

WebSphere Application Server



Load Balancer Guida alla gestione

Versione 6.1

WebSphere Application Server



Load Balancer Guida alla gestione

Versione 6.1

Nota

Prima di usare questo prodotto e le relative informazioni, leggere le informazioni contenute nella sezione Appendice E, "Avvertenze", a pagina 481.

Prima edizione (Maggio 2006)

Questa edizione si applica a:

WebSphere Application Server, Versione 6.1

e a tutte le modifiche e release successive, se non diversamente indicato nelle nuove edizioni.

Ordinare le pubblicazioni mediante il rappresentante IBM o gli uffici IBM del proprio paese.

© Copyright International Business Machines Corporation 2005. Tutti i diritti riservati.

Indice

Tabelle	xiii
--------------------------	-------------

Figure	xv
-------------------------	-----------

Informazioni su questa guida	xvii
-----------------------------------------------	-------------

Destinatari di questa guida.	xvii
Informazioni di riferimento	xvii
Accessibilità.	xvii
Come inviare i propri commenti	xvii

Documenti correlati e siti Web	xix
-------------------------------------------------	------------

Parte 1. Introduzione a Load Balancer	1
--------------------------------------------------------	----------

Capitolo 1. Panoramica di Load Balancer	3
----------------------------------------------------------	----------

Descrizione di Load Balancer	3
Componenti di Load Balancer disponibili per l'uso	3
Vantaggi di Load Balancer	4
Disponibilità elevata di Load Balancer	6
Dispatcher	6
CBR	6
Controller Cisco CSS o Controller Nortel Alteon	6
Nuove opzioni.	6

Capitolo 2. Panoramica dei componenti di Load Balancer	9
-------------------------------------------------------------------------	----------

Componenti di Load Balancer	9
Panoramica del componente Dispatcher	9
Gestione dei server locali con Dispatcher	10
Gestione dei server con Dispatcher e Metric Server	11
Gestione di server locali e remoti con Dispatcher	11
Panoramica del componente CBR (Content Based Routing)	12
Gestione di server locali con CBR	12
Panoramica del componente Site Selector	13
Gestione dei server locali e remoti con Site Selector e Metric Server	14
Panoramica del componente Controller Cisco CSS	15
Panoramica del componente Controller Nortel Alteon	16

Capitolo 3. Gestione della rete: determinazione delle funzioni di Load Balancer da utilizzare	19
----------------------------------------------------------------------------------------------------------------	-----------

Funzioni del gestore, degli advisor e di Metric Server (per i componenti Dispatcher, CBR e Site Selector)	19
Funzioni del componente Dispatcher	19
Amministrazione remota	19
Posizionamento	19
Disponibilità elevata	19

Affinità client-server	20
Bilanciamento del carico basato sulle regole	20
Instradamento basato sul contenuto con il metodo di inoltro cbr di Dispatcher	21
Bilanciamento del carico per una rete geografica	22
Mappatura delle porte.	22
Configurazione di Dispatcher su una rete privata	22
Cluster e porta jolly	22
Rilevamento di attacchi "Denial of service"	22
Registrazione binaria	22
Avvisi	23

Funzioni del componente CBR (Content Based Routing)	23
Confronto tra il componente CBR e il metodo di inoltro cbr del componente Dispatcher	23
Amministrazione remota	24
Posizionamento	24
CBR con più istanze di Caching Proxy	24
Instradamento basato sul contenuto per le connessioni SSL	24
Suddivisione in partizioni dei server	24
Bilanciamento del carico basato sulle regole	24
Affinità client-server	25
Disponibilità elevata con Dispatcher e CBR.	25
Registrazione binaria	25
Avvisi	25

Funzioni del componente Site Selector	25
Amministrazione remota	25
Posizionamento	26
Disponibilità elevata	26
Affinità client-server	26
Bilanciamento del carico basato sulle regole	26
Bilanciamento del carico per una rete geografica	26
Avvisi	27

Funzioni del componente Controller Cisco CSS	27
Amministrazione remota	27
Posizionamento	27
Disponibilità elevata	27
Registrazione binaria	27
Avvisi	28

Funzioni del componente Controller Nortel Alteon	28
Amministrazione remota	28
Posizionamento	28
Disponibilità elevata	28
Registrazione binaria	28
Avvisi	28

Capitolo 4. Installazione di Load Balancer	29
-------------------------------------------------------------	-----------

Requisiti di sistema e installazione in AIX	29
Requisiti per i sistemi AIX	29
Installazione di sistemi AIX	30
Prima dell'installazione	30
Fasi di installazione	31
Requisiti di sistema e installazione in HP-UX	33

>Requisiti per i sistemi HP-UX	33
Installazione di sistemi HP-UX	33
Prima dell'installazione	33
Fasi di installazione	33
Requisiti di sistema e installazione in Linux	34
Requisiti per i sistemi Linux	34
Installazione per i sistemi Linux	35
Prima dell'installazione	35
Fasi di installazione	35
Requisiti di sistema e installazione in Solaris	36
Requisiti in Solaris	36
Installazione in Solaris	36
Prima dell'installazione	36
Fasi di installazione	37
Requisiti di sistema e installazione in Windows	38
Requisiti per i sistemi Windows	38
Installazione di sistemi Windows	38
Prima dell'installazione	38
Fasi di installazione	39

