein Zertifikat erhalten und ein Verzeichnis so konfigurieren, dass es SSL erfordert, finden Sie in der zu Windows 2000 gelieferten Veröffentlichung *Microsoft Information and Peer Web Services Information and Planning Guide*. Der lokale URL des Dokuments, das in einem Webbrowser angezeigt werden kann, lautet

`file:///C:/WINNT/system32/inetsrv/iisadmin/htmldocs/inetdocs.htm`.

Problem: Dispatcher-Verbindung zu einer fernen Maschine

Der Dispatcher verwendet Schlüssel, die es Ihnen ermöglichen, eine Verbindung zu einer fernen Maschine herzustellen und die Maschine zu konfigurieren. Die Schlüssel geben einen RMI-Port für die Verbindung an. Sie können den RMI-Port aus Sicherheitsgründen oder bei Konflikten ändern. Wird der RMI-Port geändert, ändert sich auch der Dateiname des Schlüssels. Wenn Ihr Schlüsselverzeichnis für eine ferne Maschine mehrere Schlüssel enthält, die verschiedene RMI-Ports angeben, verwendet die Befehlszeile nur den ersten gefundenen Schlüssel. Ist dies der falsche Schlüssel, wird die Verbindung zurückgewiesen. Die Verbindung wird erst hergestellt, wenn der falsche Schlüssel gelöscht wurde.

Problem: Befehl ndcontrol oder ndadmin schlägt fehl

1. Der Befehl ndcontrol gibt die Meldung **Fehler: Server antwortet nicht** zurück. Oder der Befehl ndadmin gibt die Meldung **Fehler: Zugriff auf RMI-Server nicht möglich** zurück. Diese Fehler können auftreten, wenn der Stack Ihrer Maschine SOCKSifiziert ist. Um dieses Problem zu beheben, editieren Sie die Datei socks.cnf, damit sie die folgenden Zeilen enthält:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

2. Die Verwaltungskonsolen für Network-Dispatcher-Schnittstellen (Befehlszeile, grafische Benutzerschnittstelle und Assistenten) kommunizieren per RMI (Remote Method Invocation) mit ndserver. Für die Standardkommunikation werden zwei Ports verwendet. Einer dieser Ports ist im Start-Script für ndserver enthalten und der andere ist wahlfrei.

Der wahlfreie Port kann Fehler verursachen, wenn eine der Verwaltungskonsolen auf derselben Maschine als Firewall oder über eine Firewall ausgeführt wird. Wird beispielsweise Network Dispatcher auf derselben Maschine als Firewall ausgeführt, können beim Absetzen von ndcontrol-Befehlen Fehler wie der folgende angezeigt werden: **Fehler: Server antwortet nicht**.

Sie können diesen Fehler vermeiden, indem Sie die (im PATH enthaltene) Script-Datei ndserver editieren und den von RMI verwendeten wahlfreien Port festlegen. Nehmen Sie `-DND_RMI_SERVER_PORT=Port` in die Zeichenfolge `END_ACCESS` auf. *Port* steht hier für den von Ihnen anzugebenden Port.

Beispiel:

```
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
```

Starten Sie anschließend erneut ndserver und öffnen Sie den Datenverkehr für die Ports 10099 und 10100 oder für den Port, den Sie für die Host-Adresse, von der die Verwaltungskonsole ausgeführt wird, ausgewählt haben.

3. Derartige Fehler können auch auftreten, wenn Sie **ndserver** noch nicht gestartet haben.

Problem: Fehlermeldung "Datei nicht gefunden..." beim Anzeigen der Onlinehilfe (Windows 2000)

Wenn Sie unter Windows 2000 Netscape als Standardbrowser verwenden, wird bei diesem Fehler die Nachricht "Netscape kann die Datei

'<Dateiname>.html' (oder eine ihrer Komponenten nicht finden. Stellen Sie sicher, dass Pfad- und Dateiname stimmen und alle erforderlichen Bibliotheken verfügbar sind".

Das Problem beruht auf einer falschen Einstellung für die HTML-Dateizuordnung. Das Problem kann wie folgt gelöst werden:

1. Klicken Sie auf **Arbeitsplatz**, klicken Sie auf **Werkzeuge**, wählen Sie **Ordneroptionen** aus und klicken Sie auf die Registerkarte **Dateitypen**
2. Wählen Sie "Netscape Hypertext-Dokument" aus
3. Klicken Sie auf den Knopf **Erweitert**, wählen Sie **open** aus und klicken Sie auf den Knopf **Bearbeiten**
4. Geben Sie *NSShell* in das Feld **Anwendung**: ein (nicht in das Feld Anwendung für diesen Vorgang:) und klicken Sie auf **OK**

Problem: Irrelevante Fehlernachricht beim Starten von ndserver unter Solaris 2.7

Beim Starten von ndserver auf Plattformen mit Solaris 2.7 wird fälschlicherweise die folgende Fehlernachricht angezeigt: "stty: : No such device or address". Diese Fehlernachricht können Sie ignorieren. "ndserver" wird ordnungsgemäß ausgeführt.

Problem: Die grafische Benutzerschnittstelle (GUI) wird nicht richtig gestartet

Die grafische Benutzerschnittstelle ndadmin erfordert für eine einwandfreie Funktion einen ausreichenden Paging-Bereich. Wenn der Paging-Bereich nicht reicht, wird die GUI möglicherweise nicht vollständig gestartet. Überprüfen Sie in einem solchen Fall den Paging-Bereich und erhöhen Sie ihn gegebenenfalls.

Problem: Fehler bei der Ausführung von Dispatcher mit installiertem Caching Proxy

Wenn Sie Network Dispatcher deinstallieren, um eine andere Version zu installieren, und bei dem Versuch, die Dispatcher-Komponente zu starten, eine Fehlernachricht empfangen, überprüfen Sie, ob Caching Proxy installiert ist. Caching Proxy ist von einer der Dispatcher-Dateien abhängig. Diese Datei wird nur bei der Deinstallation von Caching Proxy deinstalliert.

Sie können dieses Problem wie folgt vermeiden:

1. Deinstallieren Sie Caching Proxy.
2. Deinstallieren Sie Network Dispatcher.
3. Installieren Sie Network Dispatcher und Caching Proxy erneut.

Problem: Die grafische Benutzerschnittstelle (GUI) wird nicht richtig angezeigt

Falls die GUI von Network Dispatcher nicht richtig angezeigt wird, überprüfen Sie die Auflösung für den Desktop des Betriebssystems. Die GUI wird am besten bei einer Auflösung von 1024 x 768 Bildpunkten angezeigt.

Problem: Unter 2000 sind die Hilfefenster manchmal von anderen offenen Fenstern verdeckt

Wenn Sie unter Windows 2000 zum ersten Mal Hilfefenster öffnen, werden diese manchmal hinter vorhandene Fenster gestellt. Klicken Sie in diesem Fall auf das Fenster, um es wieder in den Vordergrund zu stellen.

Problem: Network Dispatcher kann Rahmen nicht verarbeiten und weiterleiten

Unter Solaris haben alle Netzwerkadapter standardmäßig dieselbe MAC-Adresse. Wenn sich jeder Adapter in einem anderen IP-Teilnetz befindet, verursacht dies keine Probleme. In einer Switch-Umgebung, in der mehrere NICs mit derselben MAC-Adresse und derselben IP-Teilnetzadresse mit einem Switch kommunizieren, sendet der Switch den gesamten für die eine MAC-Adresse (und beide IP-Adressen) bestimmten Datenverkehr über eine Leitung. Nur der Adapter, der als letzter einen Rahmen über die Leitung gesendet hat, sieht die für beide Adapter bestimmten IP-Pakete. Solaris löscht unter Umständen Pakete für eine gültige IP-Adresse, die an der "falschen" Schnittstelle ankommen.

Wenn in `ibmnd.conf` nicht alle Netzschnittstellen für Network Dispatcher konfiguriert sind und die nicht in `ibmnd.conf` definierte NIC einen Rahmen empfängt, kann Network Dispatcher den Rahmen nicht verarbeiten und weiterleiten.

Sie können dieses Problem vermeiden, indem Sie die Standardeinstellung überschreiben und für jede Schnittstelle eine eindeutige MAC-Adresse definieren. Verwenden Sie den dafür den folgenden Befehl:

```
ifconfig Schnittstelle ether  
MAC-Adresse
```

Beispiel:

```
ifconfig hme0 ether 01:02:03:04:05:06
```

Problem: Beim Starten des Executors von Network Dispatcher erscheint eine blaue Anzeige

Unter Windows 2000 müssen Sie vor dem Starten des Executors eine Netzwerkkarte installiert und konfiguriert haben.

Problem: Automatische Pfaderkennung verhindert Datenrückfluss mit Network Dispatcher

Das Betriebssystem AIX enthält einen Netzparameter für die automatische Erkennung der MTU, die auf einem Pfad transportiert werden kann. Stellt das Betriebssystem während einer Transaktion mit einem Client fest, dass es für ausgehende Pakete eine kleinere MTU (größte zu übertragende Einheit) verwenden muss, veranlasst die automatische Erkennung der MTU für einen Pfad AIX, eine Route zu erstellen, um sich diese Daten merken zu können. Die neue Route ist für diese spezielle Client-IP-Adresse bestimmt und zeichnet die für das Erreichen der Adresse erforderliche MTU auf.

Nachdem die Route erstellt wurde, könnte auf den Servern ein Problem auftreten, weil die Loopback-Einheit als Alias für den Cluster verwendet wird. Wenn die Gateway-Adresse für die Route in das Teilnetz des Clusters / der Netzmaske fällt, erstellt AIX die Route zur Loopback-Adresse. Der Grund hierfür ist, dass dies die letzte Schnittstelle (Alias) war, über die dieses Teilnetz erreicht wurde.

Wenn der Cluster beispielsweise 9.37.54.69 ist, die Netzmaske 255.255.255.0 lautet und das angestrebte Gateway 9.37.54.1 ist, verwendet AIX die Loopback-Adresse für die Route. Dadurch können die Antworten des Servers die Maschine nicht verlassen und der Client wartet bis zur Überschreitung des Zeitlimits. Normalerweise sieht der Client eine Antwort vom Cluster. Danach wird die Route erstellt und der Client empfängt keine weiteren Antworten.

Für dieses Problem gibt es zwei mögliche Lösungen.

1. Inaktivieren Sie die automatische Erkennung der MTU für einen Pfad, so dass AIX nicht dynamisch Routes hinzufügt. Verwenden Sie dazu die folgenden Befehle:

no -a Listet die AIX-Einstellungen für den Netzbetrieb auf.

no -o option=value

Legt die TCP-Parameter für AIX fest.

2. Geben Sie den Aliasnamen für die Cluster-IP-Adresse auf der Loopback-Adresse mit der Netzmaske 255.255.255.255 an. Dies bedeutet, dass das über den Alias erreichbare Teilnetz nur die Cluster-IP-Adresse ist. Wenn AIX die dynamischen Routes erstellt, stimmt die IP-Adresse des Ziel-Gateways nicht mit diesem Teilnetz überein, weshalb eine Route erstellt wird, die die korrekte Netzschnittstelle verwendet. Löschen Sie anschließend die neue lo0-Route, die während der Aliasnamensumsetzung erstellt wurde. Suchen Sie dazu die Route zur Loopback-Adresse, deren Netzziel die Cluster-IP-Adresse ist, und löschen Sie sie. Dieser Schritt muss immer ausgeführt werden, wenn für den Cluster ein Aliasname erstellt wird.

Anmerkungen:

1. Bis AIX 4.3.2 ist die automatische Erkennung der MTU für einen Pfad standardmäßig inaktiviert. Ab AIX Version 4.3.3 ist sie jedoch standardmäßig aktiviert.
2. Die folgenden Befehle schalten die automatische Erkennung der MTU für einen Pfad aus und müssen bei jedem Booten des Systems ausgeführt werden. Fügen Sie diese Befehle zur Datei `/etc/rc.net` hinzu.
 - `-o udp_pmtu_discover=0`
 - `-o tcp_pmtu_discover=0`

Problem: Die Advisor-Funktionen zeigen alle Server als inaktiv an

Windows 2000 stellt eine neue Funktion mit der Bezeichnung Task Offload bereit. Bei Anwendung dieser Funktion wird die TCP-Kontrollsumme nicht vom Betriebssystem, sondern von der Adapterkarte berechnet. Dies verbessert den Durchsatz des Systems. Bei aktiviertem Task Offload melden die Advisor-Funktionen von Network Dispatcher, dass Server inaktiv sind, obwohl sie tatsächlich aktiv sind.

Das Problem besteht darin, dass die TCP-Kontrollsumme für Pakete, die von der Cluster-Adresse kommen (was für den Advisor-Datenverkehr zutrifft) nicht richtig berechnet wird.

Sie können dieses Problem vermeiden, indem Sie die Einstellungen für die Adapterkarte aufrufen und Task Offload inaktivieren.

Erstmalig wurde dieses Problem beim ANA62044 QuadPort Adapter von Adaptec beobachtet. Bei dieser Adapterkarte hat die Funktion die Bezeichnung Transmit Checksum Offload. Umgehen Sie das Problem durch Inaktivieren von Transmit Checksum Offload.

Problem: Keine hohe Verfügbarkeit im Weitverkehrsmodus von Network Dispatcher

Wenn Sie einen WAN-Dispatcher konfigurieren, müssen Sie den fernen Dispatcher auf Ihrem lokalen Dispatcher als Server in einem Cluster definieren. In der Regel werden Sie die NFA des fernen Dispatchers als Zieladresse des fernen Servers verwenden. Wenn Sie anschließend die Funktion für hohe Verfügbarkeit auf dem fernen Dispatcher konfigurieren, kann diese nicht ausgeführt werden. Der Grund hierfür ist, dass der lokale Dispatcher immer auf die primäre Maschine des fernen Standorts zeigt, wenn Sie für den Zugriff auf den fernen Server die NFA verwenden.

Sie können dieses Problem wie folgt umgehen:

1. Definieren Sie auf dem fernen Dispatcher einen zusätzlichen Cluster. Für diesen Cluster müssen Sie keine Ports oder Server definieren.
2. Fügen Sie diese Cluster-Adresse zu Ihren Scripts `goActive` und `goStandby` hinzu.
3. Definieren Sie diesen Cluster auf Ihrem lokalen Dispatcher als Server und nicht als NFA des fernen primären Dispatchers.

Wenn der ferne primäre Dispatcher aktiviert wird, richtet er auf seinem Adapter einen Aliasnamen für diese Adresse ein, so dass die Adresse Datenverkehr akzeptieren kann. Tritt ein Fehler auf, wird die Adresse auf die Ausweichmaschine versetzt. Der weitere Datenverkehr für diese Adresse wird dann von der Ausweichmaschine akzeptiert.

Problem: Beim Laden einer großen Konfigurationsdatei blockiert die GUI oder verhält sich nicht erwartungsgemäß

Wenn Sie versuchen, eine große Konfigurationsdatei (im Schnitt mit mehr als 200 `add`-Befehlen) zu laden, kann die GUI blockieren oder ein unerwartetes Verhalten zeigen. Ein solches Verhalten wäre beispielsweise ein extrem langsames Reagieren auf Anzeigeänderungen.

Dieses Problem tritt auf, weil Java nicht auf so viel Speicher zugreifen kann, wie für die Bearbeitung einer so großen Änderung der GUI erforderlich ist. Die Laufzeitumgebung bietet eine Option an, mit der der Java zur Verfügung stehende Speicherzuordnungspool vergrößert werden kann.

Die Option ist `-Xmxn`, bei der `n` die maximale Größe des Speicherzuordnungspools in Bytes angibt. Der Wert `n` muss ein Vielfaches von 1024 und größer als 2 MB sein. Nach dem Wert `n` können Sie `k` bzw. `K` für Kilobytes oder `m` bzw. `M` für Megabytes angeben. Zwei Beispiele für gültige Angaben sind `-Xmx128M` und `-Xmx81920k`. Der Standardwert ist 64 MB. Für SPARC-Plattformen mit Solaris 7 und Solaris 8 gilt ein Maximalwert von 4000m. Bei Plattformen mit Solaris 2.6 und x86 gilt ein Maximalwert von 2000m.

Fügen Sie diese Option hinzu, indem Sie wie folgt die Script-Datei `ndadmin` ändern:

- **Windows NT oder 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 &
```

Für n wird kein bestimmter Wert empfohlen. Er sollte jedoch über dem Standardwert für die Option liegen. Ein guter Ausgangswert wäre das Zweifache des Standardwertes.

Allgemeine Probleme lösen — CBR

Problem: CBR wird nicht ausgeführt

Dieses Problem kann auftreten, wenn eine andere Anwendung einen der Ports benutzt, die von CBR verwendet werden. Weitere Informationen enthält „Port-Nummern für CBR überprüfen“ auf Seite 243.

Problem: Der Befehl cbrcontrol oder ndadmin scheitert

Der Befehl cbrcontrol gibt die Nachricht „Fehler: Server antwortet nicht“ zurück, oder der Befehl ndadmin gibt die Nachricht „Fehler: Zugriff auf RMI-Server nicht möglich“ zurück. Diese Fehler können auftreten, wenn der Stack Ihrer Maschine SOCKSifiziert ist. Um dieses Problem zu beheben, editieren Sie die Datei socks.cnf, damit sie die folgenden Zeilen enthält:

```
EXCLUDE-MODULE java  
EXCLUDE-MODULE jre  
EXCLUDE-MODULE jrew  
EXCLUDE-MODULE javaw
```

Derartige Fehler können auch auftreten, wenn Sie **cbrserver** noch nicht gestartet haben.

Problem: Anforderungen werden nicht verteilt

Anforderungen werden nicht verteilt, obwohl Caching Proxy und CBR gestartet wurden. Dieser Fehler kann auftreten, wenn Sie Caching Proxy vor dem Executor starten. Ist dies der Fall, enthält das Protokoll stderr für Caching Proxy die Fehlernachricht „ndServerInit: Keine Verbindung zum Executor möglich“. Vermeiden Sie dieses Problem, indem Sie den Executor vor Caching Proxy starten.

Problem: Unter Solaris scheitert der Befehl **cbrcontrol executor start**

Unter Solaris gibt der Befehl **cbrcontrol executor start** die Nachricht : "Fehler: Executor wurde nicht gestartet" zurück. Dieser Fehler tritt auf, wenn Sie die prozessübergreifende Kommunikation (IPC, Inter-process Communication) für das System nicht so konfigurieren, dass die maximale Größe eines gemeinsam benutzten Speichersegments und die Anzahl der gemeinsam benutzten Semaphore-IDs über dem Standardwert des Betriebssystems liegen. Wenn Sie das gemeinsam benutzte Speichersegment vergrößern und die Anzahl der gemeinsam benutzten Semaphore-IDs erhöhen möchten, müssen Sie die Datei **/etc/system** editieren. Weitere Informationen zum Konfigurieren dieser Datei finden Sie auf Seite 93.

Problem: Syntax- oder Konfigurationsfehler

Wenn der URL nicht funktioniert, kann dies an einem Syntax- oder Konfigurationsfehler liegen. Überprüfen Sie bei diesem Problem folgendes:

- Stellen Sie sicher, dass die Regel korrekt konfiguriert ist. „Anhang C. Syntax der content-Regel“ auf Seite 331, enthält ausführliche Informationen.
- Geben Sie einen Befehl **cbrcontrol rule report** für diese Regel aus und überprüfen Sie, ob die Spalte 'Anzahl Ausführungen' entsprechend der Anzahl der Anforderungen erhöht wurde. Wurde der Wert korrekt erhöht, überprüfen Sie erneut die Serverkonfiguration.
- Wird die Regel nicht ausgeführt, fügen Sie eine Regel 'Immer wahr' hinzu. Geben Sie einen Befehl **cbrcontrol rule report** für die Regel 'Immer wahr' aus, um zu prüfen, ob sie ausgeführt wird.

Allgemeine Probleme lösen—Mailbox Locator

Problem: Mailbox Locator wird nicht ausgeführt

Dieser Fehler kann auftreten, wenn eine andere Anwendung einen der von Mailbox Locator verwendeten Ports benutzt. Weitere Informationen enthält „Port-Nummern für Mailbox Locator überprüfen“ auf Seite 243.

Problem: Der Befehl **mlserver** wird gestoppt

Auf einer UNIX-Plattform tritt dieser Fehler auf, **mlserver** zur die Verteilung einer großen Anzahl von IMAP/POP3-Client-Anforderungen verwendet wird und der Systemgrenzwert für Dateideskriptoren für die Anzahl der Anforderungen, die **mlserver** zu bedienen versucht, zu niedrig ist. Der **mlserver** erzeugt die folgende Ausnahmebedingung und wird dann gestoppt:

```
java.rmi.RMISecurityException: security.fd.read
```

Die protokollspezifische Proxy-Protokolldatei meldet folgendes:

```
SocketException=java.net.SocketException: Socket geschlossen
```

Lösen Sie dieses Problem, indem Sie den Grenzwert **nofiles** (AIX, Linux) oder **open files** in der Shell ändern, in der **mlserver** gestartet wird. Erhöhen Sie den Grenzwert für **nofiles** auf eine angemessene Zahl, die größer als der aktuelle Grenzwert für **nofiles** ist. Mit **ulimit -a** können Sie die aktuelle Begrenzung für **nofiles** anzeigen und mit **ulimit -n Werte** den Wert erhöhen.

Problem: Der Befehl `mlcontrol` oder `ndadmin` scheitert

Der Befehl **mlcontrol** gibt die Nachricht "Fehler: Server antwortet nicht" zurück, oder der Befehl **ndadmin** gibt die Nachricht "Fehler: Zugriff auf RMI-Server nicht möglich" zurück. Diese Fehler können auftreten, wenn der Stack Ihrer Maschine SOCKSifiziert ist. Um dieses Problem zu beheben, editieren Sie die Datei **socks.cnf**, damit sie die folgenden Zeilen enthält:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Derartige Fehler können auch auftreten, wenn Sie **mlserver** noch nicht gestartet haben.

Problem: Ein Port kann nicht hinzugefügt werden

Wenn Sie versuchen, einen Port zu einer Konfiguration hinzuzufügen, empfangen Sie unter Umständen die Nachricht **Fehler: Port kann nicht hinzugefügt werden**. Es ist möglich, dass bereits eine andere Anwendung an diesem Port empfangsbereit ist. Mailbox Locator versucht einen Proxy zu starten, der an die Cluster-IP-Adresse des im Befehl angegebenen Ports gebunden wird. Ist schon eine andere Anwendung an diese IP-Adresse gebunden oder für alle IP-Adressen dieses Ports empfangsbereit, kann der Proxy nicht gestartet werden. Wenn Sie Mailbox Locator an diesem Port verwenden möchten, müssen Sie die den Konflikt verursachende Anwendung stoppen.

Auf der Linux-Plattform kann der Dämon **xinetd** eine Listener-Funktion starten, ohne beispielsweise ein POP3-Programm auszuführen. Es ist deshalb wichtig, dass Sie mit **netstat -a** überprüfen, ob am gewünschten Port eine Anwendung empfangsbereit ist.

Problem: Empfang eines Proxy-Fehlers beim Hinzufügen eines Ports

Für Mailbox Locator generiert der Befehl **mlcontrol port add** die Fehlermeldung "Der Proxy in Cluster <Cluster>, port <Port> wurde nicht gestartet". Das Problem kann gelöst werden, indem die Cluster-Adresse auf einer NIC konfiguriert wird, bevor der Proxy gestartet wird. Vergewissern Sie sich außerdem, dass an diesem Port keine andere Anwendung ausgeführt wird, die für die Cluster-Adresse empfangsbereit ist (dazu gehören auch alle generell empfangsbereiten Anwendungen).

Allgemeine Fehler beheben — Site Selector

Problem: Site Selector wird nicht ausgeführt

Dieser Fehler kann auftreten, wenn eine andere Anwendung einen der von Site Selector verwendeten Ports benutzt. Weitere Informationen enthält „Port-Nummern für Site Selector überprüfen“ auf Seite 244.

Problem: Site Selector verteilt den Datenverkehr von Solaris-Clients nicht nach der RoundRobin-Methode

Symptom: Site Selector gewichtet von Solaris-Clients eingehende Anforderungen nicht nach der RoundRobin-Methode.

Mögliche Ursache: Solaris-Systeme führen einen Namensservice-Cache-Dämon aus. Wenn dieser Dämon aktiv ist, wird die nächste Anfrage aus diesem Cache beantwortet, ohne dass Site Selector abgefragt wird.

Lösung: Schalten Sie den Namensserver-Cache-Dämon auf der Solaris-Maschine aus.

Problem: Der Befehl sscontrol oder ndadmin scheitert

Der Befehl `sscontrol` gibt die Nachricht "Fehler: Server antwortet nicht" zurück, oder der Befehl `ndadmin` gibt die Nachricht "Fehler: Zugriff auf RMI-Server nicht möglich" zurück. Diese Fehler können auftreten, wenn der Stack Ihrer Maschine SOCKSifiziert ist. Um dieses Problem zu beheben, editieren Sie die Datei `socks.cnf`, damit sie die folgenden Zeilen enthält:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Derartige Fehler können auch auftreten, wenn Sie `ssserver` noch nicht gestartet haben.

Problem: ssserver wird unter Windows 2000 nicht gestartet

Site Selector muss an einem DNS teilnehmen können. Alle zur Konfiguration gehörenden Maschinen sollten ebenfalls an diesem System teilnehmen. Unter Windows muss nicht immer der konfigurierte Host-Name im DNS enthalten sein. Site Selector wird nur ordnungsgemäß gestartet, wenn der Host-Name der Komponente im DNS definiert ist.

Prüfen Sie, ob dieser Host im DNS definiert ist. Editieren Sie die Datei `ssserver.cmd` und löschen Sie das "w" des Eintrags "javaw". Auf diese Weise erhalten Sie weitere Fehlernachrichten.

Problem: Site Selector führt bei duplizierten Routes den Lastausgleich nicht korrekt durch

Der Namensserver von Site Selector wird an keine Adresse der Maschine gebunden. Er beantwortet alle Anfragen, die an gültige IP-Adressen auf der Maschine gerichtet sind. Site Selector verlässt sich darauf, dass das Betriebssystem die Antwort an den Client zurückgibt. Wenn die Site-Selector-Maschine mehrere Adapter enthält und eine beliebige Anzahl dieser Adapter mit demselben Teilnetz verbunden sind, sendet das Betriebssystem die Antwort an den Client unter Umständen von einer Adresse, die sich von der Adresse unterscheidet, an die der Client seine Anfrage gesendet hat. Einige Client-Anwendungen akzeptieren keine Antworten, die sie von einer Adresse empfangen, die sich von der Adresse unterscheidet, an die sie die Anfrage gesendet haben. Das erweckt den Anschein, als würde die Namensauflösung nicht funktionieren.

Allgemeine Probleme lösen—Consultant für Cisco CSS Switches

Problem: Ibcserver wird nicht gestartet

Dieser Fehler kann auftreten, wenn eine andere Anwendung einen Port verwendet, der vom Ibcserver des Consultant verwendet wird. Weitere Informationen hierzu finden Sie im Abschnitt „Port-Nummern für Cisco Consultant überprüfen“ auf Seite 245.

Problem: Der Befehl Ibccontrol oder ndadmin scheitert

Der Befehl Ibccontrol gibt die Nachricht “Fehler: Server antwortet nicht” zurück, oder der Befehl ndadmin gibt die Nachricht “Fehler: Zugriff auf RMI-Server nicht möglich” zurück. Diese Fehler können auftreten, wenn der Stack Ihrer Maschine SOCKSifiziert ist. Um dieses Problem zu beheben, editieren Sie die Datei socks.cnf, damit sie die folgenden Zeilen enthält:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Derartige Fehler können auch auftreten, wenn Sie **Ibcserver** noch nicht gestartet haben.

Problem: Für Port 14099 kann kein Eintrag in der Registrierungsdatenbank erstellt werden

Dieses Problem kann auftreten, wenn eine gültige Produktlizenz fehlt. Wenn Sie versuchen, Ibcserver zu starten, empfangen Sie die folgende Nachricht:

Ihre Lizenz ist abgelaufen. IBM Ansprechpartner oder autorisierten IBM Händler kontaktieren.

Sie können dieses Problem wie folgt lösen:

1. Falls Sie bereits versucht haben, Ibcserver zu starten, geben Sie **Ibcserver stop** ein.
2. Kopieren Sie Ihre gültige Lizenz in das Verzeichnis **...nd/servers/conf**.
3. Geben Sie **Ibcserver** ein, um den Server zu starten.

Allgemeine Fehler beheben — Metric Server

Problem: IOException für Metric Server unter Windows 2000 bei Ausführung von benutzerdefinierten Messwertdateien mit der Erweiterung .bat oder .cmd

Für Metric Server unter Windows 2000 müssen Sie für benutzerdefinierte Messwerte den vollständigen Namen angeben. Anstelle von **benutzermesswert** müssten Sie beispielsweise **benutzermesswert.bat** angeben. Der Name **benutzermesswert** ist in der Befehlszeile gültig, funktioniert jedoch nicht bei Ausführung von einer Laufzeitumgebung aus. Wenn Sie nicht den vollständigen Namen des Messwertes verwenden, empfangen Sie eine Metric Server IOException. Setzen Sie in der metricserver-Befehlsdatei die Variable LOG_LEVEL auf den Wert 3 und überprüfen Sie die Protokollausgabe. In diesem Beispiel sieht die Ausnahmebedingung wie folgt aus:

```
... java.io.IOException: CreateProcess: usermetric error=2
```

Problem: Metric Server meldet die Last nicht an die Network-Dispatcher-Maschine

Dafür, dass Metric Server keine Lastinformationen an Network Dispatcher meldet, kann es mehrere Gründe geben. Überprüfen Sie Folgendes, um die Ursache zu ermitteln:

- Vergewissern Sie sich, dass die Schlüsselringe zu Metric Server übertragen wurden.
- Prüfen Sie, ob der Host-Name der Metric-Server-Maschine im lokalen Namensserver registriert ist.
- Führen Sie einen Neustart mit einer höheren Protokollstufe durch und sehen Sie sich die Fehlnachrichten an.
- Erhöhen Sie auf der Network-Dispatcher-Maschine die Manager-Protokollstufe. Suchen Sie im Protokoll des Messwertüberwachungsprogramms nach Fehlern.

Problem: Metric-Server-Protokoll meldet, dass für den Zugriff auf den Agenten eine Kennung erforderlich ist

Das Metric-Server-Protokoll enthält diese Fehlernachricht, nachdem Schlüsselringe zum Server übertragen wurden.

Dieser Fehler wird registriert, wenn der Schlüsselring aufgrund einer Beschädigung des Schlüsselpaares nicht autorisiert werden kann. Versuchen Sie wie folgt, diesen Fehler zu beheben:

- Senden Sie den Schlüsselring erneut mit FTP und verwenden Sie die binäre Übertragungsmethode.
- Erstellen Sie einen neuen Schlüssel und verteilen Sie diesen.

Anhang A. Syntaxdiagramm lesen

Im Syntaxdiagramm wird gezeigt, wie ein Befehl angegeben wird, damit das Betriebssystem die Eingabe korrekt interpretieren kann. Lesen Sie das Syntaxdiagramm von links nach rechts und von oben nach unten entlang der horizontalen Linie (Hauptpfad).

Symbole und Interpunktion

In den Syntaxdiagrammen werden die folgenden Symbole benutzt:

Symbol	Beschreibung
--------	--------------

- | | |
|----|--|
| ▶▶ | Markiert den Anfang der Befehlssyntax. |
| ◀◀ | Markiert das Ende der Befehlssyntax. |

Alle im Syntaxdiagramm aufgeführten Interpunktionszeichen, beispielsweise Doppelpunkte, Fragezeichen und Minuszeichen, müssen wie gezeigt übernommen werden.

Parameter

In den Syntaxdiagrammen werden die folgenden Arten von Parametern benutzt:

Parameter	Beschreibung
-----------	--------------

Erforderlich	Erforderliche Parameter werden im Hauptpfad gezeigt.
---------------------	--

Optional	Optionale Parameter werden unter dem Hauptpfad gezeigt.
-----------------	---

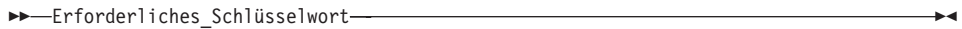
Parameter werden als Schlüsselwörter oder Variablen klassifiziert. Schlüsselwörter werden in Kleinbuchstaben gezeigt und können in Kleinbuchstaben eingegeben werden. Ein Befehlsname ist beispielsweise ein Schlüsselwort. Variablen stehen in Kursivschrift und stellen Namen oder Werte dar, die von Ihnen zur Verfügung gestellt werden müssen.

Beispiele für die Syntax

In dem folgenden Beispiel ist der Befehl **user** ein Schlüsselwort. Die erforderliche Variable ist die *Benutzer-ID* und die optionale Variable das *Kennwort*. Ersetzen Sie die Variablen durch Ihre eigenen Werte.



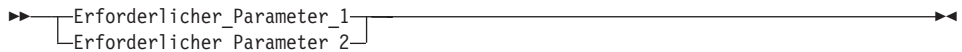
Erforderliche Schlüsselwörter: Erforderliche Schlüsselwörter und Variablen stehen im Hauptpfad.



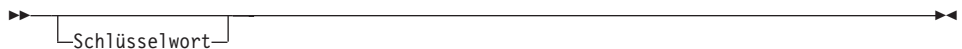
Erforderliche Schlüsselwörter und Werte **müssen** eingegeben werden.

Sich gegenseitig ausschließende Parameter aus einer Gruppe auswählen:

Sind mehrere Schlüsselwörter oder Variablen aufgeführt, die sich gegenseitig ausschließen und aus denen ein Schlüsselwort oder eine Variable ausgewählt werden muss, sind sie vertikal in alphanumerischer Anordnung aufgeführt.



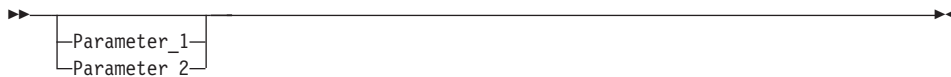
Optionale Werte: Optionale Schlüsselwörter und Variablen stehen unter dem Hauptpfad.



Sie können auswählen, ob sie optionale Schlüsselwörter oder Variablen angeben wollen oder nicht.

Optionale Schlüsselwörter oder Parameter aus einer Gruppe auswählen:

Sind mehrere Schlüsselwörter oder Variablen aufgeführt, die sich gegenseitig ausschließen und aus denen ein Schlüsselwort oder eine Variable ausgewählt werden kann, sind sie vertikal in alphanumerischer Anordnung unter dem Hauptpfad aufgeführt.



Variablen: Wörter in Kursivschrift sind *Variablen*. Erscheint eine Variable in der Syntax, muss sie wie im Text angegeben durch einen ihrer erlaubten Namen oder Werte ersetzt werden.



Zeichen, die keine alphanumerischen Zeichen sind: Enthält ein Diagramm ein Zeichen, das kein alphanumerisches Zeichen ist (beispielsweise einen Doppelpunkt, ein Anführungszeichen oder ein Minuszeichen), müssen Sie dieses Zeichen als Teil der Syntax angeben. Im folgenden Beispiel müssen Sie den Cluster und den Port im Format *Cluster:Port* angeben.



Anhang B. Befehlsreferenz für Dispatcher, CBR und Mailbox Locator

Dieser Anhang beschreibt die Verwendung der **ndcontrol**-Befehle von Dispatcher. Sie können diesen Anhang auch als Befehlsreferenz für CBR und Mailbox Locator verwenden. CBR und Mailbox Locator verwenden eine Untergruppe der Dispatcher-Befehle. Weitere Informationen hierzu finden Sie im Abschnitt „Konfigurationsunterschiede bei CBR, Mailbox Locator und Dispatcher“ auf Seite 266.

Anmerkung: Beachten Sie bei Verwendung dieses Syntaxdiagramms Folgendes:

- Ersetzen Sie für CBR "ndcontrol" durch **cbrcontrol** .
- Ersetzen Sie für Mailbox Locator "ndcontrol" durch **mlcontrol**.

Nachfolgend sind die in diesem Anhang beschriebenen Befehle aufgelistet:

- „ndcontrol advisor — Advisor steuern“ auf Seite 268
- „ndcontrol cluster — Cluster konfigurieren“ auf Seite 274
- „ndcontrol executor — Executor steuern“ auf Seite 280
- „ndcontrol file — Konfigurationsdateien verwalten“ auf Seite 285
- „ndcontrol help — Hilfetext für diesen Befehl anzeigen oder drucken“ auf Seite 287
- „ndcontrol highavailability — Hohe Verfügbarkeit steuern“ auf Seite 289
- „ndcontrol host — Ferne Maschine konfigurieren“ auf Seite 294
- „ndcontrol log — Binäre Protokolldatei steuern“ auf Seite 295
- „ndcontrol manager — Manager steuern“ auf Seite 296
- „ndcontrol metric — Systemmesswerte konfigurieren“ auf Seite 303
- „ndcontrol port — Ports konfigurieren“ auf Seite 305
- „ndcontrol rule — Regeln konfigurieren“ auf Seite 312
- „ndcontrol server — Server konfigurieren“ auf Seite 320
- „ndcontrol set — Serverprotokoll konfigurieren“ auf Seite 327
- „ndcontrol status — Aktivitätsanzeige für Manager und Advisor-Funktionen“ auf Seite 328
- „ndcontrol subagent — SNMP-Subagenten konfigurieren“ auf Seite 329

Sie können eine Minimalversion der Parameter für den Befehl "ndcontrol" eingeben. Sie müssen nur die eindeutigen Buchstaben der Parameter eingeben.

Beispiel: Wenn Sie Hilfe für den Befehl zum Speichern von Dateien aufrufen möchten, können Sie **ndcontrol h e f** anstelle von **ndcontrol help file** angeben.

Wenn Sie die Befehlszeilenschnittstelle starten möchten, setzen Sie den Befehl **ndcontrol** ab, um die Eingabeaufforderung "ndcontrol" aufzurufen.

Sie können die Befehlszeilenschnittstelle verlassen, indem Sie den Befehl **exit** oder **quit** absetzen.

Anmerkung: Die Werte der Befehlsparameter müssen in englischen Zeichen eingegeben werden. Die einzige Ausnahme hiervon bilden Host-Namen (die in den Befehlen "cluster", "server" und "highavailability" verwendet werden) und (die in Dateibefehlen verwendeten) Dateinamen.

Konfigurationsunterschiede bei CBR, Mailbox Locator und Dispatcher

Die Befehlszeilenschnittstelle von CBR und Mailbox Locator umfasst im Wesentlichen einen Teil der Befehlszeilenschnittstelle von Dispatcher. Verwenden Sie anstelle des Befehls "ndcontrol" zum Konfigurieren der Komponente den Befehl **cbrcontrol** (für die CBR-Komponente) oder den Befehl **mlcontrol** (für die Komponente Mailbox Locator).

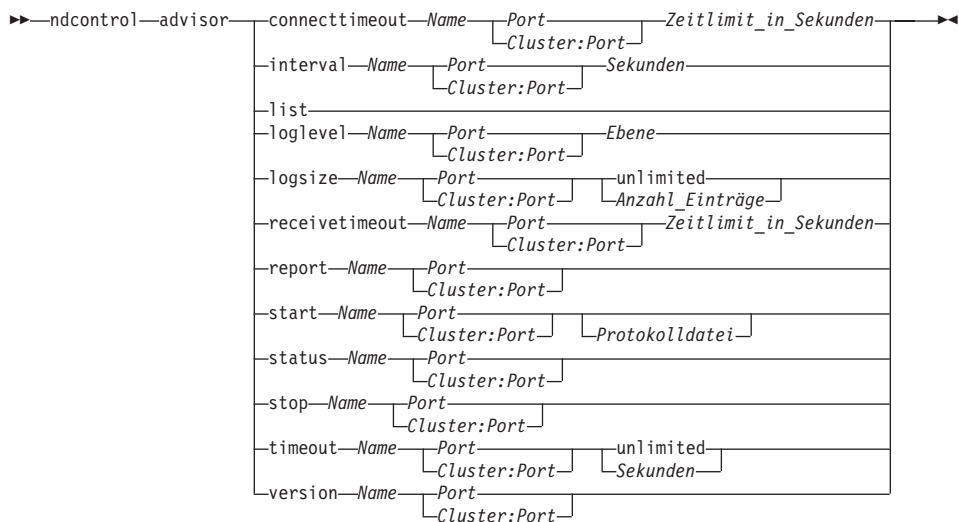
Nachfolgend sind einige der Befehle aufgelistet, die in CBR *ignoriert* werden.

1. highavailability
2. subagent
3. executor
 - report
 - set nfa <Wert>
 - set fincount <Wert>
 - set fintimeout <Wert>
 - set porttype <Wert>
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

Nachfolgend sind einige der Befehle aufgelistet, die in Mailbox Locator *ignoriert* werden.

1. highavailability
2. rule
3. subagent
4. executor
 - start
 - stop
 - report
 - set nfa <Wert>
 - set fincount <Wert>
 - set fintimeout <Wert>
 - set porttype <Wert>
5. Cluster
 - report {c}
 - set {c} porttype
6. port [add | set] {c:p} porttype
7. server [add | set] {c:p:s} router

ndcontrol advisor — Advisor steuern



connecttimeout

Definiert, wie lange eine Advisor-Funktion wartet, bevor sie meldet, dass zu einem Server keine Verbindung hergestellt werden kann. Weitere Informationen hierzu finden Sie im Abschnitt „Serververbindungs- und -empfangszeitlimit der Advisor-Funktion“ auf Seite 152.

Name

Der Name der Advisor-Funktion. Unter anderem sind die Werte **connect**, **db2**, **dns**, **ftp**, **http**, **ibmproxy (Caching Proxy)**, **imap**, **nntp**, **ping**, **pop3**, **self**, **smtp**, **ssl**, **ssl2http**, **telnet** und **wlm** möglich.

Die Namen angepasster Advisor-Funktionen haben das Format **xxxx**, wobei **ADV_xxxx** der Name der Klasse ist, die die angepasste Advisor-Funktion implementiert. Weitere Informationen hierzu finden Sie im Abschnitt „Kundenspezifische (anpassbare) Advisor-Funktion erstellen“ auf Seite 155.

Port

Die Nummer des Ports, der von der Advisor-Funktion überwacht wird.

Cluster:Port

Der Wert "Cluster" ist in den advisor-Befehlen optional, der Wert "Port" jedoch erforderlich. Wenn kein Wert für "Cluster" angegeben ist, wird die Advisor-Funktion an dem Port für alle Cluster gestartet. Wenn Sie einen Cluster angeben, wird die Advisor-Funktion an dem Port gestartet, jedoch nur für den von Ihnen genannten Cluster. Weitere Informationen hierzu finden Sie im Abschnitt „Advisor-Funktion starten und stoppen“ auf Seite 150.

Der Cluster kann als Adresse in Schreibweise mit Trennzeichen oder als symbolischer Name angegeben werden. Der Port wird als Nummer des Ports angegeben, der von der Advisor-Funktion überwacht wird.

Zeitlimit_in_Sekunden

Eine positive ganze Zahl, die das Zeitlimit in Sekunden angibt, nach dessen Ablauf die Advisor-Funktion meldet, dass zu einem Server keine Verbindung hergestellt werden kann. Dieser Wert liegt standardmäßig beim Dreifachen des für das Advisor-Intervall angegebenen Wertes.

interval

Legt fest, wie oft der Advisor Informationen von den Servern abfragt.

Sekunden

Eine positive ganze Zahl, die die Zeit zwischen den an die Server gerichteten Statusabfragen in Sekunden angibt. Der Standardwert ist 7.

list

Zeigt eine Liste der Advisor an, die derzeit Informationen an den Manager liefern.

loglevel

Legt die Protokollstufe für ein Advisor-Protokoll fest.

Stufe

Die Nummer der Stufe (0 bis 5). Der Standardwert ist 1. Je größer die Zahl ist, desto mehr Informationen werden in das Advisor-Protokoll geschrieben. Die folgenden Werte sind gültig: 0 für keine Einträge, 1 für eine minimale Protokollierung, 2 für eine Basisprotokollierung, 3 für eine normale, 4 für eine erweiterte und 5 für eine ausführliche Protokollierung.

logsize

Legt die maximale Größe eines Advisor-Protokolls fest. Wenn Sie eine maximale Größe für die Protokolldatei festlegen, findet ein Dateiumbruch statt. Hat die Datei die angegebene Größe erreicht, werden alle weiteren Einträge wieder an den Anfang der Datei geschrieben und die dort befindlichen Einträge überschrieben. Die Protokollgröße kann nicht auf einen geringeren Wert als die aktuelle Dateigröße gesetzt werden. Protokolleinträge sind mit einer Zeitmarke versehen, damit Sie die Reihenfolge, in der sie geschrieben wurden, erkennen können. Je höher Sie die Protokollstufe setzen, desto vorsichtiger müssen Sie die Protokollgröße auswählen, da die Protokolldatei sehr schnell voll ist, wenn Sie eine Protokollierung auf einer höheren Stufe wählen.

Anzahl_Sätze

Die maximale Größe der Advisor-Protokolldatei in Bytes. Sie können entweder eine positive Zahl, die größer als 0 sein muss, oder das Wort **unlimited** (unbegrenzt) angeben. Möglicherweise erreicht die Protokolldatei nicht genau die maximale Größe, bevor der Dateiumbruch stattfindet, da die Größe der Protokolleinträge variiert. Der Standardwert ist 1 MB.

receivetimeout

Definiert, wie lange eine Advisor-Funktion wartet, bevor sie meldet, dass von einem Server keine Daten empfangen werden können. Weitere Informationen hierzu finden Sie im Abschnitt „Serververbindungs- und -empfangszeitlimit der Advisor-Funktion“ auf Seite 152.

Zeitlimit_in_Sekunden

Eine positive ganze Zahl, die das Zeitlimit in Sekunden angibt, nach dessen Ablauf die Advisor-Funktion meldet, dass von einem Server keine Daten empfangen werden können. Dieser Wert liegt standardmäßig beim Dreifachen des für das Advisor-Intervall angegebenen Wertes.

report

Zeigt einen Bericht zum Advisor-Status an.

start

Den Advisor starten. Für alle Protokolle stehen Advisor zur Verfügung. Die Standard-Ports sind:

Advisor-Name	Protokoll	Port
connect	ICMP	12345
db2	privat	50000
dns	DNS	53
ftp	FTP	21
http	HTTP	80
ibmproxy	HTTP (über Caching Proxy)	80
imap	IMAP	143
nntp	NNTP	119
ping	PING	0
pop3	POP3	110
self	privat	12345
smtp	SMTP	25
ssl	HTTP	443
ssl2http	SSL	443
telnet	Telnet	23
WLM	privat	10007

Anmerkung: Die FTP-Advisor-Funktion darf nur für den FTP-Steuer-Port (21) ausgeführt werden. Starten Sie eine FTP-Advisor-Funktion nicht für den FTP-Daten-Port (20).

Protokolldatei

Der Name der Datei, in die die Verwaltungsdaten geschrieben werden. Jeder Eintrag des Protokolls wird mit einer Zeitmarke versehen.

Die Standarddatei ist *Advisor-Name_Port.log*, z. B. **http_80.log**. Wollen Sie das Verzeichnis ändern, in dem die Protokolldateien gespeichert werden, lesen Sie die Informationen unter „Pfade für die Protokolldatei ändern“ auf Seite 222. Die Standardprotokolldateien für Cluster- oder sitespezifische Advisor-Funktionen werden mit der Cluster-Adresse erstellt, z. B. **http_127.40.50.1_80.log**.

status

Zeigt den aktuellen Status aller Werte in einem Advisor an, die global gesetzt werden können. Zudem werden die Standardwerte dieser Werte angezeigt.

stop

Den Advisor stoppen.

Zeitlimit

Legt die Anzahl von Sekunden fest, in denen der Manager von dem Advisor erhaltene Informationen als gültig ansieht. Stellt der Manager fest, dass die Advisor-Informationen älter als dieses Zeitlimit sind, verwendet der Manager diese Informationen nicht zum Bestimmen Wertigkeiten für die Server am Port, die von der Advisor-Funktion überwacht werden. Dieses Zeitlimit gilt nicht, wenn die Advisor-Funktion den Manager darüber informiert hat, dass ein bestimmter Server inaktiv ist. Der Manager verwendet diese Information über den Server auch nach Überschreitung des Informationszeitlimits für die Advisor-Funktion weiter.

Sekunden

Eine positive Zahl, die die Anzahl von Sekunden darstellt, oder das Wort **unlimited** (unbegrenzt). Der Standardwert ist "unlimited".

version

Zeigt die aktuelle Advisor-Version an.

Beispiele

- Starten der Advisor-Funktion http am Port 80 für Cluster 127.40.50.1:
`ndcontrol advisor start http 127.40.50.1:80`
- Starten der Advisor-Funktion http am Port 88 für alle Cluster:
`ndcontrol advisor start http 88`
- Stoppen der Advisor-Funktion http am Port 80 für Cluster 127.40.50.1:
`ndcontrol
advisor stop http 127.40.50.1:80`
- Festlegen der Zeit (30 Sekunden), die eine HTTP-Advisor-Funktion für Port 80 wartet, bevor sie meldet, dass zu einem Server keine Verbindung hergestellt werden kann:

```
ndcontrol advisor connecttimeout http 80 30
```

- Festlegen der Zeit (20 Sekunden), die eine HTTP-Advisor-Funktion für Port 80 des Clusters 127.40.50.1 wartet, bevor sie meldet, dass zu einem Server keine Verbindung hergestellt werden kann:

```
ndcontrol advisor connecttimeout http 127.40.50.1:80 20
```

- Festlegen des Intervalls für die FTP-Advisor-Funktion (für Port 21) auf 6 Sekunden:

```
ndcontrol advisor interval ftp 21 6
```

- Geben Sie den folgenden Befehl ein, um eine Liste der Advisor anzuzeigen, die derzeit Informationen an den Manager liefern:

```
ndcontrol advisor list
```

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

ADVISOR	CLUSTER:PORT	ZEITLIMIT
http	127.40.50.1:80	unlimited
ftp	21	unlimited

- Ändern der Protokollstufe für das Advisor-Protokoll auf 0, um einen höheren Durchsatz zu erreichen:

```
ndcontrol advisor loglevel http 80 0
```

- Ändern der Protokollgröße für die Advisor-Funktion ftp am Port 21 auf 5000 Bytes:

```
ndcontrol advisor logsize ftp 21 5000
```

- Festlegen der Zeit (60 Sekunden), die eine HTTP-Advisor-Funktion (für Port 80) wartet, bevor sie meldet, dass von einem Server keine Daten empfangen werden können:

```
ndcontrol advisor receivetimeout http 80 60
```

- Anzeigen eines Berichts zum Status der Advisor-Funktion ftp (für Port 21):

```
ndcontrol advisor report ftp 21
```

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Advisor-Bericht:

Advisor-Name Ftp

Port-Nummer 21

Cluster-Adresse 9.67.131.18

Serveradresse 9.67.129.230

Last 8

Cluster-Adresse 9.67.131.18

Serveradresse 9.67.131.215

Last -1

- Anzeigen des aktuellen Status der Werte, die der Advisor-Funktion http für Port 80 zugeordnet sind:

```
ndcontrol advisor status http 80
```

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

Advisor-Status:

```
Intervall (Sekunden) ..... 7
Zeitlimit (Sekunden) ..... Unlimited
Zeitlimit für Verbindung (Sekunden) ..... 21
Zeitlimit für Empfang (Sekunden) ..... 21
Advisor-Protokolldateiname ..... Http_80.log
Protokollstufe ..... 1
Maximale Managerprotokollgröße (Bytes)... Unlimited
```

- Festlegen des Zeitlimits für Informationen der Advisor-Funktion ftp am Port 21 auf 5 Sekunden:

```
ndcontrol advisor timeout ftp 21 5
```

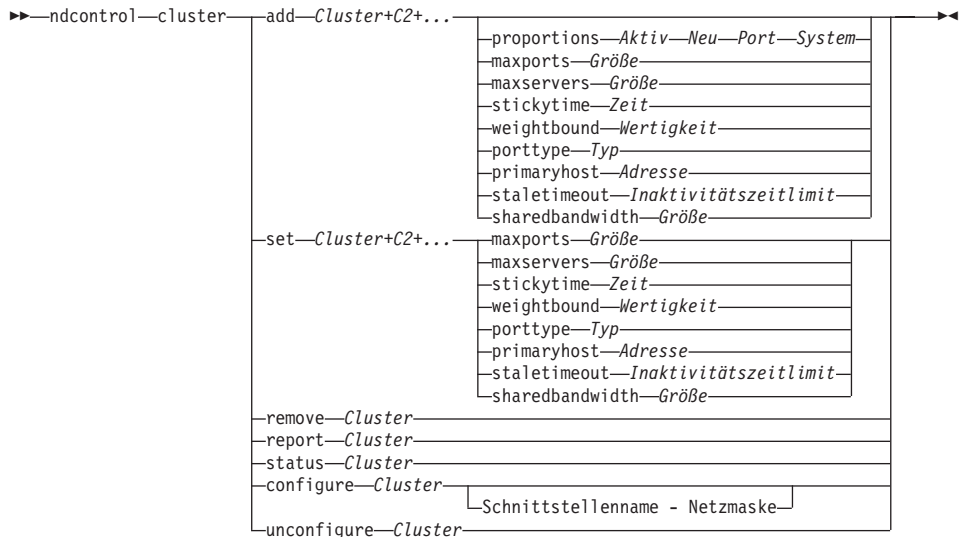
- Anzeigen der aktuellen Versionsnummer der Advisor-Funktion ssl für Port 443:

```
ndcontrol
advisor version ssl 443
```

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

```
Version: 04.00.00.00 - 07/12/2001-10:09:56-EDT
```

ndcontrol cluster — Cluster konfigurieren



add

Diesen Cluster hinzufügen. Sie müssen mindestens 1 Cluster definieren.

Cluster

Die Adresse des Clusters als symbolischer Name oder in Schreibweise mit Trennzeichen. Mit der Cluster-Adresse 0.0.0.0 kann ein Platzhalter-Cluster angegeben werden. Weitere Informationen hierzu finden Sie im Abschnitt „Platzhalter-Cluster verwenden, um Serverkonfigurationen zusammenzufassen“ auf Seite 199.

Generell können Sie einen Doppelpunkt (:) als Platzhalter verwenden. Die einzige Ausnahme hiervon bildet der Befehl "ndcontrol cluster add". Der Befehl ndcontrol cluster set : weightbound 80 bewirkt beispielsweise, dass für alle Cluster eine Wertigkeit von 80 festgelegt wird.

Anmerkung: Zusätzliche Cluster werden durch ein Pluszeichen (+) getrennt.

proportions

Legt auf Cluster-Ebene die proportionale Bedeutung von aktiven Verbindungen (*Aktiv*), von neuen Verbindungen (*Neu*), von Informationen der Advisor-Funktionen (*Port*) und von Informationen eines Systemüberwachungsprogramms wie Metric Server (*System*), anhand derer der Manager Serverwertigkeiten festlegt.

Alle diese Werte, die nachfolgend beschrieben werden, werden als Prozentsatz der Summe angegeben und müssen daher immer 100 ergeben.

Weitere Informationen hierzu finden Sie im Abschnitt „Proportionale Bedeutung von Statusinformationen“ auf Seite 145.

Aktiv

Eine Zahl von 0 bis 100 für die proportionale Wertigkeit, die den aktiven Verbindungen zugeordnet werden soll. Der Standardwert ist 50.

Neu

Eine Zahl von 0 bis 100 für die proportionale Wertigkeit, die neuen Verbindungen zugeordnet werden soll. Der Standardwert ist 50.

Port

Eine Zahl von 0 bis 100 für die proportionale Wertigkeit, die den Informationen von Advisor-Funktionen zugeordnet werden soll. Der Standardwert ist 0.

Anmerkung: Wenn eine Advisor-Funktion gestartet wird und die Port-Proportion 0 ist, setzt Network Dispatcher diesen Wert automatisch auf 1, damit der Manager die Informationen der Advisor-Funktion als Vorgabe für die Berechnung der Serverwertigkeit verwendet.

System

Eine Zahl von 0-100, die die proportionale Wertigkeit darstellt, die den Systemmesswerten von einem Programm wie Metric Server zugeordnet werden soll. Der Standardwert ist 0.

maxports

Die maximale Port-Anzahl. Der Standardwert für maxports ist 8.

Größe

Die zulässige Port-Anzahl.

maxservers

Die standardmäßige Höchstzahl von Servern pro Port. Dieser Wert kann für einzelne Ports mit **port maxservers** überschrieben werden. Der Standardwert für "maxservers" ist 32.

Größe

Die zulässige Anzahl von Servern für einen Port.

stickytime

Die Standardhaltezeit für Ports, die erstellt werden sollen. Dieser Wert kann für einzelne Ports mit dem Befehl **port stickytime** außer Kraft gesetzt werden. Der Standardwert für stickytime ist 0.

Anmerkung: Wenn Sie die Dispatcher-Weiterleitungsmethode "cbr" verwenden und für zu erstellende Ports der Wert für "stickytime" ungleich null ist, wird beim Hinzufügen eines neuen Ports die Affinität der SSL-IDs für den Port aktiviert. Sie können die Affinität der SSL-IDs für den Port inaktivieren, indem Sie "stickytime" für den Port explizit auf 0 setzen.

Zeit

Der Wert für "stickytime" in Sekunden.

weightbound

Die standardmäßige Wertigkeitsgrenze für Ports. Dieser Wert kann für einzelne Ports mit dem Befehl **port weightbound** außer Kraft gesetzt werden. Der Standardwert für weightbound ist 20.

Wertigkeit

Die Wertigkeitsgrenze.

porttype

Der Standard-Port-Typ. Dieser Wert kann für einzelne Ports mit **port porttype** überschrieben werden.

Anmerkung: Der Parameter "porttype" gilt für Dispatcher.

Typ

Gültige Werte sind **tcp**, **udp** und **both**.

primaryhost

Die NFA dieser Dispatcher-Maschine oder die NFA-Adresse der Dispatcher-Partnermaschine. In einer Konfiguration mit gegenseitiger hoher Verfügbarkeit ist ein Cluster entweder der primären Maschine oder der Ausweichmaschine zugeordnet.

Wird der primäre Host (primaryhost) eines Clusters geändert, nachdem die primäre Maschine und Partnermaschine bereits gestartet wurden, und ist die beiderseitige Hochverfügbarkeit aktiv, müssen Sie auch den neuen primären Host zur Übernahme zwingen. Außerdem müssen Sie die Scripts aktualisieren und den Cluster manuell aus der Konfiguration entfernen und dann richtig konfigurieren. Weitere Informationen hierzu finden Sie im Abschnitt „Gegenseitige hohe Verfügbarkeit“ auf Seite 53.

Adresse

Der Wert für die Adresse des primären Hosts. Der Standardwert ist die NFA-Adresse dieser Maschine.

staletimeout

Die Zeit der Inaktivität einer Verbindung in Sekunden, bevor die Verbindung entfernt wird. Der Standardwert für FTP ist 900 und für Telnet 32.000.000. Für alle anderen Protokolle liegt der Standardwert bei 300. Dieser Wert kann für einzelne Ports mit dem Befehl **port staletimeout** außer Kraft gesetzt werden. Weitere Informationen befinden sich unter „Inaktivitätszeitlimit verwenden“ auf Seite 223.

Anmerkung: Bei Mailbox Locator entspricht staletimeout dem Inaktivitätszeitlimit für automatische Abmeldung für diese Protokolle. Der Parameter "staletimeout" für Mailbox Locator hat standardmäßig den Wert 60 und setzt die Inaktivitätszeitlimits für POP3 und IMAP außer Kraft. Weitere Informationen zum Parameter "staletimeout" für Mailbox Locator finden Sie im Abschnitt „Inaktivitätszeitgeber für POP3/IMAP überschreiben“ auf Seite 104.

Inaktivitätszeitlimit

Der Wert für staletimeout.

sharedbandwidth

Die maximale Bandbreite (in Kilobytes pro Sekunde), die auf Cluster-Ebene gemeinsam genutzt werden kann. Weitere Informationen zur gemeinsam genutzten Bandbreite finden Sie in den Abschnitten „Regeln auf der Basis der reservierten und gemeinsam benutzten Bandbreite verwenden“ auf Seite 190 und „Regel "Gemeinsame Bandbreite"“ auf Seite 192.

Anmerkung: Die gemeinsam genutzte Bandbreite gilt nicht für CBR oder Mailbox Locator.

Größe

Der Parameter **sharedbandwidth** muss einen ganzzahligen Wert haben. Der Standardwert ist null. Bei einem Wert von null kann keine Bandbreite auf Cluster-Ebene gemeinsam genutzt werden.

set

Die Merkmale des Clusters festlegen.

remove

Diesen Cluster entfernen.

report

Die internen Felder des Clusters anzeigen.

Anmerkung: Der Parameter "report" gilt nicht für CBR oder Mailbox Locator.

status

Den aktuellen Status eines bestimmten Clusters anzeigen.

configure

Konfiguriert einen Cluster-Aliasnamen für die Netzschnittstellenkarte.

Anmerkung: Der Parameter "configure" gilt nicht für CBR oder Mailbox Locator.

Schnittstellenname Netzmaske

Erforderlich, wenn es sich um einen anderen als den vom Dispatcher zuerst gefundenen Aliasnamen handelt.

unconfigure

Löscht den Cluster-Aliasnamen von der Netzschnittstellenkarte.

Anmerkung: Der Parameter "unconfigure" gilt nicht für CBR oder Mailbox Locator.

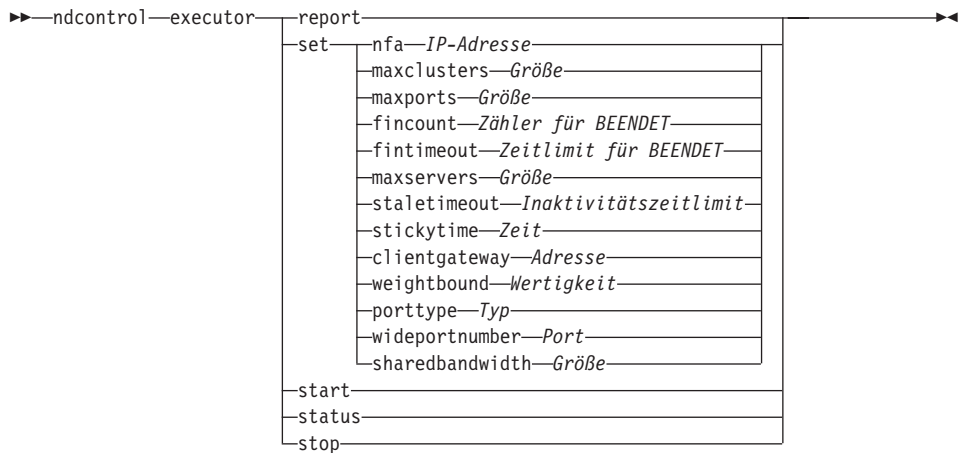
Beispiele

- Geben Sie den folgenden Befehl ein, um die Cluster-Adresse 130.40.52.153 hinzuzufügen:
`ndcontrol cluster add 130.40.52.153`
- Geben Sie den folgenden Befehl ein, um die Cluster-Adresse 130.40.52.153 zu entfernen:
`ndcontrol cluster remove 130.40.52.153`
- Festlegen der relativen Bedeutung von Vorgaben (Aktiv, Neu, Port, System), die vom Manager für Server des Clusters 9.6.54.12 empfangen werden:
`ndcontrol cluster set 9.6.54.12 proportions 60 35 5 0`
- Geben Sie den folgenden Befehl ein, um einen Platzhalter-Cluster hinzuzufügen:
`ndcontrol cluster add 0.0.0.0`
- Geben Sie den folgenden Befehl ein, um in einer Konfiguration mit beiderseitiger Hochverfügbarkeit die Cluster-Adresse 9.6.54.12 mit der NFA der Partnermaschine (9.65.70.19) als primären Host zu definieren:
`ndcontrol
cluster set 9.6.54.12 primaryhost 9.65.70.19`
- Geben Sie den folgenden Befehl ein, um den Status für Cluster-Adresse 9.67.131.167 anzuzeigen:
`ndcontrol cluster status 9.67.131.167`

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

```
Cluster-Status:
-----
Adresse ..... 9.67.131.167
Anzahl Ziel-Ports ..... 3
Standardhaltezeit ..... 0
Strd.-Zeitlimit für Inaktivität ..... 30
Strd.-Gewichtungsgrenze für Port ..... 20
Max. Anzahl Ports ..... 8
Strd.-Port-Protokoll ..... tcp/udp
Strd. max. Anzahl Server ..... 32
Proportion für aktive Verbindungen ..... 0.5
Proportion für neue Verbindungen ..... 0.5
Port-spezifische Proportion ..... 0
Proportion für Systemmetrik ..... 0
Gemeinsame Bandbreite (KBytes) ..... 0
Adresse des primären Hosts ..... 9.67.131.167
```

ndcontrol executor — Executor steuern



report

Zeigt eine statistische Momentaufnahme an, z. B. die Gesamtanzahl der empfangenen, gelöschten oder mit Fehlern weitergeleiteten Pakete usw.

Anmerkung: Der Parameter "report" gilt nicht für CBR oder Mailbox Locator.

set

Die Felder des Executors festlegen.

nfa

NFA definieren. Alle an diese Adresse gesendeten Pakete werden von der Dispatcher-Maschine nicht weitergeleitet.

Anmerkung: Der Parameter "nfa" gilt nicht für CBR oder Mailbox Locator.

IP-Adresse

Die Internet-Protocol-Adresse als symbolischer Name oder in Schreibweise mit Trennzeichen.

maxclusters

Die maximale Anzahl Cluster, die konfiguriert werden können. Der Standardwert für maxclusters ist 100.

Größe

Die maximale Anzahl Cluster, die konfiguriert werden können.

maxports

Der Standardwert für maxports für Cluster, die erstellt werden sollen.

Dieser Wert kann mit dem Befehl **cluster set** oder **cluster add** überschrieben werden. Der Standardwert für maxports ist 8.

Größe

Die Port-Anzahl.

fincount

Die Anzahl der Verbindungen, die den Status **BEENDET** haben müssen, bevor die Speicherbereinigung für Verbindungen eingeleitet wird. Der Standardwert für fincount ist 4000.

Zähler für BEENDET

Der Wert für "fincount".

Anmerkung: Der Parameter "fincount" gilt nicht für CBR oder Mailbox Locator.

fintimeout

Die Anzahl Sekunden, die eine Verbindung im Speicher verbleiben soll, nachdem die Verbindung in den Status **BEENDET** gesetzt wurde. Der Standardwert für fintimeout ist 60.

Zeitlimit für BEENDET

Der Wert für "fintimeout".

Anmerkung: Der Parameter "fintimeout" gilt nicht für CBR oder Mailbox Locator.

maxservers

Die standardmäßig geltende maximale Anzahl von Servern pro Port. Dieser Wert kann mit dem Befehl **cluster** oder **port** überschrieben werden. Der Standardwert für maxservers ist 32.

Größe

Die Anzahl Server.

staletimeout

Die Zeit der Inaktivität einer Verbindung in Sekunden, bevor die Verbindung entfernt wird. Der Standardwert für FTP ist 900 und für Telnet 32.000.000. Der Standardwert für alle anderen Ports ist 300. Dieser Wert kann mit dem Befehl **cluster** oder **port** überschrieben werden. Weitere Informationen befinden sich unter „Inaktivitätszeitlimit verwenden“ auf Seite 223.

Anmerkung: Bei Mailbox Locator entspricht "staletimeout" dem Inaktivitätszeitlimit für automatische Abmeldung für diese Protokolle. Der Parameter "staletimeout" für Mailbox Locator hat standardmäßig den Wert 60 und setzt die Inaktivitätszeitlimits für POP3 und IMAP außer Kraft. Weitere Informatio-

nen zum Parameter "staletimeout" für Mailbox Locator finden Sie im Abschnitt „Inaktivitätszeitgeber für POP3/IMAP überschreiben“ auf Seite 104.

Inaktivitätszeitlimit

Der Wert für "staletimeout".

stickytime

Die Standardhaltezeit für Ports für alle künftigen Cluster. Dieser Wert kann mit dem Befehl **cluster** oder **port** überschrieben werden. Der Standardwert für stickytime ist 0.

Zeit

Der Wert für "stickytime" in Sekunden.

clientgateway

Der Parameter "clientgateway" ist eine IP-Adresse, die für NAT/NAPT oder inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente verwendet wird. Er gibt die Router-Adresse an, über die der Antwortdatenverkehr von Network Dispatcher zu den Clients weitergeleitet wird. Der Parameter "clientgateway" muss auf einen Wert ungleich null gesetzt werden, bevor mit der Weiterleitungsmethode NAT/NAPT oder inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente ein neuer Port hinzugefügt wird. Weitere Informationen hierzu finden Sie in „NAT/NAPT-Weiterleitungsmethode (nat) des Dispatchers“ auf Seite 55 und „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)“ auf Seite 57.

Anmerkung: Der Parameter "clientgateway" gilt nur für die Dispatcher-Komponente.

Adresse

Die für den Parameter "clientgateway" angegebene Adresse ist ein symbolischer Name oder eine Adresse in Schreibweise mit Trennzeichen. Der Standardwert ist 0.0.0.0.

weightbound

Die standardmäßige Port-Wertigkeitsgrenze für alle künftigen Ports. Dieser Wert kann mit dem Befehl **cluster** oder **port** überschrieben werden. Der Standardwert für weightbound ist 20.

Wertigkeit

Der Wert für "weightbound".

porttype

Der für alle künftigen Ports gültige Standardwert für Port-Typ. Dieser Wert kann mit dem Befehl **cluster** oder **port** überschrieben werden.

Anmerkung: Der Parameter "porttype" gilt nicht für CBR oder Mailbox Locator.

Typ

Gültige Werte sind **tcp**, **udp** und **both**.

wideportnumber

Ein nicht verwendeter TCP-Port auf jeder Dispatcher-Maschine. Die *wideportnumber* muss für alle Dispatcher-Maschinen identisch sein. Der Standardwert für *wideportnumber* ist 0. Dieser Wert gibt an, dass die Weitverkehrsunterstützung nicht verwendet wird.

Anmerkung: Der Parameter "*wideportnumber*" gilt nicht für CBR oder Mailbox Locator.

Port

Der Wert für **wideportnumber**.

sharedbandwidth

Die maximale Bandbreite (in Kilobytes pro Sekunde), die auf Executor-Ebene gemeinsam genutzt werden kann. Weitere Informationen zur gemeinsam genutzten Bandbreite finden Sie in den Abschnitten „Regeln auf der Basis der reservierten und gemeinsam benutzten Bandbreite verwenden“ auf Seite 190 und „Regel „Gemeinsame Bandbreite““ auf Seite 192.

Anmerkung: Die gemeinsam genutzte Bandbreite gilt nicht für CBR oder Mailbox Locator.

Größe

Der Parameter **sharedbandwidth** muss einen ganzzahligen Wert haben. Der Standardwert ist null. Bei einem Wert von null kann keine Bandbreite auf Executor-Ebene gemeinsam genutzt werden.

start

Den Executor starten.

Anmerkung: Der Parameter "*start*" gilt nicht für Mailbox Locator.

status

Anzeigen des aktuellen Status für die im Executor definierbaren Werte und ihrer Standardeinstellungen.

stop

Stoppen des Executors. Für den Dispatcher ist "*stop*" unter Windows 2000 *kein* gültiger Parameter.

Anmerkung: Der Parameter "*stop*" gilt für den Dispatcher und für CBR.

Beispiele

- Geben Sie den folgenden Befehl ein, um die internen Zähler für den Dispatcher anzuzeigen:

```
ndcontrol executor status
```

```
Executor-Status:
```

```
-----
```

```
NFA ..... 9.67.131.151
Client-Gateway-Adresse ..... 0.0.0.0
Anzahl beendeter Verbindungen ..... 4.000
Zeitlimit beend. inakt. Verbindungen ... 60
Port-Nr. für Weitverkehrsnetz ..... 2.001
Gemeinsame Bandbreite (KBytes) ..... 0
Strd. max. Ports pro Cluster ..... 8
Max. Anzahl Cluster ..... 100
Strd. max. Anzahl Server pro Port ..... 32
Strd.-Zeitlimit für Port ..... 300
Haltezeit für Port ..... 0
Gewichtungsgrenze für Port ..... 20
Max. Anzahl Cluster ..... 100
```

- Definieren der NFA von 130.40.52.167:
- Geben Sie den folgenden Befehl ein, um die maximale Anzahl von Clustern festzulegen:

```
ndcontrol executor set nfa 130.40.52.167
```

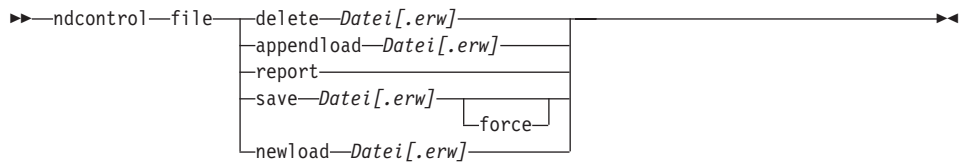
```
ndcontrol executor set maxclusters 4096
```

- Starten des Executors:
- Stoppen des Executors (**nur unter AIX, Linux und Solaris**):

```
ndcontrol executor start
```

```
ndcontrol executor stop
```

ndcontrol file — Konfigurationsdateien verwalten



delete

Die Datei löschen.

Datei[.erw]

Eine Konfigurationsdatei mit ndcontrol-Befehlen.

Die Dateierweiterung (.erw) kann vom Benutzer festgelegt oder übergangen werden.

appendload

Zum Aktualisieren der momentanen Konfiguration führt der Befehl appendload die Befehle in Ihrer Script-Datei aus.

report

Bericht über die verfügbare(n) Datei(en).

save

Sichern der aktuellen Konfiguration für Network Dispatcher in der Datei.

Anmerkung: Dateien werden in den nachfolgend genannten Verzeichnissen gespeichert und aus diesen geladen. Für *Komponente* gilt der Wert "dispatcher", "cbr" oder "ml" (Mailbox Locator).

- AIX: /usr/lpp/nd/servers/configurations/*Komponente*
- Linux: /opt/nd/servers/configurations/*Komponente*
- Solaris: /opt/nd/servers/configurations/*Komponente*
- Windows 2000:

Allgemeiner Installationsverzeichnispfad —

c:\Programme\ibm\edge\nd\servers\configurations*Komponente*

Interner Installationsverzeichnispfad —

c:\Programme\ibm\nd\servers\configurations*Komponente*

force

Wenn Sie Ihre Datei in einer vorhandenen Datei mit demselben Namen speichern möchten, verwenden Sie **force**, um die vorhandene Datei vor dem Speichern der neuen Datei zu löschen. Bei Nichtverwendung der Option "force" wird die vorhandene Datei nicht überschrieben.

newload

Laden einer neuen Konfigurationsdatei in Network Dispatcher und ausführen derselben. Die neue Konfigurationsdatei ersetzt die aktuelle Konfiguration.

Beispiele

- Geben Sie den folgenden Befehl ein, um eine Datei zu löschen:

```
ndcontrol file delete Datei3
```

Datei (Datei3) wurde gelöscht.

- Geben Sie den folgenden Befehl ein, um eine neue Konfigurationsdatei zu laden, die die aktuelle Konfiguration ersetzt:

```
ndcontrol file newload Datei1.sv
```

Datei (Datei1.sv) wurde in den Dispatcher geladen.

- Geben Sie den folgenden Befehl ein, um eine Konfigurationsdatei an die aktuelle Konfiguration anzuhängen und zu laden:

```
ndcontrol file appendload Datei2.sv
```

Datei (Datei2.sv) wurde an die aktuelle Konfiguration angehängt und geladen.

- Geben Sie den folgenden Befehl ein, um einen Bericht über Ihre Dateien anzuzeigen (die Dateien, die zuvor gesichert wurden):

```
ndcontrol file report
```

```
DATEIBERICHT:
```

```
Datei1.save
```

```
Datei2.sv
```

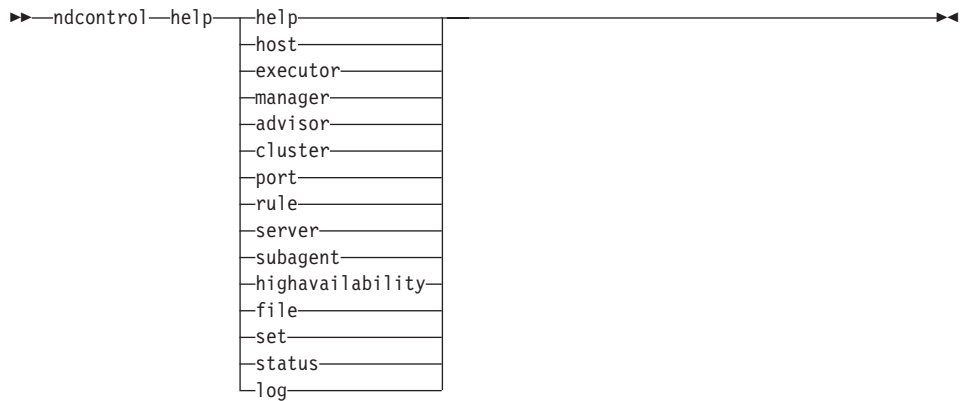
```
Datei3
```

- Geben Sie den folgenden Befehl ein, um die Konfiguration in der Datei Datei3 zu sichern:

```
ndcontrol file save Datei3
```

Die Konfiguration wurde in Datei (Datei3) gesichert.

ndcontrol help — Hilfetext für diesen Befehl anzeigen oder drucken



Beispiele

- Geben Sie den folgenden Befehl ein, um Hilfe für den Befehl ndcontrol anzufordern:

ndcontrol help

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

ARGUMENTE BEFEHL HELP:

Verwendung: help <Hilfeoption>

Beispiel: help cluster

help	- vollständigen Hilfetext drucken
advisor	- Hilfe zum Befehl advisor
cluster	- Hilfe zum Befehl cluster
executor	- Hilfe zum Befehl executor
file	- Hilfe zum Befehl file
host	- Hilfe zum Befehl host
log	- Hilfe zum Befehl log
manager	- Hilfe zum Befehl manager
metric	- Hilfe zum Befehl metric
port	- Hilfe zum Befehl port
rule	- Hilfe zum Befehl rule
server	- Hilfe zum Befehl server
set	- Hilfe zum Befehl set
status	- Hilfe zum Befehl status
subagent	- Hilfe zum Befehl subagent
highavailability	- Hilfe zum Befehl highavailability

Parameter innerhalb von <> sind Variablen.

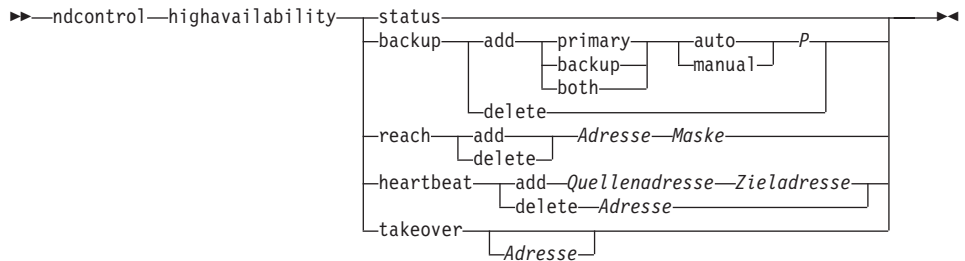
- Manchmal enthält der Hilfetext Optionen für die Variablen, die durch das Zeichen | voneinander getrennt sind:

```
fintimeout <Cluster-Adresse>|all <Zeit>
```

- Zeitlimit für beendete inaktive Verbindungen ändern
(Verwenden Sie 'all', um alle Cluster zu ändern)

ndcontrol highavailability — Hohe Verfügbarkeit steuern

Anmerkung: Das Syntaxdiagramm für "ndcontrol highavailability" gilt nicht für CBR oder Mailbox Locator.



status

Einen Bericht über die hohe Verfügbarkeit zurückgeben. Maschinen können eine von drei Statusbedingungen oder einen von drei Status haben:

Aktiv Eine bestimmte Maschine (primäre Maschine und/oder Partnermaschine) leitet Pakete weiter.

Bereitschaft

Eine bestimmte Maschine (primäre Maschine und/oder Partnermaschine) leitet keine Pakete weiter. Sie überwacht den Status eines **aktiven** Dispatchers.

Ruhend

Eine bestimmte Maschine leitet Pakete weiter und versucht nicht, Kontakt mit der Dispatcher-Partnermaschine aufzunehmen.

Darüber hinaus gibt das Schlüsselwort **status** Informationen über verschiedene untergeordnete Status zurück:

Synchronisiert

Eine bestimmte Maschine hat Kontakt mit einer anderen Dispatcher-Maschine aufgenommen.

Andere untergeordnete Status

Diese Maschine versucht, Kontakt zu ihrer Dispatcher-Partnermaschine aufzunehmen, die Kontaktaufnahme ist aber bisher nicht gelungen.

backup

Informationen über die primäre Maschine oder die Partnermaschine angeben.

add

Definiert die Funktionen der hohen Verfügbarkeit für diese Maschine und führt sie aus.

primary

Identifiziert die Dispatcher-Maschine, die die Rolle als *primäre Maschine* einnimmt.

backup

Identifiziert die Dispatcher-Maschine, die die Rolle als *Partnermaschine* einnimmt.

both

Identifiziert die Dispatcher-Maschine, die die Rolle als *primäre Maschine und Partnermaschine* einnimmt. Hierbei handelt es sich um die Funktion der beiderseitigen Hochverfügbarkeit, bei der die Rollen als primäre Maschine und als Partnermaschine auf der Basis einer Cluster-Gruppe zugeordnet werden. Weitere Informationen befinden sich unter „Gegenseitige hohe Verfügbarkeit“ auf Seite 53.

auto

Gibt eine *automatische* Wiederanlaufstrategie an, bei der die primäre Maschine das Weiterleiten von Paketen übernimmt, sobald sie wieder betriebsbereit ist.

manual

Gibt eine *manuelle* Wiederanlaufstrategie an, bei der die primäre Maschine das Weiterleiten von Paketen erst dann wieder übernimmt, wenn der Administrator den Befehl **takeover** ausgibt.

P[port]

Ein auf beiden Maschinen nicht verwendeter TCP-Port für die Nachrichten zu den Dispatcher-Überwachungssignalen. Der *Port* muss für die primäre und die Ausweichmaschine identisch sein.

delete

Entfernt diese Maschine aus der hohen Verfügbarkeit, diese Maschine kann daher nicht mehr als Partnermaschine oder als primäre Maschine benutzt werden.

reach

Hinzufügen oder Löschen der Zieladresse für den primären Dispatcher und den Ausweich-Dispatcher. Die Advisor-Funktion "reach" sendet *pings* vom primären und Ausweich-Dispatcher, um die Erreichbarkeit ihrer Ziele festzustellen.

Anmerkung: Wenn Sie das Ziel für "reach" konfigurieren, müssen Sie auch die Advisor-Funktion reach starten. Die Advisor-Funktion "reach" wird automatisch von der Manager-Funktion gestartet.

add

Fügt dem Erreichbarkeits-Advisor eine Zieladresse hinzu.

delete

Löscht eine Zieladresse aus dem Erreichbarkeits-Advisor.

Adresse

Die IP-Adresse (in Schreibweise mit Trennzeichen oder als symbolischer Name) des Zielknotens.

Maske

Eine Teilnetzmaske.

heartbeat

Definiert eine Übertragungssitzung zwischen der primären Dispatcher-Maschine und der Ausweichmaschine.

add

Teilt dem Quellen-Dispatcher die Adresse seines Partners (Zieladresse) mit.

Quellenadresse

Quellenadresse. Die Adresse (IP-Adresse oder symbolischer Name) dieser Dispatcher-Maschine.

Zieladresse

Zieladresse. Die Adresse (IP-Adresse oder symbolischer Name) der anderen Dispatcher-Maschine.

Anmerkung: Die Quellen- und die Zieladresse müssen für mindestens ein Überwachungssignalpaar die NFAs der Maschinen sein.

delete

Entfernet das Adressenpaar aus den Informationen zum Überwachungssignal. Sie können die Ziel- oder die Quellenadresse des Überwachungssignalpaares angeben.

Adresse

Die Adresse (IP-Adresse oder symbolischer Name); entweder die Ziel- oder die Quellenadresse.

takeover

Konfiguration mit einfacher Hochverfügbarkeit (Rolle der Dispatcher-Maschinen lautet entweder *primary* oder *backup*):

- Takeover weist einen Dispatcher in Bereitschaft an, aktiv zu werden und mit dem Weiterleiten von Paketen zu beginnen. Damit wird der gegenwärtig aktive Dispatcher in Bereitschaft versetzt. Der Befehl takeover muss auf der Maschine in Bereitschaft ausgegeben werden. Er wird nur ausgeführt, wenn die Strategie **manual** lautet. Der untergeordnete Status muss *synchronisiert* lauten.

Konfiguration mit beiderseitiger Hochverfügbarkeit (Rolle jeder Dispatcher-Maschine lautet *both*):

- Die Dispatcher-Maschine mit der Funktion der beiderseitigen Hochverfügbarkeit enthält zwei Cluster, die denen ihres Partners entsprechen. Einer der Cluster wird als primärer Cluster (Partner-Cluster der Partnermaschine) und der andere als Partner-Cluster (primärer Cluster der Partnermaschine) betrachtet. Takeover weist die Dispatcher-Maschine an, mit dem Weiterleiten von Paketen für den oder die Cluster der anderen Maschine zu beginnen. Der Befehl takeover kann nur ausgegeben werden, wenn der oder die Cluster der Dispatcher-Maschine den Status *Bereitschaft* haben und der untergeordnete Status *synchronisiert* lautet. Damit werden die gegenwärtig aktiven Cluster der Partnermaschine in den Bereitschaftsstatus geändert. Der Befehl takeover wird nur ausgeführt, wenn die Strategie **manual** lautet. Weitere Informationen befinden sich unter „Gegenseitige hohe Verfügbarkeit“ auf Seite 53.

Anmerkungen:

1. Beachten Sie, dass sich die *Rollen* der Maschinen (*primary*, *backup*, *both*) nicht ändern. Es ändert sich lediglich der relative *Status* (*Aktiv* oder *Bereitschaft*).
2. Es gibt drei mögliche takeover-*Scripts*: goActive, goStandby und goInOp. Lesen Sie hierzu die Informationen im Abschnitt „Scripts verwenden“ auf Seite 182.

Adresse

Der Wert für die Übernahmeadresse ist optional. Er sollte nur verwendet werden, wenn die Maschine die Rolle als *primäre Maschine und Partnermaschine* einnimmt (Konfiguration mit beiderseitiger Hochverfügbarkeit). Die angegebene Adresse ist die NFA der Dispatcher-Maschine, die normalerweise den Datenverkehr dieses Clusters weiterleitet. Erfolgt eine Übernahme beider Cluster, geben Sie die eigene NFA-Adresse des Dispatchers an.

Beispiele

- Geben Sie den folgenden Befehl ein, um den Hochverfügbarkeitsstatus einer Maschine zu überprüfen:

```
ndcontrol highavailability status
```

Ausgabe:

Hochverfügbarkeitsstatus:

```
-----  
Rolle ..... primary  
Wiederanlaufstrategie ..... manual  
Status ..... Aktiv  
Untergeordneter Status ..... Synchronisiert  
Primärer Host ..... 9.67.131.151  
Port ..... 12345  
Bevorzugtes Ziel ..... 9.67.134.223
```

Signalstatus:

```
-----  
Anzahl ..... 1
```

Erreichbark.-Status:

```
-----  
Anzahl ..... 1
```

- Hinzufügen der Sicherungsinformationen zur primären Maschine unter Verwendung der automatischen Wiederherstellungsstrategie und von Port 80:

```
ndcontrol highavailability backup add primary auto 80
```

- Geben Sie den folgenden Befehl ein, um eine Adresse hinzuzufügen, die der Dispatcher erreichen muss:

```
ndcontrol highavailability reach add 9.67.125.18
```

- Geben Sie die folgenden Befehle ein, um Überwachungssignalinformationen für die primäre Maschine und Partnermaschine hinzuzufügen:

```
Primäre Maschine - highavailability heartbeat add 9.67.111.3 9.67.186.8
```

```
Partnermaschine - highavailability heartbeat add 9.67.186.8 9.67.111.3
```

- Geben Sie den folgenden Befehl ein, wenn der Dispatcher in Bereitschaft angewiesen werden soll, aktiv zu werden, und die aktive Maschine in Bereitschaft versetzt werden soll:

```
ndcontrol highavailability takeover
```

ndcontrol host — Ferne Maschine konfigurieren

►►ndcontrol—host:—*ferner_Host*◄◄

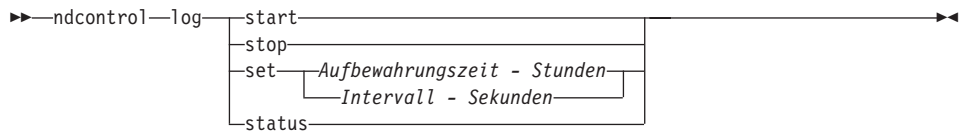
ferner_Host

Der Name der fernen Network Dispatcher-Maschine, die konfiguriert wird. Stellen Sie bei der Eingabe dieses Befehls sicher, dass sich zwischen **host:** und *ferner_Host* kein Leerzeichen befindet. Beispiel:

ndcontrol host:*ferner_Host*

Nachdem dieser Befehl in der Eingabeaufforderung ausgegeben wurde, geben Sie einen beliebigen gültigen Befehl ndcontrol ein, der für die ferne Network Dispatcher-Maschine ausgegeben werden soll.

ndcontrol log — Binäre Protokolldatei steuern



start

Binäres Protokoll starten.

stop

Binäres Protokoll stoppen.

set

Legt Felder für die binäre Protokollierung fest. Weitere Informationen zum Festlegen von Feldern für die binäre Protokollierung finden Sie im Abschnitt „Binäres Protokollieren verwenden, um Serverstatistiken zu analysieren“ auf Seite 213.

Aufbewahrung

Die Anzahl der Stunden, die binäre Protokolldateien aufbewahrt werden. Der Standardwert für retention ist 24.

Stunden

Die Anzahl der Stunden.

interval

Die Anzahl der Sekunden zwischen dem Protokollieren von Einträgen. Der Standardwert für interval ist 60.

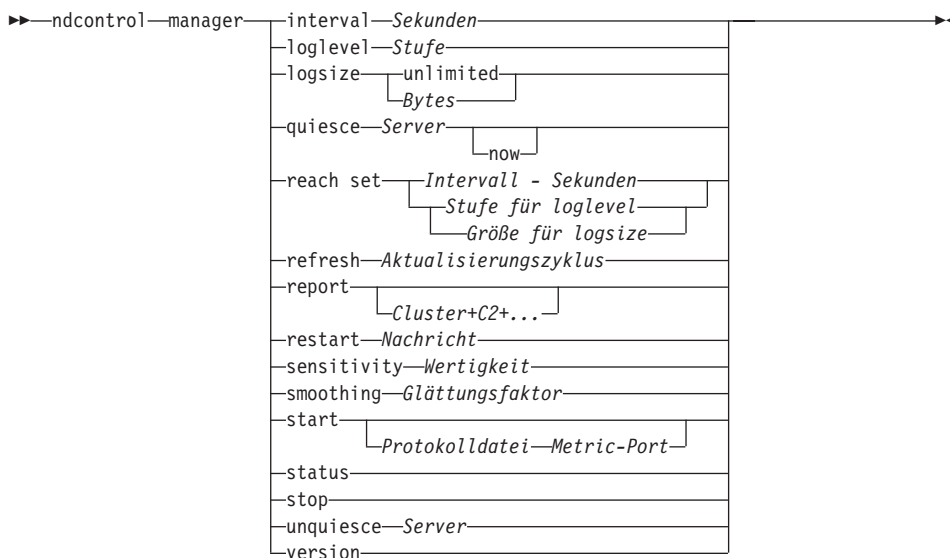
Sekunden

Die Anzahl der Sekunden.

status

Zeigt die Verweildauer und das Intervall des binären Protokolls.

ndcontrol manager — Manager steuern



interval

Legt fest, wie oft der Manager die Wertigkeit der Server für den Executor aktualisiert. Dabei werden die Kriterien aktualisiert, die der Executor für die Weiterleitung von Client-Anforderungen verwendet.

Sekunden

Eine positive Zahl, die in Sekunden darstellt, wie oft der Manager Wertigkeiten für den Executor aktualisiert. Der Standardwert ist 2.

loglevel

Festlegen der Protokollstufe für das Manager-Protokoll und das Protokoll des Messwertüberwachungsprogramms.

Stufe

Die Nummer der Stufe (0 bis 5). Je größer die Zahl, desto mehr Informationen werden in das Manager-Protokoll geschrieben. Der Standardwert ist 1. Die folgenden Werte sind gültig: 0 für keine Einträge, 1 für eine minimale Protokollierung, 2 für eine Basisprotokollierung, 3 für eine normale, 4 für eine erweiterte und 5 für eine ausführliche Protokollierung.

logsize

Legt die maximale Größe des Protokolls des Managers fest. Wenn Sie eine maximale Größe für die Protokolldatei festlegen, findet ein Dateiumbruch statt. Hat die Datei die angegebene Größe erreicht, werden alle weiteren Einträge wieder an den Anfang der Datei geschrieben und die dort befindlichen Einträge überschrieben. Die Protokollgröße kann nicht auf

einen geringeren Wert als die aktuelle Dateigröße gesetzt werden. Protokolleinträge werden mit einer Zeitmarke versehen, damit Sie erkennen können, in welcher Reihenfolge die Einträge geschrieben wurden. Je höher Sie die Protokollstufe setzen, desto vorsichtiger müssen Sie die Protokollgröße auswählen, da die Protokolldatei sehr schnell voll ist, wenn Sie eine Protokollierung auf einer höheren Stufe wählen.

Byte

Die maximale Größe in Byte für die Protokolldatei des Managers. Sie können entweder eine positive Zahl, die größer als 0 sein muss, oder das Wort **unlimited** (unbegrenzt) angeben. Möglicherweise erreicht die Protokolldatei nicht genau die maximale Größe, bevor der Dateiumbruch stattfindet, da die Größe der Protokolleinträge variiert. Der Standardwert ist 1 MB.

quiesce

Es werden keine weiteren Verbindungen an einen Server gesendet. Hier-von ausgenommen sind nur nachfolgende neue Verbindungen vom Client zum stillgelegten Server, sofern diese als "sticky" markiert sind und die Haltezeit (stickytime) nicht abgelaufen ist. Der Manager setzt die Wertigkeit für diesen Server an jedem Port, für den er definiert ist, auf 0. Diesen Befehl verwenden, wenn auf einem Server eine schnelle Wartung erfolgen soll und der Server anschließend wieder aktiviert werden soll. Wenn Sie einen stillgelegten Server aus der Konfiguration löschen und ihn der Konfiguration anschließend wieder hinzufügen, behält er nicht seinen Status, den er vor der Stilllegung hatte. Weitere Informationen hierzu finden Sie im Abschnitt „Stilllegung gehaltener Verbindungen“ auf Seite 206.

Server

Die IP-Adresse des Servers als symbolischer Name oder in Schreibweise mit Trennzeichen.

Wenn Sie die Serverpartitionierung verwenden, geben Sie den eindeutigen Namen des logischen Servers an. Weitere Informationen hierzu finden Sie im Abschnitt „Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)“ auf Seite 163.

now

Verwenden Sie quiesce "now" nur, wenn Sie die Haltezeit definiert haben und vor Ablauf der Haltezeit neue Verbindungen an einen anderen als den stillgelegten Server gesendet werden sollen. Weitere Informationen hierzu finden Sie im Abschnitt „Stilllegung gehaltener Verbindungen“ auf Seite 206.

reach set

Legt das Intervall, die Protokollstufe und die Protokollgröße für den Erreichbarkeits-Advisor fest.

refresh

Legt die Anzahl von Intervallen fest, nach denen der Manager die Informationen über neue und aktive Verbindungen für den Executor aktualisiert.

Aktualisierungszyklus

Eine positive Zahl, die die Anzahl von Intervallen darstellt. Der Standardwert ist 2.

report

Zeigt eine statistische Momentaufnahme an.

Cluster

Die Adresse des Clusters, die im Bericht angezeigt werden soll. Die Adresse kann ein symbolischer Name oder eine Adresse in Schreibweise mit Trennzeichen sein. Der Standardwert ist ein Manager-Bericht, in dem alle Cluster angezeigt werden.

Anmerkung: Zusätzliche Cluster werden durch ein Pluszeichen (+) getrennt.

restart

Startet alle Server (die nicht inaktiv sind) mit der Standardwertigkeit (1/2 der maximalen Wertigkeit).

Nachricht

Eine Nachricht, die in die Protokolldatei des Managers gestellt werden soll.

sensitivity

Legt die Mindestsensitivität für die Aktualisierung von Wertigkeiten fest. Diese Einstellung definiert, wann der Manager seine Serverwertigkeit ausgehend von externen Informationen ändern sollte.

Wertigkeit

Eine Zahl von 1 bis 100, die als prozentuale Wertigkeit verwendet werden soll. Der Standardwert 5 bewirkt eine Mindestsensitivität von 5 %.

smoothing

Festlegen eines Faktors, der Wertigkeitsabweichungen während des Lastausgleichs glättet. Ein höherer Glättungsfaktor führt zu einer weniger drastischen Änderung von Serverwertigkeiten bei Änderungen an den Netzdingungen. Ein geringerer Glättungsfaktor führt zu einer drastischen Änderung von Serverwertigkeiten.

Faktor

Eine positive Gleitkommazahl. Der Standardwert ist 1,5.

start

Den Manager starten.

Protokolldatei

Der Name der Datei, in der die Daten des Managers protokolliert werden. Jeder Eintrag im Protokoll wird mit einer Zeitmarke versehen.

Die Standarddatei wird in dem Verzeichnis **logs** installiert. Lesen Sie hierzu die Informationen in „Anhang F. Beispielkonfigurationsdateien“ auf Seite 393. Wollen Sie das Verzeichnis ändern, in dem die Protokolldateien gespeichert werden, lesen Sie die Informationen unter „Pfade für die Protokolldatei ändern“ auf Seite 222.

Metric-Port

Der von Metric Server für Meldungen zur Systembelastung verwendete Port. Wenn Sie einen Metric-Port angeben, müssen Sie auch einen Protokolldateinamen angeben. Der Standard-Metric-Port ist 10004.

status

Zeigt den aktuellen Status aller Werte in dem Manager an, die global gesetzt werden können. Zudem werden die Standardwerte dieser Werte angezeigt.

stop

Den Manager stoppen.

unquiesce

Festlegung, dass der Manager einem zuvor stillgelegten Server an jedem Port, für den er definiert ist, eine Wertigkeit größer als null zuordnen kann.

Server

Die IP-Adresse des Servers als symbolischer Name oder in Schreibweise mit Trennzeichen.

version

Zeigt die aktuelle Version des Managers an.

Beispiele

- Geben Sie den folgenden Befehl ein, um das Aktualisierungsintervall für den Manager auf 5 Sekunden zu setzen:
`ndcontrol manager interval 5`
- Geben Sie den folgenden Befehl ein, um die Stufe der Protokollierung zwecks Verbesserung der Leistung auf 0 zu setzen:
`ndcontrol manager loglevel 0`
- Geben Sie den folgenden Befehl ein, um die Größe des Protokolls des Managers auf 1.000.000 Byte zu setzen:
`ndcontrol manager logsize 1000000`
- Geben Sie den folgenden Befehl ein, um anzugeben, dass keine Verbindungen mehr an den Server an 130.40.52.153 gesendet werden sollen:
`ndcontrol manager quiesce 130.40.52.153`

- Setzen der Anzahl Aktualisierungsintervalle auf 3, bevor die Wertigkeiten aktualisiert werden:
ndcontrol manager refresh 3
- Geben Sie den folgenden Befehl ein, um eine statistische Momentaufnahme des Managers abzurufen:
ndcontrol manager report

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

HOST-TAB.VERZEI.	STATUS
9.67.129.221	AKTIV
9.67.129.213	AKTIV
9.67.134.223	AKTIV

9.67.131.18	GEWICHT		AKTIV % 48		NEU % 48		PORT % 4		SYSTEM % 0	
PORT: 80	DERZ	NEU	GW	VERBIND	GW	VERBIND	GW	LAST	GW	LAST
9.67.129.221	8	8	10	0	10	0	7	29	0	0
9.67.134.223	11	11	10	0	10	0	12	17	0	0
PORT GESAMT	19	19		0		0		46		0

9.67.131.18	GEWICHT			AKTIV % 48			NEU % 48			PORT % 4			SYSTEM % 0		
PORT: 23	DERZ	NEU	GW	VERBIND	GW	VERBIND		GW		LAST		GW		LAST	
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 GESAMT	10	10		0		0		70						0	

ADVISOR	PORT	ZEITLIMIT
reach	0	unlimited
http	80	unlimited
ftp	21	unlimited

- Neustart aller Server mit Standardwertigkeiten und Schreiben einer Nachricht in die Manager-Protokolldatei:

`ndcontrol manager restart` Neustart des Managers für Code-Aktualisierung

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

320-14:04:54 Neustart des Managers für Code-Aktualisierung

- Festlegen einer Sensitivität für Wertigkeitsänderungen von 10:
- Geben Sie den folgenden Befehl ein, um den Glättungsfaktor auf 2,0 zu setzen:

`ndcontrol manager sensitivity 10`

`ndcontrol manager smoothing 2,0`

- Geben Sie den folgenden Befehl ein, um den Manager zu starten und die Protokolldatei `ndmgr.log` anzugeben (Pfade können nicht angegeben werden):

`ndcontrol manager start ndmgr.log`

- Geben Sie den folgenden Befehl ein, um den aktuellen Status der Werte anzuzeigen, die dem Manager zugeordnet sind:

`ndcontrol manager status`

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

Manager-Status:

=====

Port für Metrik	10.004
Name der Managerprotokolldatei	manager.log
Managerprotokollstufe	1
Max. Managerprotokollgröße (Bytes)	unlimited
Sensitivitätsstufe	0,05
Glättungsfaktor	1,5
Aktualisierungsintervall (Sekunden)	2
Gewichtungsaktualisierungszyklus	2
Erreichbarkeit - Protokollstufe	1
Erreichbarkeit - Max. Protokollgröße (Bytes)	unlimited
Erreichbarkeit - Aktualisierungsintervall (Sekunden) ...	7

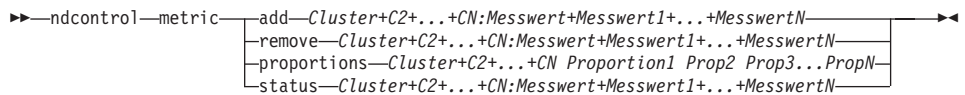
- Stoppen des Managers:
- Festlegung, dass keine neuen Verbindungen an einen Server mit der Adresse 130.40.52.153 gesendet werden sollen (Anmerkung: Verwenden Sie zum Stilllegen des Servers nur die Option "now", wenn Sie die Haltezeit festgelegt haben und neue Verbindungen bis zum Ablauf der Haltezeit an einen anderen Server gesendet werden sollen):

`ndcontrol manager stop`

`ndcontrol manager quiesce 130.40.52.153 now`

- Festlegung, dass keine neuen Verbindungen an einen Server mit der Adresse 130.40.52.153 gesendet werden sollen (Anmerkung: Wenn Sie die Haltezeit definiert haben, werden nachfolgende neue Verbindungen vom Client bis zum Ablauf der Haltezeit an diesen Server gesendet):
`ndcontrol manager quiesce 130.40.52.153`
- Festlegung, dass der Manager einem zuvor stillgelegten Server im Cluster 130.40.52.153 eine Wertigkeit größer als 0 zuordnen kann:
`ndcontrol manager unquiesce 130.40.52.153`
- Geben Sie den folgenden Befehl ein, um die aktuelle Versionsnummer des Managers aufzurufen:
`ndcontrol manager version`

ndcontrol metric — Systemmesswerte konfigurieren



add

Hinzufügen des angegebenen Messwerts.

Cluster

Die Adresse, zu der die Clients eine Verbindung herstellen. Die Adresse kann der Host-Name der Maschine oder die IP-Adresse in Schreibweise mit Trennzeichen sein. Zusätzliche Cluster werden durch ein Pluszeichen (+) getrennt.

Anmerkung: Bei Cisco Consultant entspricht die Cluster-Adresse der virtuellen IP-Adresse (VIP-Adresse) in der content-Regel des Eigners in der Konfiguration des Cisco CSS Switch.

Messwert

Name des Systemmesswerts. Es muss sich um den Namen einer ausführbaren Datei oder Script-Datei im Verzeichnis des Messwertservers handeln.

remove

Entfernen des angegebenen Messwerts.

proportions

Festlegen der Proportionen für alle diesem Objekt zugeordneten Messwerte.

status

Anzeigen des aktuellen Messwertes.

Beispiele

- Hinzufügen eines Systemmesswerts:
`sscontrol metric add Site1:Messwert1`
- Festlegen der Proportionen für einen Sitenamen mit zwei Systemmesswerten:
`sscontrol metric proportions Site1 0 100`

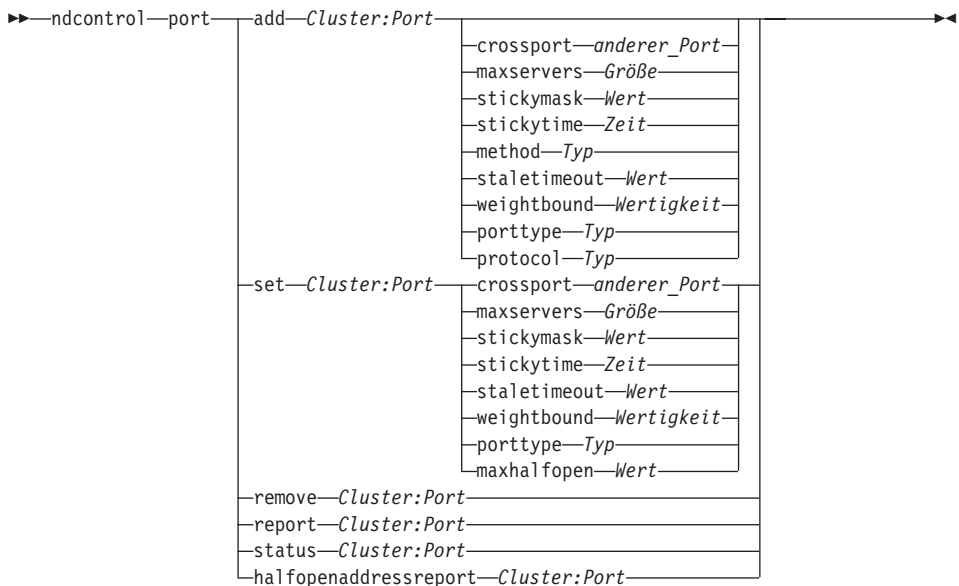
- Anzeigen des aktuellen Status der zugeordneten Messwerte:
`sscontrol metric status Site1:Messwert1`

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

Metrikstatus:

```
Cluster ..... 10.10.10.20
Metrikname ..... Messwert1
Metrikproportion ..... 50
  Server ..... plm3
    Metrikdaten ..... -1
```

ndcontrol port — Ports konfigurieren



add

Hinzufügen eines Ports zu einem Cluster. Sie müssen einen Port zu einem Cluster hinzufügen, bevor Sie Server zu diesem Port hinzufügen können. Sind keine Ports für einen Cluster vorhanden, werden alle Client-Anforderungen lokal verarbeitet. Mit diesem Befehl können Sie mehrere Ports auf einmal hinzufügen.

Anmerkung: Bei der Komponente Mailbox Locator von Network Dispatcher müssen Sie auf der Maschine einen Aliasnamen für die IP-Adresse festgelegt haben, bevor Sie einen Port hinzufügen. Der Befehl **add port** versucht, einen Java Proxy zu starten, der an den Cluster gebunden wird. Deshalb muss die IP-Adresse im IP-Stack vorhanden sein.

Unter Windows muss die Adresse in der Windows-Netzwerkconfiguration enthalten sein. Der Befehl **cluster configure** reicht nicht aus, weil er die Aliasnamensumsetzung nur simuliert und der Proxy nicht an diese simulierte IP-Adresse gebunden werden kann. Für alle anderen Betriebssysteme ist der Befehl **cluster configure** ausreichend, weil er die IP-Adresse mit `ifconfig` in einen Aliasnamen umsetzt.

Cluster

Die Adresse des Clusters als symbolischer Name oder in Schreibweise mit Trennzeichen. Sie können einen Doppelpunkt (:) als Platzhalter verwenden. Der Befehl `ndcontrol port add :80` bewirkt beispielsweise, dass Port 80 zu allen Clustern hinzugefügt wird.

Anmerkung: Zusätzliche Cluster werden durch ein Pluszeichen (+) getrennt.

Port

Nummer des Ports. Mit der Port-Nummer 0 (null) kann ein Platzhalter-Port angegeben werden.

Anmerkung: Weitere Ports werden durch ein Pluszeichen (+) getrennt angegeben.

crossport

Mit "crossport" können Sie die Affinität (Merkmal "sticky") auf mehrere Ports ausdehnen, so dass künftige Anforderungen von Clients, deren Anforderungen an verschiedenen Ports empfangen werden, dennoch an einen Server gesendet werden können. Geben Sie als Wert für crossport die Nummer des *anderen Ports* an, der in die Port-übergreifende Affinität einbezogen werden soll. Die Ports müssen die folgenden Bedingungen erfüllen, um diese Funktion verwenden zu können:

- Sie müssen dieselbe Cluster-Adresse gemeinsam benutzen.
- Sie müssen dieselben Server gemeinsam benutzen.
- Sie müssen denselben Wert (ungleich Null) für stickyttime haben.
- Sie müssen denselben Wert für stickymask haben.

Wenn Sie die Port-übergreifende Affinität aufheben möchten, setzen Sie den Wert für crossport auf seine eigene Port-Nummer zurück. Weitere Informationen zur Port-übergreifenden Affinität finden Sie im Abschnitt „Port-übergreifende Affinität“ auf Seite 204.

Anmerkung: Der Parameter "crossport" gilt nur für die Dispatcher-Komponente.

anderer_Port

Der Wert von crossport. Der Standardwert entspricht der eigenen Port-Nummer.

maxservers

Die maximale Anzahl von Servern. Der Standardwert für maxservers ist 32.

Größe

Der Wert für maxservers.

stickymask

Mit der Affinitätsadressmaske werden eingehende Client-Anforderungen auf der Basis gemeinsamer Teilnetzadressen zusammengefasst. Wenn eine Client-Anforderung eine Verbindung zu dem Port hergestellt hat, werden alle nachfolgenden Anforderungen von Clients mit derselben (durch den maskierten Abschnitt der IP-Adresse angegebenen) Teilnetzadresse an denselben Server übertragen. Weitere Informationen befinden sich unter „Affinitätsadressmaske“ auf Seite 204.

Anmerkung: Das Schlüsselwort stickymask gilt nur für die Dispatcher-Komponente.

Wert

Der Wert für stickymask ist die Anzahl der höherwertigen Bits der 32-Bit-IP-Adresse, die maskiert werden sollen. Gültige Werte sind: 8, 16, 24 und 32. Der Standardwert ist 32. Damit wird die Funktion der Affinitätsadressmaske inaktiviert.

stickytime

Das Intervall zwischen dem Schließen einer Verbindung und dem Öffnen einer neuen Verbindung, während dem ein Client an denselben Server zurückgesendet wird, der während der ersten Verbindung verwendet wurde. Nach Ablauf der Haltezeit kann der Client an einen anderen Server gesendet werden.

Für die Dispatcher-Komponente:

- Für die Dispatcher-Weiterleitungsmethode cbr
 - Wenn Sie die Haltezeit (stickytime) für den Port auf einen Wert ungleich null setzen, muss der Affinitätstyp der Regel auf den Standard (none) gesetzt sein. Die regelbasierte Affinität (passive Cookie-Affinität und URI-Affinität) kann nicht gleichzeitig festgelegt werden, wenn die Haltezeit für den Port gesetzt ist.
 - Da das Festlegen einer Haltezeit die Affinität von SSL-IDs aktiviert, können Sie für diesen Port keine content-Regel hinzufügen.
- Für die Dispatcher-Weiterleitungsmethoden mac und nat
 - Wenn Sie die Haltezeit (stickytime) für den Port auf einen Wert ungleich null setzen, können Sie in der Regel keinen Affinitätstyp festlegen. Die regelbasierte Affinität kann nicht gleichzeitig festgelegt werden, wenn die Haltezeit für den Port gesetzt ist.
 - Das Festlegen einer Haltezeit aktiviert die Affinität der IP-Adressen.
- Der Parameter "stickytime" sollte bei Verwendung der SDA-API (Server Directed Affinity) auf 1 gesetzt werden.

Für die CBR-Komponente: Wenn Sie die Haltezeit (stickytime) für den Port auf einen Wert ungleich null setzen, muss der Affinitätstyp der Regel auf den Standard (none) gesetzt sein. Die regelbasierte Affinität (passive

Cookie-Affinität, URI-Affinität, aktive Cookie-Affinität) kann nicht gleichzeitig festgelegt werden, wenn die Haltezeit für den Port gesetzt ist.

Zeit

Die Zeit in Sekunden für die Weiterleitung der Anforderungen eines Clients an denselben Server. Null gibt an, dass die Anforderungen eines Clients nicht an denselben Server weitergeleitet werden.

method

Weiterleitungsmethode. Es gibt die MAC-Weiterleitung, die NAT/NAPT-Weiterleitung und die inhaltsabhängige Weiterleitung. Die NAT/NAPT-Weiterleitungsmethode oder die inhaltsabhängige Weiterleitung können Sie *erst* hinzufügen, nachdem Sie mit dem Parameter "clientgateway" des Befehls "ndcontrol executor" eine IP-Adresse ungleich null angegeben haben. Weitere Informationen hierzu finden Sie in „NAT/NAPT-Weiterleitungsmethode (nat) des Dispatchers“ auf Seite 55 und „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)“ auf Seite 57.

Anmerkung: Wenn sich der Back-End-Server im selben Teilnetz wie die Rückkehradresse befindet und Sie die inhaltsabhängige Weiterleitung oder die NAT/NAPT-Weiterleitungsmethode verwenden, müssen Sie als Router-Adresse die Adresse des Back-End-Servers definieren.

Typ

Der Typ der Weiterleitungsmethode. Mögliche Werte sind mac, nat oder cbr. Der Standardwert ist mac (MAC-Weiterleitung).

staletimeout

Die Zeit der Inaktivität einer Verbindung in Sekunden, bevor die Verbindung entfernt wird. Für die Dispatcher- oder CBR-Komponente lautet der Standardwert 900 für Port 21 (FTP) und 32.000.000 für 23 (Telnet). Für alle anderen Ports ist der Standardwert 300. Das Inaktivitätszeitlimit kann auch auf Executor- oder Cluster-Ebene gesetzt werden. Weitere Informationen befinden sich unter „Inaktivitätszeitlimit verwenden“ auf Seite 223.

Anmerkung: Bei Mailbox Locator entspricht "staletimeout" dem Inaktivitätszeitlimit für automatische Abmeldung für diese Protokolle. Der Parameter "staletimeout" für Mailbox Locator hat standardmäßig den Wert 60 und setzt die Inaktivitätszeitlimits für POP3 und IMAP außer Kraft. Weitere Informationen zum Parameter "staletimeout" für Mailbox Locator finden Sie im Abschnitt „Inaktivitätszeitgeber für POP3/IMAP überschreiben“ auf Seite 104.

Wert

Der Wert für **staletimeout** in Sekunden.

weightbound

Legt die maximale Wertigkeit von Servern an diesem Port fest. Mit diesem Wert wird die Differenz festgelegt, die hinsichtlich der Anzahl der Anforderungen, die der Executor den einzelnen Servern zuordnet, gelten soll. Der Standardwert ist 20.

Wertigkeit

Eine Zahl von 1 bis 100 für die maximale Wertigkeitsgrenze.

porttype

Der Port-Typ.

Anmerkung: Der Parameter "porttype" gilt nur für Dispatcher.

Typ

Gültige Werte sind **tcp**, **udp** und **both**. Der Standardwert ist "both" (tcp/udp).

protocol

Der Typ des Weiterleitungsprotokolls (POP3 oder IMAP). Der Parameter "protocol" ist erforderlich, wenn ein Port für Mailbox Locator hinzugefügt wird.

Anmerkung: Der Parameter "protocol" gilt nur für Mailbox Locator.

Typ

Gültige Werte sind **POP3** und **IMAP**.

maxhalfopen

Der Schwellenwert für das Maximum halboffener Verbindungen. Verwenden Sie diesen Parameter, um mögliche DoS-Attacken festzustellen, die eine große Anzahl halboffener TCP-Verbindungen auf Servern nach sich ziehen.

Ein positiver Wert gibt an, dass überprüft wird, ob die aktuelle Anzahl halboffener Verbindungen den Schwellenwert überschreitet. Wenn der aktuelle Wert über dem Schwellenwert liegt, wird ein Alert-Script aufgerufen. Weitere Informationen finden Sie im Abschnitt „Erkennung von DoS-Attacken“ auf Seite 211.

Anmerkung: Der Parameter "maxhalfopen" gilt nur für Dispatcher.

Wert

Der Wert für "maxhalfopen". Der Standardwert ist null (es findet keine Überprüfung statt).

set

Die Felder eines Ports festlegen.

remove

Entfernen dieses Ports.

report

Bericht zu diesem Port.

status

Anzeigen des Status für den Server an diesem Port. Wenn Sie den Status für alle Ports sehen möchten, geben Sie diesen Befehl ohne *Port* an. Vergessen Sie jedoch nicht den Doppelpunkt.

Sekunden

Die Zeit in Sekunden, nach der halboffene Verbindungen zurückgesetzt werden.

halfopenaddressreport

Generiert für alle Client-Adressen (bis zu 8000 Adresspaare), deren Serverzugriff halboffene Verbindungen zur Folge hatten, Einträge im Protokoll (halfOpen.log). Außerdem werden statistische Daten an die Befehlszeile zurückgegeben. Dazu gehören unter anderem die Gesamtzahl, die größte Anzahl und die durchschnittliche Anzahl halboffener Verbindungen sowie die durchschnittliche Dauer halboffener Verbindungen (in Sekunden). Weitere Informationen hierzu finden Sie im Abschnitt „Erkennung von DoS-Attacken“ auf Seite 211.

Beispiele

- Geben Sie den folgenden Befehl ein, um die Ports 80 und 23 zur Cluster-Adresse 130.40.52.153 hinzuzufügen:
`ndcontrol port add 130.40.52.153:80+23`
- Geben Sie den folgenden Befehl ein, um einen Platzhalter-Port zur Cluster-Adresse 130.40.52.153 hinzuzufügen:
`ndcontrol port set 130.40.52.153:0`
- Für Mailbox Locator: Hinzufügen von Port 20 für das Protokoll POP3 zur Cluster-Adresse 9.37.60.91:
`mlcontrol port add 9.37.60.91:20 protocol pop3`
- Festlegen einer maximalen Wertigkeit von 10 für Port 80 an der Cluster-Adresse 130.40.52.153:
`ndcontrol port set 130.40.52.153:80 weightbound 10`
- Geben Sie den folgenden Befehl ein, um den Wert für stickyttime für die Ports 80 und 23 der Cluster-Adresse 130.40.52.153 auf 60 Sekunden zu setzen:
`ndcontrol port set 130.40.52.153:80+23 stickyttime 60`
- Geben Sie den folgenden Befehl ein, um die Port-übergreifende Affinität von Port 80 zu Port 23 für die Cluster-Adresse 130.40.52.153 zu setzen:
`ndcontrol port set 130.40.52.153:80 crossport 23`
- Entfernen von Port 23 aus dem Cluster mit der Adresse 130.40.52.153:
`ndcontrol port remove 130.40.52.153:23`

- Abrufen des Status für Port 80 an der Cluster-Adresse 9.67.131.153:
ndcontrol port status 9.67.131.153:80

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Port-Status:

```
-----
Port-Nummer ..... 80
Cluster-Adresse ..... 9.67.131.153
Anzahl Server ..... 2
Zeitlimit für Inaktivität ..... 30
Gewichtungsgrenze ..... 20
Max. Anzahl Server ..... 32
Haltezeit ..... 0
Port-Typ ..... tcp/udp
Weiterleitungsmethode..... MAC-gestützte Weiterleitung
StickyBits der Maske ..... 32
Port-übergreifende Affinität ... 80
Max. Anz. halb geöffneter Verb. 0
```

- Abrufen des Berichts zu Adressen mit halboffenen Verbindungen für Port 80 an der Cluster-Adresse 9.67.127.121:
ndcontrol port halfopenaddressreport 9.67.127.121:80

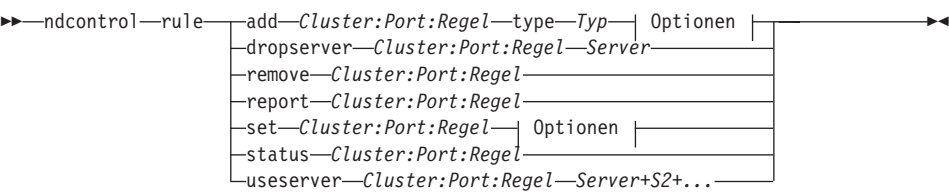
Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Bericht zu halboffenen Verbindungen wurde erfolgreich erstellt.

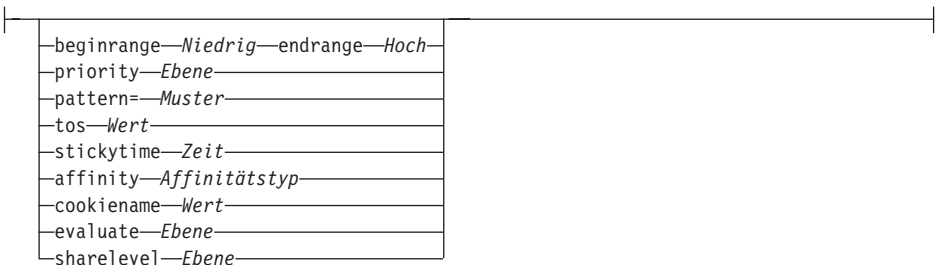
```
Adressenbericht zu halb geöffneten Verbindungen für Cluster:
Port = 9.67.127.121:80
Summe Adressen mit halb geöffneten Verbindungen ..... 0
Gesamtanzahl halb geöffneten Verbindungen ..... 0
Größte Anzahl halb geöffneten Verbindungen ..... 0
Durchschnittliche Zahl halb geöffneten Verbindungen ... 0
Durchschnittl. Zeit für halb geöffnete Verb. (Sek.) ... 0
Summe empfangener halb geöffneten Verbindungen ..... 0
```

ndcontrol rule — Regeln konfigurieren

Anmerkung: Die Syntaxdiagramme für den Befehl "rule" gelten nicht für Mailbox Locator.



Optionen:



add
Diese Regel zu einem Port hinzufügen.

Cluster
Die Adresse des Clusters als symbolischer Name oder in Schreibweise mit Trennzeichen. Sie können einen Doppelpunkt (:) als Platzhalter verwenden. Der Befehl `ndcontrol rule add :80:RegelA type Typ` bewirkt beispielsweise, dass RegelA für alle Cluster zu Port 80 hinzugefügt wird.

Anmerkung: Zusätzliche Cluster werden durch ein Pluszeichen (+) getrennt.

Port
Nummer des Ports. Sie können einen Doppelpunkt (:) als Platzhalter verwenden. Der Befehl `ndcontrol rule add ClusterA::RegelA type Typ` bewirkt beispielsweise, dass RegelA zu allen Ports für ClusterA hinzugefügt wird.

Anmerkung: Weitere Ports werden werden durch ein Pluszeichen (+) getrennt angegeben.

Regel

Der für die Regel ausgewählte Name. Dieser Name kann eine beliebige Kombination aus alphanumerischen Zeichen, Unterstreichungszeichen, Silbentrennungsstrichen und Punkten sein. Der Name kann 1 bis 20 Zeichen lang sein und darf keine Leerzeichen enthalten.

Anmerkung: Zusätzliche Regeln werden durch ein Pluszeichen (+) getrennt.

type

Die Art der Regel.

Typ

Die Auswahlmöglichkeiten für *Typ* sind:

ip Die Regel basiert auf der Client-IP-Adresse.

Zeit Die Regel basiert auf der Uhrzeit.

Verbindung

Die Regel basiert auf der Anzahl der Verbindungen pro Sekunde für den Port. Diese Regel kann nur verwendet werden, wenn der Manager aktiv ist.

aktiv Die Regel basiert auf der Gesamtzahl der aktiven Verbindungen für den Port. Diese Regel kann nur verwendet werden, wenn der Manager aktiv ist.

port Die Regel basiert auf dem Client-Port.

Anmerkung: Der Parameter "port" gilt nicht für CBR.

Service

Diese Regel basiert auf dem Feld für die Service-Art (Type of Service = TOS) im IP-Header.

Anmerkung: Service gilt nur für die Dispatcher-Komponente.

reservedbandwidth

Diese Regel basiert auf der Bandbreite (in Kilobytes pro Sekunde), die von einer Servergruppe bereitgestellt wird. Weitere Informationen finden Sie unter „Regeln auf der Basis der reservierten und gemeinsam benutzten Bandbreite verwenden“ auf Seite 190 und „Regel "Reservierte Bandbreite"“ auf Seite 192.

Anmerkung: Der Parameter "reservedbandwidth" gilt nur für die Dispatcher-Komponente.

sharedbandwidth

Diese Regel basiert auf der Bandbreite (in Kilobytes pro Sekunde), die auf Executor- oder Cluster-Ebene gemeinsam genutzt wird.

Weitere Informationen finden Sie unter „Regeln auf der Basis der reservierten und gemeinsam benutzten Bandbreite verwenden“ auf Seite 190 und „Regel "Gemeinsame Bandbreite"“ auf Seite 192.

Anmerkung: Der Parameter "sharedbandwidth" gilt nur für die Dispatcher-Komponente.

true Diese Regel ist immer wahr. Sie kann mit der Anweisung ELSE in der Programmierlogik verglichen werden.

Inhalt Diese Regel beschreibt einen regulären Ausdruck, der mit den URLs verglichen wird, die vom Client angefordert werden. Dies gilt für Dispatcher und CBR.

beginrange

Der untere Wert des Bereichs, mit dem bestimmt wird, ob die Regel wahr ist oder nicht.

Niedrig

Hängt von der Art der Regel ab. Die Art des Werts und der Standardwert werden nachfolgend nach der Art der Regel aufgelistet:

ip Die Adresse des Clients als symbolischer Name oder in Schreibweise mit Trennzeichen. Der Standardwert ist 0.0.0.0.

Zeit Eine ganze Zahl. Der Standardwert ist 0. Er stellt Mitternacht dar.

Verbindung

Eine ganze Zahl. Der Standardwert ist 0.

aktiv Eine ganze Zahl. Der Standardwert ist 0.

Port Eine ganze Zahl. Der Standardwert ist 0.

Reservierte Bandbreite

Eine ganze Zahl (Kilobytes pro Sekunde). Der Standardwert ist 0.

endrange

Der obere Wert des Bereichs, mit dem bestimmt wird, ob die Regel wahr ist oder nicht.

Hoch

Hängt von der Art der Regel ab. Die Art des Werts und der Standardwert werden nachfolgend nach der Art der Regel aufgelistet:

ip Die Adresse des Clients als symbolischer Name oder in Schreibweise mit Trennzeichen. Der Standardwert ist 255.255.255.254.

Zeit Eine ganze Zahl. Der Standardwert ist 24. Er stellt Mitternacht dar.

Anmerkung: Beim Definieren des Anfangsbereichs (beginrange) und Endbereichs (endrange) der Zeitintervalle ist darauf zu achten, dass jeder Wert eine ganze Zahl sein muss, die nur den Stundenteil der Uhrzeit darstellt. Es werden keine Teilwerte einer Stunde angegeben. Soll beispielsweise die Stunde von 3 Uhr bis 4 Uhr angegeben werden, geben Sie für beginrange 3 und für endrange ebenfalls 3 an. Damit werden alle Minuten von 3 Uhr bis 3 Uhr 59 angegeben. Wird für beginrange 3 und für endrange 4 angegeben, wird die zweistündige Periode von 3 Uhr bis 4 Uhr 59 angegeben.

Verbindung

Eine ganze Zahl. Der Standardwert ist 2 hoch 32 minus 1.

aktiv

Eine ganze Zahl. Der Standardwert ist 2 hoch 32 minus 1.

Port

Eine ganze Zahl. Der Standardwert ist 65535.

Reservierte Bandbreite

Eine ganze Zahl (Kilobytes pro Sekunde). Der Standardwert ist 2 hoch 32 minus 1.

Priorität

Die Reihenfolge, in der die Regeln überprüft werden.

Ebene

Eine ganze Zahl. Wird die Priorität der ersten hinzugefügten Regel nicht angegeben, wird sie vom Dispatcher standardmäßig auf 1 gesetzt. Wird eine nachfolgende Regel hinzugefügt, wird ihre Priorität standardmäßig als 10 + der derzeit niedrigsten Priorität aller vorhandenen Regeln berechnet. Angenommen, es ist eine Regel mit der Priorität 30 vorhanden. Sie fügen eine neue Regel hinzu und setzen ihre Priorität auf 25 (die, wie Sie wissen, eine *höhere* Priorität als 30 ist). Anschließend fügen Sie eine dritte Regel ohne Angabe einer Priorität hinzu. Die Priorität der dritten Regel wird wie folgt berechnet: 40 (30 + 10).

pattern

Gibt das Muster an, das für eine Regel der des Typs "content" verwendet werden soll.

Muster

Das zu verwendende Muster. Weitere Informationen zu gültigen Werten finden Sie in „Anhang C. Syntax der content-Regel“ auf Seite 331.

tos

Gibt den Wert für "Type of Service" (TOS) an, der für die Regel der Art **Service** verwendet wird.

Anmerkung: TOS gilt nur für die Dispatcher-Komponente.

Wert

Die aus 8 Zeichen bestehende Zeichenfolge, die für den tos-Wert verwendet werden soll. Gültige Zeichen sind: 0 (binäre Null), 1 (binäre Eins) und x (beliebig). Beispiel: 0xx1010x. Weitere Informationen hierzu finden Sie im Abschnitt „Regeln verwenden, die auf der Service-Art (Type of Service = TOS) basieren“ auf Seite 190.

stickytime

Gibt die für eine Regel zu verwendende Haltezeit an. Wenn der Parameter "affinity" des Befehls "rule" auf "activecookie" gesetzt wird, muss "stickytime" auf einen Wert ungleich null gesetzt werden, um diesen Affinitätstyp zu aktivieren. Die Haltezeit für die Regel gilt nicht für Regeln mit dem Affinitätstyp "passivecookie" oder "uri".

Weitere Informationen hierzu finden Sie im Abschnitt „Aktive Cookie-Affinität“ auf Seite 207.

Anmerkung: Der Parameter "stickytime" für Regeln gilt nur für die CBR-Komponente.

Zeit

Zeit in Sekunden.

affinity

Gibt den für eine Regel zu verwendenden Affinitätstyp an: Aktive Cookie-Affinität, passive Cookie-Affinität, URI-Affinität oder Keine.

Der Affinitätstyp "activecookie" aktiviert eine Lastverteilung des Webdatenverkehrs mit Affinität an einen Server. Die Affinität basiert auf Cookies, die von Network Dispatcher generiert werden.

Der Affinitätstyp "passivecookie" aktiviert die Verteilung von Webdatenverkehr mit Affinität zu einem Server ausgehend von den Identifizierungs-Cookies, die von den Servern generiert werden. Für die passive Cookie-Affinität müssen Sie den Parameter "cookieName" verwenden.

Der Affinitätstyp "URI" aktiviert den Lastausgleich für Webdatenverkehr auf Caching-Proxy-Servern mit effektiver Vergrößerung des Cache.

Weitere Informationen hierzu finden Sie in den Abschnitten „Aktive Cookie-Affinität“ auf Seite 207, „Passive Cookie-Affinität“ auf Seite 209 und „URI-Affinität“ auf Seite 210.

Anmerkung: Die Affinität gilt für Regeln, die mit der Dispatcher-Weiterleitungsmethode cbr konfiguriert wurden, und für die CBR-Komponente.

Affinitätstyp

Mögliche Werte für den Affinitätstyp sind: Keine (Standardwert), Aktives Cookie, Passives Cookie oder URI.

cookieName

Ein vom Administrator willkürlich festgelegter Name, der als Kennung für Network Dispatcher verwendet wird. Nach diesem Namen muss Network Dispatcher die HTTP-Header-Anforderung durchsuchen. Der Cookie-Name dient neben dem Cookie-Wert als Kennung für Network Dispatcher, so dass Network Dispatcher nachfolgende Anforderungen einer Website immer an dieselbe Servermaschine senden kann. Der Cookie-Name kann nur für die Affinität "Passives Cookie" angewendet werden.

Weitere Informationen hierzu finden Sie im Abschnitt „Passive Cookie-Affinität“ auf Seite 209.

Anmerkung: Der Cookie-Name gilt für Regeln, die mit der Dispatcher-Weiterleitungsmethode cbr konfiguriert wurden, und für die CBR-Komponente.

Wert

Wert des Cookie-Namens.

evaluate

Diese Option ist nur für die Dispatcher-Komponente verfügbar. Sie gibt an, ob die Regelbedingungen für alle Server an einem Port oder für alle Server in einer Regel ausgewertet werden sollen. Diese Option ist nur für Regeln gültig, die Entscheidungen ausgehend von den Kenndaten der Server treffen. Dazu gehören die Regeln "Aktive Verbindungen" und "Reservierte Bandbreite". Weitere Informationen hierzu finden Sie im Abschnitt „Regeloption für Serverauswertung“ auf Seite 196.

Ebene

Mögliche Werte sind "port" oder "rule". Der Standardwert ist "port".

sharelevel

Dieser Parameter gilt nur für die Regel "Gemeinsam genutzte Bandbreite". Er gibt an, ob die gemeinsame Nutzung von Bandbreite auf Cluster- oder Executor-Ebene stattfindet. Bei gemeinsamer Nutzung von Bandbreite auf Cluster-Ebene steht innerhalb eines Clusters Port-übergreifend eine maximale Bandbreite zur gemeinsamen Nutzung zur Verfügung. Bei gemeinsamer Nutzung von Bandbreite auf Executor-Ebene steht für Cluster innerhalb der gesamten Dispatcher-Konfiguration eine maximale Bandbreite zur gemeinsamen Nutzung zur Verfügung. Weitere Informationen hierzu finden Sie im Abschnitt „Regel "Gemeinsame Bandbreite"“ auf Seite 192.

Ebene

Mögliche Werte sind "executor" oder "cluster".

dropserver

Einen Server aus einem Regelsatz entfernen.

Server

Die IP-Adresse der TCP-Servermaschine als symbolischer Name oder in Schreibweise mit Trennzeichen.

Wenn Sie die Serverpartitionierung verwenden, geben Sie den eindeutigen Namen des logischen Servers an. Weitere Informationen hierzu finden Sie im Abschnitt „Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)“ auf Seite 163.

Anmerkung: Zusätzliche Server werden durch ein Pluszeichen (+) getrennt.

remove

Eine oder mehrere Regeln, die durch Pluszeichen voneinander getrennt sind, entfernen.

report

Die internen Werte einer oder mehrerer Regeln anzeigen.

set

Werte für diese Regel festlegen.

status

Die einstellbaren Werte einer oder mehrerer Regeln anzeigen.

useserver

Server in einen Regelsatz einfügen.

Beispiele

- Hinzufügen einer immer gültigen Regel ohne Angabe eines Anfangs- oder Endbereichs:

```
ndcontrol rule add 9.37.67.100:80:trule type true priority 100
```
- Erstellen einer Regel, die den Zugriff auf einen Bereich von IP-Adressen unterbindet, der in diesem Fall mit "9:" beginnt:

```
ndcontrol rule add 9.37.131.153:80:ni type ip b 9.0.0.0 e 9.255.255.255
```
- Soll eine Regel erstellt werden, die die Verwendung eines bestimmten Servers in der Zeit von 11 Uhr bis 15 Uhr angibt, den folgenden Befehl eingeben:

```
ndcontrol rule add Cluster1:80:timerule type time beginrange 11 endrange 14
ndcontrol rule useserver Cluster1:80:timerule Server05
```


- Soll eine Regel erstellt werden, die auf dem Inhalt des TOS-Bytefelds im IP-Header basiert, den folgenden Befehl eingeben:

```
ndcontrol rule add 9.67.131.153:80:tosrule type service tos 0xx1001x
```

- Erstellen einer Regel ausgehend von der reservierten Bandbreite, die einer Gruppe von Servern (die innerhalb der Regel ausgewertet wird) zugeordnet wird, um Daten mit einer Geschwindigkeit von 100 Kilobytes pro Sekunde zu liefern:

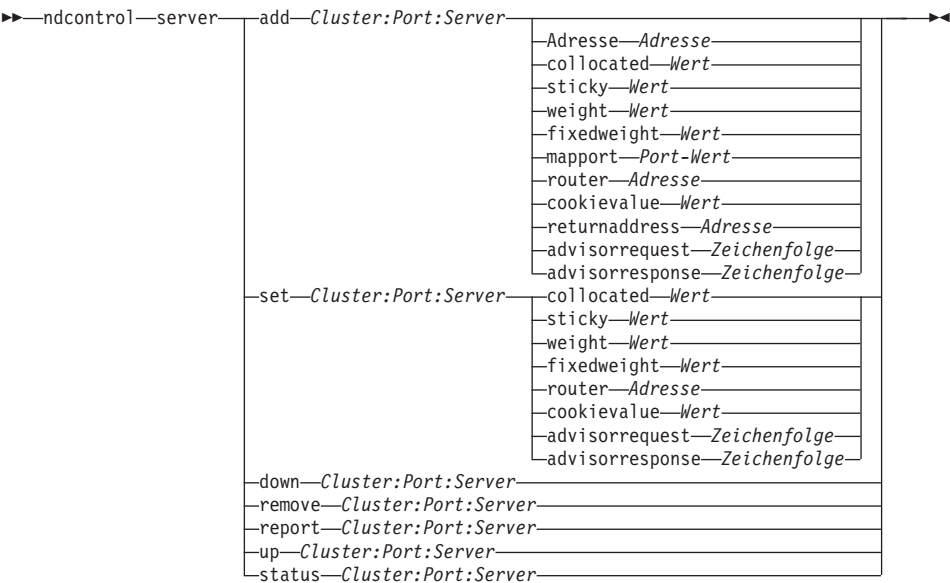
```
ndcontrol rule add 9.67.131.153:80:rbwrule type reservedbandwidth  
beginrange 0 endrange 100 evaluate rule
```

- Erstellen einer Regel ausgehend von der gemeinsam genutzten Bandbreite, bei der es sich um verfügbar gemachte Bandbreite auf Cluster-Ebene handelt, die nicht genutzt wurde (Anmerkung: Zuerst müssen Sie mit dem Befehl "ndcontrol cluster" die maximale Bandbreite in Kilobytes pro Sekunde angeben, die auf Cluster-Ebene gemeinsam genutzt werden kann):