Parte 2. Componente Dispatcher . . . 41

Capitolo 5. Configurazione rapida . . . 43

Elementi richiesti	43
Preparazione	44
Configurazione del componente Dispatcher.	45
Configurazione mediante la riga comandi	45
Verifica della configurazione.	45
Configurazione mediante l'interfaccia utente grafica (GUI)	46
Configurazione guidata	46
Tipi di configurazione cluster, port e server.	46

Capitolo 6. Pianificazione del Dispatcher 49

Considerazioni sulla pianificazione	49
Metodi di inoltro	50
Instradamento a livello MAC del Dispatcher (metodo di inoltro mac)	51
NAT/NAPT del Dispatcher (metodo di inoltro nat)	51
Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)	53
Operazioni di esempio per configurare i metodi di inoltro nat o cbr del Dispatcher.	54
Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)	55
Suddivisione in partizioni del server mediante advisor HTTP o HTTPS	56
Esempio di configurazione di un server fisico in server logici	56
Disponibilità elevata	57
Disponibilità elevata di tipo semplice.	57
Disponibilità elevata reciproca	58

Capitolo 7. Configurazione del Dispatcher 61

Panoramica delle attività di configurazione.	61
Metodi di configurazione.	61

Riga comandi.	62
Script	62
GUI	63
Configurazione mediante la procedura guidata	64
Configurazione della macchina Dispatcher	64
Fase 1. Avvio della funzione server	66
Fase 2. Avvio della funzione executor.	66
Fase 3. Definizione dell'indirizzo non inoltrabile (se diverso dal nome host)	66
Fase 4. Definizione di un cluster e impostazione delle relative opzioni	67
Fase 5. Creazione dell'alias della scheda di interfaccia di rete (NIC)	67
Fase 6. Definizione delle porte e impostazioni delle relative opzioni	68
Fase 7. Definizione delle macchine server con bilanciamento del carico	68
Fase 8. Avvio della funzione gestore (facoltativo)	69
Fase 9. Avvio della funzione advisor (facoltativo)	69
Fase 10. Impostazione delle proporzioni dei cluster secondo necessità	69
Configurazione delle macchine server per il bilanciamento del carico	70
Fase 1. Creazione dell'alias dell'unità loopback	70
Fase 2. Ricerca di un instradamento supplementare	74
Fase 3. Rimozione di un instradamento supplementare	74
Fase 4. Verifica della corretta configurazione del server	75
Alternative per l'aggiunta dell'alias loopback Linux quando si utilizza il metodo di inoltro mac di Load Balancer	76

Capitolo 8. Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6 . . . 79

Piattaforme supportate per Load Balancer per IPv4 e IPv6	80
Piattaforme supportate per il bilanciamento del carico nello spazio utente.	80
Considerazioni speciali sulla piattaforma Linux	80
Limitazioni dei server di backend	80
Installazione di Load Balancer per IPv4 e IPv6.	81
Considerazioni speciali e limitazioni per Load Balancer per IPv4 e IPv6	81
Configurazione degli indirizzi locali del collegamento IPv6	81
Coppie omogenee di cluster/server	82
Funzioni di Dispatcher non supportate	82
Configurazione degli advisor	82
Configurazione della funzione di disponibilità elevata	83
Pozionamento dei server	83
Funzione di affinità per i sistemi che vengono eseguiti nello spazio utente (Linux)	84
Configurazione di Metric Server	84
Abilitazione dell'elaborazione dei pacchetti IPv6 in Load Balancer per IPv4 e IPv6	85
Creazione dell'alias del dispositivo interfaccia in Load Balancer per IPv4 e IPv6	86

Operazioni di configurazione del cluster per Linux suzSeries	89
Comandi Dispatcher (dscontrol) in Load Balancer per IPv4 e IPv6	89
Differenze di sintassi dei comandi	89
Comandi dscontrol supportati	90
Comandi dscontrol non supportati	93

Parte 3. Componente Content Based Routing (CBR) 95

Capitolo 9. Configurazione di avvio rapido 97

Elementi richiesti	97
Fasi di preparazione	97
Configurazione del componente CBR.	98
Configurazione mediante la riga comandi	98
Verifica della configurazione.	99
Configurazione mediante l'interfaccia utente grafica (GUI)	100
Configurazione mediante la procedura guidata	100
Tipi di configurazioni di cluster, porte, server	100

Capitolo 10. Pianificazione di Content Based Routing 103

Considerazioni sulla pianificazione	103
Bilanciamento del carico di richieste per tipi diversi di contenuto	104
Suddivisione del contenuto del sito per ottimizzare i tempi di risposta.	104
Backup del contenuto del server Web	105
Uso di più processi Caching Proxy per migliorare l'utilizzo della CPU	105
Uso del bilanciamento del carico basato sulle regole con CBR.	105
Bilanciamento del carico tra connessioni protette (SSL)	105
Bilanciamento del carico client-proxy in SSL e proxy-server in HTTP	106

Capitolo 11. Configurazione di Content Based Routing 107

Panoramica delle attività di configurazione	107
Metodi di configurazione	107
Riga comandi	108
Script	109
GUI	109
Configurazione guidata	110
Configurazione della macchina CBR.	111
Fase 1. Configurazione di Caching Proxy per l'uso di CBR.	111
Fase 2. Avvio della funzione server	113
Fase 3. Avvio della funzione executor	113
Fase 4. Definizione di un cluster e impostazione delle relative opzioni	113
Fase 5. Creazione dell'alias della scheda di interfaccia di rete (NIC) (facoltativa).	113
Fase 6. Definizione delle porte e impostazioni delle relative opzioni	114

Fase 7. Definizione delle macchine server con bilanciamento del carico	115
Fase 8. Aggiunta di regole alla configurazione	115
Fase 9. Aggiunta di server alle regole	115
Fase 10. Avvio della funzione gestore (facoltativo)	115
Fase 11. Avvio della funzione advisor (facoltativo)	115
Fase 12. Impostazione delle proporzioni dei cluster secondo necessità	116
Fase 13. Avvio di Caching Proxy	116
Esempio di configurazione di CBR	116

Parte 4. Componente Site Selector 117

Capitolo 12. Configurazione di avvio rapido 119

Elementi richiesti	119
Fasi di preparazione	119
Configurazione del componente Site Selector.	120
Configurazione mediante la riga comandi	120
Verifica della configurazione	121
Configurazione mediante l'interfaccia utente grafica (GUI)	121
Configurazione mediante la procedura guidata	121

Capitolo 13. Pianificazione di Site Selector. 123

Considerazioni sulla pianificazione	123
Considerazioni su TTL	125
Uso della funzione di prossimità della rete	126

Capitolo 14. Configurazione di Site Selector. 127

Panoramica delle attività di configurazione	127
Metodi di configurazione	127
Riga comandi	127
Script	128
GUI	129
Configurazione guidata	129
Configurazione della macchina Site Selector	130
Fase 1. Avvio della funzione server	130
Fase 2. Avvio del Server dei nomi	130
Fase 3. Definizione di un nome del sito e impostazione delle relative opzioni	130
Fase 4. Definizione delle macchine server con bilanciamento del carico.	131
Fase 5. Avvio della funzione gestore (facoltativo)	131
Fase 6. Avvio della funzione advisor (facoltativo)	131
Fase 7. Definizione della metrica del sistema (facoltativo)	131
Fase 8. Impostazione delle proporzioni del nome del sito secondo necessità	131
Configurazione della macchina server per il bilanciamento del carico.	131

Parte 5. Componente Controller Cisco CSS 133

Capitolo 15. Configurazione di avvio rapido 135

Elementi richiesti	135
Fasi di preparazione	135
Configurazione del componente Cisco CSS	
Controller	136
Configurazione mediante la riga comandi	136
Verifica della configurazione	137
Configurazione mediante l'interfaccia utente grafica (GUI)	137

Capitolo 16. Pianificazione di Controller Cisco CSS 139

Requisiti di sistema	139
Considerazioni sulla pianificazione	139
Posizione del consultant nella rete	140
Disponibilità elevata	142
Calcolo dei pesi	142
Individuazione dei problemi	143

Capitolo 17. Configurazione di Controller Cisco CSS 145

Panoramica delle attività di configurazione	145
Metodi di configurazione	145
Riga comandi	145
XML	146
GUI	147
Configurazione della macchina Controller per switch Cisco CSS	148
Fase 1. Avvio della funzione del server	148
Fase 2. Avvio dell'interfaccia della riga comandi	148
Fase 3. Configurazione del consultant	148
Fase 3. Configurazione di un ownercontent	149
Fase 4. Verifica della corretta definizione dei servizi	149
Fase 5. Configurazione delle metriche	149
Fase 6. Avvio del consultant	149
Fase 7. Avvio di Metric Server (facoltativo)	149
Fase 8. Configurazione della disponibilità elevata (facoltativa)	149
Verifica della configurazione	150

Parte 6. Componente Controller Nortel Alteon 151

Capitolo 18. Configurazione di avvio rapido 153

Elementi richiesti	153
Fasi di preparazione	154
Configurazione del componente Controller Nortel Alteon.	154
Configurazione mediante la riga comandi	154
Verifica della configurazione	155
Configurazione mediante l'interfaccia utente grafica (GUI)	155

Capitolo 19. Pianificazione di Controller Nortel Alteon 157

Requisiti di sistema	157
Considerazioni sulla pianificazione	157
Posizione del consultant nella rete	158
Attributi server sullo switch (impostati dal controller)	160
Configurazione dei server di backup	161
Configurazione dei gruppi	162
Disponibilità elevata	162
Ottimizzazione	164
Individuazione dei problemi	164