```
ndcontrol cluster set 9.67.131.153 sharedbandwidth 200
```

```
ndcontrol rule add 9.67.131.153:80:shbwrule type sharedbandwidth  
sharelevel cluster
```

ndcontrol server — Server konfigurieren



add
Diesen Server hinzufügen.

Cluster
Die Adresse des Clusters als symbolischer Name oder in Schreibweise mit Trennzeichen. Sie können einen Doppelpunkt (:) als Platzhalter verwenden. Der Befehl `ndcontrol server add :80:ServerA` bewirkt beispielsweise, dass ServerA für alle Cluster zu Port 80 hinzugefügt wird.

Anmerkung: Zusätzliche Cluster werden durch ein Pluszeichen (+) getrennt.

Port
Nummer des Ports. Sie können einen Doppelpunkt (:) als Platzhalter verwenden. Der Befehl `ndcontrol server add ::ServerA` bewirkt beispielsweise, dass ServerA für alle Cluster zu allen Ports hinzugefügt wird.

Anmerkung: Weitere Ports werden durch ein Pluszeichen (+) getrennt angegeben.

Server
Der *Server* ist die eindeutige IP-Adresse der TCP-Servermaschine als symbolischer Name oder in Schreibweise mit Trennzeichen.
Wenn Sie einen eindeutigen Namen verwenden, der nicht in eine IP-Adresse aufgelöst wird, müssen Sie den Befehl **ndcontrol server add** mit

dem Serverparameter **address** verwenden. Weitere Informationen hierzu finden Sie im Abschnitt „Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)“ auf Seite 163.

Anmerkung: Zusätzliche Server werden durch ein Pluszeichen (+) getrennt.

Adresse

Die eindeutige IP-Adresse der TCP-Servermaschine als Host-Name oder in der Schreibweise mit Trennzeichen. Falls der Servername nicht aufgelöst werden kann, müssen Sie die Adresse der physischen Servermaschine angeben. Weitere Informationen hierzu finden Sie im Abschnitt „Serverpartitionierung - Konfigurieren logischer Server für einen physischen Server (IP-Adresse)“ auf Seite 163.

Adresse

Wert für die Adresse des Servers.

collocated

Mit dem Parameter "collocated" können Sie angeben, ob der Dispatcher auf einer der Servermaschinen installiert ist, für die er den Lastausgleich durchführt. Die Option "collocated" gilt nicht für die Windows-2000-Plattform.

Anmerkung: Der Parameter "collocated" ist nur gültig, wenn die Dispatcher-Weiterleitungsmethode mac oder nat verwendet wird. Mailbox Locator, Site Selector und Cisco Consultant können auf allen Plattformen verknüpft werden, erfordern jedoch nicht dieses Schlüsselwort. Weitere Informationen hierzu finden Sie im Abschnitt „Verknüpfte Server verwenden“ auf Seite 166.

Wert

Wert für collocated: ja oder nein. Der Standardwert ist Nein.

sticky

Ermöglicht einem Server, die Einstellung für "stickytime" an seinem Port zu überschreiben. Bei Verwendung des Standardwertes "yes" bleibt die normale normale Affinität wie für den Port definiert erhalten. Bei Verwendung des Wertes "no" wird der Client beim Absetzen der nächsten Anforderung an diesem Port *nicht* wieder an diesen Server verwiesen. Dies gilt unabhängig von der Einstellung für "stickytime" des Ports. Dies ist in bestimmten Situationen nützlich, wenn Regeln verwendet werden. Weitere Informationen hierzu finden Sie im Abschnitt „Überschreibung der Regelaaffinität“ auf Seite 205.

Wert

Wert für sticky: ja oder nein. Der Standardwert ist Ja.

weight

Eine Zahl von 0 bis 100 (die den angegebenen Wert für die Wertigkeitsgrenze des Ports nicht überschreiten darf) zur Angabe der Wertigkeit für diesen Server. Wird die Wertigkeit auf 0 gesetzt, werden keine neuen Anforderungen an den Server gesendet, die derzeit aktiven Verbindungen zu diesem Server werden jedoch nicht beendet. Der Standardwert entspricht der Hälfte der für den Port angegebenen Wertigkeitsgrenze. Ist der Manager aktiv, wird diese Einstellung schnell überschrieben.

Wert

Wertigkeit des Servers.

fixedweight

Mit der Option "fixedweight" können Sie angeben, ob der Manager die Serverwertigkeit ändern soll. Wird der Wert für "fixedweight" auf "yes" gesetzt, kann der Manager die Serverwertigkeit nicht ändern. Weitere Informationen hierzu finden Sie im Abschnitt „Feste Wertigkeiten vom Manager“ auf Seite 147.

Wert

Wert für fixedweight: ja oder nein. Der Standardwert ist Nein.

mapport

Zuordnen der Nummer des Ziel-Ports für die Client-Anforderung (die für den Dispatcher angegeben ist) zur Nummer des Server-Ports zu, an dem der Dispatcher den Lastausgleich für die Client-Anforderungen durchführt. Erlaubt Network Dispatcher, die Anforderung eines Clients auf einem Port zu empfangen und sie an einen anderen Port auf der Servermaschine zu übertragen. Mit "mapport" können Sie den Lastausgleich für eine Client-Anforderung auf einem Server durchführen, auf dem mehrere Serverdämonen aktiv sind.

Anmerkung: Der Parameter "mapport" gilt für Dispatcher (bei Verwendung der Weiterleitungsmethode nat oder cbr) und für CBR. Weitere Informationen zum Dispatcher finden Sie in den Abschnitten „NAT/NAPT-Weiterleitungsmethode (nat) des Dispatchers“ auf Seite 55 und „Inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente (cbr)“ auf Seite 57. Weitere Informationen zu CBR können Sie dem Abschnitt „SSL-Datenverkehr vom Client zum Proxy und HTTP-Datenverkehr vom Proxy zum Server verteilen“ auf Seite 85 entnehmen.

Port-Wert

Nummer des zugeordneten Ports. Der Standardwert ist die Nummer des Ziel-Ports für die Client-Anforderung.

router

Wenn Sie ein Weitverkehrsnetz konfigurieren, ist dies die Adresse des

Routers zum fernen Server. Der Standardwert ist 0. Er gibt einen lokalen Server an. Wurde die Router-Adresse eines Servers einmal auf einen anderen Wert als Null gesetzt (gibt einen fernen Server an), kann die Adresse nicht mehr auf Null zurückgesetzt werden, um einen lokalen Server anzugeben. Der Server muss stattdessen entfernt und dann erneut ohne Angabe einer Router-Adresse hinzugefügt werden. Genauso kann ein als lokal definierter Server (Router-Adresse = 0) nicht als ferner Server definiert werden, indem die Router-Adresse geändert wird. Der Server muss entfernt und erneut hinzugefügt werden. Weitere Informationen hierzu finden Sie im Abschnitt „Dispatcher-WAN-Unterstützung konfigurieren“ auf Seite 168.

Anmerkung: Der Parameter "router" gilt nur für Dispatcher. Wenn Sie die Weiterleitungsmethode nat oder cbr verwenden, müssen Sie beim Hinzufügen eines Servers zur Konfiguration die Router-Adresse angeben.

Adresse

Wert der Adresse des Routers.

cookievalue

Der Parameter "cookievalue" ist ein zufälliger Wert, der die Serverseite des aus Cookie-Namen und Cookie-Wert bestehenden Paares. Der Cookie-Wert dient neben dem Cookie-Namen als Kennung, mit der Network Dispatcher nachfolgende Client-Anforderungen an nur einen Server senden kann. Weitere Informationen hierzu finden Sie im Abschnitt „Passive Cookie-Affinität“ auf Seite 209.

Anmerkung: Der Parameter "cookievalue" ist für Dispatcher (bei Verwendung der Weiterleitungsmethode cbr) und CBR gültig.

Wert

Ein zufälliger Wert. Standardmäßig ist kein Cookie-Wert angegeben.

returnaddress

Eine eindeutige IP-Adresse oder ein eindeutiger Host-Name. Diese Adresse wird auf der Dispatcher-Maschine konfiguriert und wird vom Dispatcher bei der Lastverteilung der Client-Anforderung an den Server als Quellenadresse verwendet. Auf diese Weise wird sichergestellt, dass der Server das Paket an die Dispatcher-Maschine zurückgibt und es nicht direkt an den Client sendet. (Der Dispatcher leitet das IP-Paket dann an den Client weiter.) Sie müssen den Wert für die Rückkehradresse beim Hinzufügen des Servers angeben. Die Rückkehradresse kann nur geändert werden, wenn Sie den Server entfernen und dann erneut hinzufügen. Die Rückkehradresse darf nicht mit dem Wert für Cluster, Server oder NFA übereinstimmen.

Anmerkung: Der Parameter "returnaddress" gilt nur für Dispatcher. Wenn Sie die Weiterleitungsmethode nat oder cbr verwenden, müssen Sie beim Hinzufügen eines Servers zur Konfiguration die Rückkehradresse angeben.

Adresse

Wert der Rückkehradresse.

advisorrequest

Die HTTP-Advisor-Funktion verwendet die Zeichenfolge "advisorrequest", um den Status der Server abzufragen. Dieser Wert ist nur für die Server gültig, die mit dem HTTP-Advisor zusammenarbeiten. Zum Aktivieren dieses Wertes müssen Sie die HTTP-Advisor-Funktion starten. Weitere Informationen hierzu finden Sie im Abschnitt „Option 'Anforderung/ Antwort (URL)' der HTTP-Advisor-Funktion" auf Seite 165.

Anmerkung: Der Parameter "advisorrequest" gilt für die Komponenten Dispatcher und CBR.

Zeichenfolge

Wert der Zeichenfolge, die von der HTTP-Advisor-Funktion verwendet wird. Der Standardwert ist HEAD / HTTP/1.0.

Anmerkung: Wenn die Zeichenfolge ein Leerzeichen enthält, gilt Folgendes:

- Bei Absetzen des Befehls von der Shell-Eingabeaufforderung **ndcontrol>>** müssen Sie die Zeichenfolge in Anführungszeichen setzen. Beispiel: **server set Cluster:Port:Server advisorrequest "head / http/2.0"**
- Beim Absetzen des Befehls **ndcontrol** an der Eingabeaufforderung des Betriebssystems müssen Sie dem Text die Zeichen "\" voranstellen und den Text mit den Zeichen \"\" beenden. Beispiel: **ndcontrol server set Cluster:Port:Server advisorrequest "\"head / http/2.0\""**

advisorresponse

Die Antwortzeichenfolge der Advisor-Funktion, nach der die HTTP-Advisor-Funktion die HTTP-Antwort durchsucht. Dieser Wert ist nur für die Server gültig, die mit dem HTTP-Advisor zusammenarbeiten. Zum Aktivieren dieses Wertes müssen Sie die HTTP-Advisor-Funktion starten. Weitere Informationen hierzu finden Sie im Abschnitt „Option 'Anforderung/ Antwort (URL)' der HTTP-Advisor-Funktion" auf Seite 165.

Anmerkung: Der Parameter "advisorresponse" gilt für die Komponenten Dispatcher und CBR.

Zeichenfolge

Wert der Zeichenfolge, die von der HTTP-Advisor-Funktion verwendet wird. Der Standardwert ist null.

Anmerkung: Wenn die Zeichenfolge ein Leerzeichen enthält, gilt Folgendes:

- Bei Absetzen des Befehls von der Shell-Eingabeaufforderung **ndcontrol>>** müssen Sie die Zeichenfolge in Anführungszeichen setzen.
- Beim Absetzen des Befehls **ndcontrol** an der Eingabeaufforderung des Betriebssystems müssen Sie dem Text die Zeichen "\" voranstellen und den Text mit den Zeichen \"\" beenden.

down

Diesen Server als inaktiv markieren. Durch diesen Befehl werden alle aktiven Verbindungen zu diesem Server unterbrochen, und es wird verhindert, dass weitere Verbindungen oder Pakete an diesen Server gesendet werden.

remove

Diesen Server entfernen.

report

Bericht über diesen Server erstellen.

set

Werte für diesen Server festlegen.

status

Status der Server anzeigen.

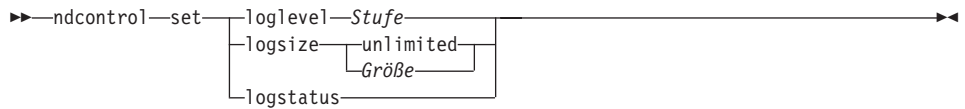
up Diesen Server als "aktiv" kennzeichnen. Der Dispatcher sendet jetzt neue Verbindungen zu diesem Server.

Beispiele

- Hinzufügen des Servers mit der Adresse 27.65.89.42 zum Port 80 an der Cluster-Adresse 130.40.52.153:
`ndcontrol server add 130.40.52.153:80:27.65.89.42`
- Setzen des Servers an der Adresse 27.65.89.42 auf "nonsticky" (Merkmal zur Außerkraftsetzung der Regelaffinität):
`ndcontrol server set 130.40.52.153:80:27.65.89.42 sticky nein`
- Geben Sie den folgenden Befehl ein, um den Server an 27.65.89.42 als "ausgefallen" zu kennzeichnen:
`ndcontrol server down 130.40.52.153:80:27.65.89.42`

- Geben Sie den folgenden Befehl ein, um den Server 27.65.89.42 von allen Ports aller Cluster zu entfernen:
`ndcontrol server remove ::27.65.89.42`
- Geben Sie den folgenden Befehl ein, um den Server an 27.65.89.42 als Zusammengeführt zu definieren (Server befindet sich auf derselben Maschine wie der Network Dispatcher):
`ndcontrol server set 130.40.52.153:80:27.65.89.42 collocated yes`
- Festlegen der Wertigkeit 10 für den Server 27.65.89.42 am Port 80 für die Cluster-Adresse 130.40.52.153:
`ndcontrol server set 130.40.52.153:80:27.65.89.42 weight 10`
- Geben Sie den folgenden Befehl ein, um den Server an 27.65.89.42 als "aktiv" zu kennzeichnen:
`ndcontrol server up 130.40.52.153:80:27.65.89.42`
- Geben Sie den folgenden Befehl ein, um einen fernen Server hinzuzufügen:
`ndcontrol server add 130.40.52.153:80:130.60.70.1 router 130.140.150.0`
- Zielsetzung, dass die HTTP-Advisor-Funktion eine HTTP-URL-Anforderung HEAD / HTTP/2.0 für Server 27.65.89.42 am HTTP-Port 80 abfragt:
`ndcontrol server set 130.40.52.153:80:27.65.89.42
 advisorrequest "\"HEAD / HTTP/2.0\""`

ndcontrol set — Serverprotokoll konfigurieren



loglevel

Die Stufe, auf der ndserver seine Aktivitäten protokolliert.

Stufe

Der Standardwert für **loglevel** ist 0. Der gültige Bereich ist 0 bis 5. Die folgenden Werte sind gültig: 0 für keine Einträge, 1 für eine minimale Protokollierung, 2 für eine Basisprotokollierung, 3 für eine normale, 4 für eine erweiterte und 5 für eine ausführliche Protokollierung.

logsize

Die maximale Anzahl von Byte, die in der Protokolldatei protokolliert werden können.

Größe

Der Standardwert für "logsize" ist 1 MB.

logstatus

Zeigt die Einstellungen des Serverprotokolls (Protokollstufe und -größe) an.

►►ndcontrol—status◄◄

Beispiele

- Geben Sie den folgenden Befehl ein, um festzustellen, ob der Manager und die Advisor aktiv sind:
`ndcontrol status`

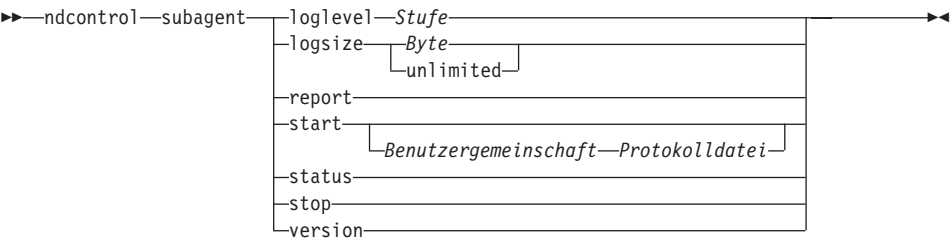
Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Executor wurde gestartet.
Manager wurde gestartet.

ADVISOR	PORT	ZEITLIMIT
reach	0	unlimited
http	80	unlimited
ftp	21	unlimited

ndcontrol subagent — SNMP-Subagent konfigurieren

Anmerkung: Die Syntaxdiagramme für den Befehl "ndcontrol subagent" gelten für CBR und Mailbox Locator.



loglevel

Die Stufe, auf der der Subagent seine Aktivitäten in einer Datei protokolliert.

Stufe

Die Nummer der Stufe (0 bis 5). Je größer die Zahl, desto mehr Informationen werden in das Manager-Protokoll geschrieben. Der Standardwert ist 1. Die folgenden Werte sind gültig: 0 für keine Einträge, 1 für eine minimale Protokollierung, 2 für eine Basisprotokollierung, 3 für eine normale, 4 für eine erweiterte und 5 für eine ausführliche Protokollierung.

logsize

Festlegen der Maximalen Größe des Subagentenprotokolls in Bytes. Der Standardwert ist 1 MB. Wenn Sie eine maximale Größe für die Protokolldatei festlegen, findet ein Dateiumbruch statt. Hat die Datei die angegebene Größe erreicht, werden alle weiteren Einträge wieder an den Anfang der Datei geschrieben und die dort befindlichen Einträge überschrieben. Die Protokollgröße kann nicht auf einen geringeren Wert als die aktuelle Dateigröße gesetzt werden. Protokolleinträge werden mit einer Zeitmarke versehen, damit Sie erkennen können, in welcher Reihenfolge die Einträge geschrieben wurden. Je höher Sie die Protokollstufe setzen, desto vorsichtiger müssen Sie die Protokollgröße auswählen, da die Protokolldatei sehr schnell voll ist, wenn Sie eine Protokollierung auf einer höheren Stufe wählen.

Byte

Die maximale Größe in Byte für die Protokolldatei des Subagenten. Sie können entweder eine positive Zahl, die größer als 0 sein muss, oder das Wort **unlimited** (unbegrenzt) angeben. Möglicherweise erreicht die Protokolldatei nicht genau die maximale Größe, bevor der Dateiumbruch stattfindet, da die Größe der Protokolleinträge variiert. Der Standardwert ist "unlimited".

report

Zeigt eine statistische Momentaufnahme an.

start

Den Subagenten starten.

Benutzergemeinschaft

Der Name der SNMP-Benutzergemeinschaft, den Sie als Sicherheitskennwort verwenden können. Der Standardwert ist public.

Protokolldatei

Der Name der Datei, in der die Daten des SNMP-Subagenten protokolliert werden. Jeder Eintrag im Protokoll wird mit einer Zeitmarke versehen. Der Standardwert ist subagent.log. Die Standarddatei wird in dem Verzeichnis **logs** installiert. Weitere Informationen hierzu finden Sie in „Anhang F. Beispielkonfigurationsdateien“ auf Seite 393. Wollen Sie das Verzeichnis ändern, in dem die Protokolldateien gespeichert werden, lesen Sie die Informationen unter „Pfade für die Protokolldatei ändern“ auf Seite 222.

status

Zeigt den aktuellen Status aller Werte in dem SNMP-Subagenten an, die global gesetzt werden können. Zudem werden die Standardwerte dieser Werte angezeigt.

version

Zeigt die aktuelle Version des Subagenten an.

Beispiele

- Geben Sie den folgenden Befehl ein, um den Subagenten mit dem Benutzer-gemeinschaftsnamen bigguy zu starten:
`ndcontrol subagent start bigguy bigguy.log`

Anhang C. Syntax der content-Regel

Dieser Anhang beschreibt die Syntax der content-Regel (des Musters) für die CBR-Komponente und die Weiterleitungsmethode "cbr" der Dispatcher-Komponente sowie Szenarien und Beispiele für ihre Verwendung.

Syntax der content-Regel

Diese Angaben gelten nur, wenn Sie als Regeltyp "content" ausgewählt haben.

Beachten Sie bei der Syntax des gewünschten Musters die folgenden Einschränkungen:

- Geben Sie keine Leerzeichen ein.
- Sonderzeichen muss wie folgt ein umgekehrter Schrägstrich (\) vorangestellt werden:
 - * Platzhalterzeichen (entspricht 0 bis x beliebigen Zeichen)
 - (linke runde Klammer für logische Gruppierung
 -) rechte runde Klammer für logische Gruppierung
 - & logisches UND
 - | logisches ODER
 - ! logisches NICHT

Reservierte Schlüsselwörter

Auf reservierte Schlüsselwörter folgt immer ein Gleichheitszeichen „=".

Methode

HTTP-Methode in der Anforderung, z. B. GET, POST usw.

URI Pfad der URL-Anforderung

Version

Spezifische Version der Anforderung, entweder HTTP/1.0 oder HTTP/1.1

Host Wert vom Host: Header.

Anmerkung: In HTTP/1.0-Protokollen optional.

<Schlüssel>

Ein gültiger HTTP-Header-Name, nach dem Dispatcher suchen kann. Beispiele für HTTP-Header sind User-Agent, Connection, Referer usw.

Ein Browser, der `http://www.firma.com/pfad/webseite.htm` aufruft, kann folgende Werte ergeben:

```
Method=GET
URI=/pfad/webseite.htm
Version=/HTTP/1.1
Host=www.firma.com
Connection=Keep-Alive
Referer=http://www.firma.com/pfad/externwebseite.htm
```

Anmerkung: Die Shell des Betriebssystems interpretiert Sonderzeichen wie "&" unter Umständen und konvertiert sie in alternativen Text, bevor sie von **cbrcontrol** ausgewertet werden.

Der folgende Befehl ist beispielsweise nur gültig, wenn die Eingabeaufforderung **cbrcontrol>>** verwendet wird.

```
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/*
```

Wenn dieser Befehl mit Sonderzeichen an der Eingabeaufforderung des Betriebssystems funktionieren soll, müssen Sie den pattern-Wert wie folgt in Anführungszeichen (" ") setzen:

```
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/*"
```

Fehlen die Anführungszeichen, könnte beim Speichern der Regel in CBR ein Teil des Musters abgeschnitten werden. An der Eingabeaufforderung "**cbrcontrol>>**" wird die Verwendung von Anführungszeichen nicht unterstützt.

Nachfolgend finden Sie eine Zusammenstellung möglicher Szenarien und Beispiele für die Mustersyntax.

Szenario 1:

Zur Konfiguration für einen Cluster-Namen gehört eine Gruppe von Webservern für standardmäßigen HTML-Inhalt, eine weitere Gruppe von Webservern mit WebSphere Application Server für Servlet-Anforderungen, eine dritte Gruppe von Lotus-Notes-Servern für NSF-Dateien usw. Der Zugriff auf die Client-Daten ist erforderlich, um zwischen den angeforderten Seiten unterscheiden zu können. Die Daten müssen außerdem an die jeweils geeigneten Server gesendet werden. Die Erkennungsregeln für das content-Muster ermöglichen die für diese Tasks notwendige Trennung. Es wird eine Reihe von Regeln konfiguriert, die die nötige Trennung der Anforderungen automatisch vornehmen.

Mit den folgenden Befehlen können Sie die genannte Trennung in drei Gruppen erreichen:

```
>>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
```

Wenn Network Dispatcher eine Anforderung für eine NSF-Datei empfängt, wird zuerst die servlets-Regel angewendet, bei der jedoch keine Übereinstimmung gefunden wird. Anschließend wird die Anforderung mit der notes-Regel abgeglichen und eine Übereinstimmung festgestellt. Die Client-Daten werden auf Server3 und Server4 verteilt.

Szenario 2

Ein weiteres allgemeines Szenario ist die Steuerung unterschiedlicher interner Gruppen durch die Hauptwebsite. Beispiel: `www.firma.com/software` bezieht verschiedene Server und Inhalte aus dem Bereich `www.firma.com/hardware` ein. Da alle Anforderungen vom Root-Cluster `www.firma.com` ausgehen, sind content-Regeln erforderlich, um die URI-Unterscheidung für den Lastausgleich vorzunehmen. Die Regel für dieses Szenario würde etwa wie folgt aussehen:

```
>>rule add Cluster1:80:Bereich1 type content pattern uri=/software/* priority 1
>>rule uses Cluster1:80:Bereich1 Server1+Server2

>>rule add Cluster1:80:Bereich2 type content pattern uri=/hardware/* priority 2
>>rule uses Cluster1:80:Bereich2 Server3+Server4
```

Szenario 3

Bei bestimmten Kombinationen ist die Reihenfolge wichtig, in der die Regeln durchsucht werden. Im Szenario 2 wurden die Clients beispielsweise ausgehend von einem Verzeichnis in ihrem Anforderungspfad aufgeteilt. Der Zielverzeichnispfad kann jedoch auf verschiedenen Ebenen dieses Pfades vorhanden sein und dort jeweils zu anderen Ergebnissen führen.

So ist das Ziel `www.firma.com/pcs/fixes/software` beispielsweise von `www.firma.com/mainframe/fixes/software` verschieden. Die Regeln müssen dieser Möglichkeit Rechnung tragen und so konfiguriert werden, dass die nicht zu vielen Szenarien gleichzeitig gerecht werden. Die Platzhaltersuche „uri=*/software/*“ wäre in diesem Falle zu breit angelegt.

Alternative Regeln könnten wie folgt strukturiert sein:

Mit einer kombinierten Suche kann hier eine Eingrenzung vorgenommen werden:

```
>>rule add Cluster1:80:pcs type content pattern (uri=/pcs/*)&(uri=*/software/*)
>>rule uses Cluster 1:80:pcs Server1
```

In Fällen, wo keine Kombinationen anwendbar sind, ist die Reihenfolge wichtig:

```
>>rule add Cluster1:80:pc1 type content pattern uri=/pcs/*
>>rule uses Cluster1:80:pc1 Server2
```

Die zweite Regel wird angewendet, wenn „pcs“ im Verzeichnis nicht an erster Stelle, sondern an einer späteren Stelle erscheint.

```
>>rule add Cluster1:80:pc2 type content pattern uri=*/pcs/*
>>rule uses Cluster1:80:pc2 Server3
```

In fast allen Fällen sollten Sie die Regeln durch eine Standardregel **always true** ergänzen, die für alles gelten, was nicht unter die übrigen Regeln fällt. In Szenarien, in denen alle Server für einen bestimmten Client nicht in Frage kommen, könnte dies auch ein Server mit der Antwort „Die Site ist derzeit nicht verfügbar, versuchen Sie es später erneut“ sein.

```
>>rule add Cluster1:80:sorry type true priority 100
>>rule uses Cluster1:80:sorry Server5
```

Anhang D. Befehlsreferenz für Site Selector

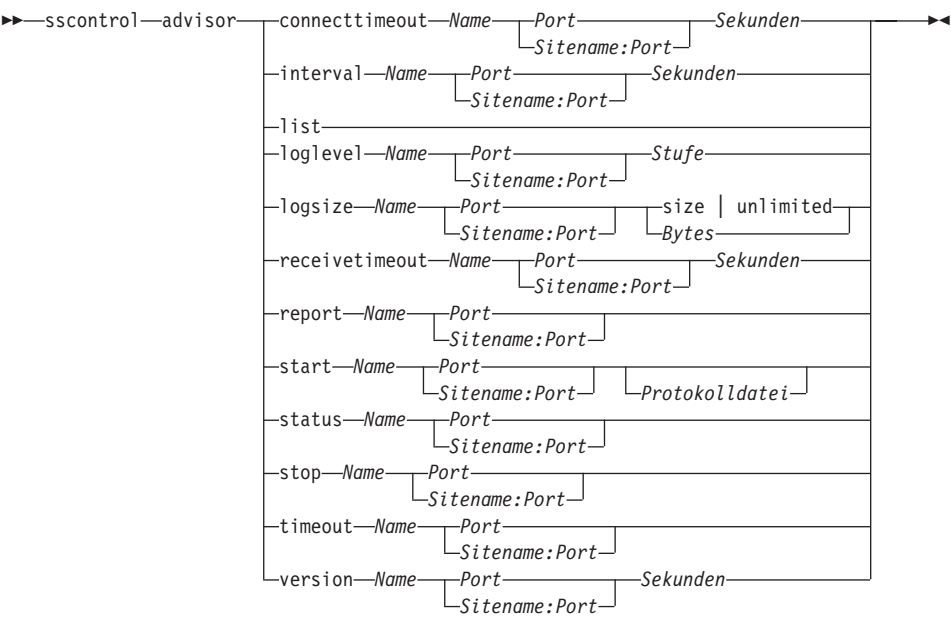
Dieser Anhang beschreibt die Verwendung der folgenden **sscontrol**-Befehle für Site Selector:

- „sscontrol advisor — Advisor-Funktion steuern“ auf Seite 336
- „sscontrol file — Konfigurationsdateien verwalten“ auf Seite 341
- „sscontrol help — Hilfetext für diesen Befehl anzeigen oder drucken“ auf Seite 343
- „sscontrol manager — Manager steuern“ auf Seite 344
- „sscontrol metric — Systemmesswerte konfigurieren“ auf Seite 349
- „sscontrol nameserver — Namensserver steuern“ auf Seite 350
- „sscontrol rule — Regeln konfigurieren“ auf Seite 351
- „sscontrol server — Server konfigurieren“ auf Seite 355
- „sscontrol set — Serverprotokoll konfigurieren“ auf Seite 357
- „sscontrol sitename — Sitenamen konfigurieren“ auf Seite 358
- „sscontrol status — Aktivitätsanzeige für Manager und Advisor-Funktionen“ auf Seite 362

Sie können eine Minimalversion der Parameter für den Befehl "sscontrol" eingeben. Sie müssen nur die eindeutigen Buchstaben der Parameter eingeben. Beispiel: Wenn Sie Hilfe für den Befehl zum Speichern von Dateien aufrufen möchten, können Sie **sscontrol he f** anstelle von **sscontrol help file** eingeben.

Anmerkung: Die Werte der Befehlsparameter müssen in englischen Zeichen eingegeben werden. Die einzige Ausnahme hiervon bilden Host-Namen (die in den Befehlen "cluster" und "server" verwendet werden) und (die in Dateibefehlen verwendeten) Dateinamen.

sscontrol advisor — Advisor-Funktion steuern



connecttimeout

Definiert, wie lange eine Advisor-Funktion wartet, bevor sie meldet, dass zu einem Server keine Verbindung hergestellt werden kann. Weitere Informationen hierzu finden Sie im Abschnitt „Serververbindungs- und -empfangszeitlimit der Advisor-Funktion“ auf Seite 152.

Name

Der Name der Advisor-Funktion. Mögliche Werte sind **http**, **ftp**, **ssl**, **smtp**, **imap**, **pop3**, **nnntp**, **telnet**, **connect**, **ping**, **WLM** und **WTE**. Die Namen angepasster Advisor-Funktionen haben das Format xxxx, wobei ADV_xxxx der Name der Klasse ist, die die angepasste Advisor-Funktion implementiert.

Port

Die Nummer des Ports, der von der Advisor-Funktion überwacht wird.

Sekunden

Eine positive ganze Zahl, die die Zeit in Sekunden angibt, nach deren Ablauf die Advisor-Funktion meldet, dass zu einem Server keine Verbindung hergestellt werden kann. Dieser Wert liegt standardmäßig beim Dreifachen des für das Advisor-Intervall angegebenen Wertes.

interval

Legt fest, wie oft der Advisor Informationen von den Servern abfragt.

Sekunden

Eine positive ganze Zahl, die die Zeit zwischen den an die Server gerichteten Statusabfragen in Sekunden angibt. Der Standardwert ist 7.

list

Zeigt eine Liste der Advisor an, die derzeit Informationen an den Manager liefern.

loglevel

Legt die Protokollstufe für ein Advisor-Protokoll fest.

Stufe

Die Nummer der Stufe (0 bis 5). Der Standardwert ist 1. Je größer die Zahl ist, desto mehr Informationen werden in das Advisor-Protokoll geschrieben. Gültige Werte:

- 0 entspricht keiner Protokollierung
- 1 entspricht einer minimalen Protokollierung
- 2 entspricht einer Basisprotokollierung
- 3 entspricht einer normalen Protokollierung
- 4 entspricht einer erweiterten Protokollierung
- 5 entspricht einer ausführlichen Protokollierung.

logsize

Legt die maximale Größe eines Advisor-Protokolls fest. Wenn Sie für die Protokolldatei eine maximale Größe festlegen, werden bei Erreichen der Größe die vorherigen Protokolleinträge überschrieben. Die Protokollgröße kann nicht auf einen geringeren Wert als die aktuelle Dateigröße gesetzt werden. Protokolleinträge sind mit einer Zeitmarke versehen, damit Sie die Reihenfolge, in der sie geschrieben wurden, erkennen können. Je höher Sie die Protokollstufe setzen, desto vorsichtiger müssen Sie die Protokollgröße auswählen, da die Protokolldatei sehr schnell voll ist, wenn Sie eine Protokollierung auf einer höheren Stufe wählen.

Größe | unbegrenzt

Die maximale Größe der Advisor-Protokolldatei in Bytes. Sie können entweder eine positive Zahl, die größer als 0 sein muss, oder **unlimited** (unbegrenzt) angeben. Da die Protokolleinträge unterschiedlich lang sind, wird mit dem Überschreiben von Einträgen unter Umständen schon vor Erreichen der exakten maximalen Größe begonnen. Der Standardwert ist 1 MB.

receivetimeout

Definiert, wie lange eine Advisor-Funktion wartet, bevor sie meldet, dass von einem Server keine Daten empfangen werden können. Weitere Informationen hierzu finden Sie im Abschnitt „Serververbindungs- und -empfangszeitlimit der Advisor-Funktion“ auf Seite 152.

Sekunden

Eine positive ganze Zahl, die die Zeit in Sekunden angibt, nach deren Ablauf die Advisor-Funktion meldet, dass von einem Server keine Daten empfangen werden können. Dieser Wert liegt standardmäßig beim Dreifachen des für das Advisor-Intervall angegebenen Wertes.

report

Anzeigen eines Berichts zum Advisor-Status.

start

Den Advisor starten. Für alle Protokolle stehen Advisor zur Verfügung. Die Standard-Ports sind:

Advisor-Name	Protokoll	Port
Connect	nicht anwendbar	benutzerdefiniert
db2	privat	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

Name

Der Name der Advisor-Funktion.

Sitename:Port

Der Wert "Sitename" ist in den advisor-Befehlen optional, der Wert "Port" jedoch erforderlich. Wird der Wert "Sitename" nicht angegeben, wird die Advisor-Funktion für alle verfügbaren konfigurierten Sitenamen ausgeführt. Bei Angabe eines Sitenamens wird die Advisor-Funktion nur für den von Ihnen angegebenen Sitenamen ausgeführt. Zusätzliche Sitenamen werden durch ein Pluszeichen (+) voneinander getrennt.

Protokolldatei

Der Name der Datei, in die die Verwaltungsdaten geschrieben werden. Jeder Eintrag des Protokolls ist mit einer Zeitmarke versehen.

Die Standarddatei ist *Advisor-Name_Port.log*, z. B. **http_80.log**. Informationen zum Ändern des Verzeichnisses, in dem Protokolldateien gespeichert werden, finden Sie im Abschnitt „Pfade für die Protokolldatei ändern“ auf Seite 222.

Sie können nur eine Advisor-Funktion pro Sitenamen starten.

status

Anzeigen des aktuellen Status sowie der Standardeinstellungen für alle globalen Werte einer Advisor-Funktion.

stop

Den Advisor stoppen.

Zeitlimit

Legt die Zeit in Sekunden fest, in der der Manager von der Advisor-Funktion erhaltene Informationen als gültig ansieht. Stellt der Manager fest, dass die Advisor-Informationen älter als dieses Zeitlimit sind, verwendet der Manager diese Informationen nicht zum Bestimmen Wertigkeiten für die Server am Port, die von der Advisor-Funktion überwacht werden. Dieses Zeitlimit gilt nicht, wenn die Advisor-Funktion den Manager darüber informiert hat, dass ein bestimmter Server inaktiv ist. Der Manager verwendet diese Informationen über den Server auch, nachdem die Advisor-Informationen das Zeitlimit überschritten haben.

Sekunden

Eine positive Zahl, die die Sekunden angibt, oder **unlimited**. Der Standardwert ist "unlimited".

version

Zeigt die aktuelle Advisor-Version an.

Beispiele

- Festlegen der Zeit (30 Sekunden), die eine HTTP-Advisor-Funktion (für Port 80) wartet, bevor sie meldet, dass zu einem Server keine Verbindung hergestellt werden kann:

```
sscontrol advisor connecttimeout http 80 30
```

- Festlegen des Intervalls für die FTP-Advisor-Funktion (für Port 21) auf 6 Sekunden:

```
sscontrol advisor interval ftp 21 6
```

- Geben Sie den folgenden Befehl ein, um eine Liste der Advisor anzuzeigen, die derzeit Informationen an den Manager liefern:

```
sscontrol advisor list
```

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

ADVISOR	SITENAME:PORT	ZEITLIMIT	

http	80	unlimited	
ftp	21	unlimited	

- Ändern der Protokollstufe für das Protokoll der Advisor-Funktion http für den Sitenamen "meineSite" in 0, um einen höheren Durchsatz zu erreichen:

```
sscontrol advisor loglevel http meineSite:80 0
```

- Ändern der Protokollgröße der Advisor-Funktion ftp für den Sitenamen "meineSite" in 5000 Bytes:

```
sscontrol advisor  
logsize ftp meineSite:21 5000
```

- Festlegen der Zeit (60 Sekunden), die eine HTTP-Advisor-Funktion (für Port 80) wartet, bevor sie meldet, dass von einem Server keine Daten empfangen werden können:

```
sscontrol advisor receivetimeout http 80 60
```

- Anzeigen eines Berichts zum Status der Advisor-Funktion ftp (für Port 21):

```
sscontrol  
advisor report ftp 21
```

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Advisor-Bericht:

```
Advisor-Name ..... http  
Port-Nummer ..... 80
```

```
Sitename ..... meineSite  
Serveradresse ..... 9.67.129.230  
Last ..... 8
```

- Geben Sie den folgenden Befehl ein, um den Advisor mit der Datei ftpadv.log zu starten:

```
sscontrol advisor start ftp 21 ftpadv.log
```

- Anzeigen des aktuellen Status der Werte, die der Advisor-Funktion http zugeordnet sind:

```
sscontrol advisor status http 80
```

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

Advisor-Status:

```
Intervall (Sekunden) ..... 7  
Zeitlimit (Sekunden) ..... Unlimited  
Zeitlimit für Verbindung (Sekunden) ..... 21  
Zeitlimit für Empfang (Sekunden) ..... 21  
Advisor-Protokolldateiname ..... Http_80.log  
Protokollstufe ..... 1  
Maximale Managerprotokollgröße (Bytes)... Unlimited
```

- Stoppen der Advisor-Funktion http am Port 80:

```
sscontrol advisor stop http 80
```

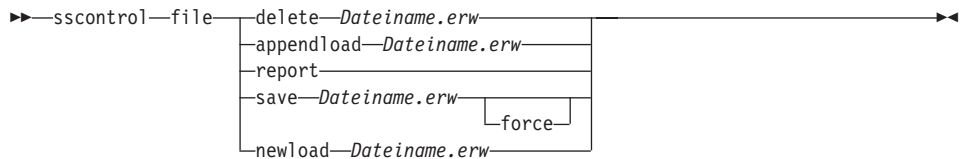
- Festlegen eines Zeitlimits für Advisor-Informationen von 5 Sekunden:

```
sscontrol advisor timeout ftp 21 5
```

- Ermitteln der aktuellen Versionsnummer für die Advisor-Funktion ssl:

```
sscontrol advisor version ssl 443
```

sscontrol file — Konfigurationsdateien verwalten



delete

Die Datei löschen.

Datei.erw

Eine Konfigurationsdatei.

Die Dateierweiterung (.*erw*) ist optional und kann beliebig gewählt werden.

appendload

Hinzufügen einer Konfigurationsdatei zur aktuellen Konfiguration und laden der Datei in Site Selector.

report

Bericht über die verfügbare(n) Datei(en).

save

Sichern der aktuellen Konfiguration für Site Selector in der Datei.

Anmerkung: Dateien werden in den nachfolgend genannten Verzeichnissen gespeichert und aus diesen geladen:

- AIX: /usr/lpp/nd/servers/configurations/ss
- Linux: /opt/nd/servers/configurations/ss
- Solaris: /opt/nd/servers/configurations/ss
- Windows 2000:

Allgemeiner Installationsverzeichnispfad —

c:\Programme\ibm\edge\nd\servers\configurations\Komponente

Interner Installationsverzeichnispfad —

c:\Programme\ibm\nd\servers\configurations\Komponente

force

Wenn Sie Ihre Datei in einer vorhandenen Datei mit demselben Namen speichern möchten, verwenden Sie **force**, um die vorhandene Datei vor dem Speichern der neuen Datei zu löschen. Bei Nichtverwendung der Option "force" wird die vorhandene Datei nicht überschrieben.

newload

Laden einer neuen Konfigurationsdatei in Site Selector. Die neue Konfigurationsdatei ersetzt die aktuelle Konfiguration.

Beispiele

- Geben Sie den folgenden Befehl ein, um eine Datei zu löschen:
`sscontrol file delete Datei3`

Datei (Datei3) wurde gelöscht.
- Geben Sie den folgenden Befehl ein, um eine neue Konfigurationsdatei zu laden, die die aktuelle Konfiguration ersetzt:
`sscontrol file newload Datei1.sv`

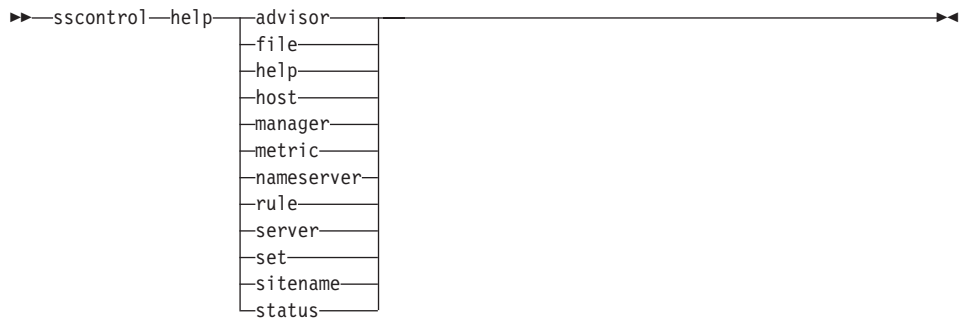
Datei (Datei1.sv) wurde in den Dispatcher geladen.
- Geben Sie den folgenden Befehl ein, um eine Konfigurationsdatei an die aktuelle Konfiguration anzuhängen und zu laden:
`sscontrol file appendload Datei2.sv`

Datei (Datei2.sv) wurde an die aktuelle Konfiguration angehängt und geladen.
- Geben Sie den folgenden Befehl ein, um einen Bericht über Ihre Dateien anzuzeigen (die Dateien, die zuvor gesichert wurden):
`sscontrol file report`

DATEIBERICHT:
Datei1.save
Datei2.sv
Datei3
- Geben Sie den folgenden Befehl ein, um die Konfiguration in der Datei Datei3 zu sichern:
`sscontrol file save Datei3`

Die Konfiguration wurde in Datei (Datei3) gesichert.

sscontrol help — Hilfetext für diesen Befehl anzeigen oder drucken



Beispiele

- Hilfetext zum Befehl "sscontrol" abrufen:

```
sscontrol help
```

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

ARGUMENTE BEFEHL HELP:

Verwendung: `help <Hilfeoption>`

Beispiel: `help name`

```
help      - vollständigen Hilfetext drucken
advisor  - Hilfe zum Befehl advisor
file      - Hilfe zum Befehl file
host      - Hilfe zum Befehl host
manager   - Hilfe zum Befehl manager
metric    - Hilfe zum Befehl metric
sitename  - Hilfe zum Befehl sitename
nameserver - Hilfe zum Befehl nameserver
rule      - Hilfe zum Befehl rule
server    - Hilfe zum Befehl server
set       - Hilfe zum Befehl set
status    - Hilfe zum Befehl status
```

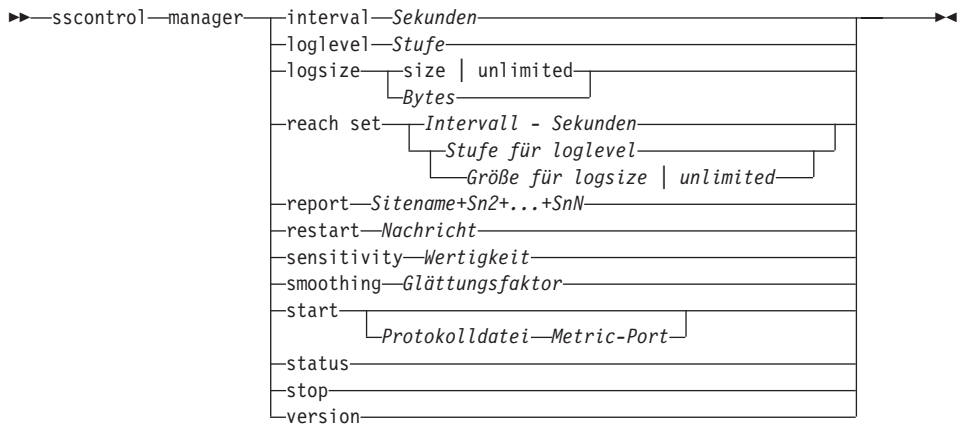
Parameter innerhalb von < > sind Variablen.

- Manchmal enthält der Hilfetext Optionen für die Variablen, die durch das Zeichen | voneinander getrennt sind:

```
logsize <Bytezahl | unlimited>
```

- Maximale Anzahl Bytes für Protokolldatei festlegen

sscontrol manager — Manager steuern



interval

Legt fest, wie oft der Manager die Wertigkeit der Server aktualisiert.

Sekunden

Eine positive Zahl, die in Sekunden darstellt, wie oft der Manager Wertigkeiten aktualisiert. Der Standardwert ist 2.

loglevel

Festlegen der Protokollstufe für das Manager-Protokoll und das Protokoll des Messwertüberwachungsprogramms.

Stufe

Die Nummer der Stufe (0 bis 5). Je größer die Zahl, desto mehr Informationen werden in das Manager-Protokoll geschrieben. Der Standardwert ist 1. Gültige Werte:

- 0 entspricht keiner Protokollierung
- 1 entspricht einer minimalen Protokollierung
- 2 entspricht einer Basisprotokollierung
- 3 entspricht einer normalen Protokollierung
- 4 entspricht einer erweiterten Protokollierung
- 5 entspricht einer ausführlichen Protokollierung.

logsize

Legt die maximale Größe des Protokolls des Managers fest. Wenn Sie für die Protokolldatei eine maximale Größe festlegen, wird die Protokollierung bei Erreichen der Größe am Anfang der Datei fortgesetzt, so dass die vorherigen Protokolleinträge überschrieben werden. Die Protokollgröße kann nicht auf einen geringeren Wert als die aktuelle Dateigröße gesetzt werden. Protokolleinträge sind mit einer Zeitmarke versehen, damit Sie

die Reihenfolge, in der sie geschrieben wurden, erkennen können. Je höher Sie die Protokollstufe setzen, desto vorsichtiger müssen Sie die Protokollgröße auswählen, da die Protokolldatei sehr schnell voll ist, wenn Sie eine Protokollierung auf einer höheren Stufe wählen.

Bytes

Die maximale Größe in Byte für die Protokolldatei des Managers. Sie können entweder eine positive Zahl, die größer als 0 sein muss, oder **unlimited** (unbegrenzt) angeben. Da die Protokolleinträge unterschiedlich lang sind, wird mit dem Überschreiben von Einträgen unter Umständen schon vor Erreichen der exakten maximalen Größe begonnen. Der Standardwert ist 1 MB.

reach set

Legt das Intervall, die Protokollstufe und die Protokollgröße für die Advisor-Funktion "reach" fest.

report

Zeigt eine statistische Momentaufnahme an.

Sitename

Der Sitename, der im Bericht angezeigt werden soll. Dies ist ein nicht auflösbarer Host-Name, den der Client abfragt. Der Sitename muss ein vollständig qualifizierter Domänenname sein.

Anmerkung: Zusätzliche Sitenamen werden durch ein Pluszeichen (+) voneinander getrennt.

restart

Startet alle Server (die nicht inaktiv sind) mit der Standardwertigkeit (1/2 der maximalen Wertigkeit).

Nachricht

Eine Nachricht, die in die Protokolldatei des Managers gestellt werden soll.

sensitivity

Legt die Mindestsensitivität für die Aktualisierung von Wertigkeiten fest. Diese Einstellung definiert, wann der Manager seine Serverwertigkeit ausgehend von externen Informationen ändern sollte.

Wertigkeit

Eine Zahl von 0 bis 100, die als prozentuale Wertigkeit verwendet wird. Der Standardwert 5 bewirkt eine Mindestsensitivität von 5 %.

smoothing

Festlegen eines Faktors, der Wertigkeitsabweichungen während des Lastausgleichs glättet. Ein höherer Glättungsfaktor führt zu einer weniger drastischen Änderung von Serverwertigkeiten bei Änderungen an den

Netzbedingungen. Ein geringerer Glättungsfaktor führt zu einer drastischen Änderung der Serverwertigkeiten.

Faktor

Eine positive Gleitkommazahl. Der Standardwert ist 1,5.

start

Den Manager starten.

Protokolldatei

Der Name der Datei, in der die Daten des Managers protokolliert werden. Jeder Eintrag des Protokolls ist mit einer Zeitmarke versehen.

Die Standarddatei ist im Verzeichnis **logs** installiert. Lesen Sie hierzu die Informationen in „Anhang F. Beispielkonfigurationsdateien“ auf Seite 393. Wollen Sie das Verzeichnis ändern, in dem die Protokolldateien gespeichert werden, lesen Sie die Informationen unter „Pfade für die Protokolldatei ändern“ auf Seite 222.

Metric-Port

Der Port, an dem Metric Server Systembelastungen meldet. Wenn Sie einen Metric-Port angeben, müssen Sie auch einen Protokolldateinamen angeben. Der Standard-Metric-Port ist 10004.

status

Anzeigen des aktuellen Status sowie der Standardeinstellungen für alle globalen Werte des Managers.

stop

Den Manager stoppen.

version

Zeigt die aktuelle Version des Managers an.

Beispiele

- Geben Sie den folgenden Befehl ein, um das Aktualisierungsintervall für den Manager auf 5 Sekunden zu setzen:
`sscontrol manager interval 5`
- Geben Sie den folgenden Befehl ein, um die Stufe der Protokollierung zwecks Verbesserung der Leistung auf 0 zu setzen:
`sscontrol manager loglevel 0`
- Geben Sie den folgenden Befehl ein, um die Größe des Protokolls des Managers auf 1.000.000 Byte zu setzen:
`sscontrol manager logsize 1000000`
- Geben Sie den folgenden Befehl ein, um eine statistische Momentaufnahme des Managers abzurufen:
`sscontrol manager report`

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

SERVER	STATUS
9.67.129.221	AKTIV
9.67.129.213	AKTIV
9.67.134.223	AKTIV

LEGENDE ZUM MANAGERBERICHT

CPU	CPU-Last
MEM	Speicherlast
SYS	Systemmetrik
JETZT	Aktuelle Gewichtung
NEU	Neue Gewichtung
GWT	Gewichtung

meineSite	GWT	CPU 49 %	MEM 50 %	PORT 1 %	SYS 0 %
	JETZT NEU	GWT LAST	GWT LAST	GWT LAST	GWT LAST
9.37.56.180	10 10	-99 -1	-99 -1	-99 -1	0 0
SUMMEN:	10 10	-1	-1	-1	0

ADVISOR	SITENAME:PORT	ZEITLIMIT
http	80	unlimited

- Neustart aller Server mit Standardwertigkeit und Schreiben einer Nachricht in die Manager-Protokolldatei:

`sscontrol manager restart` Neustart des Managers für Codeaktualisierung

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

320-14:04:54 Neustart des Managers für Codeaktualisierung

- Setzen der Sensitivität für Wertigkeitsänderungen auf 10:

`sscontrol manager sensitivity 10`

- Geben Sie den folgenden Befehl ein, um den Glättungsfaktor auf 2,0 zu setzen:

`sscontrol manager smoothing 2.0`

- Geben Sie den folgenden Befehl ein, um den Manager zu starten und die Protokolldatei `ndmgr.log` anzugeben (Pfade können nicht angegeben werden):

`sscontrol manager start ndmgr.log`

- Geben Sie den folgenden Befehl ein, um den aktuellen Status der Werte anzuzeigen, die dem Manager zugeordnet sind:

```
sscontrol manager status
```

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

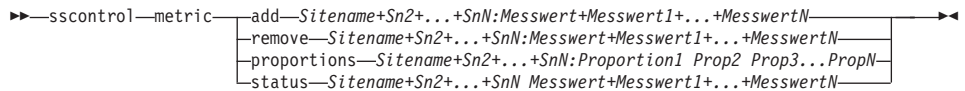
Manager-Status:

=====

```
Metrik-Port ..... 10004
Name der Managerprotokolldatei ..... manager.log
Managerprotokollstufe ..... 1
Max. Managerprotokollgröße (Bytes) ..... unlimited
Sensitivitätsstufe ..... 5
Glättungsfaktor ..... 1,5
Aktualisierungsintervall (Sekunden) ..... 2
Gewichtungsaktualisierungszyklus ..... 2
Erreichbarkeit - Protokollstufe ..... 1
Erreichbarkeit - Max. Protokollgröße (Bytes) ..... unlimited
Erreichbarkeit - Aktualisierungsintervall (Sekunden) ... 7
```

- Stoppen des Managers:
sscontrol manager stop
- Geben Sie den folgenden Befehl ein, um die aktuelle Versionsnummer des Managers aufzurufen:
sscontrol manager version

sscontrol metric — Systemmesswerte konfigurieren



add

Hinzufügen des angegebenen Messwerts.

Sitename

Der konfigurierte Sitename. Zusätzliche Sitenamen werden durch ein Pluszeichen (+) voneinander getrennt.

Messwert

Name des Systemmesswerts. Es muss sich um den Namen einer ausführbaren Datei oder Script-Datei im Verzeichnis des Messwertservers handeln.

remove

Entfernen des angegebenen Messwerts.

proportions

Der Parameter "proportions" gibt die Wichtigkeit an, die jedem Messwert verglichen mit anderen zugeordnet wird, wenn die Messwerte kombiniert werden, um die Systembelastung eines Servers zu ermitteln.

status

Anzeigen der aktuellen Serverwerte für diesen Messwert.

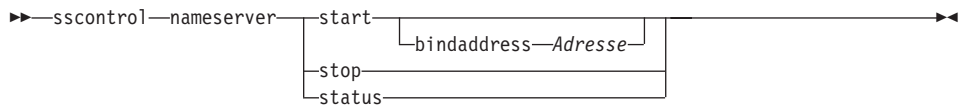
Beispiele

- Hinzufügen eines Systemmesswerts:
`sscontrol metric add Site1:Messwert1`
- Festlegen der Proportionen für einen Sitenamen mit zwei Systemmesswerten:
`sscontrol metric proportions Site1 0 100`
- Anzeigen des aktuellen Status der zugeordneten Messwerte:
`sscontrol metric status Site1:Messwert1`

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

```
Metrikstatus:
-----
Sitename ..... Site1
Metrikname ..... Messwert1
Metrikproportion ..... 50
  Server ..... 9.37.56.100
  Metrikdaten .... -1
```

sscontrol nameserver — Namensserver steuern



start

Starten des Namensservers.

bindaddress

Startet den Namensserver, der an die angegebene Adresse gebunden ist. Der Namensserver antwortet nur auf Anfragen, die an diese Adresse gerichtet sind.

Adresse

Eine auf der Maschine mit Site Selector konfigurierte Adresse (IP-Adresse oder symbolischer Name).

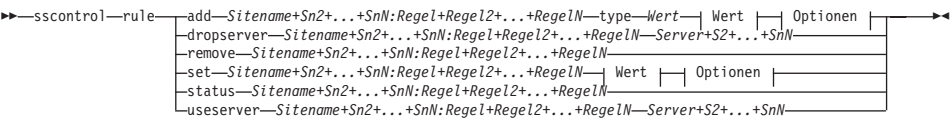
stop

Stoppt den Namensserver.

status

Zeigt den Status des Namensservers an.

sscontrol rule — Regeln konfigurieren



Optionen:

beginrange	Niedrig	endrange	Hoch
priority	Wert		
metricname	Wert		

add

Diese Regel zu einem Sitenamen hinzufügen.

Sitename

Ein nicht auflösbarer Host-Name, den der Client abfragt. Der Sitename muss ein vollständig qualifizierter Domänenname sein. Zusätzliche Sitenamen werden durch ein Pluszeichen (+) voneinander getrennt.

Regel

Der für die Regel ausgewählte Name. Dieser Name kann eine beliebige Kombination aus alphanumerischen Zeichen, Unterstreichungszeichen, Silbentrennungsstrichen und Punkten sein. Der Name kann 1 bis 20 Zeichen lang sein und darf keine Leerzeichen enthalten.

Anmerkung: Zusätzliche Regeln werden durch ein Pluszeichen (+) getrennt.

type

Der Regeltyp.

Typ

Die Auswahlmöglichkeiten für *Typ* sind:

ip Die Regel basiert auf der Client-IP-Adresse.

metricall

Die Regel basiert auf dem aktuellen Messwert für alle Server der Gruppe.

metricavg

Die Regel basiert auf dem Durchschnitt der aktuellen Messwerte für alle Server der Gruppe.

time Die Regel basiert auf der Uhrzeit.

wahr Diese Regel ist immer wahr. Sie kann mit der Anweisung ELSE in der Programmierlogik verglichen werden.

beginrange

Der untere Wert des Bereichs, mit dem bestimmt wird, ob die Regel wahr ist oder nicht.

Niedrig

Hängt von der Art der Regel ab. Die Art des Werts und der Standardwert werden nachfolgend nach der Art der Regel aufgelistet:

ip Die Adresse des Clients als symbolischer Name oder in Schreibweise mit Trennzeichen. Der Standardwert ist 0.0.0.0.

Zeit Eine ganze Zahl. Der Standardwert ist 0. Er stellt Mitternacht dar.

metricall

Eine ganze Zahl. Der Standardwert ist 100.

metricavg

Eine ganze Zahl. Der Standardwert ist 100.

endrange

Der obere Wert des Bereichs, mit dem bestimmt wird, ob die Regel wahr ist oder nicht.

Hoch

Hängt von der Art der Regel ab. Die Art des Werts und der Standardwert werden nachfolgend nach der Art der Regel aufgelistet:

ip Die Adresse des Clients als symbolischer Name oder in Schreibweise mit Trennzeichen. Der Standardwert ist 255.255.255.254.

Zeit Eine ganze Zahl. Der Standardwert ist 24. Er stellt Mitternacht dar.

Anmerkung: Beim Definieren des Anfangsbereichs (beginrange) und Endbereichs (endrange) der Zeitintervalle ist darauf zu achten, dass jeder Wert eine ganze Zahl sein muss, die nur den Stundenteil der Uhrzeit darstellt. Es werden keine Teilwerte einer Stunde angegeben. Soll beispielsweise die Stunde von 3 Uhr bis 4 Uhr angegeben werden, geben Sie für beginrange 3 und für endrange ebenfalls 3 an. Damit werden alle Minuten von 3 Uhr bis 3 Uhr 59 angegeben. Wird "beginrange" auf 3 und "endrange" auf 4 gesetzt, ergibt sich ein fast zweistündiger Zeitraum von 3.00 Uhr bis 4.59 Uhr.

metricall

Eine ganze Zahl. Der Standardwert ist 2 hoch 32 minus 1.

metricavg

Eine ganze Zahl. Der Standardwert ist 2 hoch 32 minus 1.

Priorität

Die Reihenfolge, in der die Regeln überprüft werden.

Stufe

Eine ganze Zahl. Wenn Sie für die erste Regel, die Sie hinzufügen, keine Priorität angeben, setzt Site Selector die Priorität standardmäßig auf 1. Wird eine weitere Regel hinzugefügt, wird deren Priorität standardmäßig mit der folgenden Formel errechnet: 10 + derzeit niedrigste Priorität für alle vorhandenen Regeln. Beispiel: Sie haben eine Regel mit der Priorität 30. Sie fügen nun eine neue Regel hinzu und setzen deren Priorität auf 25 (also auf eine *höhere* Priorität als 30). Anschließend fügen Sie eine dritte Regel ohne Angabe einer Priorität hinzu. Als +Priorität der dritten Regel wird 40 ermittelt (30 + 10).

metricname

Name des für eine Regel gemessenen Messwerts.

dropserver

Einen Server aus einem Regelsatz entfernen.

Server

Die IP-Adresse der TCP-Servermaschine als symbolischer Name oder in Schreibweise mit Trennzeichen.

Anmerkung: Zusätzliche Sitenamen werden durch ein Pluszeichen (+) voneinander getrennt.

remove

Eine oder mehrere Regeln, die durch Pluszeichen voneinander getrennt sind, entfernen.

set

Werte für diese Regel festlegen.

status

Anzeigen aller Werte für eine oder mehrere Regel(n).

useserver

Server in einen Regelsatz einfügen.

Beispiele

- Hinzufügen einer immer gültigen Regel ohne Angabe eines Anfangs- oder Endbereichs:

```
sscontrol rule add Sitename:Regelname type true priority 100
```

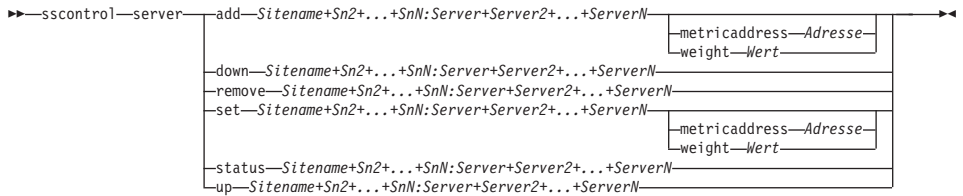
- Erstellen einer Regel, die den Zugriff auf einen Bereich von IP-Adressen unterbindet, der in diesem Fall mit "9" beginnt:

```
sscontrol rule add Sitename:Regelname type ip b 9.0.0.0 e 9.255.255.255
```

- Soll eine Regel erstellt werden, die die Verwendung eines bestimmten Servers in der Zeit von 11 Uhr bis 15 Uhr angibt, den folgenden Befehl eingeben:

```
sscontrol rule add Sitename:Regelname type time beginrange 11 endrange 14  
sscontrol rule useserver Sitename:Regelname Server05
```

sscontrol server — Server konfigurieren



add

Diesen Server hinzufügen.

Sitename

Ein nicht auflösbarer Host-Name, den der Client abfragt. Der Sitename muss ein vollständig qualifizierter Domänenname sein. Zusätzliche Sitenamen werden durch ein Pluszeichen (+) voneinander getrennt.

Server

Die IP-Adresse der TCP-Servermaschine als symbolischer Name oder in Schreibweise mit Trennzeichen.

Anmerkung: Zusätzliche Server werden durch ein Pluszeichen (+) getrennt.

metricaddress

Die Adresse des Metric-Servers.

Adresse

Die Adresse des Servers als symbolischer Name oder in Schreibweise mit Trennzeichen.

weight

Eine Zahl von 0 bis 100 (die den Wert für die Wertigkeitsobergrenze des angegebenen Sitenamens nicht überschreiten darf) zur Angabe der Wertigkeit für diesen Server. Wird die Wertigkeit auf 0 gesetzt, werden keine neuen Anforderungen an den Server gesendet. Der Standardwert entspricht der Hälfte der Wertigkeitsobergrenze für den angegebenen Sitenamen. Ist der Manager aktiv, wird diese Einstellung schnell überschrieben.

Wert

Die Wertigkeit des Servers.

down

Diesen Server als inaktiv markieren. Dieser Befehl verhindert, dass weitere Anforderungen an diesen Server übergeben werden.

remove

Diesen Server entfernen.

set

Werte für diesen Server festlegen.

status

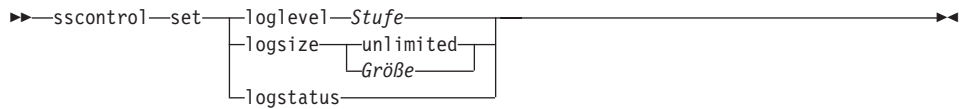
Status der Server anzeigen.

up Diesen Server als "aktiv" kennzeichnen. Site Selector übergibt neue Anforderungen an diesen Server.

Beispiele

- Hinzufügen des Servers 27.65.89.42 zum Sitenamen Site1:
sscontrol
server add Site1:27.65.89.42
- Geben Sie den folgenden Befehl ein, um den Server an 27.65.89.42 als "ausgefallen" zu kennzeichnen:
sscontrol server down Site1:27.65.89.42
- Entfernen des Servers 27.65.89.42 für alle Sitenamen:
sscontrol server remove :27.65.89.42
- Geben Sie den folgenden Befehl ein, um den Server an 27.65.89.42 als "aktiv" zu kennzeichnen:
sscontrol server up Site1:27.65.89.42

sscontrol set — Serverprotokoll konfigurieren



loglevel

Die Stufe für die Protokollierung von sserver-Aktivitäten.

Stufe

Der Standardwert für **loglevel** ist 0. Gültige Werte sind:

- 0 entspricht keiner Protokollierung
- 1 entspricht einer minimalen Protokollierung
- 2 entspricht einer Basisprotokollierung
- 3 entspricht einer normalen Protokollierung
- 4 entspricht einer erweiterten Protokollierung
- 5 entspricht einer ausführlichen Protokollierung.

logsize

Die maximale Anzahl von Byte, die in der Protokolldatei protokolliert werden können.

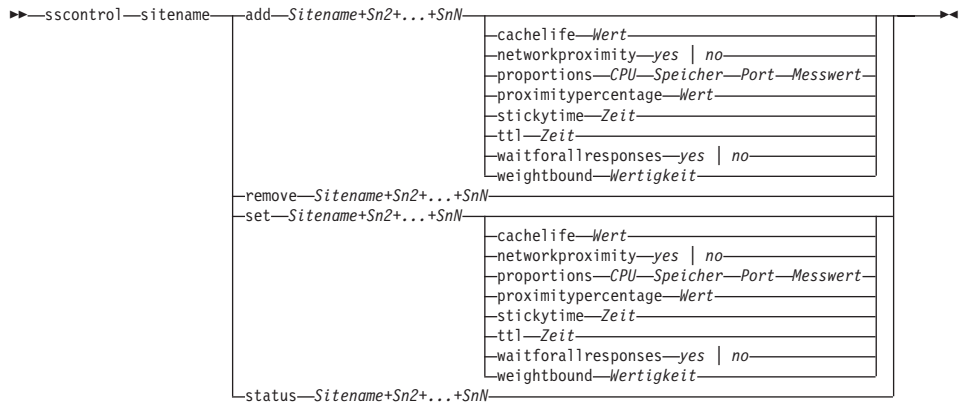
Größe

Der Standardwert für "logsize" ist 1 MB.

logstatus

Zeigt die Einstellungen des Serverprotokolls (Protokollstufe und -größe) an.

sscontrol sitename — Sitenamen konfigurieren



add

Hinzufügen eines neuen Sitenamens.

Sitename

Ein nicht auflösbarer Host-Name, der vom Client angefragt wird. Zusätzliche Sitenamen werden durch ein Pluszeichen (+) voneinander getrennt.

cachelife

Die Zeitperiode, während der eine Proximitätsantwort gültig und im Cache gespeichert bleibt. Der Standardwert ist 1800. Weitere Informationen hierzu finden Sie im Abschnitt „Netzproximität verwenden“ auf Seite 117.

Wert

Eine positive Zahl, die angibt, wie viele Sekunden eine Proximitätsantwort gültig ist und im Cache gespeichert wird.

networkproximity

Legt die Netzproximität des Servers zum anfordernden Client fest. Verwenden Sie diese Proximitätsantwort bei der Lastausgleichsentscheidung. Die Proximität ist "Ein" oder "Aus". Weitere Informationen hierzu finden Sie im Abschnitt „Netzproximität verwenden“ auf Seite 117.

Wert

Zur Auswahl stehen "yes" oder "no". Der Standardwert "no" bedeutet, dass die Netzproximität inaktiviert ist.

proportions

Festlegen der proportionalen Bedeutung von CPU, Speicher, Port (Advisor-Informationen) und Systemmesswerten für den Metric Server. Anhand dieser Proportionen legt der Manager die Serverwertigkeiten fest. Jeder dieser Werte wird als Prozentsatz der Summe angegeben, die immer bei 100 liegt.

CPU Prozentsatz der auf jeder am Lastausgleich beteiligten Servermaschine genutzten CPU (Vorgabe vom Agenten Metric Server).

Speicher Prozentsatz des auf jeder am Lastausgleich beteiligten Servermaschine genutzten Speichers (Vorgabe vom Agenten Metric Server).

Port Vorgaben von den am Port empfangsbereiten Advisor-Funktionen.

System Vorgaben von Metric Server.

proximitypercentage

Legt die Bedeutung der Proximitätsantwort, gemessen am Status des Servers (Wertigkeit vom Manager), fest. Weitere Informationen hierzu finden Sie im Abschnitt „Netzproximität verwenden“ auf Seite 117.

Wert

Der Standardwert ist 50.

stickytime

Das Intervall, in dem ein Client dieselbe Server-ID empfängt, die zuvor auf die erste Anfrage zurückgegeben wurde. Der Standardwert für "stickytime" ist 0 und bedeutet, dass für den Sitenamen keine Haltezeit gilt.

Zeit

Eine positive Zahl ungleich null, die die Zeit in Sekunden angibt, in der der Client dieselbe Server-ID empfängt, die zuvor auf die erste Anfrage zurückgegeben wurde.

ttl Legt die Lebensdauer fest. Dieser Parameter gibt an, wie lange ein anderer Namensserver die aufgelöste Antwort zwischenspeichert. Der Standardwert ist 5.

Wert

Eine positive Zahl, die angibt, wie viele Sekunden der Namensserver die aufgelöste Antwort zwischenspeichert.

waitforallresponses

Legt fest, ob vor der Beantwortung der Client-Anfrage auf alle Proximitätsantworten der Server gewartet werden soll. Weitere Informationen hierzu finden Sie im Abschnitt „Netzproximität verwenden“ auf Seite 117.

Wert

Zur Auswahl stehen "yes" oder "no". Der Standardwert ist "yes".

weightbound

Eine Zahl, die die maximale Wertigkeit angibt, die für Server dieser Site festgelegt werden kann. Der für den Sitenamen festgelegte weightbound-Wert kann mit **server weight** für einzelne Server überschrieben werden. Der Standardwert für "sitename weightbound" ist 20.

Wertigkeit

Der Wert für "weightbound".

set

Festlegen der Merkmale für den Sitenamen.

remove

Entfernen dieses Sitenamens.

status

Anzeigen des aktuellen Status für einen bestimmten Sitenamen.

Beispiele

- Hinzufügen eines Sitenamens:
`sscontrol sitename add 130.40.52.153`
- Aktivieren der Netzproximität:
`sscontrol sitename set meineSite networkproximity yes`
- Festlegen einer Caching-Zeit von 1900000 Sekunden:
`sscontrol sitename set meineSite cachelife 1900000`
- Festlegen eines Proximitätsprozentsatzes von 45:
`sscontrol sitename set meineSeite proximitypercentage 45`
- Festlegung für einen Sitenamen, dass vor einer Reaktion nicht auf alle Antworten gewartet werden soll:
`sscontrol
sitename set meineSite waitforallresponses no`
- Festlegen einer Lebensdauer von 7 Sekunden:
`sscontrol sitename set meineSite ttl 7`
- Festlegen der proportionalen Bedeutung von cpuload, memload, Port und Systemmesswert:
`sscontrol sitename
set meineSite proportions 50 48 1 1`
- Entfernen eines Sitenamens:
`sscontrol sitename remove 130.40.52.153`

- Anzeigen des Status für den Sitenamen meineSite:
sscontrol sitename status meineSite

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Status des Sitenamens:

```

-----
SiteName ..... meineSite
Gewichtungsgrenze ..... 20
TTL ..... 5
Haltezeit ..... 0
Anzahl Server ..... 1
Proportion für CpuLoad ..... 49
Proportion für MemLoad ..... 50
Proportion für Port ..... 1
Proportion für Systemmetrik ..... 0
Advisor am Port ..... 80
Verwendete Proximität ..... N

```

►►sscontrol—status◄◄

Beispiele

- Geben Sie den folgenden Befehl ein, um festzustellen, welche Funktionen ausgeführt werden:
sscontrol status

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Namensserver wurde gestartet.
Manager wurde gestartet.

	ADVISOR		SITENAME:PORT		ZEITLIMIT	
	http		80		unlimited	

Anhang E. Befehlsreferenz für Consultant für Cisco CSS Switches

Dieser Anhang beschreibt die Verwendung der folgenden **lbcontrol**-Befehle für Consultant für Cisco CSS Switches:

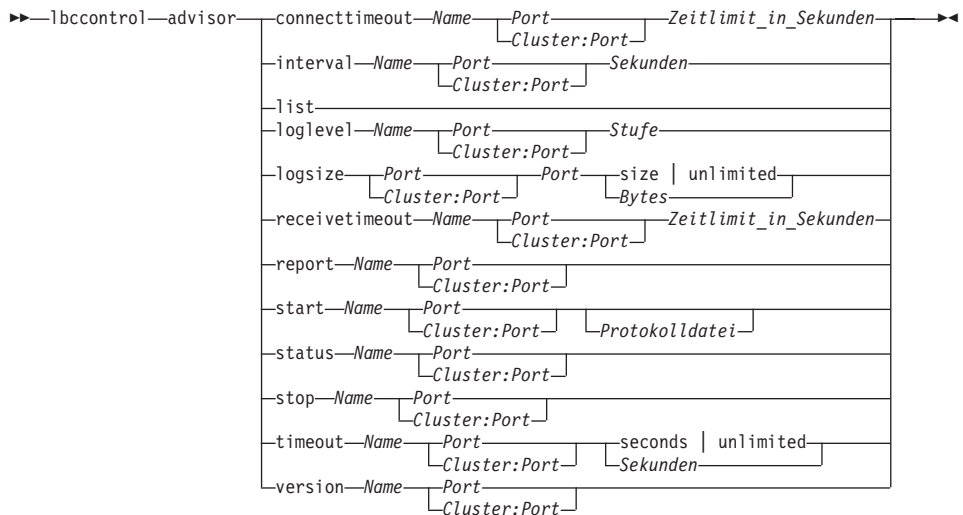
- „lbcontrol advisor — Advisor steuern“ auf Seite 364
- „lbcontrol cluster — Cluster konfigurieren“ auf Seite 369
- „lbcontrol executor — Executor steuern“ auf Seite 371
- „lbcontrol file — Konfigurationsdateien verwalten“ auf Seite 373
- „lbcontrol help — Hilfetext für diesen Befehl anzeigen oder drucken“ auf Seite 375
- „lbcontrol host — Ferne Maschine konfigurieren“ auf Seite 376
- „lbcontrol log — Binäre Protokolldatei steuern“ auf Seite 377
- „lbcontrol manager — Manager steuern“ auf Seite 378
- „lbcontrol metric — Systemmesswerte konfigurieren“ auf Seite 384
- „lbcontrol port — Ports konfigurieren“ auf Seite 386
- „lbcontrol server — Server konfigurieren“ auf Seite 388
- „lbcontrol set — Serverprotokoll konfigurieren“ auf Seite 390
- „lbcontrol status — Aktivitätsanzeige für Manager und Advisor-Funktionen“ auf Seite 391

Sie können eine Minimalversion der Parameter für den Befehl **ndcontrol** eingeben. Sie müssen nur die eindeutigen Buchstaben der Parameter eingeben. Beispiel: Wenn Sie Hilfe für den Befehl zum Speichern von Dateien aufrufen möchten, können Sie **lbcontrol he f** anstelle von **lbcontrol help file** eingeben.

Der Präfix **lbc** weist auf den Lastausgleich für Consultant hin.

Anmerkung: Die Werte der Befehlsparameter müssen in englischen Zeichen eingegeben werden. Die einzige Ausnahme hiervon bilden Host-Namen (die in den Befehlen **cluster** und **server** verwendet werden) und (die in Dateibefehlen verwendeten) Dateinamen.

lbccontrol advisor — Advisor steuern



connecttimeout

Definiert, wie lange eine Advisor-Funktion wartet, bevor sie meldet, dass zu einem Server keine Verbindung hergestellt werden kann. Weitere Informationen hierzu finden Sie im Abschnitt „Serververbindungs- und -empfangszeitlimit der Advisor-Funktion“ auf Seite 152.

Name

Der Name der Advisor-Funktion. Mögliche Werte sind **http**, **ftp**, **ssl**, **smtp**, **imap**, **pop3**, **nntp**, **telnet**, **connect**, **ping** und **WTE**. Die Namen angepasster Advisor-Funktionen haben das Format **xxxx**, wobei **ADV_xxxx** der Name der Klasse ist, die die angepasste Advisor-Funktion implementiert.

Port

Die Nummer des Ports, der von der Advisor-Funktion überwacht wird.

Zeitlimit_in_Sekunden

Eine positive ganze Zahl, die die Zeit in Sekunden angibt, nach deren Ablauf die Advisor-Funktion meldet, dass zu einem Server keine Verbindung hergestellt werden kann. Dieser Wert liegt standardmäßig beim Dreifachen des für das Advisor-Intervall angegebenen Wertes.

interval

Legt fest, wie oft der Advisor Informationen von den Servern abfragt.

Sekunden

Eine positive ganze Zahl, die die Zeit zwischen den an die Server gerichteten Statusabfragen in Sekunden angibt. Der Standardwert ist 15.

list

Zeigt eine Liste der Advisor an, die derzeit Informationen an den Manager liefern.

loglevel

Legt die Protokollstufe für ein Advisor-Protokoll fest.

Stufe

Die Nummer der Stufe (0 bis 5). Der Standardwert ist 1. Je größer die Zahl ist, desto mehr Informationen werden in das Advisor-Protokoll geschrieben. Die folgenden Werte sind gültig: 0 für keine Einträge, 1 für eine minimale Protokollierung, 2 für eine Basisprotokollierung, 3 für eine normale, 4 für eine erweiterte und 5 für eine ausführliche Protokollierung.

logsize

Legt die maximale Größe eines Advisor-Protokolls fest. Wenn Sie für die Protokolldatei eine maximale Größe festlegen, wird die Protokollierung bei Erreichen der Größe am Anfang der Datei fortgesetzt, so dass die vorherigen Protokolleinträge überschrieben werden. Die Protokollgröße kann nicht auf einen geringeren Wert als die aktuelle Dateigröße gesetzt werden. Protokolleinträge sind mit einer Zeitmarke versehen, damit Sie die Reihenfolge, in der sie geschrieben wurden, erkennen können. Je höher Sie die Protokollstufe setzen, desto vorsichtiger müssen Sie die Protokollgröße auswählen, da die Protokolldatei sehr schnell voll ist, wenn Sie eine Protokollierung auf einer höheren Stufe wählen.

Anzahl_Sätze

Die maximale Größe der Advisor-Protokolldatei in Bytes. Sie können entweder eine positive Zahl, die größer als 0 sein muss, oder das Wort **unlimited** (unbegrenzt) angeben. Da die Protokolleinträge unterschiedlich lang sind, wird mit dem Überschreiben von Einträgen unter Umständen schon vor Erreichen der exakten maximalen Größe begonnen. Der Standardwert ist 1 MB.

receivetimeout

Definiert, wie lange eine Advisor-Funktion wartet, bevor sie meldet, dass von einem Server keine Daten empfangen werden können. Weitere Informationen hierzu finden Sie im Abschnitt „Serververbindungs- und -empfangszeitlimit der Advisor-Funktion“ auf Seite 152.

Zeitlimit_in_Sekunden

Eine positive ganze Zahl, die die Zeit in Sekunden angibt, nach deren Ablauf die Advisor-Funktion meldet, dass von einem Server keine Daten empfangen werden können. Dieser Wert liegt standardmäßig beim Dreifachen des für das Advisor-Intervall angegebenen Wertes.

report

Anzeigen eines Berichts zum Advisor-Status.

start

Den Advisor starten. Für alle Protokolle stehen Advisor zur Verfügung.
Die Standard-Ports sind:

Advisor-Name	Protokoll	Port
connect	ICMP	12345
db2	privat	50000
ftp	FTP	21
http	HTTP	80
ibmproxy	HTTP (über 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	privat	10007

Anmerkung: Die FTP-Advisor-Funktion darf nur für den FTP-Steuer-Port (21) ausgeführt werden. Starten Sie eine FTP-Advisor-Funktion nicht für den FTP-Daten-Port (20).

Protokolldatei

Der Name der Datei, in die die Verwaltungsdaten geschrieben werden.
Jeder Satz im Protokoll wird mit einer Zeitmarke versehen.

Die Standarddatei ist *Advisor-Name_Port.log*, z. B. **http_80.log**. Wollen Sie das Verzeichnis ändern, in dem die Protokolldateien gespeichert werden, lesen Sie die Informationen unter „Pfade für die Protokolldatei ändern“ auf Seite 222.

Legen Sie die Manager-Proportionen fest, um sicherzustellen, dass die Advisor-Informationen verwendet werden.

status

Anzeigen des aktuellen Status aller globalen Werte der Advisor-Funktion mit den zugehörigen Standardeinstellungen.

stop

Den Advisor stoppen.

Zeitlimit

Legt die Zeit in Sekunden fest, in der der Manager von der Advisor-Funk-

tion erhaltene Informationen als gültig ansieht. Stellt der Manager fest, dass die Advisor-Informationen älter als die hier angegebene Zeit sind, verwendet der Manager diese Informationen nicht zum Bestimmen Wertigkeiten für die Server am Port, die von der Advisor-Funktion überwacht werden. Dieses Zeitlimit gilt nicht, wenn die Advisor-Funktion den Manager darüber informiert, dass ein bestimmter Server inaktiv ist. Der Manager verwendet diese Informationen über den Server auch, nachdem die Advisor-Informationen das Zeitlimit überschritten haben.

Sekunden

Eine positive Zahl, die die Anzahl von Sekunden darstellt, oder das Wort **unlimited** (unbegrenzt). Der Standardwert ist "unlimited".

version

Zeigt die aktuelle Advisor-Version an.

Beispiele

- Festlegen der Zeit (30 Sekunden), die eine HTTP-Advisor-Funktion (für Port 80) wartet, bevor sie meldet, dass zu einem Server keine Verbindung hergestellt werden kann:

```
lbcontrol advisor connecttimeout http 80 30
```

- Festlegen des Intervalls für die FTP-Advisor-Funktion (für Port 21) auf 6 Sekunden:

```
lbcontrol  
advisor interval ftp 21 6
```

- Geben Sie den folgenden Befehl ein, um eine Liste der Advisor anzuzeigen, die derzeit Informationen an den Manager liefern:

```
lbcontrol advisor list
```

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

ADVISOR	PORT	ZEITLIMIT
http	80	unlimited
ftp	21	unlimited

- Ändern der Protokollstufe für das Advisor-Protokoll auf 0, um einen höheren Durchsatz zu erreichen:
lbcontrol advisor loglevel http 80 0
- Ändern der Advisor-Protokollgröße in 5.000 Bytes:
lbcontrol advisor logsize ftp 21 5000
- Festlegen der Zeit (60 Sekunden), die eine HTTP-Advisor-Funktion (für Port 80) wartet, bevor sie meldet, dass von einem Server keine Daten empfangen werden können:

```
lbcontrol advisor receivetimeout http 80 60
```

- Anzeigen eines Berichts zum Status der Advisor-Funktion ftp (für Port 21):

```
lbcontrol
advisor report ftp 21
```

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Advisor-Bericht:

```
Advisor-Name ..... Ftp
Port-Nummer ..... 21

Cluster-Adresse ..... 9.67.131.18
Serveradresse ..... 9.67.129.230
Last ..... 8
```

```
Cluster-Adresse ..... 9.67.131.18
Serveradresse ..... 9.67.131.215
Last ..... -1
```

- Geben Sie den folgenden Befehl ein, um den Advisor mit der Datei ftpadv.log zu starten:

```
lbcontrol advisor start ftp 21 ftpadv.log
```

- Anzeigen des aktuellen Status der Werte, die der Advisor-Funktion http zugeordnet sind:

```
lbcontrol
advisor status http 80
```

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

Advisor-Status:

```
Intervall (Sekunden) ..... 15
Zeitlimit (Sekunden) ..... Unlimited
Zeitlimit für Verbindung (Sekunden) ..... 21
Zeitlimit für Empfang (Sekunden) ..... 21
Advisor-Protokolldateiname ..... Http_80.log
Protokollstufe ..... 1
Maximale Managerprotokollgröße (Bytes)... Unlimited
```

- Stoppen der Advisor-Funktion http am Port 80:

```
lbcontrol
advisor stop http 80
```

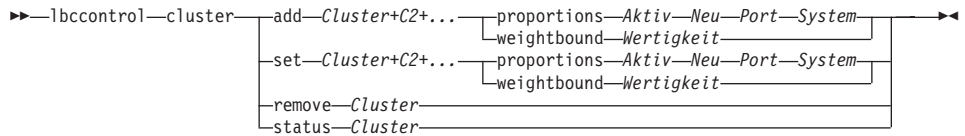
- Setzen des Zeitlimits für Advisor-Informationen auf 5 Sekunden:

```
lbcontrol advisor timeout ftp 21 5
```

- Ermitteln der aktuellen Versionsnummer für die Advisor-Funktion ssl:

```
lbcontrol
advisor version ssl 443
```

lbcontrol cluster — Cluster konfigurieren



add

Diesen Cluster hinzufügen. Sie müssen mindestens 1 Cluster definieren.

weightbound

Legt die maximale Wertigkeit von Servern an diesem Port fest. Dieser Parameter beeinflusst, wie stark sich die Anzahl der Anforderungen, die Cisco CSS Switch den einzelnen Servern zuteilt, unterscheidet. Der Standardwert ist 10.

Wertigkeit

Die Wertigkeitsgrenze.

set

Die Merkmale des Clusters festlegen.

proportions

Legt die relative Wichtigkeit von aktiven Verbindungen (*Aktiv*), von neuen Verbindungen (*Neu*), von Advisor-Informationen (*Port*) und der Informationen von Metric Server (*System*) fest, die der Manager für die Festlegung der Serverwertigkeit verwendet. Alle diese Werte, die nachfolgend beschrieben werden, werden als Prozentsatz der Summe angegeben und müssen daher immer 100 ergeben. Weitere Informationen hierzu finden Sie im Abschnitt „Proportionale Bedeutung von Statusinformationen“ auf Seite 145.

Aktiv

Eine Zahl von 0 bis 100 für die proportionale Wertigkeit, die den aktiven Verbindungen zugeordnet wird. Der Standardwert ist 50.

Neu

Eine Zahl von 0 bis 100 für die proportionale Wertigkeit, die den neuen Verbindungen zugeordnet wird. Der Standardwert ist 50.

Port

Eine Zahl von 0 bis 100 für die proportionale Wertigkeit, die den Informationen von Advisor-Funktionen zugeordnet wird. Der Standardwert ist 0.

System

Eine Zahl von 0 bis 100 für die proportionale Wertigkeit, die den Informationen von den Systemmesswerten zugeordnet wird. Der Standardwert ist 0.

remove

Diesen Cluster entfernen.

status

Den aktuellen Status eines bestimmten Clusters anzeigen.

Beispiele

- Geben Sie den folgenden Befehl ein, um die Cluster-Adresse 130.40.52.153 hinzuzufügen:
`lbcontrol cluster add 130.40.52.153`
- Geben Sie den folgenden Befehl ein, um die Cluster-Adresse 130.40.52.153 zu entfernen:
`lbcontrol
cluster remove 130.40.52.153`
- Geben Sie den folgenden Befehl ein, um die relative Bedeutung festzulegen, die der von dem Manager erhaltenen Eingabe zugeordnet werden soll:
`lbcontrol cluster proportions 60 35 5 0`
- Geben Sie den folgenden Befehl ein, um den Status für Cluster-Adresse 9.67.131.167 anzuzeigen:
`lbcontrol cluster status 9.67.131.167`

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

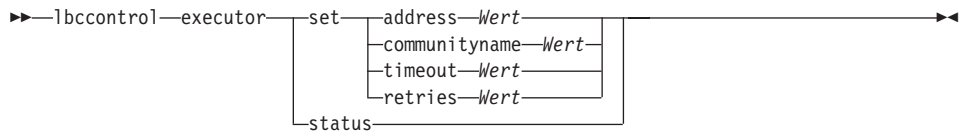
Cluster-Status:

```

Adresse ..... 9.67.131.167
Anzahl Ziel-Ports ..... 3
Strd.-Gewichtungsgrenze für Port ..... 10
Proportion für aktive Verbindungen ..... 49
Proportion für neue Verbindungen ..... 49
Port-spezifische Proportion ..... 2
Proportion für Systemmetrik ..... 0

```

lbcontrol executor — Executor steuern



set

Die Felder des Executors festlegen.

Adresse

Die IP-Adresse oder der Host-Name, die bzw. der für Kontakte zum Cisco CSS Switch zu Verwaltungszwecken verwendet wird. Weitere Informationen hierzu finden Sie in der Veröffentlichung *Cisco Content Services Switch Basic Configuration Guide*.

Wert

Gültige IP-Adresse oder gültiger Host-Name.

communityname

Der für die SNMP-Kommunikation mit dem Cisco CSS Switch verwendete Name der SNMP-Benutzergemeinschaft. Weitere Informationen hierzu finden Sie in der Veröffentlichung *Cisco Content Services Switch Basic Configuration Guide*.

Wert

Der Standardwert ist "public" mit Schreib- und Lesezugriff.

timeout

Die Zeit in Sekunden, nach der für SNMP-Anfragen von Cisco Consultant beim Cisco CSS Switch eine Zeitlimitüberschreitung festgestellt wird. Cisco Consultant verwendet SNMP, um Informationen vom Cisco CSS Switch abzurufen. Falls Nachrichten in der Datei `manager.log` auf häufige Zeitlimitüberschreitungen hinweisen, können Sie diesen Wert entsprechend anpassen.

Wert

Der Standardwert ist 3.

retries

Die Häufigkeit, mit der Cisco Consultant eine an den Cisco CSS Switch abgesetzte SNMP-Abfrage wiederholt. Falls Nachrichten in der Datei `manager.log` auf ein häufiges Scheitern von SNMP-Abfragen hinweisen, können Sie diesen Wert entsprechend anpassen.

Wert

Der Standardwert ist 2.

status

Anzeigen des aktuellen Status für die im Executor definierbaren Werte und ihrer Standardeinstellungen.

Beispiele

- Anzeigen der internen Zähler für Cisco Consultant:

```
lbccontrol executor status
```

```
Executor-Status:
```

```
-----
```

```
Adresse ..... 9.67.131.151
```

```
Community-Name ..... public
```

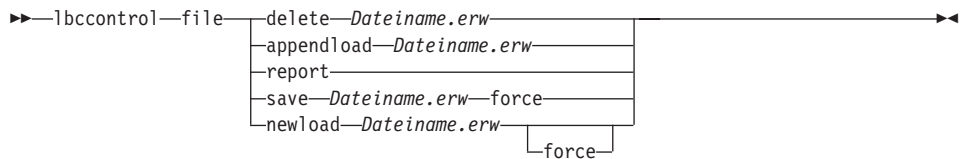
```
Zeitlimitwert ..... 3
```

```
Anzahl Wiederholungen ..... 2
```

- Festlegen der Adresse 130.40.52.167:

```
lbccontrol executor set address 130.40.52.167
```

lbccontrol file — Konfigurationsdateien verwalten



delete

Die Datei löschen.

Dateiname.erw

Eine Konfigurationsdatei.

Die Dateierweiterung (.*erw*) ist optional und kann beliebig gewählt werden.

appendload

Hinzufügen einer Konfigurationsdatei zur aktuellen Konfiguration und laden der Datei in Cisco Consultant.

report

Bericht über die verfügbare(n) Datei(en).

save

Sichern der aktuellen Konfiguration für Cisco Consultant in der Datei.

Anmerkung: Dateien werden in den nachfolgend genannten Verzeichnissen gespeichert und aus diesen geladen:

- AIX: **/usr/lpp/nd/servers/configurations/lbc**
- Linux: **/opt/nd/servers/configurations/lbc**
- Solaris: **/opt/nd/servers/configurations/lbc**
- Windows 2000:

Allgemeiner Installationsverzeichnispfad —

c:\Programme\ibm\edge\nd\servers\configurations\Komponente

Interner Installationsverzeichnispfad —

c:\Programme\ibm\nd\servers\configurations\Komponente

force

Wenn Sie Ihre Datei in einer vorhandenen Datei mit demselben Namen speichern möchten, verwenden Sie **force**, um die vorhandene Datei vor dem Speichern der neuen Datei zu löschen. Bei Nichtverwendung der Option "force" wird die vorhandene Datei nicht überschrieben.

newload

Laden einer neuen Konfigurationsdatei in Cisco Consultant. Die neue Konfigurationsdatei ersetzt die aktuelle Konfiguration.

Beispiele

- Geben Sie den folgenden Befehl ein, um eine Datei zu löschen:
`lbcontrol file delete Datei3`

Datei (Datei3) wurde gelöscht.
- Geben Sie den folgenden Befehl ein, um eine neue Konfigurationsdatei zu laden, die die aktuelle Konfiguration ersetzt:
`lbcontrol file newload Datei1.sv`

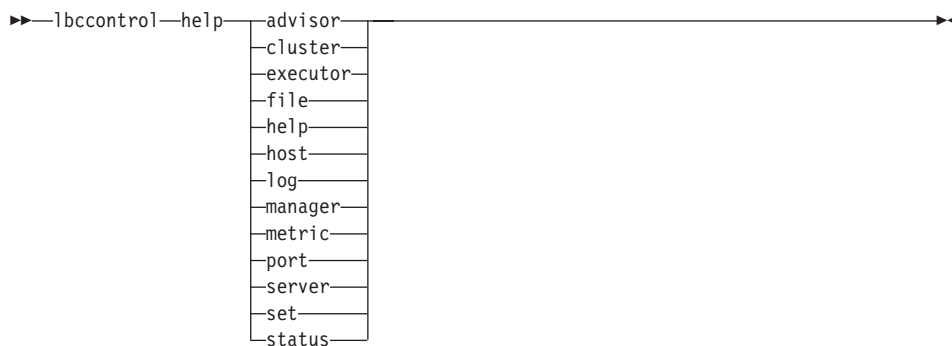
Datei (Datei1.sv) wurde in den Dispatcher geladen.
- Geben Sie den folgenden Befehl ein, um eine Konfigurationsdatei an die aktuelle Konfiguration anzuhängen und zu laden:
`lbcontrol file appendload Datei2.sv`

Datei (Datei2.sv) wurde an die aktuelle Konfiguration angehängt und geladen.
- Geben Sie den folgenden Befehl ein, um einen Bericht über Ihre Dateien anzuzeigen (die Dateien, die zuvor gesichert wurden):
`lbcontrol file report`

DATEIBERICHT:
Datei1.save
Datei2.sv
Datei3
- Geben Sie den folgenden Befehl ein, um die Konfiguration in der Datei Datei3 zu sichern:
`lbcontrol file save Datei3`

Die Konfiguration wurde in Datei (Datei3) gesichert.

lbccontrol help — Hilfetext für diesen Befehl anzeigen oder drucken



Beispiele

- Hilfetext zum Befehl "lbccontrol" abrufen:

```
lbccontrol help
```

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

```
ARGUMENTE BEFEHL HELP:
```

```
-----
```

```
Verwendung:  help <Hilfeoption>
```

```
Beispiel:    help cluster
```

executor	- Hilfe zum Befehl executor
cluster	- Hilfe zum Befehl cluster
port	- Hilfe zum Befehl port
server	- Hilfe zum Befehl server
manager	- Hilfe zum Befehl manager
metric	- Hilfe zum Befehl metric
advisor	- Hilfe zum Befehl advisor
file	- Hilfe zum Befehl file
host	- Hilfe zum Befehl host
log	- Hilfe zum Befehl log
set	- Hilfe zum Befehl set
status	- Hilfe zum Befehl status
help	- vollständigen Hilfetext drucken

Parameter innerhalb von < > sind Variablen.

lbcontrol host — Ferne Maschine konfigurieren

►—lbcontrol—host:—*ferner_Host*—►◀

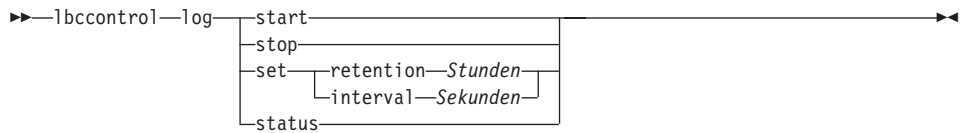
ferner_Host

Der Name der fernen Maschine mit Cisco Consultant, die konfiguriert wird. Bei Eingabe dieses Befehls müssen Sie darauf achten, dass Sie zwischen **host:** und *ferner_Host* kein Leerzeichen eingeben. Beispiel:

```
lbcontrol host:ferner_Host
```

Setzen Sie diesen Befehl an einer Eingabeaufforderung ab. Geben Sie dann einen gültigen lbcontrol-Befehl ein, der an die ferne Maschine mit Cisco Consultant abgesetzt werden soll.

lbccontrol log — Binäre Protokolldatei steuern



start

Binäres Protokoll starten.

stop

Binäres Protokoll stoppen.

set

Legt Felder für die binäre Protokollierung fest. Weitere Informationen zum Festlegen von Feldern für die binäre Protokollierung finden Sie im Abschnitt „Binäres Protokollieren verwenden, um Serverstatistiken zu analysieren“ auf Seite 213.

retention

Die Zeit in Stunden, die binäre Protokolldateien aufbewahrt werden.
Der Standardwert für retention ist 24.

Stunden

Die Anzahl der Stunden.

interval

Die Anzahl der Sekunden zwischen dem Protokollieren von Einträgen.
Der Standardwert für interval ist 60.

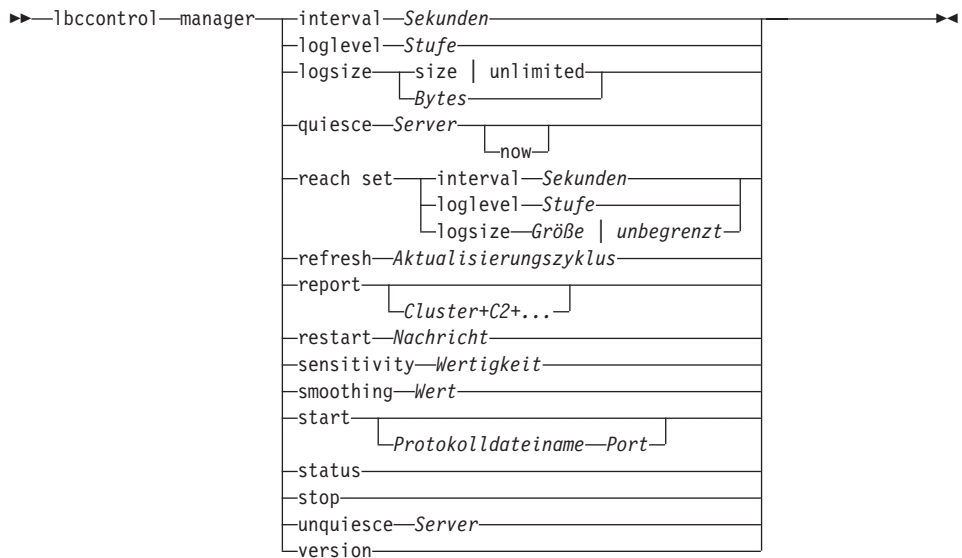
Sekunden

Die Anzahl der Sekunden.

status

Zeigt die Verweildauer und das Intervall des binären Protokolls.

lbcontrol manager — Manager steuern



interval

Legt fest, wie oft der Manager die Wertigkeit der Server für den Cisco CSS Switch aktualisiert. Dabei werden die Kriterien aktualisiert, die der Cisco CSS Switch für die Weiterleitung von Client-Anforderungen verwendet.

Sekunden

Eine positive Zahl, die in Sekunden darstellt, wie oft der Manager Wertigkeiten für den Cisco CSS Switch aktualisiert. Der Standardwert ist 15 mit einem Mindestintervall von 10. Wenn Sie versuchen, das Manager-Intervall auf einen kleineren Wert als 10 Sekunden zu setzen, wird es auf 10 Sekunden gesetzt. Wir empfehlen die Verwendung des Standard-Manager-Intervalls von 15 Sekunden, da der Cisco CSS Switch nicht von häufigeren Aktualisierungen profitieren kann.

loglevel

Legt die Protokollstufe für das Protokoll des Managers fest.

Stufe

Die Nummer der Stufe (0 bis 5). Je größer die Zahl, desto mehr Informationen werden in das Manager-Protokoll geschrieben. Der Standardwert ist 1. Die folgenden Werte sind gültig: 0 für keine Einträge, 1 für eine minimale Protokollierung, 2 für eine Basisprotokollierung, 3 für eine normale, 4 für eine erweiterte und 5 für eine ausführliche Protokollierung.

logsize

Legt die maximale Größe des Protokolls des Managers fest. Wenn Sie für die Protokolldatei eine maximale Größe festlegen, wird die Protokollierung bei Erreichen der Größe am Anfang der Datei fortgesetzt, so dass die vorherigen Protokolleinträge überschrieben werden. Die Protokollgröße kann nicht auf einen geringeren Wert als die aktuelle Dateigröße gesetzt werden. Protokolleinträge erhalten Zeitmarken, die die Reihenfolge angeben, in der sie geschrieben wurden. Je höher Sie die Protokollstufe setzen, desto vorsichtiger müssen Sie die Protokollgröße auswählen, da die Protokolldatei sehr schnell voll ist, wenn Sie eine Protokollierung auf einer höheren Stufe wählen.

Bytes

Die maximale Größe in Byte für die Protokolldatei des Managers. Sie können entweder eine positive Zahl, die größer als 0 sein muss, oder das Wort **unlimited** (unbegrenzt) angeben. Möglicherweise erreicht die Protokolldatei nicht genau die maximale Größe, bevor der Dateiumbruch stattfindet, da die Größe der Protokolleinträge variiert. Der Standardwert ist 1 MB.

quiesce

Gibt an, dass keine weiteren Verbindungen an einen Server gesendet werden sollen. Der Manager setzt die Wertigkeit für diesen Server an jedem Port, für den er definiert ist, auf 0 und sendet dann einen suspend-Befehl an den Cisco CSS Switch. Verwenden Sie diesen Befehl, wenn Sie einen Server für kurze Wartungsarbeiten stilllegen und dann wieder aktivieren möchten. Wenn Sie einen Server mit ausgesetztem Betrieb aus der Konfiguration entfernen und anschließend wieder zur Konfiguration hinzufügen, hat er nicht mehr den Status, den er vor Aussetzung des Betriebs hatte.

Server

Die IP-Adresse des Servers als symbolischer Name oder in Schreibweise mit Trennzeichen.

reach

Legt das Intervall, die Protokollstufe und die Protokollgröße für den Erreichbarkeits-Advisor fest.

refresh

Festlegen der Anzahl Intervalle, nach denen beim Cisco CSS Switch eine Aktualisierung der Informationen zu neuen und aktiven Verbindungen angefordert wird.

Aktualisierungszyklus

Eine positive Zahl, die die Anzahl von Intervallen darstellt. Der Standardwert ist 1.

report

Zeigt eine statistische Momentaufnahme an.

Cluster

Die Adresse des Clusters, die im Bericht angezeigt werden soll. Die Adresse kann ein symbolischer Name oder eine Adresse in Schreibweise mit Trennzeichen sein. Der Standardwert ist ein Manager-Bericht, in dem alle Cluster angezeigt werden.

Anmerkung: Zusätzliche Cluster werden durch ein Pluszeichen (+) getrennt.

restart

Startet alle Server (die nicht inaktiv sind) mit der Standardwertigkeit (1/2 der maximalen Wertigkeit).

Nachricht

Eine Nachricht, die in die Protokolldatei des Managers gestellt werden soll.

sensitivity

Legt die Mindestsensitivität für die Aktualisierung von Wertigkeiten fest. Diese Einstellung definiert, wann der Manager seine Serverwertigkeit ausgehend von externen Informationen ändern sollte.

Wertigkeit

Eine Zahl von 0 bis 100, die als prozentuale Wertigkeit verwendet werden soll. Der Standardwert 5 bewirkt eine Mindestsensitivität von 5 %.

smoothing

Festlegen eines Faktors, der Wertigkeitsabweichungen während des Lastausgleichs glättet. Ein höherer Glättungsfaktor führt zu einer weniger drastischen Änderung von Serverwertigkeiten bei Änderungen an den Netzdingungen. Ein geringerer Glättungsfaktor führt zu einer drastischen Änderung der Serverwertigkeiten.

Wert

Eine positive Gleitkommazahl. Der Standardwert ist 1,5.

start

Den Manager starten.

Protokolldateiname

Der Name der Datei, in der die Daten des Managers protokolliert werden. Jeder Eintrag des Protokolls ist mit einer Zeitmarke versehen.

Die Standarddatei ist im Verzeichnis **logs** installiert. Lesen Sie hierzu die Informationen in „Anhang F. Beispielkonfigurationsdateien“ auf Seite 393. Informationen zum Ändern des Verzeichnisses, in dem die Protokolldateien gespeichert werden, können Sie dem Abschnitt „Pfade für die Protokolldatei ändern“ auf Seite 222 entnehmen.

Metric-Port

Der Port, über den der Metric Server kommuniziert. Wenn Sie einen Metric-Port angeben, müssen Sie auch einen Protokolldateinamen angeben. Der Standard-Metrik-Port ist 10004.

status

Anzeigen des aktuellen Status aller globalen Werte des Managers mit den zugehörigen Standardeinstellungen.

stop

Den Manager stoppen.

unquiesce

Festlegung, dass der Manager einem zuvor stillgelegten Server an jedem Port, für den er definiert ist, eine Wertigkeit größer als null zuordnen kann. Der Manager sendet einen Aktivierungsbefehl an den Cisco CSS Switch.

Server

Die IP-Adresse des Servers als symbolischer Name oder in Schreibweise mit Trennzeichen.

version

Zeigt die aktuelle Version des Managers an.

Beispiele

- Geben Sie den folgenden Befehl ein, um das Aktualisierungsintervall für den Manager auf 5 Sekunden zu setzen:
`lbcontrol manager interval 5`
- Geben Sie den folgenden Befehl ein, um die Stufe der Protokollierung zwecks Verbesserung der Leistung auf 0 zu setzen:
`lbcontrol manager loglevel 0`
- Geben Sie den folgenden Befehl ein, um die Größe des Protokolls des Managers auf 1.000.000 Byte zu setzen:
`lbcontrol manager logsize 1000000`
- Festlegung, dass keine weiteren Verbindungen an den Server 130.40.52.153 gesendet werden sollen:
`lbcontrol manager quiesce 130.40.52.153`
- Setzen der Anzahl Aktualisierungsintervalle auf 3, bevor die Wertigkeiten aktualisiert werden:
`lbcontrol manager refresh 3`
- Geben Sie den folgenden Befehl ein, um eine statistische Momentaufnahme des Managers abzurufen:
`lbcontrol manager report`

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

```
lbccontrol>>manager report
```

HOST-TAB.VERZEI.		STATUS	
	Server6	AKTIV	
	Server5	AKTIV	
	Server4	AKTIV	
	Server3	AKTIV	
	Server2	AKTIV	
	Server1	AKTIV	

9.67.154.35	GEWICHT	AKTIV % 49	NEU % 50	PORT % 1	SYSTEM % 0					
PORT: 80	JETZT	NEU	GWT	VERB	GWT	VERB	GWT	LAST	GWT	LAST
Server1	4	4	5	0	5	0	3	301	-9999	-1
Server2	5	5	5	0	5	0	6	160	-9999	-1
PORT GESAMT:	9	9		0		0		461		-2

9.67.154.35	GEWICHT	AKTIV % 49	NEU % 50	PORT % 1	SYSTEM % 0					
PORT: 443	JETZT	NEU	GWT	VERB	GWT	VERB	GWT	LAST	GWT	LAST
Server3	4	4	5	0	5	0		0	-9999	-1
Server4	5	5	5	0	5	0	0	0	-9999	-1
PORT GESAMT:	9	9		0		0		0		-2

9.67.154.34	GEWICHT	AKTIV % 49	NEU % 50	PORT % 1	SYSTEM % 0					
PORT: 80	JETZT	NEU	GWT	VERB	GWT	VERB	GWT	LAST	GWT	LAST
Server5	5	5	5	0	5	0	5	160	-9999	-1
Server6	0	0	5	0	5	0	-9999	-1	-9999	-1
PORT GESAMT:	5	5		0		0		159		-2

ADVISOR	PORT	ZEITLIMIT
http	80	unlimited

- Neustart aller Server mit Standardwertigkeit und Schreiben einer Nachricht in die Manager-Protokolldatei:

`lbcontrol manager restart` Neustart des Managers für Codeaktualisierung

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

320-14:04:54 Neustart des Managers für Codeaktualisierung

- Setzen der Sensitivität für Wertigkeitsänderungen auf 10:
`lbcontrol manager sensitivity 10`
- Geben Sie den folgenden Befehl ein, um den Glättungsfaktor auf 2,0 zu setzen:
`lbcontrol manager smoothing 2.0`
- Geben Sie den folgenden Befehl ein, um den Manager zu starten und die Protokolldatei `ndmgr.log` anzugeben (Pfade können nicht angegeben werden):
`lbcontrol manager start ndmgr.log`
- Geben Sie den folgenden Befehl ein, um den aktuellen Status der Werte anzuzeigen, die dem Manager zugeordnet sind:

`lbcontrol manager status`

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

Manager-Status:

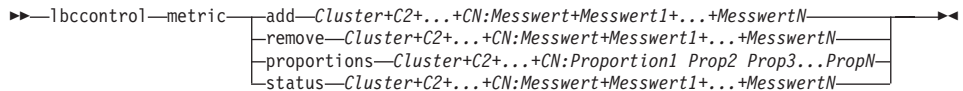
=====

Metrik-Port	10004
Name der Managerprotokolldatei	manager.log
Managerprotokollstufe	1
Max. Managerprotokollgröße (Bytes)	unlimited
Sensitivitätsstufe	0,05
Glättungsfaktor	1,5
Aktualisierungsintervall (Sekunden)	2
Gewichtungsaktualisierungszyklus	1
Erreichbarkeit - Protokollstufe	1
Erreichbarkeit - Max. Protokollgröße (Bytes)	unlimited
Erreichbarkeit - Aktualisierungsintervall (Sekunden) ...	7

- Stoppen des Managers:
`lbcontrol manager stop`
- Geben Sie den folgenden Befehl ein, um die aktuelle Versionsnummer des Managers aufzurufen:

`lbcontrol manager version`

lbcontrol metric — Systemmesswerte konfigurieren



add

Hinzufügen eines Messwerts.

Cluster

Die Adresse, zu der die Clients eine Verbindung herstellen. Die Adresse kann der Host-Name der Maschine oder die IP-Adresse in Schreibweise mit Trennzeichen sein. Zusätzliche Cluster werden durch ein Pluszeichen (+) getrennt.

Anmerkung: Bei Cisco Consultant entspricht die Cluster-Adresse der virtuellen IP-Adresse (VIP-Adresse) in der content-Regel des Eigners in der Konfiguration des Cisco CSS Switch.

Messwert

Der Systemmesswert. Die folgenden Messwerte stehen zur Auswahl:

- cpuload
- memload
- Port
- Systemmesswerte.

remove

Entfernen dieses Messwerts.

proportions

Festlegen der Proportionen für die diesem Objekt zugeordneten Messwerte.

status

Anzeigen des aktuellen Messwertes.

Beispiele

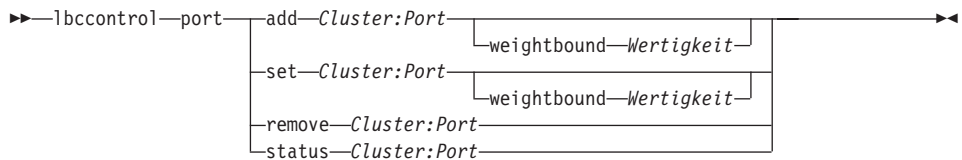
- Hinzufügen eines Systemmesswerts:
`lbcontrol metric add 10.10.10.20:Messwert1`
- Festlegen der Proportionen für einen Cluster mit zwei Systemmesswerten:
`lbcontrol metric proportions 10.10.10.20 48 52`
- Anzeigen des aktuellen Status der zugeordneten Messwerte:
`lbcontrol metric status 10.10.10.20:Messwert1`

Dieser Befehl erzeugt eine Ausgabe, die ungefähr wie folgt aussieht:

Metrikstatus:

```
Cluster ..... 10.10.10.20
Metrikname ..... Messwert1
Metrikproportion ..... 52
  Server ..... 9.37.56.100
  Metrikdaten .... -1
```

lbcontrol port — Ports konfigurieren



add

Hinzufügen eines Ports zu einem Cluster. Sie müssen einen Port zu einem Cluster hinzufügen, bevor Sie Server zu diesem Port hinzufügen können. Sind keine Ports für einen Cluster vorhanden, werden alle Client-Anforderungen lokal verarbeitet. Mit diesem Befehl können Sie mehrere Ports auf einmal hinzufügen.

weightbound

Legt die maximale Wertigkeit von Servern an diesem Port fest. Dieser Parameter beeinflusst, wie stark sich die Anzahl der Anforderungen, die Cisco CSS Switch den einzelnen Servern zuteilt, unterscheidet. Der Standardwert ist 10.

Wertigkeit

Eine Zahl von 1-10 bis 100 für die maximale Wertigkeitsgrenze.

set

Festlegen der Felder eines Ports.

remove

Entfernen dieses Ports.

status

Anzeigen des Status für den Server an diesem Port. Wenn Sie den Status für alle Ports sehen möchten, geben Sie diesen Befehl ohne *Port* an. Sie dürfen jedoch nicht den Doppelpunkt vergessen.

Beispiele

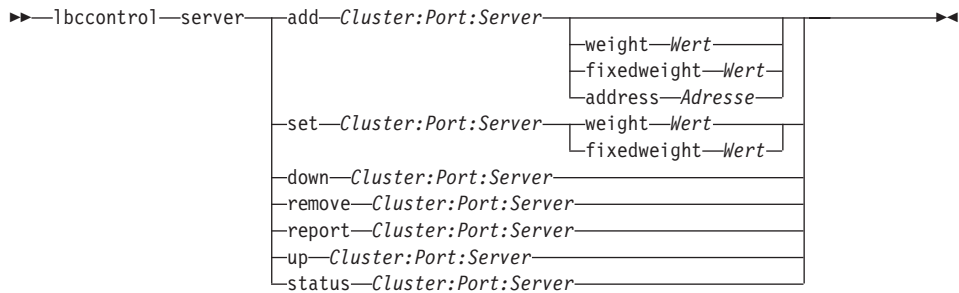
- Geben Sie den folgenden Befehl ein, um die Ports 80 und 23 zur Cluster-Adresse 130.40.52.153 hinzuzufügen:
`lbcontrol port add 130.40.52.153:80+23`
- Festlegen der maximalen Wertigkeit 10 für Port 80 an der Cluster-Adresse 130.40.52.153:
`lbcontrol port set 130.40.52.153:80 weightbound 10`
- Entfernen von Port 23 aus dem Cluster mit der Adresse 130.40.52.153:
`lbcontrol port remove 130.40.52.153:23`
- Abrufen des Status für Port 80 an der Cluster-Adresse 9.67.131.153:
`lbcontrol port status 9.67.131.153:80`

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Port-Status:

Port-Nummer	80
Cluster-Adresse	9.67.131.153
Anzahl Server	2
Gewichtungsgrenze	10

lbcontrol server — Server konfigurieren



add

Diesen Server hinzufügen.

Cluster

Die Adresse des Clusters als symbolischer Name oder in Schreibweise mit Trennzeichen.

Anmerkung: Zusätzliche Cluster werden durch ein Pluszeichen (+) getrennt.

Port

Die Nummer des Ports.

Anmerkung: Zusätzliche Ports werden durch ein Pluszeichen (+) voneinander getrennt.

Server

Die eindeutige IP-Adresse der TCP-Servermaschine als symbolischer Name oder in Schreibweise mit Trennzeichen. Wenn Sie einen eindeutigen symbolischen Namen verwenden, der nicht in eine IP-Adresse aufgelöst wird, müssen Sie den Befehl **lbcontrol server add** mit dem Attribut "address" verwenden.

weight

Eine Zahl von 0 bis 10, die die Wertigkeit dieses Servers angibt. Wird die Wertigkeit auf 0 gesetzt, werden keine neuen Anforderungen an den Server gesendet, die derzeit aktiven Verbindungen zu diesem Server werden jedoch nicht beendet. Der Standardwert ist die Hälfte der für den Port angegebenen maximalen Wertigkeit. Wenn der Manager aktiv ist und "fixedweight" auf "no" gesetzt ist, wird diese Einstellung schnell überschrieben.

Wert

Angabe der Wertigkeit.

fixedweight

Mit der Option "fixedweight" können Sie angeben, ob der Manager die Serverwertigkeit ändern soll. Wird der Wert für "fixedweight" auf "yes" gesetzt, kann der Manager die Serverwertigkeit nicht ändern. Weitere Informationen hierzu finden Sie im Abschnitt „Feste Wertigkeiten vom Manager“ auf Seite 147.

Wert

Angabe der festen Wertigkeit. Standardeinstellung ist 'no'.

Adresse

Die eindeutige IP-Adresse der TCP-Servermaschine als symbolischer Name oder in Schreibweise mit Trennzeichen. Falls der Servername nicht aufgelöst wird (was z. B. bei einem logischen Servernamen der Fall ist), müssen Sie die Adresse der physischen Servermaschine angeben.

Wert

Die eindeutige Kennung der Servermaschine. Falls der Servername nicht aufgelöst werden kann, müssen Sie das Attribut "address" angeben.

down

Diesen Server als inaktiv markieren. Der Cisco CSS Switch hört auf, Verbindungen an diesen Server zu senden.

remove

Diesen Server entfernen.

report

Bericht über diesen Server erstellen.

set

Werte für diesen Server festlegen.

up Diesen Server als aktiv markieren. Der Cisco CSS Switch sendet neue Verbindungen an diesen Server.

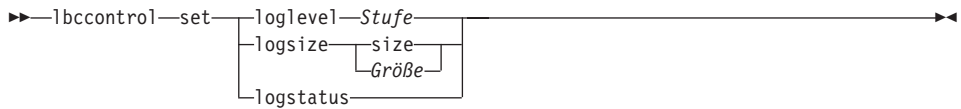
status

Status der Server anzeigen.

Beispiele

- Hinzufügen des Servers mit der Adresse 27.65.89.42 zum Port 80 an der Cluster-Adresse 130.40.52.153:
`lbcontrol server add 130.40.52.153:80:27.65.89.42`
- Geben Sie den folgenden Befehl ein, um den Server 27.65.89.42 von allen Ports aller Cluster zu entfernen:
`lbcontrol server remove ::27.65.89.42`
- Festlegen der Wertigkeit 10 für Server 27.65.89.42 am Port 80 der Cluster-Adresse 130.40.52.153:
`lbcontrol
server set 130.40.52.153:80:27.65.89.42 weight 10`

lbcontrol set — Serverprotokoll konfigurieren



loglevel

Die Stufe für die Protokollierung von lbserver-Aktivitäten.

Stufe

Der Standardwert für **loglevel** ist 1. Der gültige Bereich umfasst die Werte 0 bis 5. Die folgenden Werte sind gültig: 0 für keine Einträge, 1 für eine minimale Protokollierung, 2 für eine Basisprotokollierung, 3 für eine normale, 4 für eine erweiterte und 5 für eine ausführliche Protokollierung.

logsize

Die maximale Anzahl Bytes, die in der Protokolldatei protokolliert werden.

Größe

Der Standardwert für "logsize" ist 1 MB.

logstatus

Zeigt die Einstellungen des Serverprotokolls (Protokollstufe und -größe) an.

lbcontrol status — Aktivitätsanzeige für Manager und Advisor-Funktionen

►►—lbcontrol—status—◄◄

Beispiele

- Geben Sie den folgenden Befehl ein, um festzustellen, ob der Manager und die Advisor aktiv sind:

```
lbcontrol status
```

Die Ausgabe dieses Befehls sieht etwa wie folgt aus:

Manager wurde gestartet.

ADVISOR	PORT		ZEITLIMIT

http	80		unlimited
ftp	21		unlimited

Anhang F. Beispielkonfigurationsdateien

Dieser Anhang enthält Beispielkonfigurationsdateien für die Dispatcher-Komponente von Network Dispatcher.

Beispielkonfigurationsdateien für Network Dispatcher

Die Beispieldateien finden Sie im Verzeichnis `.../nd/servers/samples/`.

Dispatcher-Konfigurationsdatei—AIX, Red Hat Linux und Solaris

```
#!/bin/ksh
#
# configuration.sample - Beispielkonfigurationsdatei für die
# Dispatcher-Komponente
#
#
# Dieses Script muss vom Benutzer "root" ausgeführt werden.
#
# iam='wer bin ich'

# if [ "$iam" != "root" ] if [ "$iam" != "root" ]
# then
# echo "Zur Ausführung dieses Scripts müssen Sie als root angemeldet sein"
# exit 2
# fi

#
# Starten Sie zunächst den Server
#
# ndserver start
# sleep 5

#
# Starten Sie dann den Executor.
#
# ndcontrol executor start

#
# Der Dispatcher kann vor dem Löschen der Dispatcher-Software
# jederzeit mit den Befehlen "ndcontrol executor stop" und
# "ndserver stop" zum Stoppen von Executor und Server entfernt
# werden.
#
# Der nächste Konfigurationsschritt für den Dispatcher ist das
# Festlegen der NFA und der Cluster-Adresse(n).
#
# Die NFA wird für den Fernzugriff auf die Dispatcher-Maschine
# zu Verwaltungs- oder Konfigurationszwecken verwendet. Diese
# Adresse ist erforderlich, da der Dispatcher Pakete an die
```

```

# Cluster-Adresse(n) weiterleitet.
#
# Die CLUSTER-Adresse ist der Host-Name (oder die IP-Adresse)
# zu dem (bzw. zu der) ferne Clients eine Verbindung herstellen.
#
# Host-Namen und IP-Adressen können sind an jeder Stelle dieser
# Datei beliebig gegeneinander austauschbar.
#

# NFA=Host-Name.Domäne.Name
# CLUSTER=www.IhreFirma.com

# echo "NFA wird geladen"
# ndcontrol executor set nfa $NFA

#
# Der nächste Konfigurationsschritt für den Dispatcher ist
# das Erstellen eines Clusters. Der Dispatcher leitet an die
# Cluster-Adresse gesendete Anforderungen an die entsprechenden,
# für diesen Cluster definierten Servermaschinen weiter. Mit
# Dispatcher können Sie mehrere Cluster-Adressen konfigurieren
# und bedienen.

# Verwenden Sie für CLUSTER2, CLUSTER3 usw. eine ähnliche Konfiguration.
#

# echo "Erste CLUSTER-Adresse wird geladen"
# ndcontrol cluster add $CLUSTER

#
# Jetzt müssen die Ports definiert werden, die dieser Cluster
# verwendet. Alle vom Dispatcher an einem definierten Port
# empfangenen Anforderungen werden an den entsprechenden Port
# einer der Servermaschinen weitergeleitet.
#

# echo "Ports für CLUSTER $CLUSTER werden erstellt"

# ndcontrol port add $CLUSTER:20+21+80

#
# Der letzte Schritt ist das Hinzufügen der einzelnen Servermaschinen
# zu den Ports dieses Clusters.
# Auch hier können Sie entweder den Host-Namen oder die IP-Adresse der
# Servermaschinen verwenden.
#

# SERVER1=Servername1.Domäne.Name
# SERVER2=Servername2.Domäne.Name
# SERVER3=Servername3.Domäne.Name

# echo "Servermaschinen werden hinzugefügt"
# ndcontrol server add $CLUSTER:20+21+80:
# $SERVER1+$SERVER2+$SERVER3

```

```

#
# Jetzt werden die Lastausgleichskomponenten von Dispatcher
# gestartet. Die Hauptkomponente ist der Manager. Die
# sekundären Komponenten sind die Advisor-Funktionen. Sind
# Manager und Advisor-Funktionen nicht aktiv, sendet der
# Dispatcher Anforderungen in einem RoundRobin-Format.
# Sobald der Manager gestartet ist, werden Wertigkeitsentscheidungen
# auf der Grundlage der Anzahl neuer und aktiver Verbindungen
# getroffen und eingehende Anforderungen an den am besten geeigneten
# Server gesendet. Die Advisor-Funktionen geben dem Manager
# Einblick in die Fähigkeit eines Servers, Anforderungen zu bedienen,
# und können feststellen, ob ein Server aktiv ist. Erkennt eine
# Advisor-Funktion, dass ein Server inaktiv ist, wird dieser
# entsprechend markiert (sofern die Manager-Proportionen
# auf das Einbeziehen von Advisor-Eingaben gesetzt sind) und es
# werden keine weiteren Anforderungen an den Server weitergeleitet.

# Der letzte Schritt beim Konfigurieren der Lastausgleichskomponenten
# ist das Festlegen der Manager-Proportionen. Der Manager aktualisiert
# die Wertigkeit der Server ausgehend von vier verschiedenen Ansätzen:
#   1. Anzahl der aktiven Verbindungen für jeden Server.
#   2. Anzahl der neuen Verbindungen zu jedem Server.
#   3. Eingaben von den Advisor-Funktionen.
#   4. Eingaben von der Advisor-Funktion auf Systemebene.
# Diese Proportionen müssen in der Summe 100 ergeben. Sie können
# die Manager Proportionen beispielsweise wie folgt festlegen:
#   ndcontrol manager proportions 48 48 0 0
# Damit fließen die aktiven und neuen Verbindungen mit jeweils 48 %
# in die Gewichtungentscheidung ein. Die Advisor-Funktionen fließen
# zu 4 % ein und die Systemeingaben werden nicht berücksichtigt.
#
# ANMERKUNG. Standardmäßig sind die Manager-Proportionen auf 50 50 0 0 gesetzt.
#

# echo "Manager wird gestartet..."
# ndcontrol manager start

# echo "FTP-Advisor-Funktion wird an Port 21 gestartet ..."
# ndcontrol advisor start ftp 21
# echo "HTTP-Advisor-Funktion wird an Port 80 gestartet ..."
# ndcontrol advisor start http 80
# echo "Telnet-Advisor-Funktion wird an Port 23 gestartet ..."
# ndcontrol advisor start telnet 23
# echo "SMTP-Advisor-Funktion wird an Port 25 gestartet ..."
# ndcontrol advisor start smtp 25
# echo "POP3-Advisor-Funktion wird an Port 110 gestartet ..."
# ndcontrol advisor start pop3 110
# echo "NNTP-Advisor-Funktion wird an Port 119 gestartet ..."
# ndcontrol advisor start nntp 119
# echo "SSL-Advisor-Funktion wird an Port 443 gestartet ..."
# ndcontrol advisor start ssl 443
#

# echo "Manager-Proportionen werden festgelegt..."
# ndcontrol manager proportions 58 40 2 0

```

```

#
# Der letzte Konfigurationsschritt für die Dispatcher-Maschine
# ist das Festlegen eines Aliasnamens für die Netzschnittstellenkarte (NIC).
#
# ANMERKUNG: Verwenden Sie diesen Befehl NICHT in einer Umgebung mit hoher
# Verfügbarkeit. Die NIC und die Loopback-Adresse werden von den
# go*-Scripts konfiguriert.
# ndcontrol cluster configure $CLUSTER

# Wenn die Cluster-Adresse sich auf einer von der NFA abweichenden
# NIC oder in einem abweichenden Teilnetz befindet, verwenden Sie für
# den Befehl "cluster configure" das folgende Format:
# ndcontrol cluster configure $CLUSTER tr0 0xfffff800
# tr0 ist hier die NIC (tr1 die zweite Token-Ring-Karte, en0
# die erste Ethernet-Karte) und 0xfffff800 ist eine für
# Ihre Site gültige Teilnetzmaske.
#

#
# Die folgenden Befehle aktivieren die Standardwerte.
# Verwenden Sie diese Befehle als Ausgangspunkt für Änderungen der Standardwerte.
# 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
#
```

Dispatcher-Konfigurationsdatei—Windows

Die folgende Konfigurationsdatei ist die Network Dispatcher-Beispielkonfigurationsdatei **configuration.cmd.sample**, die mit Windows verwendet wird.

```
@echo off
rem configuration.cmd.sample - Beispielkonfigurationsdatei für die
rem Dispatcher-Komponente.
rem

rem ndserver muss im Fenster "Dienste" gestartet werden.

rem

rem
rem Starten Sie dann den Executor.
rem
rem call ndcontrol executor start

rem

rem Der nächste Konfigurationsschritt für den Dispatcher
rem ist das Festlegen der NFA und der Cluster-Adresse(n).
rem

rem Die NFA wird für den Fernzugriff auf die Dispatcher-Maschine
rem zu Verwaltungs- oder Konfigurationszwecken verwendet. Diese
rem Adresse ist erforderlich, da der Dispatcher Pakete an die
rem Cluster-Adresse(n) weiterleitet.

rem
rem Die CLUSTER-Adresse ist der Host-Name (oder die IP-Adresse)
rem zu dem (bzw. zu der) ferne Clients eine Verbindung herstellen.
rem

rem Host-Namen und IP-Adressen können sind an jeder Stelle dieser
rem Datei beliebig gegeneinander austauschbar.
rem NFA=[Non-Forwarding Address]
rem CLUSTER=[Cluster-Name]
rem

rem set NFA=Host-Name.Domäne.Name
rem set CLUSTER=www.IhreFirma.com

rem echo "NFA wird geladen"
rem call ndcontrol executor set nfa %NFA%

rem
rem Mit den folgenden Befehlen werden die Standardwerte festgelegt.
rem Verwenden Sie diese Befehle zum Ändern der Standardwerte.
```

```

rem call ndcontrol executor set fintimeout 30
rem call ndcontrol executor set fincount 4000
rem
rem Der nächste Konfigurationsschritt für den Dispatcher ist
rem das Erstellen eines Clusters. Der Dispatcher leitet an die
rem Cluster-Adresse gesendete Anforderungen an die entsprechenden,
rem für diesen Cluster definierten Servermaschinen weiter. Mit
rem Dispatcher können Sie mehrere Cluster-Adressen konfigurieren
rem und bedienen.
rem Verwenden Sie für CLUSTER2, CLUSTER3 usw. eine ähnliche Konfiguration.
rem

rem echo "Erste CLUSTER-Adresse wird geladen"
rem call ndcontrol cluster add %CLUSTER%

rem
rem Jetzt müssen die Ports definiert werden, die dieser Cluster
rem verwendet. Alle vom Dispatcher an einem definierten Port
rem empfangenen Anforderungen werden an den entsprechenden Port
rem einer der Servermaschinen weitergeleitet.
rem

rem echo "Ports für CLUSTER %CLUSTER% werden erstellt"
rem call ndcontrol port add %CLUSTER%:20+21+80

rem
rem Der letzte Schritt ist das Hinzufügen der einzelnen Servermaschinen
rem zu den Ports dieses Clusters. Auch hier können Sie entweder den
rem Host-Namen oder die IP-Adresse der Servermaschinen verwenden.
rem

rem set SERVER1=Servername1.Domäne.Name
rem set SERVER2=Servername2.Domäne.Name
rem set SERVER3=Servername3.Domäne.Name

rem echo "Servermaschinen werden hinzugefügt"
rem call ndcontrol server add %CLUSTER%:20+21+80:
rem %SERVER1%+%SERVER2%+%SERVER3%

rem
rem Jetzt werden die Lastausgleichskomponenten von Dispatcher
rem gestartet. Die Hauptkomponente ist der Manager. Die
rem sekundären Komponenten sind die Advisor-Funktionen. Sind
rem Manager und Advisor-Funktionen nicht aktiv, sendet der
rem Dispatcher Anforderungen in einem RoundRobin-Format.
rem Sobald der Manager gestartet ist, werden Wertigkeitsentscheidungen
rem auf der Grundlage der Anzahl neuer und aktiver Verbindungen
rem getroffen und eingehende Anforderungen an den am besten geeigneten
rem Server gesendet. Die Advisor-Funktionen geben dem Manager
rem Einblick in die Fähigkeit eines Servers, Anforderungen zu bedienen,
rem und können feststellen, ob ein Server aktiv ist. Erkennt eine
rem Advisor-Funktion, dass ein Server inaktiv ist, wird dieser
rem entsprechend markiert (sofern die Manager-Proportionen
rem auf das Einbeziehen von Advisor-Eingaben gesetzt sind) und es
rem werden keine weiteren Anforderungen an den Server weitergeleitet.

```



```

rem Der letzte Schritt beim Konfigurieren der Lastausgleichskomponenten
rem ist das Festlegen der Manager-Proportionen. Der Manager aktualisiert
rem die Wertigkeit der Server ausgehend von vier verschiedenen Ansätzen:

rem 1. Anzahl der aktiven Verbindungen für jeden Server.
rem 2. Anzahl der neuen Verbindungen zu jedem Server.
rem 3. Eingaben von den Advisor-Funktionen.
rem 4. Eingaben von der Advisor-Funktion auf Systemebene.
rem
rem Diese Proportionen müssen in der Summe 100 ergeben. Sie können
rem die Manager Proportionen beispielsweise wie folgt festlegen:
rem     ndcontrol cluster set <Cluster> proportions 48 48 4 0
rem Damit fließen die aktiven und neuen Verbindungen mit jeweils 48 %
rem in die Gewichtungsentscheidung ein. Die Advisor-Funktionen fließen
rem zu 4 % ein und die Systemeingaben werden nicht berücksichtigt.
rem
rem ANMERKUNG. Standardmäßig sind die Manager-Proportionen auf
rem 50 50 0 0 gesetzt.

rem echo "Manager wird gestartet..."
rem call ndcontrol manager start

rem echo "FTP-Advisor-Funktion wird an Port 21 gestartet ..."
rem call ndcontrol advisor start ftp 21
rem echo "HTTP-Advisor-Funktion wird an Port 80 gestartet ..."
rem call ndcontrol advisor start http 80
rem echo "Telnet-Advisor-Funktion wird an Port 23 gestartet..."
rem call ndcontrol advisor start telnet 23
rem echo "SMTP-Advisor-Funktion wird an Port 25 gestartet ..."
rem call ndcontrol advisor start smtp 25
rem echo "POP3-Advisor-Funktion wird an Port 110 gestartet..."
rem call ndcontrol advisor start pop3 110
rem echo "NNTP-Advisor-Funktion wird an Port 119 gestartet..."
rem call ndcontrol advisor start nntp 119
rem echo "SSL-Advisor-Funktion wird an Port 443 gestartet..."
rem call ndcontrol advisor start ssl 443
rem

rem echo "Cluster-Proportionen werden festgelegt..."
rem call ndcontrol cluster set %CLUSTER% proportions 58 40 2 0

rem
rem Der letzte Konfigurationsschritt für die Dispatcher-Maschine
rem ist das Festlegen eines Aliasnamens für die Netzschnittstellenkarte (NIC).
rem
rem ANMERKUNG: Verwenden Sie diesen Befehl NICHT in einer Umgebung mit hoher
rem Verfügbarkeit. Die NIC und die Loopback-Adresse werden von den
rem go*-Scripts konfiguriert.
rem
rem ndcontrol cluster configure %CLUSTER%

rem Wenn die Cluster-Adresse sich auf einer von der NFA abweichenden
rem NIC oder in einem abweichenden Teilnetz befindet, verwenden Sie für
rem den Befehl "cluster configure" das folgende Format:
rem ndcontrol cluster configure %CLUSTER% tr0 0xfffff800

```

```

rem tr0 ist hier die NIC (tr1 die zweite Token-Ring-Karte, en0
rem die erste Ethernet-Karte) und 0xffff800 ist eine für
rem Ihre Site gültige Teilnetzmaske.
rem

rem
rem Mit den folgenden Befehlen werden die Standardwerte festgelegt.
rem Verwenden Sie diese Befehle als Ausgangspunkt zum Ändern der Standardwerte.
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

```

Beispiel-Advisor-Funktion

Nachfolgend ist die Advisor-Beispieldatei **ADV_sample** wiedergegeben.