Capitolo 20. Configurazione di Controller Nortel Alteon 167

Panoramica delle attività di configurazione	167
Metodi di configurazione	167
Riga comandi	167
XML	168
GUI	169
Impostazione di Controller Nortel Alteon	170
Fase 1. Avvio della funzione del server	170
Fase 2. Avvio dell'interfaccia della riga comandi	170
Fase 3. Definizione di un consultant Switch Nortel Alteon Web	170
Fase 4. Aggiunta di un servizio a un consultant dello switch	170
Fase 5. Configurazione delle metriche	171
Fase 6. Avvio del consultant	171
Fase 7. Configurazione della disponibilità elevata (facoltativa)	171
Fase 8. Avvio di Metric Server (facoltativo)	171
Fase 9. Aggiornamento della configurazione di Controller Nortel Alteon.	171
Verifica della configurazione	172

Parte 7. Funzioni e caratteristiche avanzate di Load Balancer 173

Capitolo 21. Funzioni gestore, advisor e Metric Server per Dispatcher, CBR e Site Selector. 175

Ottimizzazione del bilanciamento del carico in Load Balancer	176
Proporzione di importanza attribuita alle informazioni sullo stato	176
Pesi	177
Intervalli del gestore	179
Soglia di sensibilità	179
Indice di arrotondamento	179
Uso degli script per generare un avviso o registrare un malfunzionamento dei server	180
Advisor	181
Funzionamento degli advisor	181
Avvio e arresto di un advisor	182
Intervalli dell'advisor.	183
Timeout report dell'advisor.	183
Timeout di connessione e timeout di ricezione dell'advisor per i server	183

Nuovi tentativi dell'advisor	184
Elenco di advisor	184
Configurazione dell'advisor HTTP o HTTPS utilizzando l'opzione richiesta/risposta (URL)	186
Utilizzo dell'advisor autonomo in una configurazione WAN a due livelli	187
Creazione di advisor personalizzati	188
Advisor WAS	189
Convenzione di denominazione	189
Compilazione	189
Esecuzione	190
Routine richieste	190
Ordine di ricerca	191
Denominazione e percorso	191
Advisor di esempio	191
Metric Server	191
Restrizione WLM	192
Prerequisiti	192
Modalità d'uso di Metric Server	192
Advisor Workload Manager	193
Restrizione Metric Server	194

Capitolo 22. Funzioni avanzate di Dispatcher, CBR e Site Selector 195

Utilizzo dei server posizionati	196
Per il componente Dispatcher	197
Per il componente CBR	198
Per il componente Site Selector	198
Disponibilità elevata	198
Configurazione della disponibilità elevata	199
Capacità di rilevamento di errori mediante heartbeat e la destinazione accessibile	201
Strategia di ripristino	202
Utilizzo di script	202
Configurazione di posizionamento e elevata disponibilità (sistemi Windows)	205
Configurazione del bilanciamento del carico in base alle regole	205
Modalità di valutazione delle regole	206
Utilizzo delle regole basate sull'indirizzo IP del client	207
Utilizzo delle regole basate sulla porta client	207
Utilizzo delle regole basate sull'ora del giorno	207
Utilizzo delle regole basate sul tipo di servizio (TOS, type of service)	208
Utilizzo delle regole basate sulle connessioni al secondo	208
Utilizzo delle regole basate sul numero totale di connessioni attive	208
Utilizzo delle regole basate sulla larghezza di banda riservata e condivisa	209
Regola Metric all	211
Regola media metrica	211
Utilizzo di regole il cui valore è sempre true	212
Utilizzo delle regole basate sul contenuto delle richieste	212
ignora affinità di porta	213
Aggiunta di regole alla configurazione	213
Opzione di valutazione dei server per le regole	213
Funzionamento della funzione di affinità di Load Balancer	214

Funzionamento con affinità disabilitata	215
Funzionamento con affinità abilitata	215
Affinità multiporta	215
Maschera indirizzo affinità (stickymask)	216
Gestione della disattivazione delle connessioni server	217
Opzione di affinità della regola basata sul contenuto della richiesta client	217
Affinità cookie attivo	218
Affinità cookie passivo	219
Affinità URI	220
Configurazione del supporto di Dispatcher per una rete geografica	221
Sintassi dei comandi	222
Utilizzo di advisor remoti con il supporto rete geografica di Dispatcher	223
Esempio di configurazione	225
Supporto GRE (Generic Routing Encapsulation)	227
Utilizzo di un collegamento esplicito	228
Utilizzo di una configurazione di rete privata	228
Utilizzo del cluster jolly per combinare le configurazioni di server	229
Utilizzo di cluster jolly per bilanciare il carico dei firewall	230
Utilizzo del cluster jolly con Caching Proxy per proxy trasparente	230
Utilizzo della porta jolly per indirizzare il traffico per una porta non configurata	231
Porta jolly per la gestione del traffico FTP	231
Rilevamento attacco di tipo Denial of service	231
Uso della registrazione binaria per analizzare le statistiche dei server	232
Utilizzo di un client posizionato	234

Capitolo 23. Funzioni avanzate di Controller Cisco CSS e Controller Nortel Alteon 235

Posizionamento	235
Disponibilità elevata	235
Configurazione	236
Rilevamento degli errori	237
Strategia di ripristino	237
Esempi	238
Ottimizzazione del bilanciamento del carico in Load Balancer	238
Importanza attribuita alle informazioni metriche	238
Pesi	239
Tempi di inattività nel calcolo dei pesi	239
Soglia di sensibilità	239
Advisor	240
Funzionamento degli advisor	240
Tempi di inattività dell'advisor	241
Timeout di connessione e timeout di ricezione dell'advisor per i server	241
Tentativi dell'advisor	241
Creazione di advisor personalizzati	242
Convenzione di denominazione	243
Compilazione	243
Esecuzione	244
Routine richieste	244

Ordine di ricerca	244
Denominazione e percorso	245
Advisor di esempio	245
Metric Server	245
Prerequisiti	245
Modalità d'uso di Metric Server	245
Advisor WLM (Workload Manager)	247
Uso della registrazione binaria per analizzare le statistiche dei server	247
Uso degli script per generare un avviso o registrare un malfunzionamento dei server	249

Parte 8. Gestione e risoluzione dei problemi di Load Balancer 251

Capitolo 24. Funzionamento e gestione di Load Balancer 253

Amministrazione remota di Load Balancer	253
RMI (Remote Method Invocation)	254
Amministrazione basata sul Web	255
Uso dei log di Load Balancer	257
Per Dispatcher, CBR e Site Selector	257
Per Cisco CSS Controller e Controller Nortel Alteon.	258
Uso del componente Dispatcher	259
Avvio e arresto di Dispatcher	260
Uso del valore timeout di inattività	260
Uso di fintimeout e staledtimeout per controllare la pulizia dei record di connessioni.	260
Notifica GUI — Opzione del menu Monitor	261
Uso del protocollo SNMP (Simple Network Management Protocol) con il componente Dispatcher	261
Utilizzo di ipchains o iptables per rifiutare tutto il traffico sulla macchina Load Balancer (sistemi Linux).	267
Uso del componente CBR (Content Based Routing)	268
Avvio e arresto di CBR	268
Controllo di CBR	268
Uso dei log di CBR	269
Uso del componente Site Selector.	269
Avvio e arresto di Site Selector	269
Controllo di Site Selector	269
Uso dei log di Site Selector	269
Uso del componente Controller Cisco CSS.	269
Avvio e arresto di Controller Cisco CSS	269
Controllo di Controller Cisco CSS	269
Uso dei log di Controller Cisco CSS	270
Uso del componente Controller Nortel Alteon	270
Avvio e arresto di Controller Nortel Alteon	270
Controllo di Controller Nortel Alteon	270
Uso dei log di Controller Nortel Alteon	270
Uso del componente Metric Server	270
Avvio e arresto di Metric Server	270
Uso dei log di Metric Server	271

Capitolo 25. Risoluzione dei problemi 273

Raccolta delle informazioni per la risoluzione dei problemi	273
-----------------------------------------------------------------------	-----

Informazioni generali (sempre richieste)	273
Problemi di disponibilità elevata (HA)	274
Problemi di advisor	275
Problemi di CBR (Content Based Routing).	275
Impossibile raggiungere il cluster.	276
Tutte le soluzioni non hanno esito	276
Aggiornamenti	277
Codice Java	277
Link utili	277
Tabelle di risoluzione dei problemi	277
Controllo dei numeri di porta di Dispatcher	290
Controllo dei numeri di porta di CBR	291
Controllo dei numeri di porta di Site Selector	292
Controllo dei numeri di porta di Cisco CSS Controller	293
Controllo dei numeri di porta di Controller Nortel Alteon.	293
Risoluzione di problemi comuni—Dispatcher.	294
Problema: mancata esecuzione di Dispatcher	294
Problema: Dispatcher e il server non rispondono	294
Problema: le richieste di Dispatcher non vengono sottoposte a bilanciamento	294
Problema: la funzionalità di disponibilità elevata di Dispatcher non funziona.	295
Problema: impossibile aggiungere heartbeat (piattaforma Windows)	295
Problema: instradamenti in eccesso (Windows 2000)	295
Problema: gli advisor non funzionano correttamente	296
Problema: Dispatcher, Microsoft IIS e SSL non funzionano (piattaforma Windows)	296
Problema: connessione di Dispatcher a una macchina in remoto	296
Problema: esecuzione errata dei comandi dscontrol o lbadm	296
Problema: messaggio di errore "Impossibile trovare il file..." quando si tenta di visualizzare la guida in linea (piattaforma Windows)	297
Problema: l'interfaccia utente grafica (GUI) non viene avviata correttamente	297
Problema: errore nell'esecuzione di Dispatcher con Caching Proxy installato	297
Problema: l'interfaccia utente grafica (GUI) non viene visualizzata correttamente	298
Problema: sulla piattaforma Windows, le finestre della guida a volte scompaiono dietro altre finestre aperte	298
Problema: Load Balancer non può elaborare e inoltrare un frame.	298
Problema: viene visualizzata una schermata blu quando si avvia l'executor di Load Balancer	298
Problema: il percorso di Discovery impedisce il traffico di ritorno con Load Balancer	298
Problema: la disponibilità elevata nella modalità Wide Area di Load Balancer non funziona.	299
Problema: la GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni	300