```

/**
 * ADV_sample: HTTP-Advisor-Funktion von Network Dispatcher
 *
 * Diese Klasse definiert eine angepasste Beispiel-Advisor-Funktion für Network
 * Dispatcher. Diese angepasste Advisor-Funktion erweitert wie alle anderen
 * Advisor-Funktionen den Advisor-Basiscode ADV_Base.
 * Es ist der Advisor-Basiscode, der die meisten Advisor-Funktionen ausführt.
 * Dazu gehört das Zurückmelden von Belastungen an Network Dispatcher für
 * den Wertigkeitsalgorithmus von Network Dispatcher.

```

```

* Darüber hinaus stellt der Advisor-Basiscode Socket-Verbindungen her,
* schließt Sockets und stellt Sende- und Empfangsmethoden für die Advisor-
* Funktion bereit. Die Advisor-Funktion selbst wird nur zum Senden von
* Daten an den Port bzw. Empfangen von Daten vom Port des empfohlenen
* Servers verwendet.
* Die TCP-Methoden innerhalb des Advisor-Basiscodes werden zeitlich
* gesteuert, um die Last zu berechnen. Mit einer Markierung der Methode
* "constructor" in in ADV_base kann bei Bedarf die vorhandene Last
* mit der neuen, von der Advisor-Funktion zurückgegebenen Last
* überschrieben werden.
*
* Anmerkung: Der Advisor-Basiscode stellt in angegebenen Intervallen
* die Last ausgehend von einem in der Methode "constructor" gesetzten
* Wert für den Wertigkeitsalgorithmus bereit. Ist die eigentliche
* Advisor-Funktion noch nicht abgeschlossen, so dass sie keinen gültigen
* Lastwert zurückgeben kann, verwendet der Advisor-Basiscode die
* bisherige Last.
*
* NAMEN
*
* Es gilt die folgende Namenskonvention:
*
* - Die Datei muss sich in den folgenden Network-Dispatcher-
*   Verzeichnissen befinden:
*
*       nd/servers/lib/CustomAdvisors/
*       (Widows 2000: nd\servers\lib\CustomAdvisors)
*
* - Der Name der Advisor-Funktion muss den Präfix "ADV_" haben. Zum Starten
*   der Advisor-Funktion genügt jedoch der Name. Die Advisor-Funktion
*   "ADV_sample" kann beispielsweise mit "sample" gestartet werden.
*
* - Der Name der Advisor-Funktion muss in Kleinbuchstaben angegeben werden.
*
* Unter Beachtung dieser Regeln wird auf dieses Beispiel wie folgt verwiesen:
*
*   <Basisverzeichnis>/lib/CustomAdvisors/ADV_sample.class
*
*
* Advisor-Funktionen müssen wie für Network Dispatcher generell gültig
* mit der erforderlichen Java-Version kompiliert werden.
* Um den Zugriff auf die Network-Dispatcher-Klassen zu gewährleisten, müssen
* Sie sicherstellen, dass die Datei ibmnd.jar (aus dem Unterverzeichnis "lib"
* des Basisverzeichnisses) im CLASSPATH des Systems enthalten ist.
*
*
* Von ADV_Base bereitgestellte Methoden:
*
* - ADV_Base (Constructor):
*
*   - Parameter
*     - String sName = Name der Advisor-Funktion
*     - String sVersion = Version der Advisor-Funktion
*     - int iDefaultPort = Standard-Port-Nummer für die Advisor-Funktion
*     - int iInterval = Intervall für die Ausführung der Advisor-Funktion

```

```

*      für die Server
*      - String sDefaultLogFileName = Nicht verwendet; muss als "" übergeben
*        werden.
*      - boolean replace = True - Den vom Advisor-Basiscode Lastwert
*                                ersetzen
*                                False - Zu dem vom Advisor-Basiscode berechneten Lastwert
*                                      addieren
*      - Rückgabe
*      - constructor-Methoden haben keine Rückgabewerte.
*
* Da der Advisor-Basiscode auf Threads basiert, stehen verschiedene andere
* Methoden für Advisor-Funktionen zur Verfügung. Auf diese kann mit dem von
* getLoad() übergebenen Parameter CALLER verwiesen werden.
*
* Es handelt sich um die folgenden Methoden:
*
* - send - Informationspaket über die eingerichtete Socket-Verbindung
*         an den Server am angegebenen Port senden.
*   - Parameter
*     - String sDataString - Daten werden in Form einer Zeichenfolge
*                           gesendet
*   - Rückgabe
*     - int RC - Null gibt unabhängig vom erfolgreichen/gescheiterten Senden
*               der Daten an, dass die Daten gesendet wurden. Eine negative
*               ganze Zahl zeigt einen Fehler an.
*
* - receive - Empfang von Informationen von der Socket-Verbindung.
*   - Parameter
*     - StringBuffer sbDataBuffer - Die während des Aufrufs von "receive"
*                                   empfangenen Daten
*   - Rückgabe
*     - int RC - Null gibt unabhängig vom erfolgreichen/gescheiterten Empfang
*               der Daten an, dass die Daten gesendet wurden. Eine negative
*               ganze Zahl zeigt einen Fehler an.
*
* Falls die vom Advisor-Basiscode bereitgestellte Funktionalität nicht
* ausreicht, können Sie die gewünschte Funktion innerhalb des Advisors
* erstellen. Die vom Advisor-Basiscode bereitgestellten Methoden werden
* dann ignoriert.
*
* Eine wichtige Frage hinsichtlich der zurückgegebenen Last ist, ob
* sie auf die vom Advisor-Basiscode generierte Last angewendet oder
* ersetzt werden soll. Es gibt gültige Instanzen für beide Situationen.
*
* Dieses Beispiel entspricht im Wesentlichen der HTTP-Advisor-Funktion
* von Network Dispatcher und funktioniert sehr einfach:
* Es wird eine Sende-anforderung (HTTP HEAD) abgesetzt. Bei Empfang einer
* Antwort wird die Methode getLoad beendet und der Advisor-Basiscode
* angewiesen, die Ablaufsteuerung der Anforderung zu stoppen. Die Methode
* ist damit abgeschlossen. Die zurückgegebenen Informationen werden keiner
* Syntaxanalyse unterzogen. Die Last basiert auf der für das Senden und
* und Empfangen benötigten Zeit.
*/

```

```

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;

    // Anmerkung: Die meisten Serverprotokolle erfordern am Ende von Nachrichten
    // eine Zeilenschaltung ("\r") und einen Zeilenvorschub ("\n"). Sollte dies
    // für Sie zutreffen, nehmen Sie sie an dieser Stelle in Ihre Zeichenfolge
    // auf.
    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.
     *
     * Parameter: Keine. An die constructor-Methode für ADV_Base müssen
     * jedoch mehrere Parameter übergeben werden.
     */
    public ADV_sample()
    {
        super( ADV_NAME,
              "2.0.0.0-03.27.98",
              ADV_DEF_ADV_ON_PORT,
              ADV_DEF_INTERVAL,
              "", // not used
              false);
        super.setAdvisor( this );
    }

    /**
     * ADV_AdvisorInitialize
     *
     * Eine Advisor-spezifische Initialisierung, die nach dem Start der
     * Advisor-Funktion stattfinden muss.
     * Diese Methode wird nur einmal aufgerufen und in der Regel nicht verwendet.
     */
    public void ADV_AdvisorInitialize()
    {
        return;
    }

    /**
     * getLoad()
     */

```

```

* Diese Methode wird vom Advisor-Basiscode aufgerufen, um die Operation der
* Advisor-Funktion auf der Grundlage protokollspezifischer Details zu beenden.
* In diesem Beispiel sind nur eine Sende- und eine Empfangsoperation
* notwendig. Wenn eine komplexere Logik erforderlich ist, können mehrere
* Sende- und Empfangsoperationen ausgeführt werden.
* Es könnte beispielsweise eine Antwort empfangen werden. Die sich aus der
* Syntaxanalyse dieser Antwort ergebenden Informationen könnten eine
* weitere Sende- und Empfangsoperation nach sich ziehen.
*
* Parameter:
*
* - iConnectTime - Derzeitige Last entsprechend der Zeit, die für das
*                   Herstellen der Verbindung zum Server über den
*                   angegebenen Port benötigt wurde.
*
* - caller - Verweis auf die Advisor-Basisklasse, wo die von Network
*             Dispatcher bereitgestellten Methoden einfache TCP-Anforderungen
*             wie Sende- und Empfangsaufrufe durchführen sollen.
*
* Ergebnisse:
*
* - Last: Ein in Millisekunden angegebener Wert, der entsprechend der
*         Markierung "replace" der constructor-Methode zur vorhandenen Last
*         addiert wird oder die vorhandene Last ersetzt.
*
*         Je größer die Last ist, desto länger benötigte der Server für die
*         Antwort. Um so höher wird in Network Dispatcher auch die Wertigkeit
*         für den Lastausgleich ausfallen.
*
*         Wenn der Wert negativ ist, wird von einem Fehler ausgegangen. Ein Fehler
*         von einer Advisor-Funktion zeigt an, dass der Server, den die Advisor-
*         Funktion zu erreichen versucht, nicht zugänglich und inaktiv ist.
*         Network Dispatcher versucht nicht, die Last an einen inaktiven Server
*         weiterzuleiten. Der Server wird von Network Dispatcher wieder in den
*         Lastausgleich einbezogen, wenn ein positiver Wert empfangen wird.
*
*         Der Wert null wird nur sehr selten zurückgegeben und von Network
*         Dispatcher als unbekannter Status interpretiert, auf den Network
*         Dispatcher reagiert, indem er dem Server eine hohe Wertigkeit
*         zuordnet.
*/
public int getLoad(int iConnectTime, ADV_Thread caller)
{
    int iRc;
    int iLoad = ADV_HOST_INACCESSIBLE; // -1

    // Send tcp request
    iRc = caller.send(ADV_SEND_REQUEST);
    if (iRc >= 0)
    {
        // Empfang ausführen
        StringBuffer sbReceiveData = new StringBuffer("");
        iRc = caller.receive(sbReceiveData);

        // Bei erfolgreichem Empfang wird als Lastwert null zurückgegeben.

```

```

// Dies liegt daran, dass die Markierung "replace" auf "false" gesetzt
// ist und so angibt, dass die von der Basis-Advisor-Funktion generierte
// Last verwendet werden soll.
// Da die zurückgegebenen Daten nicht verarbeitet wurden, ist keine
// zusätzliche Last nötig.

// Anmerkung: Es ist bekannt, dass die Last des Advisor-Basiscodes
// ungleich null sein wird, so dass ein Lastwert von null nicht zur
// Berechnung der Wertigkeit zurückgegeben wird.
    if (iRc >= 0)
    {
        iLoad = 0;
    }
    return iLoad;
}

} // Ende von ADV_sample

```

Anhang G. Beispiel für eine Client-/Serverkonfiguration mit hoher Verfügbarkeit unter Verwendung von Dispatcher, CBR und Caching Proxy

Dieser Anhang beschreibt das Einrichten einer Client-/Serverkonfiguration mit hoher Verfügbarkeit, die das Leistungsspektrum der Komponenten von Network Dispatcher (Dispatcher und CBR) mit dem von Caching Proxy verbindet.

Servermaschine einrichten

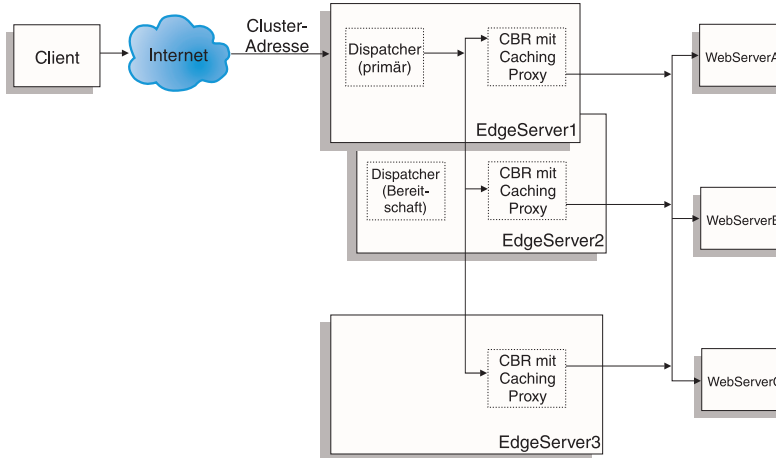


Abbildung 30. Beispiel für eine Client-/Serverkonfiguration mit hoher Verfügbarkeit unter Verwendung von Dispatcher, CBR und Caching Proxy

Die Servermaschine in Abb. 30 ist wie folgt konfiguriert:

- EdgeServer1: primäre Dispatcher-Maschine (hohe Verfügbarkeit), die mit CBR und Caching Proxy verknüpft ist und die Last auf Webserver verteilt.
- EdgeServer2: Bereitschafts-Dispatcher-Maschine (hohe Verfügbarkeit), die mit CBR und Caching Proxy verknüpft ist.
- EdgeServer3: Maschine mit CBR und Caching Proxy.
- WebServerA, WebServerB, WebServerC: Ausweichwebserver.

Abb. 30 zeigt eine grundlegende Darstellung mehrerer Server (EdgeServer1, EdgeServer2, EdgeServer3), die die Last auf mehrere Back-End-Webserver verteilen. Die CBR-Komponente verwendet Caching Proxy für eine vom Inhalt

des URL abhängige Weiterleitung von Anforderungen an die Back-End-Webserver. Die Dispatcher-Komponente verteilt die Last der CBR-Komponenten auf alle Edge-Server. Die Dispatcher-Funktion für hohe Verfügbarkeit stellt sicher, dass Anforderungen an die Back-End-Server auch dann möglich sind, wenn die primäre Maschine mit hoher Verfügbarkeit (EdgeServer1) ausfällt.

Basisrichtlinien für die Konfiguration:

- Konfigurieren Sie Caching Proxy auf allen Edge-Servern identisch. Zur Verbesserung der Zugriffsmöglichkeiten auf die Webseiten der Back-End-Server sollten Sie Caching Proxy für das Speicher-Caching konfigurieren. So könne die Edge-Server häufiger angeforderte Webseiten zwischenspeichern. Weitere Informationen zum Konfigurieren von Caching Proxy finden Sie im *IBM WebSphere Edge Server (Multiplattform) Administratorhandbuch*.
- Definieren Sie für die Network-Dispatcher-Komponenten CBR und Dispatcher identische Cluster-Adressen und Ports.
- Konfigurieren Sie die CBR-Komponente auf allen Edge-Servern gleich. Verwenden Sie an den Ports, die Sie für den Cluster definieren möchten, die Webserver A, B und C. Weitere Informationen zum Konfigurieren von finden Sie in „Kapitel 7. Content Based Routing konfigurieren“ auf Seite 87.
- Konfigurieren Sie die Dispatcher-Komponente auf den Edge-Servern 1 und 2 identisch. Definieren Sie an den Ports, die als Cluster-Ports definiert werden sollen, an denen Dispatcher einen Lastausgleich durchführt, alle Edge-Server als zu verwendende Server. Weitere Informationen zum Konfigurieren von Dispatcher finden Sie in „Kapitel 5. Dispatcher konfigurieren“ auf Seite 61.
- Konfigurieren Sie den Edge-Server 1 als primäre Maschine mit hoher Verfügbarkeit und den Edge-Server 2 als Bereitschaftsmaschine (Sicherung) mit hoher Verfügbarkeit. Weitere Informationen hierzu finden Sie im Abschnitt „Hohe Verfügbarkeit“ auf Seite 177.

Anmerkung:

1. Der Host-Name (z. B. www.firma.com), der der Cluster-Adresse zugeordnet ist, muss die Anweisung "Hostname" in der Konfigurationsdatei von Caching Proxy aktualisiert werden.
2. Wenn Sie vermeiden möchten, dass die Back-End-Serveradressen im URL angezeigt werden, müssen Sie unter Umständen die Anweisung "SendRevProxyName" in der Konfigurationsdatei von Caching Proxy auf "yes" setzen.
3. Sie können sicherstellen, dass das Webspeicher-Caching effizient genutzt wird, indem Sie in der Konfigurationsdatei von Caching Proxy die Anweisung "Caching" auf "ON" und den Wert für die Anweisung "CacheMemory" auf die erforderliche Größe setzen.

4. Soll die Zwischenspeicherung auf der Basis des ankommenden URL-Namens und nicht der IP-Adresse erfolgen, fügen Sie in der Konfigurationsdatei von Caching Proxy im Abschnitt "Mapping Rules" eine zusätzliche Zeile mit der Anweisung "Proxy" hinzu.

Beispielzeilen für die vorgenannten Schritte 1-4:

```
Hostname          www.firma.com
SendRevProxyName  yes
Caching           ON
CacheMemory       128000 K
Proxy             /* http://www.firma.com/* www.firma.com
```

5. Vergessen Sie nicht, für die Cluster-Adresse auf der Netz-schnittstellenkarte für EdgeServer1 und auf der Loopback-Einheit der übrigen Edge-Server einen Aliasnamen festzulegen.
6. Wenn Sie die Edge-Server auf einer Linux-Plattform verwenden, müssen Sie einen Patch-Code für den Linux-Kernel installieren. Weitere Informationen hierzu finden Sie im Abschnitt „Patch-Code für Linux-Kernel (zum Unterdrücken von ARP-Antworten an der Loopback-Schnittstelle) installieren“ auf Seite 77.
7. Wenn Sie CBR mit content-Regeln verwenden, dürfen Sie nicht die Port-Affinität (stickytime) anwenden, da andernfalls die content-Regeln beim Verarbeiten von Anforderungen an die Back-End-Webserver nicht erfüllt werden.

Beispielkonfigurationsdateien:

Die folgenden Beispielkonfigurationsdateien ähneln den Dateien, die beim Einrichten einer Edge-Server-Konfiguration, wie sie in Abb. 30 auf Seite 407 dargestellt ist, erstellt werden. Die Beispielkonfigurationsdateien sind Dateien für die Network-Dispatcher-Komponenten Dispatcher und CBR. In der Beispielkonfiguration wird für jede Edge-Server-Maschine ein Ethernet-Adapter verwendet und alle Adressen befinden sich innerhalb eines privaten Teilnetzes. In den Beispielkonfigurationsdateien sind für die angegebenen Maschinen die folgenden IP-Adressen angegeben:

- EdgeServer1 (primärer Edge-Server mit hoher Verfügbarkeit): 192.168.1.10
- EdgeServer2 (Auschweich-Edge-Server mit hoher Verfügbarkeit): 192.168.1.20
- EdgeServer3 (Edge-Server für Web-Caching): 192.168.1.30
- Cluster-Adresse der Website: 192.168.1.11
- WebServerA-C (Back-End-Webserver: 192.168.1.71, 192.168.1.72 und 192.168.1.73)

Beispielkonfigurationsdatei für die Dispatcher-Komponente auf dem primären Edge-Server mit hoher Verfügbarkeit:

```
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
```

Beispielkonfigurationsdatei für die CBR-Komponente auf den Edge-Servern:

```
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_Regel type content
    pattern (URI=*WSA*)|(URI=*wsA*) priority 21
cbrcontrol rule useserver 192.168.1.11:80:webA_Regel webserverA

cbrcontrol rule add 192.168.1.11:80:webB_Regel type content
    pattern (URI=/WS_B*) priority 22
cbrcontrol rule useserver 192.168.1.11:80:webB_Regel webserverB