Problema: lbadm si scollega dal server dopo l'aggiornamento della configurazione	301
Problema: gli indirizzi IP non vengono risolti correttamente sulla connessione remota.	301
Problema: l'interfaccia di Load Balancer in coreano visualizza font sovrapposti o indesiderati su AIX e Linux	301
Problema: su Windows, l'indirizzo alias viene restituito al posto dell'indirizzo locale quando si immettono comandi quale hostname	301
Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP .	302
Problema: comportamento imprevisto quando si esegue "rmmod ibmlb" (Linux)	302
Problema: tempo di risposta eccessivo durante l'esecuzione di comandi sulla macchina Dispatcher	302
Problema: per il metodo di inoltro MAC, gli advisor SSL o HTTPS non registrano i carichi del server	303
Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web	303
Problema: il lotto socket è abilitato e il server Web esegue il binding a 0.0.0.0	303
Problema: su Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	304
Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java	304
Problema: su Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi	304
Problema: su Windows, si verificano problemi nella risoluzione di un indirizzo IP in un nome host quando su una scheda sono configurati più indirizzi	305
Problema: su Windows, gli advisor non funzionano in un'installazione a disponibilità elevata dopo un'interruzione della rete	306
Problema: su Linux, non utilizzare il comando "IP address add" quando si crea un alias per cluster multipli sull'unità loopback	307
Problema: messaggio di errore "Indirizzo router non specificato o non valido per il metodo della porta"	307
Problema: su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati	308
Problema: si verifica un ritardo durante il caricamento della configurazione di Load Balancer	308
Problema: su Windows, viene visualizzato un messaggio di errore che segnala un conflitto di indirizzi IP	308
Problema: in una configurazione a disponibilità elevata, sono attive entrambe le macchine, primaria e di riserva	309

Problema: le richieste client hanno esito negativo quando si tenta di restituire risposte con pagine di grandi dimensioni	309
Problema: sui sistemi Windows, si verifica un errore "Il server non risponde" quando si immette un comando dscontrol o lbadm.	309
Problema: le macchine Dispatcher a disponibilità elevata potrebbero non sincronizzarsi su Linux per S/390 sui driver qeth	310
Problema: suggerimenti sulla configurazione dell'HA (high availability)	310
Problema: su Linux, esistono delle limitazioni alla configurazione del Dispatcher quando si utilizzano server zSeries o S/390 che utilizzano schede Open System Adapter (OSA).	312
Problema: su alcune versioni Linux, si verifica una mancanza di memoria quando viene eseguito il Dispatcher con il gestore e gli advisor	314
Problema: su SUSE Linux Enterprise Server 9, Dispatcher inoltra i pacchetti, ma i pacchetti non raggiungono il server di backend.	314
Problema: su Windows, un messaggio di conflitto di indirizzi IP viene visualizzato durante un takeover HA	315
Problema: Linux iptables può interferire con l'instradamento dei pacchetti	315
Problema: impossibile aggiungere un server IPv6 alla configurazione di Load Balancer su sistemi Solaris	316
Messaggio di avvertenza Java visualizzato quando si installano le fix di servizio	316
Aggiornamento della serie di file Java fornita con l'installazione di Load Balancer	317
Risoluzione di problemi comuni—CBR	317
Problema: mancata esecuzione di CBR	317
Problema: esecuzione errata dei comandi cbrcontrol o lbadm.	317
Problema: le richieste non vengono sottoposte a bilanciamento del carico.	318
Problema: su Solaris, il comando cbrcontrol executor start non riesce.	318
Problema: errore di sintassi o di comunicazione	318
Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP .	318
Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web	318
Problema: sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	319
Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java	319
Problema: su Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi	319