cbrcontrol rule add 192.168.1.11:80:webC_Regel type content
    pattern URI=*webC* priority 23
cbrcontrol rule useserver 192.168.1.21:80:webC_Regel webserverC
```

Anhang H. Weitere Ressourcen

Zugriff auf die Befehlszeile

In vielen Situationen können Sie Tasten oder Tastenkombinationen verwenden, um Operationen auszuführen, für die auch die Maus benutzt werden kann. Viele Menüaktionen können von der Tastatur aus aufgerufen werden.

Anweisungen für den Einsatz der Tastatur finden Sie in der Dokumentation zum verwendeten Betriebssystem.

Onlinehilfefunktion aufrufen

Network Dispatcher stellt eine Onlinehilfefunktion bereit, die die Tasks beschreibt, die Sie beim Installieren, Planen, Konfigurieren und Verwenden des Produkts ausführen müssen.

Wenn Sie Hilfe zum aktuellen Fenster benötigen, klicken Sie auf das Fragezeichen (?) in der oberen rechten Ecke des Fensters. Es werden die folgenden Optionen angeboten:

Hilfe für Feld

Kontextsensitiver Hilfetext für die Task, die Sie gerade ausführen.

Vorgehensweise

Eine Liste von Tasks mit Bezug zum aktuellen Fenster.

Inhaltsverzeichnis

Ein Inhaltsverzeichnis aller Hilfetexte.

Index Ein alphabetisch geordneter Index der Hilfethemen.

Referenzinformationen

Zusätzliche Informationen zur Verwendung von Network Dispatcher finden Sie an folgenden Stellen:

- Website zu WebSphere Edge Server:
<http://www.ibm.com/software/webservers/edgeserver>
- Website mit technischen Informationen zu Network Dispatcher:
<http://www.ibm.com/software/webservers/edgeserver/support.html>
Geben Sie im Suchfeld "Network Dispatcher" ein und wählen Sie als Suchoption **Hints and tips** aus.

Anhang I. Bemerkungen

Hinweise auf IBM Produkte, Programme und Dienstleistungen in dieser Veröffentlichung bedeuten nicht, dass IBM diese in allen Ländern, in denen IBM vertreten ist, anbietet. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme oder Dienstleistungen in Verbindung mit Fremdprodukten und Fremddienstleistungen liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Veröffentlichung ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

Site Counsel
IBM Corporation
P.O. Box 12195
3039 Cornwallis Avenue
Research Triangle Park, NC 27709-2195
USA

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der IBM Kundenvereinbarung.

Die Veröffentlichung dient nicht für Produktionszwecke. IBM übernimmt keine Haftung. Die in dieser Veröffentlichung aufgeführten Beispiele sollen lediglich zur Veranschaulichung und zu keinem anderen Zweck dienen.

Dieses Produkt enthält Computersoftware, die von CERN erstellt oder zur Verfügung gestellt wurde. Ein entsprechender Hinweis ist in allen Produkten enthalten, die CERN-Computersoftware oder Komponenten dieser Software enthalten.

Marken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

AIX

IBM

IBMLink

LoadLeveler

OS/2

NetView

WebSphere

Lotus ist in gewissen Ländern eine eingetragene Marke der Lotus Development Corporation.

Domino ist in gewissen Ländern eine Marke der Lotus Development Corporation.

Tivoli ist in gewissen Ländern eine eingetragene Marke von Tivoli Systems, Inc.

Java und alle Java-basierten Marken und Logos sind in gewissen Ländern Marken oder eingetragene Marken von Sun Microsystems, Inc.

Solaris ist in gewissen Ländern eine Marke von Sun Microsystems, Inc.

Microsoft und Windows 2000 sind in gewissen Ländern Marken oder eingetragene Marken der Microsoft Corporation.

Cisco ist in gewissen Ländern eine eingetragene Marke von Cisco Systems, Inc.

HP ist in gewissen Ländern eine Marke der Hewlett-Packard Company.

Linux ist eine eingetragene Marke von Linus Torvalds.

Red Hat ist eine eingetragene Marke von Red Hat, Inc.

UNIX ist in gewissen Ländern eine eingetragene Marke von The Open Group.

Mit ** gekennzeichnete Namen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Glossar

A

ACK. Ein Steuerungsbit (zur Bestätigung), das keinen Platz in der Folge beansprucht. Es zeigt an, dass das Bestätigungsfeld dieses Segments die nächste Folgennummer angibt, die der Absender dieses Segments erwartet. Dadurch wird der Empfang aller bisherigen Folgennummern bestätigt.

Adresse. Der eindeutige Code, der jeder Einheit oder Workstation zugeordnet wird, die mit einem Netz verbunden ist. Eine Standard-IP-Adresse ist ein 32-Bit-Adressfeld. Dieses Feld enthält zwei Abschnitte. Der Abschnitt ist die Netzadresse, der zweite die Host-Nummer.

Advisor-Funktion. Die Advisor-Funktionen sind Bestandteil von Network Dispatcher. Advisor-Funktionen erfassen und analysieren Rückmeldungen von einzelnen Servern und informieren die Manager-Funktion.

Agent. (1) In der Systemverwaltung ein Benutzer, der für eine bestimmte Interaktion die Rolle eines Agenten übernommen hat. (2) Eine Definitionseinheit, die verwaltete Objekte repräsentiert. Dies geschieht durch (a) die Ausgabe von Mitteilungen zu den Objekten und (b) die Bearbeitung von Manager-Anforderungen für Verwaltungsoperationen zum Ändern oder Abfragen der Objekte.

Aliasname. Ein zusätzlicher Name, der einem Server zugeordnet wird. Der Aliasname macht den Server vom Namen seiner Host-Maschine unabhängig. Der Aliasname muss im Domänennamensserver definiert sein.

Aliasname der Loopback-Einheit. Eine der Loopback-Schnittstelle zugeordnete alternative IP-Adresse. Die alternative Adresse hat den nützlichen Nebeneffekt, dass keine Werbung auf einer realen Schnittstelle stattfindet.

Als aktiv markieren. Einem Server das Empfangen neuer Verbindungen erlauben.

Als inaktiv markieren. Alle aktiven Verbindungen zu einem Server werden unterbrochen und das Senden neuer Verbindungen oder Pakete an diesen Server wird unterbunden.

Anfangsbereich. Bei regelbasierten Lastausgleich der niedrigste Wert, der für eine Regel angegeben wird. Der Standardwert hängt vom Regeltyp ab.

API. Anwendungsprogrammierschnittstelle. Die Schnittstelle (Anrufvereinbarungen), durch die ein Anwendungsprogramm auf Dienste des Betriebssystems und andere Dienste zugreift. Eine API ist auf Quellcodeebene definiert und bietet eine Abstraktionsstufe zwischen der Anwendung und dem Kernel (oder anderen privilegierten Dienstprogrammen), um die Portierbarkeit des Codes sicherzustellen.

Assistent. Ein Dialog innerhalb einer Anwendung, der einen Benutzer schrittweise bei der Ausführung einer bestimmten Task anleitet.

Ausweichmaschine. Bei der Funktion für hohe Verfügbarkeit von Dispatcher die Partnermaschine der primären Maschine. Sie überwacht den Status der primären Maschine und übernimmt ggf. deren Aufgaben. Siehe auch "Hohe Verfügbarkeit" und "Primäre Maschine".

B

Bandbreite. Die Differenz zwischen der höchsten und der niedrigsten Frequenz eines Übertragungskanals. Die Datenmenge, die pro Sekunde über eine bestimmte Kommunikationsverbindung gesendet werden kann.

Binäre Protokollierung. Erlaubt das Speichern von Serverdaten in Binärdateien, die anschließend verarbeitet werden, um die zeitabhängig gesammelten Serverdaten zu analysieren.

C

Caching Proxy. Ein Caching-Proxyserver, der durch sehr effiziente Caching-Schemata die Antwortzeit für Endbenutzer verkürzen hilft. Flexible PICS-Filter unterstützen Netzadministratoren bei der Steuerung des Zugriffs auf webbasierte Informationen an einem zentralen Standort.

CBR. Content Based Routing. Eine Komponente von Network Dispatcher. CBR verteilt zusammen mit Caching Proxy eingehende Client-Anforderungen ausgehend vom Inhalt der Webseite und unter Verwendung bestimmter Regeltypen auf HTTP- oder HTTPS-Server.

cbrcontrol. Stellt die Schnittstelle zur Komponente Content Based Routing von Network Dispatcher bereit.

cbrserver. Bearbeitet beim Content Based Routing die Anfragen von Executor, Manager und Advisor-Funktionen.

CGI. Common Gateway Interface. Ein Standard für den Austausch von Informationen zwischen einem Webserver und einem externen Programm. Das externe Programm kann in einer beliebigen vom Betriebssystem unterstützten Sprache geschrieben sein und führt Tasks aus, die der Server normalerweise nicht ausführt, z. B. die Formularverarbeitung.

CGI-Script. Ein CGI-Programm, das in einer Script-basierten Sprache wie Perl oder REXX geschrieben ist und mit der Common Gateway Interface Tasks ausführt, die der Server in der Regel nicht ausführt, z. B. die Formularverarbeitung.

Cisco Consultant. Eine Komponente von Network Dispatcher. Cisco Consultant stellt mit der Network-Dispatcher-Technologie Echtzeitdaten zum Lastausgleich für den Cisco Content Services Switch bereit.

Cisco CSS Switch. Switches der Cisco CSS 11000 Series, die zur Weiterleitung von Paketen und Inhalten verwendet werden.

Client. Ein Datenverarbeitungssystem oder -prozess, das bzw. der einen Dienst von einem anderen Datenverarbeitungssystem oder -prozess anfordert. Eine Workstation oder ein Personal Computer, die bzw. der HTML-Dokumente von einem Lotus Domino Go Webserver anfordert, ist beispielsweise ein Client dieses Servers.

Cluster. Im Kontext der Dispatcher-Komponente eine Gruppe von TCP- oder UDP-Servern, die für denselben Zweck verwendet werden und mit einem Host-Namen identifiziert werden. Siehe auch "Zelle".

Cluster-Adresse. Im Kontext der Dispatcher-Komponente die Adresse, zu der Clients eine Verbindung herstellen.

Cluster-Server. Ein Server, den der Dispatcher mit anderen Servern zu einem virtuellen Server zusammenfasst. Network Dispatcher verteilt den TCP- oder UDP-Datenverkehr auf diese Cluster-Server.

D

Dämon. (DAEMon, Disk And Execution Monitor) Ein Programm, das nicht explizit beteiligt ist, sondern ruht und darauf wartet, dass eine oder mehrere bestimmte Bedingungen eintreten. Der Verursacher der Bedingung muss nichts von dem wartenden Dämon wissen (obwohl ein Programm häufig eine Aktion aus genau dem Grund ausführt, weil es weiß, dass damit implizit ein Dämon aufgerufen wird).

Dienst. Eine von Knoten bereitgestellte Funktion wie HTTP, FTP oder Telnet.

Dispatcher. Eine Komponente von Network Dispatcher, die den TCP- oder UDP-Datenverkehr effizient auf Gruppen einzeln verbundener Server verteilt. Die Dispatcher-Maschine ist der Server, der den Dispatcher-Code ausführt.

Domänennamensserver. DNS. Ein vielseitig einsetzbarer, verteilter und replizierter Datenabfragedienst, der hauptsächlich im Internet für die Umsetzung von Host-Namen in Internet-Adressen verwendet wird. Bezeichnet außerdem die Darstellung des Host-Namens im Internet, obwohl ein solcher Name eigentlich ein vollständig qualifizierter Domänenname ist. Der DNS kann in der Weise konfiguriert werden, dass er basierend auf den Domänen im gesuchten Namen eine Folge von Namensservern verwendet, bis er eine Übereinstimmung findet.

E

Endbereich. Beim regelbasierten Lastausgleich der höchste für eine Regel angegebene Wert. Die Standardeinstellung ist vom Regeltyp abhängig.

Ethernet. Ein Standardtyp eines lokalen Netzes (LAN). Dieser Standard erlaubt mehreren Stationen den beliebigen Zugriff auf das Übertragungsmedium ohne Koordination, verhindert durch Trägerprüfung und Verzögerung Konkurrenzsituationen und beseitigt Konkurrenzsituationen durch Kollisionserkennung und Übertragung. Die von Ethernet verwendeten Softwareprotokolle variieren, umfassen aber TCP/IP.

Executor. Eine von mehreren Dispatcher-Funktionen. Der Executor leitet Anforderungen an die TCP- oder UDP-Server weiter, überwacht die Anzahl neuer, aktiver und beendeter Verbindungen und führt für beendete oder zurückgesetzte Verbindungen eine Garbage Collection durch. Der Executor liefert die neuen und aktiven Verbindungen an die Manager-Funktion. Der Executor von Cisco Consultant enthält die Konfigurationsdaten und die für die Verbindung zum Cisco CSS Switch erforderlichen Informationen.

F

FIN. Ein Steuerungsbit (finis), das eine Folgenummer belegt. Damit wird angezeigt, dass der Sender keine weiteren Daten oder Steuerzeichen sendet, die einen Platz in der Folge beanspruchen.

FIN-Status. Der Status einer Transaktion, die beendet wurde. Ist eine Transaktion im FIN-Status, kann der Garbage Collector von Network Dispatcher den für diese Verbindung reservierten Speicher bereinigen.

Firewall. Ein Computer, der ein privates Netz (z. B. ein Unternehmen) mit einem öffentlichen Netz (z. B. dem Internet) verbindet. Er enthält Programme, die den Zugriff zwischen zwei Netzen einschränken. Siehe auch *Proxy-Gateway*.

FTP (File Transfer Protocol). Ein Anwendungsprotokoll, das von Computern in einem Netz für die Übertragung von Dateien verwendet wird. FTP erfordert für den Zugriff auf Dateien eines fernen Host-Systems eine Benutzer-ID und manchmal auch ein Kennwort.

G

Gateway. Eine Funktionseinheit, die zwei Computernetze mit unterschiedlichen Architekturen verbindet.

Gegenseitige hohe Verfügbarkeit. Bei gegenseitiger hoher Verfügbarkeit können zwei Dispatcher-Maschinen primäre Maschinen sein und gleichzeitig als Ausweichmaschine der jeweils anderen Dispatcher-Maschine verwendet werden. Siehe auch "Ausweichmaschine", "Hohe Verfügbarkeit", "Primäre Maschine".

GRE. Generic Routing Encapsulation. Ein Protokoll, das die Übertragung eines beliebigen Netzprotokolls A über ein beliebiges anderes Protokoll B ermöglicht, indem es die Pakete von A in GRE-Paketen kapselt, die dann in den Paketen von B enthalten sind.

H

Haltezeit. Das Intervall zwischen dem Schließen einer Verbindung und dem Öffnen einer neuen Verbindung. Innerhalb dieses Intervalls wird der Client an denselben Server wie bei der ersten Verbindung vermittelt. Nach Ablauf der Haltezeit kann der Client an einen anderen Server vermittelt werden.

Hohe Verfügbarkeit. Eine Dispatcher-Funktion, die die Übernahme der Aufgaben eines Dispatchers durch einen anderen ermöglicht, sollte der erste Dispatcher ausfallen.

Host. Ein mit einem Netz verbundener Computer, der ein Eingangspunkt für dieses Netz bildet. Ein Host kann ein Client, ein Server oder beides gleichzeitig sein.

Host-Name. Der einem Host zugeordnete symbolische Name. Host-Namen werden über einen Domänennamensserver in IP-Adressen aufgelöst.

HTML. Hypertext Markup Language. Die Sprache, die zum Erstellen von Hypertext-Dokumenten benutzt wird. Hypertext-Dokumente enthalten Links zu anderen Dokumenten mit zusätzlichen Informationen zum hervorgehobenen Begriff oder Thema. HTML steuert beispielsweise das Format von Text und die Position von Eingabefeldern in Formularen sowie die navigierbaren Links.

HTTP (Hypertext Transfer Protocol). Das Protokoll, das zum Übertragen und Anzeigen von Hypertext-Dokumenten verwendet wird.

I

ICMP. Internet Control Message Protocol. Ein Nachrichtensteuerungs- und Fehlermeldungsprotokoll zwischen einem Host-Server und einem Gateway zum Internet.

IMAP. Internet Message Access Protocol. Ein Protokoll, mit dem ein Client auf E-Mail-Nachrichten auf einem Server zugreifen und diese bearbeiten kann. Es ermöglicht für ferne ferne Nachrichtenordner (Mailboxes) dieselbe Art der Bearbeitung wie für lokale Mailboxes.

Internet. Der weltweite Verbund von Netzen, die die Internet-Protokollgruppe verwenden und öffentlich zugänglich sind.

Intranet. Ein sicheres privates Netz, das Internet-Standards und -Anwendungen (wie Webbrowser) in die vorhandene Computerinfrastruktur für den Netzbetrieb integriert.

IP. Internet Protocol. Ein verbindungsloses Protokoll zur Weiterleitung von Daten über ein Netz oder miteinander verbundene Netze. IP agiert als Vermittler zwischen den höheren Protokollschichten und der Bitübertragungsschicht.

IP-Adresse. Internet-Protocol-Adresse. Eine eindeutige 32-Bit-Adresse, die die tatsächliche Position jeder Einheit oder Workstation in einem Netz angibt. Diese Adresse wird auch als Internet-Adresse bezeichnet.

IPSEC. Internet Protocol Security. Ein sich entwickelnder Standard für die Sicherheit der Vermittlungs- oder Paketebene bei der Netzkommunikation.

L

LAN. Local Area Network (lokales Netz). Ein Computernetz mit Einheiten, die innerhalb eines begrenzten geografischen Bereichs verbunden sind, um miteinander zu kommunizieren, und mit einem größeren Netz verbunden werden können.

lbc. Load-Balancing Consultant

lbccontrol. Die Schnittstelle zwischen Cisco Consultant und dem Cisco CSS Switch.

lbcservice. Enthält in Cisco Consultant die Konfigurationsdaten und führt die Befehle aus.

Loopback-Schnittstelle. Eine Schnittstelle, die nicht erforderliche Übertragungsfunktionen umgeht, wenn die Informationen an eine Definitionseinheit innerhalb desselben Systems adressiert sind.

M

MAC-Adresse. Ein LAN-Konzept oder LAN-Emulationskonzept.

Mailbox Locator. Eine Komponente von Network Dispatcher. Für die Protokolle IMAP und POP3 ist Mailbox Locator ein Proxy, der ausgehend von der Benutzer-ID und dem Kennwort einen geeigneten Server wählt.

Manager. Eine der Funktionen von Network Dispatcher. Der Manager legt ausgehend von internen Zählern des Executors und Rückmeldungen der Advisor-Funktionen Wertigkeiten fest. Der Executor verwendet die Wertigkeiten dann für den Lastausgleich.

Messwert. Ein Prozess oder Befehl, der einen numerischen Wert zurückgibt, der beim Lastausgleich im Netz verwendet werden kann, z. B. die Anzahl der derzeit angemeldeten Benutzer.

Metric Server. Früher bekannt als Server Monitor Agent (SMA). Metric Server stellt systemspezifische Messwerte für den Manager von Network Dispatcher bereit.

MIB. (1) Management Information Base. Eine Gruppe von Objekten, auf die mit einem Netzwerkverwaltungsprotokoll zugegriffen werden kann. (2) Eine Definition für Verwaltungsinformationen, die die von einem Host oder Gateway verfügbaren Informationen und die zulässigen Operationen angibt.

mlcontrol. Die Schnittstelle zur Komponente Mailbox Locator von Network Dispatcher.

mlserver. Enthält in Mailbox Locator die Konfigurationsdaten und führt die Befehle aus.

N

ndcontrol. Die Schnittstelle zur Dispatcher-Komponente von Network Dispatcher.

ndserver. Bearbeitet in der Dispatcher-Komponente die Anforderungen von der Befehlszeile an Executor, Manager und Advisor-Funktionen.

Netzmaske. Bei Internet-Teilnetzen eine 32-Bit-Maske, mit der die Teilnetzadressbits im Host-Abschnitt einer IP-Adresse identifiziert werden.

Netzproximität. Die Proximität zweier vernetzter Einheiten wie Client und Server, die Site Selector durch Messung der durchschnittlichen Laufzeit ermittelt.

Netzverwaltungsstation. In SNMP (Simple Network Management Protocol) eine Station, die Verwaltungsanwendungsprogramme ausführt, mit denen Netzelemente überwacht und gesteuert werden.

NIC. Network Interface Card. Eine Adapterschaltkarte, die in einem Computer installiert ist, um eine physische Verbindung zu einem Netz zu ermöglichen.

Nicht für Weiterleitung bestimmte Adresse (NFA). Die für Verwaltungs- und Konfigurationszwecke verwendete primäre IP-Adresse der Network-Dispatcher-Maschine.

NNTP. Network News Transfer Protocol. Ein TCP/IP-Protokoll zur Übertragung von Nachrichten.

P

Paket. Die Dateneinheit, die im Internet oder einem anderen paketvermittelten Netz zwischen Ursprung und Ziel weitergeleitet wird.

PICS. Platform for Internet Content Selection. PICS-fähige Clients ermöglichen den Benutzern, selbst zu bestimmen, welche Bewertungsdienste sie verwenden möchten und welche Bewertungen der einzelnen Dienste akzeptabel bzw. inakzeptabel sind.

Ping. Ein Befehl, der ICMP-Echoanforderungspakete (ICMP = Internet Control Message Protocol) an einen Host, einen Gateway oder einen Router sendet und eine Antwort erwartet.

POP3. Post Office Protocol 3. Ein Protokoll, das zum Austausch von Netzpost und zum Zugriff auf Mailboxes benutzt wird.

Port. Eine Nummer, die eine abstrakte Übertragungseinheit bezeichnet. Webserver verwenden standardmäßig Port 80.

Port-übergreifende Affinität. Die Port-übergreifende Affinität ist eine Affinität (Haltefunktion), die sich über mehrere Ports erstreckt. Siehe auch "Haltezeit".

Port-Umsetzung für Netzadressen. NAT (Network Address Port Translation), auch als Port-Zuordnung bekannt. Mit NAT können Sie auf einem physischen Server mehrere Serverdämonen konfigurieren, die an verschiedenen Port-Nummern empfangsbereit sind.

Primäre Maschine. Bei der Funktion für hohe Verfügbarkeit der Dispatcher-Komponente die Maschine, die aktiv Pakete weiterleitet. Die zugehörige Partner- oder Ausweichmaschine überwacht den Status der primären Maschine und übernimmt ggf. deren Aufgaben. Siehe auch "Ausweichmaschine" und "Hohe Verfügbarkeit".

Priorität. Bei dem auf Regeln basierenden Lastausgleich das Maß an Bedeutung, das einer bestimmten Regel beigemessen wird. Der Dispatcher wertet die Regeln beginnend bei der ersten Prioritätsebene bis hin zur letzten Prioritätsebene aus.

Privates Netz. Ein separates Netz, in dem der Dispatcher aus Gründen des Durchsatzes mit Cluster-Servern kommuniziert.

Protokoll. Die Regeln, die den Betrieb von Funktionseinheiten eines DFV-Systems steuern, wenn eine Kommunikation stattfinden soll. Protokolle können Details der unteren Ebene zu Schnittstellen zwischen Maschinen festlegen, wie beispielsweise die Reihenfolge, in der die Bits eines Byte gesendet werden. Sie können auch Austauschprozesse der höheren Ebene zwischen Anwendungsprogrammen festlegen, z. B. die Dateiübertragung.

Q

Quality of Service (QoS). Leistungsmerkmale eines Netzdienstes wie Durchsatz, Transitverzögerung und Priorität. Bei einigen Protokollen können Pakete oder Datenströme QoS-Anforderungen enthalten.

Quellenadresse. Bei der Funktion für hohe Verfügbarkeit des Dispatchers die Adresse der Partnermaschine, die Überwachungssignale sendet.

R

reach. Eine Advisor-Funktion des Dispatchers, die ping-Aufrufe an eine bestimmte Zieladresse absetzt und meldet, ob die Zieladresse antwortet.

reach-Adresse. Bei der Funktion für hohe Verfügbarkeit von Dispatcher die Zieladresse, an die die Advisor-Funktion ping-Aufrufe absetzen soll, um festzustellen, ob die Zieladresse antwortet.

Regel. Beim regelbasierten Lastausgleich ein Mechanismus zum Gruppieren von Servern, der die Auswahl eines Servers ausgehend von anderen Informationen als der Zieladresse und dem Port ermöglicht.

Regeltyp. Beim regelbasierten Lastausgleich ein Anzeiger für die Informationen, die ausgewertet werden müssen, um zu bestimmen, ob eine Regel erfüllt wird.

RMI. Remote Method Invocation. Teil der Bibliothek der Programmiersprache Java, der einem Java-Programm, das auf einem Computer ausgeführt wird, ermöglicht, auf Objekte und Methoden eines auf einem anderen Computer ausgeführten Java-Programms zuzugreifen.

Root. Die uneingeschränkte Berechtigung zum Zugriff auf und Ändern von beliebigen Teilen des Betriebssystems AIX, Red Hat Linux oder Solaris. Diese Berechtigung wird normalerweise dem Benutzer erteilt, der das System verwaltet.

Route. Der Pfad für den Datenaustausch im Netz von der Ursprungsadresse zu der Zieladresse.

Router. Eine Einheit, die Pakete zwischen Netzen weiterleitet. Die Weiterleitungsentscheidung wird ausgehend von Informationen der Vermittlungsschicht und von Route-Tabellen, die häufig von Routing-Produkten erstellt werden, getroffen.

RPM. Red Hat Package Manager.

Rückkehradresse. Eine eindeutige IP-Adresse oder ein eindeutiger Host-Name. Die Rückkehradresse wird auf der Dispatcher-Maschine konfiguriert und vom Dispatcher bei der Verteilung der Client-Anforderungen auf die Server als Quellenadresse verwendet.

S

Schreibweise mit Trennzeichen. Die syntaktische Darstellung eines 32-Bit-Integers, das aus vier 8-Bit-Zahlen besteht, die in Dezimalschreibweise angegeben werden und durch Punkte voneinander getrennt sind. Dient zur Darstellung von IP-Adressen.

Server. Ein Computer, der gemeinsam genutzte Dienste für andere Computer über ein Netz bereitstellt, z. B. ein Dateiserver, ein Druckserver oder ein Postserver.

Serveradresse. Der eindeutige Code, der jedem Computer zugeordnet wird, der gemeinsam genutzte Dienste für andere Computer über ein Netz bereitstellt, z. B. einem Dateiserver, einem Druckserver oder einem Postserver. Eine Standard-IP-Adresse ist ein 32-Bit-Adressfeld. Die Serveradresse kann die IP-Adresse in Schreibweise mit Trennzeichen oder der Host-Name sein.

Servermaschine. Ein Server, den der Dispatcher mit anderen Servern zu einem virtuellen Server zusammenfasst. Der Dispatcher verteilt den Datenverkehr auf die Servermaschinen. Synonym für Cluster-Server.

Shell. Die Software, die Befehlszeilen von der Workstation eines Benutzers akzeptiert und verarbeitet. Die Korn-Shell ist eine von mehreren verfügbaren UNIX-Shells.

Sitename. Ein Sitename ist ein nicht auflösbarer Host-Name, den der Client anfordert. Beispiel: Eine Website hat drei Server (1.2.3.4, 1.2.3.5 und 1.2.3.6), die für den Sitenamen *www.dnsload.com* konfiguriert sind. Wenn ein Client diesen Sitenamen anfordert, wird eine der drei Server-IP-Adressen als Auflösung zurückgegeben. Der Sitename muss ein vollständig qualifizierter Domänenname wie *dnsload.com* sein. Ein nicht qualifizierter Name, z. B. *dnsload*, ist als Sitename ungültig.

Site Selector. Eine DNS-gestützte Lastausgleichskomponente von Network Dispatcher. Site Selector verteilt die Last auf Server innerhalb eines Weitverkehrsnetzes (WAN) und verwendet dafür Messungen und Wertigkeiten, die von der auf diesen Servern aktiven Komponente Metric Server erfasst werden.

Skalierbar. Im Kontext des Leistungsspektrums eines Systems die schnelle Anpassung an Schwankungen bei der Auslastung. Ein skalierbares System kann beispielsweise gut an größere oder kleinere Netze angepasst werden und Tasks unterschiedlicher Komplexität ausführen.

SMTP. Simple Mail Transfer Protocol. In der Internet-Protokollgruppe ein Anwendungsprotokoll zum Übertragen von Post zwischen Benutzern in der Internet-Umgebung. SMTP gibt die Post austauschfolgen und das Nachrichtenformat an. SMTP setzt voraus, dass TCP (Transmission Control Protocol) das zugrundeliegende Protokoll ist.

SNMP. Simple Network Management Protocol. Das in STD 15, RFC 1157, definierte Internet-Standardprotokoll, das für die Verwaltung von Knoten in einem IP-Netz entwickelt wurde. SNMP ist nicht auf TCP/IP beschränkt. Es kann zum Verwalten und Überwachen aller Arten von Einrichtungen verwendet werden, einschließlich Computer, Router, Vernetzungs-Hubs, Toaster und Jukeboxes.

SPARC. Scalable Processor Architecture.

sscontrol. Die Schnittstelle zur Komponente Site Selector von Network Dispatcher.

SSL. Secure Sockets Layer. Ein bekanntes Sicherheitsschema, das von der Netscape Communications Corporation in Zusammenarbeit mit RSA Data Security, Inc. entwickelt wurde und dem Client ermöglicht, den Server zu authentifizieren und alle Daten und Anforderungen zu verschlüsseln. Der URL eines mit SSL gesicherten Servers beginnt mit https und nicht mit http.

ssserver. Bearbeitet für die Komponente Site Selector die Anforderungen von der Befehlszeile an Sitenamen, Manager und Advisor-Funktionen.

Standardeinstellung. Ein Wert, ein Attribut oder eine Option, die verwendet werden, wenn keine explizite Angabe vorliegt.

Stilllegen. Das Beenden eines Prozesses mit vollständigem normalem Abschluss laufender Operationen.

strategy. Bei der Funktion für hohe Verfügbarkeit des Dispatchers ein Schlüsselwort, das angibt, wie eine ausgefallene Maschine wiederhergestellt werden soll.

SYN. Ein Steuerungsbit im eingehenden Segment, das eine Folgenummer belegt und bei der Initialisierung einer Verbindung angibt, wo die Folgenummernvergabe beginnt.

T

TCP. Transmission Control Protocol. Ein im Internet verwendetes Übertragungsprotokoll. TCP ermöglicht einen zuverlässigen Austausch von Informationen zwischen Hosts. TCP verwendet IP als zugrundeliegendes Protokoll.

TCP/IP . Transmission Control Protocol/Internet Protocol. Eine Protokollgruppe, die die Übertragung zwischen Netzen unabhängig von den in den einzelnen Netzen verwendeten Übertragungstechnologien ermöglicht.

TCP-Servermaschine. Ein Server, den Network Dispatcher mit anderen Servern zu einem virtuellen Server zusammenfasst. Network Dispatcher verteilt den TCP-Datenverkehr auf die TCP-Servermaschinen. Synonym für Cluster-Server.

Teilnetzmaske. Bei Internet-Teilnetzen eine 32-Bit-Maske, mit der die Teilnetzadressbits im Host-Abschnitt einer IP-Adresse identifiziert werden.

Telnet. Terminalemulationsprotokoll. Ein TCP/IP-Anwendungsprotokoll für Fernverbindungsdienste. Mit Telnet kann ein Benutzer so auf einen fernen Host zugreifen, als wäre seine Workstation direkt mit diesem fernen Host verbunden.

TOS. Type of Service (Diensttyp). Ein 1-Byte-Feld im IP-Header des SYN-Pakets.

TTL. DNS TTL (Time To Live) ist die Zeit in Sekunden, die ein Client die Namensauflösungsantwort zwischenspeichern kann.

U

Überwachungssignal. Ein einfaches Paket, das zwischen zwei Dispatcher-Maschinen im Modus für hohe Verfügbarkeit übertragen wird und vom Bereitschafts-Dispatcher zur Überwachung des Zustandes des aktiven Dispatchers verwendet wird.

UDP. User Datagram Protocol. In der Internet-Protokollgruppe ein Protokoll für einen unzuverlässigen, verbindungslosen Datagrammdienst. Mit UDP kann ein Anwendungsprogramm auf einer Maschine oder ein Prozess ein Datenpaket an ein Anwendungsprogramm auf einer anderen Maschine oder einen anderen Prozess senden. UDP benutzt das Internet Protocol (IP) zum Senden von Datenpaketen.

Umsetzer für Netzadressen. NAT (Network Address Translator), virtuelles LAN. Eine Hardwareeinheit, die zur Zeit in Entwicklung ist und zur Erweiterung der vorhandenen Internet-Adressen verwendet werden soll. Sie erlaubt duplizierte IP-Adressen innerhalb einer Firma und eindeutiger Adressen außerhalb der Firma.

URI. Universal Resource Identifier. Die codierte Adresse für jede Ressource im Web, z. B. ein HTML-Dokument, ein Bild, ein Videoclip, ein Programm usw.

URL. Uniform Resource Locator. Eine standardisierte Angabe der Position eines Objektes, in der Regel einer Webseite im Internet. URLs sind das im World Wide Web verwendete Adressenformat. In HTML-Dokumenten gibt der URL das Ziel eines Hyperlink an, bei dem es sich häufig um ein anderes HTML-Dokument handelt (das eventuell auf einem anderen Computer gespeichert ist).

V

Verknüpfen. Ist keine dedizierte Maschine vorhanden, wird Network Dispatcher auf der Maschine installiert, für die der Lastausgleich durchgeführt wird.

Anmerkung: Die Verknüpfung ist nur unter den Betriebssystemen AIX, Red Hat Linux und Solaris möglich.

Verknüpfung mehrerer Adressen. Die Verknüpfung mehrerer Adressen ermöglicht dem Kunden, in der Konfiguration für den verknüpften Server eine andere Adresse als die NFA anzugeben. Siehe auch "Verknüpfen".

Verwalteter Knoten. In der Internet-Kommunikation eine Workstation, ein Server oder ein Router mit einem Netzverwaltungsagenten. Im Internet Protocol (IP) enthält der verwaltete Knoten normalerweise einen SNMP-Agenten (SNMP = Simple Network Management Protocol).

Vollständig qualifizierter Domänenname. Der vollständige Name eines Systems, bestehend aus dem lokalen Host-Namen und dem Domännennamen einschließlich einer Domäne der höchsten Ebene. Wenn

"venera" ein Host-Name ist, wäre "venera.isi.edu" beispielsweise ein vollständig qualifizierter Domänenname. Anhand eines vollständig qualifizierten Domännennamen sollte für jeden Host im Internet eine eindeutige Internet-Adresse bestimmt werden können. Dieser Prozess wird als "Namensauflösung" bezeichnet und verwendet das Domännennamensystem (DNS).

VPN. Virtuelles privates Netz. Ein Netz, das aus einem oder mehreren gesicherten IP-Tunnel(n) besteht, die zwei oder mehr Netze verbinden.

W

WAN. Wide Area Network (Weitverkehrsnetz). Ein Netz, das Übertragungsdienste für einen geografisches Gebiet bereitstellt, das größer als das von einem lokalen Netz oder einem Hochgeschwindigkeitsnetz versorgte Gebiet ist. Ein WAN kann öffentliche Übertragungseinrichtungen verwenden oder zur Verfügung stellen.

WAP. Wireless Application Protocol. Ein offener internationaler Standard für Anwendungen, die festnetzunabhängige Kommunikation verwenden, z. B. Internet-Zugriff über ein Handy.

WAS. Websphere Application Server.

Web. Das Netz von HTTP-Servern, das Programme und Dateien enthält, von denen viele Hypertext-Dokumente mit Links zu anderen Dokumenten auf HTTP-Servern sind. Das Web wird auch als World Wide Web bezeichnet.

WLM. Workload Manager. Eine zum Dispatcher gehörige Advisor-Funktion. WLM ist für Server auf OS/390-Großrechnern bestimmt, die die Komponente MVS Workload Manager (WLM) ausführen.

Z

Zeitlimit. Das Zeitintervall, das für die Ausführung einer Operation zugeteilt wurde.

Zieladresse. Die Adresse der Partnermaschine mit hoher Verfügbarkeit, an die Überwachungssignale und Antworten gesendet werden.

Index

A

- Abgleich von Consultant und CSS 129
- Advisor
 - Cisco Consultant
 - Berichtszeitlimit 366
 - Liste 366
 - starten 366, 368
 - Status anzeigen 366
 - Dispatcher-Komponente
 - Berichtszeitlimit 271
 - Intervall 151
 - Liste 272
 - Serververbindungszeitlimit 152
 - Einschränkung unter Linux 150
 - Liste 270, 366
 - Site Selector
 - Berichtszeitlimit 339
 - list 337
 - loglevel 337
 - Serverempfangszeitlimit 337
 - starten 338, 340
 - Version 339
- Advisor-Funktion
 - Anforderung/Antwort der HTTP-Advisor-Funktion 165
 - Beispielkonfigurationsdateien 400
 - cbrcontrol 268
 - Cisco Consultant
 - Berichtszeitlimit 368
 - Intervall 364, 367
 - Liste 365
 - Name 364
 - Port 364
 - Serverempfangszeitlimit 365, 367
 - Serververbindungszeitlimit 364, 367
 - Status anzeigen 368
 - Statusbericht 368
 - stoppen 366, 368
 - Version 367, 368
 - Dispatcher-Komponente 149
 - Advisor-Funktion "self" 155, 176
 - Advisor-Funktion ssl2http 85, 154
- Advisor-Funktion (*Forts.*)
 - Dispatcher-Komponente (*Forts.*)
 - anpassen 155
 - Bericht 273
 - Berichtszeitlimit 152
 - Intervall 272
 - Liste 153
 - Name 268
 - Port 275
 - schnelle Ausfallerkennung 152
 - Serverempfangszeitlimit 152, 270
 - Serververbindungszeitlimit 268, 271
 - starten 71
 - starten/stoppen 150
 - Statusbericht 272
 - stoppen 271
 - Version 273
 - lbcontrol 364
 - mlcontrol 268
 - ndcontrol 268
 - Site Selector
 - Berichtszeitlimit 340
 - Intervall 336, 339
 - Liste 338, 339
 - Name 336
 - Port 268, 336
 - Serverempfangszeitlimit 340
 - Serververbindungszeitlimit 336, 339
 - Statusbericht 338, 340
 - stoppen 339, 340
 - Version 340
 - sscontrol 336, 343
 - starten 138
 - URL-Option der HTTP-Advisor-Funktion 165
- Advisor-Funktionen
 - Dispatcher-Komponente
 - Caching-Proxy-Advisor-Funktion 154
 - Serverempfangszeitlimit 272
 - starten 271
- Advisor-Funktionen, Komponente von Network Dispatcher
 - Liste 367
 - starten 70
 - Statusbericht 365
- Affinität (Bindung)
 - Affinitätsadressmaske 204
 - aktive Cookie-Affinität 207, 316
 - Funktionsweise 202
 - Mailbox Locator 104
 - passive Cookie-Affinität 207, 209, 316
 - Port-übergreifende Affinität 204, 205, 306
 - quiesce now 206, 297, 301
 - Regeloption 207
 - SDA (Server Directed Affinity) 202
 - SSL-ID (Weiterleitungsmethode cbr) 57, 58
 - sticky (Außerkräftsetzen der Regelaffinität) 205, 206, 321
 - stickymask 204, 307
 - stickytime 57, 58, 202, 204, 307, 316
 - Überschreibung der Regelaffinität 205
 - URI-Affinität 207, 210, 316
- Affinitätsadressmaske 204, 307
- AIX
 - installieren 13
 - Voraussetzungen 12
- Aktive Cookie-Affinität 207, 316
- Aktive Verbindungen 215
- Aliasname
 - für NIC 96
 - Loopback-Einheit 71
 - Patch-Code für Linux-Kernel 72, 77
 - NIC 67
- Allgemeiner Schlüssel
 - für ferne Authentifizierung 219
- An-/Abmeldung 11
- Ändern
 - Anzahl beendeter Verbindungen 224
 - Inaktivitätszeitgeber 224
 - Standardzeit für Beendigung inaktiver Verbindungen 224
- Anzahl beendeter Verbindungen 224

Anzeige

globale Werte und ihre Standard-einstellungen

für einen Advisor 273, 339, 340

für Manager 301, 346, 348, 381, 383

interne Zähler 284, 372

Liste

Advisor, die Messungen durchführen 272, 339, 367

Statistik 300, 345, 346, 379, 381

Status

ein Cluster oder alle Cluster 279, 370

Server für einen Port 311, 386, 387

Statusbericht für eine Advisor-Funktion 272, 338, 340, 365

Versionsnummer

von Advisor 273, 339, 340

von Manager 302, 346, 348, 381, 383

apCnsvHits 215

apSvcConnections 215

Assistent für Konfiguration

Dispatcher 5

Auflösung, GUI 250

Ausweichmaschine, hohe Verfügbarkeit 52

konfigurieren 178

B

Befehle

cbrcontrol

advisor 268

cluster 274

executor 280

file 285

help 287

host 294

log 295

manager 296

metric 303

port 305

rule 312

server 320

set 327

status 328

Cisco Consultant 363

iconfig 69, 170

Aliasnamen für die Loopback-Einheit angeben 72

lbcontrol

advisor 364

Befehle (Forts.)

lbcontrol (Forts.)

cluster 369

executor 371

file 373

help 375

host 376

log 377

manager 378

metric 384

port 386

Server konfigurieren 388

set 390

status 391

mlcontrol

advisor 268

cluster 274

executor 280

file 285

help 287

host 294

log 295

manager 296

metric 303

port 305

server 320

set 327

status 328

ndconfig 69, 171

ndcontrol

advisor 268

Cluster 274

Eingabeaufforderung 266

executor 280

file 285

help 287

hohe Verfügbarkeit steuern 289

Host 294

log 295

manager 296

metric 303

port 305

rule 312

server 320

set 327

SNMP-Subagenten konfigurieren 329

status 328

zum Definieren der NFA 67, 284, 371, 372

zum Definieren eines Ports 69

zur Definition eines Servers 70

Befehle (Forts.)

ndcontrol (Forts.)

zur Steuerung der Advisor-Funktion 70, 71

zur Steuerung des Managers 70, 71

netstat

zur Überprüfung der IP-Adressen und Aliasnamen 74

Site Selector 335

sscontrol

advisor 336

file 341

help 343

manager 344

metric 349

nameserver 350

rule 351

server 355

set 357

sitename 358

status 362

weiterleiten

zum Löschen einer zusätzlichen Route 74, 75

Befehlsreferenzen

lesen 261

Befehlszeile

Konfigurationsbeispiel 4

Zugriff 411

Beispiel für einen schnellen Start 1

Beispiele

lokale Server verwalten 37, 38, 41, 42, 44, 46

schneller Start 1

Beispielkonfigurationsdateien 393

Advisor-Funktion 400

Dispatcher-Komponente 393

Dispatcher-Komponente (Windows) 397

Bemerkungen 413

Benutzer-Exit, Scripts 149

Denial of Service (DoS) erkennen 211

managerAlert 149

managerClear 149

serverDown 149

serverUp 149

Binäre Protokollierung für Serverstatistik 213, 223

Bindung (Affinität)

Affinitätsadressmaske 204

aktive Cookie-Affinität 207, 316

Funktionsweise 202

Bindung (Affinität) (Forts.)

- passive Cookie-Affinität 207, 209, 316
 - Port-übergreifende Affinität 204, 205, 306
 - quiesce now 206, 297, 301
 - SDA (Server Directed Affinity) 202
 - sticky (Außerkräftsetzen der Regelaaffinität) 205, 206, 321
 - stickymask 204, 307
 - stickytime 57, 58, 202, 204, 307, 316
 - Überschreibung der Regelaaffinität 205
 - URI-Affinität 207, 316
- Bindungsspezifische Server 69, 70, 150, 170

C

Caching Proxy 83

- für CBR konfigurieren 93
- Caching-Proxy-Advisor-Funktion 154

CBR

- Aliasname für NIC 96
 - Anforderungen werden nicht verteilt 254
 - cbrcontrol scheitert 254
 - cbrcontrol scheitert unter Solaris 255
 - Einstellungen für Lastausgleich 144
 - Hardware- und Softwarevoraussetzungen 81
 - ifconfig, Befehl 96
 - Konfiguration
 - CBR-Maschine konfigurieren 93
 - Tasks im Überblick 87
 - mit Caching Proxy
 - Advisor-Funktion ssl2http 85 konfigurieren 100
 - Schlüsselwort "mapport" 85
 - SSL-Verbindungen 84
 - Übersicht 82
 - mit der Dispatcher-Komponente 57
 - ndadmin scheitert 254
 - planen 81
 - starten und stoppen 231
 - Syntax- oder Konfigurationsfehler 255
 - Tabellen zur Fehlerbehebung 238
- CBR (Forts.)
- wird nicht ausgeführt 254
- cbr, Weiterleitungsmethode 57
- stickytime 57, 58
- cbrcontrol, Befehl
- advisor 268
 - cluster 274
 - executor 280
 - file 285
 - help 287
 - host 294
 - log 295
 - manager 296
 - metric 303
 - port 305
 - rule 312
 - server 320
 - set 327
 - status 328
- Cisco Consultant
- Befehle 363
 - Einstellung für Lastausgleich
 - Zeitlimit für Advisor-Funktion 364
 - Einstellungen für Lastausgleich
 - Berichtszeitlimit für Advisor-Funktion 366, 368
 - Zeitlimit für Advisor-Funktion 365, 367
 - Executor 128
 - für Port 14099 kann kein Eintrag in der Registrierungsdatenbank erstellt werden 259
 - Hardware- und Softwarevoraussetzungen 127
 - Konfiguration
 - Beispiel 46
 - CSS-Maschine konfigurieren 136
 - Tasks im Überblick 133
 - lbcontrol 128
 - lbcontrol scheitert 258
 - lbserver 128
 - Manager 128
 - ndadmin 128
 - ndadmin scheitert 258
 - planen 127
 - starten 233
 - starten und stoppen 233
 - Tabellen zur Fehlerbehebung 240
 - verwenden 233
 - wird nicht gestartet 258
- Cluster
- Adresse konfigurieren 67

Cluster (Forts.)

- Anzahl beendeter Verbindungen ändern 224
 - Anzeige
 - Status dieses Clusters 279, 370
 - cbrcontrol 274
 - definieren 137
 - Definition 67, 279, 370
 - entfernen 279, 360, 369, 370
 - hinzufügen 279, 370
 - lbcontrol 369
 - mlcontrol 274
 - ndcontrol 274
 - Platzhalter 67
 - Proportionen festlegen 71, 138
 - proportions 274
 - Standardzeit für Beendigung inaktiver Verbindungen ändern 224
- Cluster-spezifisch
- Proportionen 359
- collocated (Schlüsselwort) 167, 326
- connecttimeout
- Cisco Consultant 364
 - Site Selector 336
- Content Based Routing 29
- Einstellungen für Lastausgleich 144
 - Hardware- und Softwarevoraussetzungen 81
 - Konfiguration
 - CBR-Maschine konfigurieren 93
 - Tasks im Überblick 87
 - mit der Dispatcher-Komponente 57
 - planen 81
 - Tabellen zur Fehlerbehebung 238
 - verwenden 231
- content-Regel 57, 195

D

Datei

- cbrcontrol 285
 - lbcontrol 373
 - mlcontrol 285
 - ndcontrol 285
 - sscontrol 341
- DB2-Advisor-Funktion 154
- default.cfg 66, 96, 109, 123
- Definition
- Cluster 279, 370
 - NFA 67, 284, 371, 372

Definition (Forts.)

- Port für einen Cluster 69, 310, 386, 387
- Server für einen Port 70, 325, 356, 389

Deinstallieren

- unter AIX 14
- unter Linux 19
- unter Solaris 22
- unter Windows 2000 25

Dispatcher

- Konfiguration
 - TCP-Servermaschinen konfigurieren 71

Dispatcher-Komponente

- Advisor arbeiten nicht korrekt 247
- Advisor-Funktionen zeigen alle Server als inaktiv an 252
- automatische Pfaderkennung verhindert Datenrückfluss mit Network Dispatcher 251
- blaue Anzeige beim Starten des Executors 250
- Content Based Routing 57
- Einstellungen für Lastausgleich 144
 - Advisor-Intervalle 151
 - Berichtszeitlimit für Advisor-Funktion 152
 - Glättungsfaktor 148
 - Manager-Intervalle 147
 - proportionale Bedeutung von Statusinformationen 145
 - Sensitivitätsschwelle 148
 - Serverzeitlimit der Advisor-Funktion 152
 - Wertigkeiten 146
- Fehler bei installiertem Caching Proxy 249
- Fehler beim Starten von ndserver unter Solaris 2.7 249
- GUI startet nicht richtig 249
- GUI wird nicht richtig angezeigt 250
- Hardware- und Softwarevoraussetzungen 49
- Hilfefenster kann nicht geöffnet werden 248
- Hilfefenster sind nicht zu sehen 250
- hohe Verfügbarkeit funktioniert nicht 246
- kein Lastausgleich für Anfragen 246

Dispatcher-Komponente (Forts.)

- keine hohe Verfügbarkeit im Weitverkehrsmodus von Network Dispatcher 252
- Konfiguration
 - Konfiguration der Dispatcher-Maschine 64
 - privates Netz konfigurieren 198
 - Tasks im Überblick 61
- MAC-Weiterleitung 54
- MS IIS und SSL funktionieren nicht 247
- NAT/NAPT 55
- ndadmin scheitert 248
- ndcontrol scheitert 248
- planen 49
- Rahmen kann nicht weitergeleitet werden 250
- Server antwortet nicht 245
- SNMPD arbeitet nicht korrekt 247
- starten 223
- Tabellen zur Fehlerbehebung 235
- Überwachungssignal kann nicht hinzugefügt werden 246
- unerwartetes Verhalten beim Laden einer großen Konfigurationsdatei 253
- Verbindung zu einer fernen Maschine 247
- verwenden 223
- wird nicht ausgeführt 245
- zusätzliche Routes (Windows 2000) 247
- DoS-Attacke erkennen 211
 - halfopenaddressreport 310
 - maxhalfopen 309
- DPID2 226

E

Einstellung

- Anzahl der Abfragen des Executors durch den Manager 148, 300, 379, 381
- Cluster-Adresse 69
- Glättungsfaktor 149, 301, 345, 347, 380, 383
- Intervallzeit
 - für Advisor zur Abfrage der Server 272, 339, 364, 367
 - für Manager zur Aktualisierung des Executors 147, 299, 344, 346, 378, 381

Einstellung (Forts.)

- maximale Größe des Protokolls für Advisor 221, 272, 337, 340, 365, 367
- für Manager 299, 344, 346, 379, 381
- maximale Wertigkeit
 - für Server an einem bestimmten Port 146, 310, 386, 387
- Name der Protokolldatei 338, 366
 - für Manager 346, 380
- NFA 64
- proportionale Bedeutung beim Lastausgleich 279
- Protokollstufe
 - für Advisor 221, 272, 339, 365, 367
 - für Manager 344, 378
- Sensitivität für Aktualisierung von Wertigkeiten 148, 301, 345, 347, 380, 383
- Wertigkeit für einen Server 299, 302, 326, 356, 381, 389
- Einstellungen, Anzeige aller globalen Werte
 - für einen Advisor 273, 339, 340
 - für Manager 301, 346, 348, 381, 383
- entfernen
 - Cluster 279, 360, 369, 370
 - Port von einem Cluster 310, 386, 387
 - Server von einem Port 326, 355, 356, 389
 - zusätzliche Route 75
- Ethernet-NIC
 - ibmnd.conf
 - für Solaris konfigurieren 65
- Executor
 - cbrcontrol 280
 - lbcontrol 371
 - mlcontrol 280
 - ndcontrol 280
 - starten 284, 372
 - stoppen 284
- Explizite Verbindung 197

F

Fehlerbehebung 235

- Advisor arbeiten nicht korrekt 247
- Advisor-Funktionen zeigen alle Server als inaktiv an 252

Fehlerbehebung (Forts.)

- allgemeine Probleme und Lösungen 245, 247, 254, 255, 257, 258, 259
- Anforderungen werden nicht verteilt 254
- automatische Pfaderkennung verhindert Datenrückfluss mit Network Dispatcher 251
- Befehl cbrcontrol oder ndadmin scheitert 254
- Befehl cbrserver wird gestoppt 255
- Befehl lbcontrol oder ndadmin scheitert 258
- Befehl mlcontrol oder ndadmin scheitert 256
- Befehl ndcontrol oder ndadmin scheitert 248
- Befehl sscontrol oder ndadmin scheitert 257
- blaue Anzeige beim Starten des Executors von Network Dispatcher 250
- CBR wird nicht ausgeführt 254
- cbrcontrol scheitert unter Solaris 255
- Dispatcher, Microsoft IIS und SSL arbeiten nicht 247
- Dispatcher-Anforderungen werden nicht weitergeleitet 246
- Dispatcher-Funktion für hohe Verfügbarkeit arbeitet nicht 246
- Dispatcher und Server antworten nicht 245
- Dispatcher wird nicht ausgeführt 245
- ein Port kann nicht hinzugefügt werden 256
- Empfang eines Mailbox-Locator-Fehlers beim Hinzufügen eines Ports 256
- Fehler bei der Ausführung von Dispatcher mit installiertem Caching Proxy 249
- Fehlernachricht bei dem Versuch, Onlinehilfetexte anzuzeigen 248
- für Port 14099 kann kein Eintrag in der Registrierungsdatenbank erstellt werden 259
- GUI startet nicht richtig 249
- GUI wird nicht richtig angezeigt 250

Fehlerbehebung (Forts.)

- Hilfefenster sind nicht zu sehen 250
- Hinzufügen des Überwachungssignals nicht möglich 246
- IOException für Metric Server unter Windows 2000 259
- irrelevante Fehlernachricht beim Starten von ndserver unter Solaris 2.7 249
- keine hohe Verfügbarkeit im Weitverkehrsmodus von Network Dispatcher 252
- lbserver wird nicht gestartet 258
- Mailbox Locator wird nicht ausgeführt 255
- Metric Server meldet keine Last 259
- Metric-Server-Protokoll meldet, dass für den Zugriff auf den Agenten eine Kennung erforderlich ist 260
- Network Dispatcher kann Rahmen nicht verarbeiten und weiterleiten 250
- Site Selector führt den Lastausgleich nicht korrekt durch 258
- Site Selector wendet keine RoundRobin-Methode an (Solaris) 257
- Site Selector wird nicht ausgeführt 257
- SNMPD arbeitet nicht korrekt 247
- ssserver wird unter Windows 2000 nicht gestartet 257
- Syntax- oder Konfigurationsfehler 255
- unerwartetes Verhalten beim Laden einer großen Konfigurationsdatei 253
- vom Dispatcher verwendete Port-Nummern 242
- von CBR verwendete Port-Nummern 243
- von Cisco Consultant verwendete Port-Nummern 245
- von Mailbox Locator verwendete Port-Nummern 243
- von Site Selector verwendete Port-Nummern 244
- zusätzliche Routes 247
- Fehlerbehebung, Tabellen CBR 238

Fehlerbehebung, Tabellen (Forts.)

- Cisco Consultant 240
- Dispatcher-Komponente 235
- Mailbox Locator 238
- Metric Server 241
- Site Selector 239
- Feldspezifischer Hilfetext 411
- Fernverwaltung 23, 219
- Festlegen
 - cbrcontrol 327
 - lbcontrol 390
 - mlcontrol 327
 - ndcontrol 327
 - sscontrol 357
- Firewall 25
- ftp-Advisor 268, 336
- G**
 - Garbage Collection 224
 - Gegenseitige hohe Verfügbarkeit 53, 177, 178
 - primaryhost 276, 279
 - Scripts 183
 - Übernahme 182
 - Glättungsfaktor einstellen 149, 301, 345, 347, 380, 383
 - goActive 183
 - goIdle 184
 - goInOp 184
 - goStandby 183
 - Grafische Benutzerschnittstelle (GUI) 6
 - GRE (Generic Routing Encapsulation)
 - OS/390 175
 - WAN-Unterstützung 175
 - GUI 6
 - Auflösung 250
- H**
 - Hardwarevoraussetzungen
 - CBR 81
 - Cisco Consultant 127
 - Dispatcher-Komponente 49
 - Mailbox Locator 101
 - Site Selector 113
 - highavailChange 184
 - Hilfe
 - cbrcontrol 287
 - lbcontrol 375
 - mlcontrol 287
 - ndcontrol 287
 - Hilfe, online 411
 - Hinzufügen
 - Cluster 279, 370

Hinzufügen (*Forts.*)

Port zu einem Cluster 69, 310,
386, 387

Server zu einem Port 70, 325,
356, 389

Hohe Verfügbarkeit 29, 48, 52, 177

gegenseitig 178, 276, 279, 292

gegenseitige 53

konfigurieren 178

ndcontrol 289

primaryhost 276, 279

Scripts 182

goActive 183

goIdle 184

goInOp 184

goStandby 183

highavailChange 184

Host

cbrcontrol 294

lbcontrol 376

mlcontrol 294

ndcontrol 294

http-Advisor 268, 336

I

ibmnd.conf

für Solaris konfigurieren 65

ibmproxy 84, 93

Advisor-Funktion 154

ifconfig, Befehl 69, 72, 96, 170

imap

überschreiben 104

Inaktivitätszeitlimit 223, 277, 281,
308

Installation planen 27, 49, 113

installieren

unter Linux 18

Installieren

Network Dispatcher 11

unter AIX 13

unter Solaris 21

unter Windows 2000 24, 25

Intervall, Einstellung

Advisor fragt Server ab 272,
339, 364, 367

Manager aktualisiert Wertigkeiten
für den Executor 147, 299, 344,
346, 378, 381

Manager fragt Executor ab 148,
300, 379, 381

J

Java Runtime Environment

(JRE) 13, 18, 21

K

Kein Zugriff 411

Konfiguration

Abgleich von Consultant und

CSS 129

Assistent 5

Beispieldateien 393

Cisco Consultant 133

Cluster definieren 137

Cluster-Proportionen festle-
gen 138

Content Based Routing 87

Dispatcher-Komponente 61

erweiterte Tasks 141

Mailbox Locator 105

Manager starten 138

Methoden

Assistent (CBR) 92

Assistent (Dispatcher) 64

Assistent (Mailbox Loca-
tor) 108

Assistent (Site Selector) 122

Befehlszeile (CBR) 88

Befehlszeile (Cisco Consul-
tant) 134

Befehlszeile (Dispatcher) 62

Befehlszeile (Mailbox Loca-
tor) 106

Befehlszeile (Site Selec-
tor) 120

GUI (CBR) 90

GUI (Cisco Consultant) 135

GUI (Dispatcher) 63

GUI (Mailbox Locator) 107

GUI (Site Selector) 121

Scripts (CBR) 90

Scripts (Cisco Consul-
tant) 135

Scripts (Dispatcher) 62

Scripts (Mailbox Loca-
tor) 107

Scripts (Site Selector) 120

Metric Server 138

Port 137

prüfen 75

Server mit Lastausgleich definie-
ren 137

Site Selector 119

testen 139

Kundenspezifische (anpassbare)

Advisor-Funktion 155

L

Lastausgleichseinstellungen (optimie-
ren) 144

lbcontrol, Befehl

advisor 364

Cluster 369

executor 371

file 373

help 375

host 376

log 377

manager 378

metric 384

port 386

server 388

set 390

status 391

lbcsver

wird nicht gestartet 245, 258

Limit für Anzahl beendeter Verbin-
dungen

ändern 224

Linux

installieren 18

Patch-Code für Kernel

Versionen 2.2.12, 2.2.13 80

Versionen 2.4.x 78

Voraussetzungen 17

Löschen

Cluster 279, 360, 369, 370

Port von einem Cluster 310, 386,
387

Server von einem Port 326, 355,
356, 389

zusätzliche Route 75

Löschen zusätzlicher Routes 75

M

mac, Weiterleitungsmethode 54

Mailbox Locator

Befehl mlserver wird

gestoppt 255

ein Port kann nicht hinzugefügt
werden 256

Einstellungen für Lastaus-
gleich 144

Hardware- und Softwarevoraus-
setzungen 101

Inaktivitätszeitlimit 277, 281,
308

Konfiguration

Maschine konfigurieren 109

Tasks im Überblick 105

mlcontrol scheitert 256

mlserver 102

ndadmin scheitert 256

planen 101

- Mailbox Locator (*Forts.*)
 - Proxy-Fehler beim Hinzufügen eines Ports 256
 - staletimeout 277, 281, 308
 - starten und stoppen 232
 - Tabellen zur Fehlerbehebung 238
 - Übersicht 102
 - verwenden 232
 - Weiterleitungsprotokoll 309, 310
 - wird nicht ausgeführt 255
- Manager
 - cbrcontrol 296
 - festе Wertigkeit 147
 - lbcontrol 378
 - mlcontrol 296
 - ndcontrol 296
 - Proportionen 145, 369
 - sscontrol 344
 - starten 70, 71, 138, 301, 346, 347, 380, 383
 - stoppen 301, 346, 348, 381, 383
 - Version 302, 346, 348, 381, 383
- Marken 415
- maximale Wertigkeit einstellen
 - für Server an einem bestimmten Port 146, 310, 386, 387
- Mehrere Adressen verknüpfen 70
- Messwert
 - cbrcontrol 303
 - lbcontrol 384
 - mlcontrol 303
 - ndcontrol 303
 - sscontrol 349
- Metric Server
 - IOException für Metric Server unter Windows 2000 259
 - Metric Server meldet keine Last 259
 - Metric-Server-Protokoll meldet, dass für den Zugriff auf den Agenten eine Kennung erforderlich ist 260
 - starten 138
 - starten und stoppen 234
 - Tabellen zur Fehlerbehebung 241
 - Übersicht 161
 - verwenden 234
- Migration 11
- mlcontrol, Befehl (*Forts.*)
 - help 287
 - host 294
 - log 295
 - manager 296
 - metric 303
 - port 305
 - server 320
 - set 327
 - status 328
- N**
- Namensserver
 - sscontrol 350
- NAT, Weiterleitungsmethode 55
- ndconfig 171
 - Befehl 69
- ndcontrol, Befehl
 - advisor 70, 71, 268
 - Befehlsparameter abkürzen 266
 - cluster 274
 - Eingabeaufforderung 266
 - executor 67, 280
 - file 285
 - help 287
 - highavailability 289
 - host 294
 - log 295
 - manager 70, 71, 296
 - metric 303
 - port 69, 305
 - rule 312
 - server 70, 320
 - set 327
 - status 328
 - subagent 329
- ndkeys 162, 220
- ndserver
 - starten 4
- netstat, Befehl 74
- Network Dispatcher
 - Beispiel für einen schnellen Start 1
 - Betrieb und Verwaltung 219, 233
 - erweiterte Konfigurations-Tasks 141
 - Fehlerbehebung 235
 - Funktionen 27, 36
 - Hardwarevoraussetzungen 49, 81, 101, 113, 127
 - installieren 11
 - Konfiguration des sDispatcher-Komponente 64, 93, 109, 123
- Network Dispatcher (*Forts.*)
 - Konfiguration des (*Forts.*)
 - Site Selector 119
 - konfigurieren
 - CBR 87
 - Cisco Consultant 133
 - Mailbox Locator 105
 - Softwarevoraussetzungen 49, 81, 101, 113, 127
 - Überlegungen bei der Planung 49, 113
 - Übersicht 27, 36
 - Vorteile 29
- Netzadressenkonvertierung (NAT) 54, 55
- Netzproximität 117
- Neue Merkmale von Version 2.0
 - Anforderung/Antwort der HTTP-Advisor-Funktion 34
 - Cisco Consultant 31
 - Cluster-spezifische Proportionen 34
 - DB2-Advisor-Funktion 35
 - DoS-Erkennung (Denial of Service) 35
 - erweiterte Benutzer-Exits 35
 - inhaltsabhängige Weiterleitung durch die Dispatcher-Komponente 33
 - Mailbox Locator 32
 - Metric Server 31
 - NAT und NAPT 32
 - passive Cookie-Affinität 33
 - Serverpartitionierung 34
 - site- oder Cluster-spezifische Advisor-Funktionen 34
 - Site Selector 31
 - Unterstützung der Landessprache für Linux und Solaris 31
 - Unterstützung für AIX Version 5.1 30
 - Unterstützung für neuen Chinesisch-Standard 31
 - Unterstützung für Red Hat Linux Version 7.1 30
 - Unterstützung für SuSE Linux Version 7.1 30
 - URI-Affinität 33
 - verbesserte Benutzerfreundlichkeit von CBR 32
- Neue Verbindungen 215
- Neue Verbindungen, Bedeutung von Proportionen festlegen 145, 275, 369

Neustart aller Server mit Standardwertigkeit 301, 345, 347, 380, 383

NFA
definieren 67
festlegen 284, 371, 372

NIC
Aliasname 67
Ethernet (für Solaris) 65
zuordnen (für Windows 2000) 68

O

Onlinehilfefunktion 411
OS/390
GRE-Unterstützung 175

P

Passive Cookie-Affinität 207, 209, 316

Planen
CBR 81
Cisco Consultant 127
Dispatcher-Komponente 49
Mailbox Locator 101
Site Selector 113

Platzhalter-Cluster 67, 279
für den Lastausgleich von Firewalls 200
mit Caching Proxy für transparente Weiterleitung 201
zum Zusammenfassen von Serverkonfigurationen 199

Platzhalter-Port 69, 310
Advisor-Funktion "ping" 154
für Übertragung von Datenverkehr mit nicht konfiguriertem Port 201

pop3
überschreiben 104

Port
cbrcontrol 305
Konfiguration 137
lbcontrol 386
mlcontrol 305
ndcontrol 305

Port-übergreifende Affinität 204, 306

Port-Umsetzung für Netzadressen (NAPT) 55

Ports
Anzeige
Status von Servern an diesem Port 311, 386, 387
entfernen 310, 386, 387
für Advisor 268, 336

Ports (Forts.)

für Cluster definieren 69, 310, 386, 387
hinzufügen 310, 386, 387
maximale Wertigkeit festlegen 146, 310, 386, 387
Platzhalter 69

Primärer Host 178
primaryhost 279
Privater Schlüssel
für ferne Authentifizierung 219

Privates Netz, Benutzung mit Dispatcher 198

Produktkomponenten 50

Proportionale Bedeutung für Lastausgleich festlegen 145, 279

Proportionen 138

Protokoll
binär für für Serverstatistik 213
binär für Serverstatistik 295, 377
CBR-Protokolle verwenden 232
cbrcontrol 295

Dateinamen festlegen
für Advisor-Funktion 338, 366

für Manager 346, 380

Größe einstellen
für Advisor 221, 272, 337, 340, 365, 367

für den Manager 221

für den Server 221

für den Subagenten 221

für Manager 299, 344, 346, 379, 381

lbcontrol 377

mlcontrol 295

ndcontrol 295

Stufe einstellen

für Advisor 221, 272, 339, 365, 367

für den Manager 221

für den Server 221

für den Subagenten 221

für Manager 344, 378

von Cisco Consultant verwenden 234

von Mailbox Locator verwenden 232

von Metric Server verwenden 234

von Network Dispatcher verwenden 221

von Site Selector verwenden 233

Proximitätsoptionen 117

R

Regel

sscontrol 351

Regelaffinität außer Kraft setzen
Server 321, 325

Regelbasierter Lastausgleich 185

aktive Verbindungen pro

Port 189, 313

Auswertungsoption 196

Client-IP-Adresse 188, 313, 318, 351, 354

Client-Port 190, 313

Diensttyp (TOS) 190, 313, 319

Durchschnitt der Messwerte 193
gemeinsame genutzte Bandbreite 190, 192, 313, 319

immer gültig 194, 314, 318, 352, 354

Inhalt der Anforderung 57, 195, 314

Messwert für alle 193

metricall 351

metricavg 351

Option für Serverauswertung 196

Regelauswahl für die einzelnen Komponenten 186

reservierte Bandbreite 190, 192, 313, 319

Uhrzeit 188, 313, 318, 351, 354

Verbindungen pro Sekunde 188, 313

Ressourcen 411

RMI (Remote Method Invocation) 219

route, Befehl 74, 75

Routes, zusätzliche 74

rule

cbrcontrol 312

ndcontrol 312

S

Schlüssel

ndkeys 161, 220

Scripts 182

Benutzer-Exit 149

goActive 183

goldle 184

goInOp 184

goStandby 183

highavailChange 184

SDA (Server Directed Affinity) 165, 202

Secure Sockets Layer 70

- Sensitivität für Aktualisierung der Wertigkeit einstellen 148, 301, 345, 347, 380, 383
- Server
 - Adresse 321, 389
 - advisorrequest 324
 - advisorresponse 324
 - alle mit Standardwertigkeit neu starten 301, 345, 347, 380, 383
 - als aktiv markieren 326, 356
 - als inaktiv markieren 325, 355, 356
 - cbrcontrol 320
 - collocated 321, 326
 - cookievalue 323
 - entfernen 326, 355, 356, 389
 - fixedweight 322
 - für einen Port definieren 70, 325, 356, 389
 - hinzufügen 325, 356, 389
 - lbcontrol 388
 - logisch 163
 - mapport 85, 322
 - mlcontrol 320
 - ndcontrol 320
 - nonsticky (Außerkraftsetzen der Regelaaffinität) 321, 325
 - Partitionierung 163
 - physisch 163
 - returnaddress 323
 - router 322
 - sscontrol 355
 - stillegen 299, 381
 - stillegen 206, 297, 301
 - weight 322
 - Wertigkeit festlegen 326, 356, 389
 - wieder in Betrieb nehmen 302, 381
- Server als 'Aktiv' kennzeichnen 326, 356
- Server als 'Ausgefallen' kennzeichnen 325, 355, 356
- Server Directed Affinity (SDA) 165, 202
- Server markieren als
 - aktiv 326, 356
 - inaktiv 325, 355, 356
- Sicherung der hohen Verfügbarkeit 289
- Simple Network Management Protocol (SNMP) 225
- Site Selector
 - Befehle 335
- Site Selector (*Forts.*)
 - Einstellungen für Lastausgleich 144
 - Hardware- und Softwarevoraussetzungen 113
 - kein korrekter Lastausgleich bei duplizierten Routes 258
 - Konfiguration
 - Maschine konfigurieren 123
 - Tasks im Überblick 119
 - Konfigurationsbeispiel 44
 - Lastausgleich für HA-Dispatcher 185
 - ndadmin scheitert 257
 - planen 113
 - sscontrol scheitert 257
 - ssserver wird unter Windows 2000 nicht gestartet 257
 - starten und stoppen 233
 - Tabellen zur Fehlerbehebung 239
 - Übersicht 43
 - verteilt Datenverkehr von Solaris-Clients nicht nach der Round-Robin-Methode 257
 - verwenden 233
 - wird nicht ausgeführt 257
- Sitename
 - sscontrol 358
- SNMP 221, 225
- Softwarevoraussetzungen
 - CBR 81
 - Cisco Consultant 127
 - Dispatcher-Komponente 49
 - Mailbox Locator 101
 - Site Selector 113
- Solaris
 - Befehl "apr publish" 69
 - Dispatcher-Maschine konfigurieren 65
 - installieren 21
 - Voraussetzungen 21
- sscontrol, Befehl
 - advisor 336
 - file 341
 - help 343
 - manager 344
 - metric 349
 - nameserver 350
 - rule 351
 - server 355
 - set 357
 - sitename 358
 - status 362
- SSL 70
- SSL-Verbindungen
 - Advisor-Funktion 153
 - Fehler beim Aktivieren 247
 - für CBR 84, 85
 - ibmproxy konfigurieren 84
 - ssl2http, Advisor-Funktion 85, 154
 - Standardzeit für Beendigung inaktiver Verbindungen
 - ändern 224
- Starten
 - Advisor-Funktion 70, 71, 271, 338, 340
 - Cisco Consultant 233
 - Dispatcher 4
 - Executor 67, 284, 372
 - Manager 70, 71, 301, 346, 347, 380, 383
 - Metric Server 234
 - Server 66, 67
 - Site Selector 233
- starten und stoppen
 - CBR 231
 - Mailbox Locator 232
- Starten und stoppen
 - Dispatcher 223
- Statistische Momentaufnahme anzeigen 300, 345, 346, 379, 381
- Status
 - cbrcontrol 328
 - lbcontrol 391
 - mlcontrol 328
 - ndcontrol 328
- Statusanzeige
 - alle Cluster 370
 - einen Cluster 370
 - Server für einen bestimmten Port 311, 386, 387
- Stilllegen eines Servers 206, 297, 299, 301, 381
- Stoppen
 - Advisor-Funktion 271, 339, 340
 - Cisco Consultant 233
 - Executor 284
 - Manager 301, 346, 348, 381, 383
- Subagenten 221, 225
- ndcontrol 329
- Syntaxdiagramme
 - Beispiele 262
 - Interpunktion 261
 - lesen 261
 - Parameter 261
 - Symbole 261
- Systemmesswerte
 - konfigurieren 303, 349, 384

Systemmesswerte (*Forts.*)

proportionale Bedeutung festlegen 145, 274, 275, 369

T

Tastatur 411

Testen

Konfiguration 139

U

Überprüfen

zusätzliche Route 74

Überschreibung der Regelaaffinität

Server 205

Übersicht

Konfiguration der Dispatcher-Komponente 61

Konfiguration von CBR 87

Konfiguration von Cisco Consultant 133

Konfiguration von Mailbox Locator 105

Konfiguration von Site Selector 119

Überwachen, Menüoption 225

URI-Affinität 207, 210, 316

V

Verbindungen, Bedeutung von Proportionen festlegen 145, 279

Verknüpfen von Network Dispatcher und Server 64, 70, 166, 170, 321, 326

Version anzeigen

Advisor-Funktion 273, 339, 340

Manager 302, 346, 348, 381, 383

Verwaltung von Network Dispatcher 219

Verwendung von Network Dispatcher 219

Voraussetzungen

AIX 12

Linux 17

Solaris 21

Windows 2000 23

Vorgehensweise 411

W

WAN-Unterstützung 168

mit fernem Dispatcher 168

mit fernem Advisor-Funktionen 170

mit GRE 175

WAS-Advisor-Funktion 156

Weiterleitungsmethode

cbr 57

Weiterleitungsmethode (*Forts.*)

mac 54, 56

mac, nat oder cbr 58, 308

NAT 55

Weitverkehrsunterstützung

Konfigurationsbeispiel 172

Wertigkeit

festlegen

für einen Server 326, 356, 389

Grenzwert für alle Server an einem Port 146, 310, 386, 387

Festlegung durch den Manager 147, 217

xml-Beispiel 217

Windows 2000

Befehl "cluster configure" 68

Dispatcher-Maschine konfigurieren 66

installieren 24

ndconfig, Befehl 69

Voraussetzungen 23

Workload Manager (WLM), Advisor-Funktion 159

Z

Zugriffsmöglichkeit 411

Zuordnungsdatei adressieren

Beispiel 198

Zusätzliche Routes 74, 75

Antwort

WebSphere Edge Server (Multiplattform)
Network Dispatcher
Administratorhandbuch
Version 2.0

IBM Form GC12-2505-04

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen. Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre IBM Geschäftsstelle, Ihren IBM Geschäftspartner oder Ihren Händler.

Unsere Telefonauskunft "HALLO IBM" (Telefonnr.: 01803/31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.

Kommentare:

Danke für Ihre Bemühungen.

Sie können ihre Kommentare betr. dieser Veröffentlichung wie folgt senden:

- Als Brief an die Postanschrift auf der Rückseite dieses Formulars
- Als E-Mail an die folgende Adresse: ibmterm@de.ibm.com

Name

Adresse

Firma oder Organisation

Rufnummer

E-Mail-Adresse

Antwort
GC12-2505-04



IBM Deutschland GmbH
SW TSC Germany

70548 Stuttgart



GC12-2505-04