Problema: su Windows, si verificano problemi nella risoluzione di un indirizzo IP su un nome host quando su una scheda sono configurati più indirizzi	319
Risoluzione di problemi comuni—Site Selector . . .	320
Problema: mancata esecuzione di Site Selector . . .	320
Problema: Site Selector non esegue il round-robin del traffico dai client Solaris . . .	320
Problema: esecuzione errata dei comandi sscontrol o lbadmin	320
Problema: sserver non si avvia su piattaforma Windows	321
Problema: Site Selector con instradamenti duplicati non esegue correttamente il bilanciamento del carico	321
Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP . . .	321
Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web	321
Problema: sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	321
Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java	322
Problema: su Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi	322
Risoluzione di problemi comuni—Controller Cisco CSS	322
Problema: mancato avvio di ccoserver	322
Problema: esecuzione errata dei comandi cocontrol o lbadmin	322
Problema: impossibile creare il registro sulla porta 13099	323
Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP . . .	323
Problema: viene ricevuto un errore di connessione durante l'aggiunta di un consultant . . .	323
Problema: i pesi non vengono aggiornati sullo switch	324
Problema: il comando di aggiornamento non ha aggiornato la configurazione del consultant . . .	324
Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web	324
Problema: sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	324
Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java	324
Risoluzione di problemi comuni—Controller Nortel Alteon	325
Problema: mancato avvio di nalserver	325
Problema: esecuzione errata dei comandi nalcontrol o lbadmin	325

Problema: impossibile creare il registro sulla porta 14099	325
Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP . . .	326
Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web	326
Problema: viene ricevuto un errore di connessione durante l'aggiunta di un consultant . . .	326
Problema: i pesi non vengono aggiornati sullo switch	326
Problema: il comando di aggiornamento non ha aggiornato la configurazione del consultant . . .	326
Problema: su Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	327
Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java	327
Risoluzione di problemi comuni—Metric Server . . .	327
Problema: Metric Server IOException su piattaforma Windows durante l'esecuzione di file di metrica utente .bat o .cmd	327
Problema: Metric Server non notifica i carichi alla macchina Load Balancer	327
Problema: nel log di Metric Server è riportato "La firma è necessaria per l'accesso all'agente" . . .	328
Problema: su AIX, durante l'esecuzione di Metric Server in condizioni di carico pesante l'output del comando ps -vg può risultare corrotto	328
Problema: impostazione di Metric Server in una configurazione a due livelli, con bilanciamento del carico mediante Site Selector tra Dispatcher a disponibilità elevata	328
Problema: gli script eseguiti su macchine Solaris multi-CPU producono messaggi console indesiderati	329
Problema: su Load Balancer per IPv6, non è possibile richiamare i valori da Metric Server su sistemi Linux	330
Problema: dopo oaver avviato Metric Server, il valore della metrica restituisce -1	331

Parte 9. Riferimenti sui comandi 333

Capitolo 26. Come leggere un diagramma della sintassi 335

Simboli e punteggiatura	335
Parametri	335
Esempi di sintassi	335

Capitolo 27. Riferimenti sui comandi per Dispatcher e CBR 337

Differenze di configurazione tra CBR e Dispatcher	338
dscontrol advisor — controlla l'advisor	339
dscontrol binlog — controlla il file di log binario	344
dscontrol cluster — configura i cluster	345
dscontrol executor — controlla l'executor	349

dscontrol file — gestisce i file di configurazione	354
dscontrol help — visualizza o stampa la guida per il comando in questione.	356
dscontrol highavailability — controlla la disponibilità elevata	357
dscontrol host — configura una macchina remota	361
dscontrol logstatus — visualizza le impostazioni log del server	362
dscontrol manager — controlla il gestore	363
dscontrol metric — configura le metriche di sistema	368
dscontrol port — configura le porte	369
dscontrol rule — configura le regole	375
dscontrol server — configura i server	381
dscontrol set — configura il log del server.	387
dscontrol status — mostra se il gestore e gli advisor sono in esecuzione	388
dscontrol subagent — configura l'agente secondario SNMP	389

Capitolo 28. Riferimenti sui comandi per Site Selector 391

sscontrol advisor — controlla l'advisor	392
sscontrol file — gestisce i file di configurazione	397
sscontrol help — visualizza o stampa la guida per il comando in questione.	399
sscontrol logstatus — visualizza le impostazioni log del server	400
sscontrol manager — controlla il gestore	401
sscontrol metric — configura le metriche di sistema	406
sscontrol nameserver — controlla il server dei nomi	407
sscontrol rule — configura le regole	408
sscontrol server — configura i server	411
sscontrol set — configura il log del server.	413
sscontrol sitename — configura un sitename	414
sscontrol status — mostra se il gestore e gli advisor sono in esecuzione	417

Capitolo 29. Riferimenti sui comandi per Cisco CSS Controller 419

ccocontrol consultant — configura e controlla un consultant	420
ccocontrol controller — gestione del controller	423
ccocontrol file — gestisce i file di configurazione	425
ccocontrol help — Visualizza o stampa la guida per questo comando	426
ccocontrol highavailability — controlla la disponibilità elevata	427
ccocontrol metriccollector — configura lo strumento di raccolta delle metriche.	430

ccocontrol ownercontent — controlla il nome proprietario e la regola di contenuto.	432
ccocontrol service — configura un servizio	435

Capitolo 30. Riferimenti sui comandi per Controller Nortel Alteon 437

nalcontrol consultant — configura e controlla un consultant	438
nalcontrol controller — gestisce il controller	441
nalcontrol file — gestisce i file di configurazione	443
nalcontrol help — visualizza o stampa la guida del comando	444
nalcontrol highavailability — controlla la disponibilità elevata	445
nalcontrol metriccollector — configura lo strumento di raccolta delle metriche.	448
nalcontrol server — configura un server	450
nalcontrol service — configura un servizio	452

Appendice A. GUI: istruzioni generali 455

Appendice B. Sintassi della regola di contenuto (modello) 463

Sintassi della regola di contenuto (modello):	463
Parole chiave riservate	463

Appendice C. File di configurazione di esempio 467

File di configurazione di Load Balancer di esempio	467
File di configurazione di Dispatcher — sistemi AIX, Linux e Solaris	467
File di configurazione di Dispatcher — sistemi Windows.	470
Advisor di esempio	473

Appendice D. Esempio di configurazione di disponibilità elevata a due livelli con Dispatcher, CBR e Caching Proxy 477

Configurazione della macchina server	477
--------------------------------------	-----

Appendice E. Avvertenze 481

Marchi	483
--------	-----

Glossario 485

Indice analitico. 495

Tabelle

1. immagini installp in AIX	30	11. Configurazione delle attività per il componente Controller Nortel Alteon . . .	167
2. Comandi di installazione AIX	32	12. Attività di configurazione avanzate di Load Balancer	175
3. Dettagli sull'installazione del pacchetto HP-UX per Load Balancer	33	13. Attività di configurazione avanzate di Load Balancer	195
4. Attività di configurazione per la funzione Dispatcher	61	14. tabella di risoluzione dei problemi di Dispatcher	278
5. Comandi per creare l'alias dell'unità loopback (lo0) per Dispatcher	71	15. Tabella di risoluzione dei problemi di CBR	284
6. Comandi per eliminare instradamenti supplementari per il Dispatcher	75	16. tabella di risoluzione dei problemi di Site Selector	285
7. Attività di configurazione per il componente CBR	107	17. tabella di risoluzione dei problemi di Controller per switch Cisco CSS	287
8. Comandi per creare l'alias della NIC	114	18. tabella di risoluzione dei problemi di Controller Nortel Alteon	288
9. Configurazione delle attività per il componente Site Selector	127	19. Tabella di risoluzione dei problemi di Metric Server	289
10. Configurazione delle attività per il componente Controller Cisco CSS	145		

Figure

1. Esempio di rappresentazione fisica di un sito dove i server locali sono gestiti da Dispatcher	10	28. Una configurazione Controller Nortel Alteon semplice	153
2. Esempio di un sito dove i server sono gestiti da Dispatcher e Metric Server	11	29. Esempio di consultant connesso dietro lo switch	159
3. Esempio di un sito dove i server locali e remoti sono gestiti da Dispatcher	11	30. Esempio di consultant connesso attraverso una rete intranet davanti allo switch	160
4. Esempio di un sito dove i server locali sono gestiti da CBR.	13	31. Esempio di consultant dietro lo switch e dell'interfaccia utente davanti allo switch	160
5. Esempio di un sito dove i server locali e remoti sono gestiti da Site Selector e Metric Server	14	32. Esempio di consultant configurato con server di backup.	162
6. Esempio di un sito dove i server locali sono gestiti da Controller Cisco CSS e Metric Server.	16	33. Esempio della disponibilità elevata di Controller Nortel Alteon e Switch Nortel Alteon Web	164
7. Esempio di un sito dove i server locali sono gestiti da Controller Nortel Alteon	17	34. Esempio di una configurazione WAN a due livelli utilizzando l'advisor autonomo	187
8. Una semplice configurazione Dispatcher locale	43	35. Esempio di una configurazione costituita da un unico segmento LAN	222
9. Esempio di Dispatcher configurato con un unico cluster e 2 porte	46	36. Esempio di configurazione che utilizza server locali e remoti	222
10. Esempio di Dispatcher configurato con due cluster, ognuno con una porta	47	37. Configurazione di esempio di rete geografica con Load Balancer remoti	225
11. Esempio di Dispatcher configurato con 2 cluster, ognuno con 2 porte	48	38. Configurazione di esempio di rete geografica con piattaforma server che supporta GRE	227
12. Esempio d'uso dei metodi di inoltro nat o cbr del Dispatcher	54	39. Esempio di una rete privata che utilizza Dispatcher	229
13. Esempio di un Dispatcher che utilizza la disponibilità elevata di tipo semplice	57	40. Comandi SNMP in Sistemi Linux e UNIX	262
14. Esempio di un Dispatcher che utilizza la disponibilità elevata reciproca	58	41. L'interfaccia utente grafica (GUI) con l'espansione del componente Dispatcher visualizzata nella struttura ad albero.	456
15. Esempio degli indirizzi IP necessari per la macchina Dispatcher	66	42. L'interfaccia utente grafica (GUI) con l'espansione del componente CBR visualizzata nella struttura ad albero.	457
16. Una configurazione semplice di CBR locale	97	43. L'interfaccia utente grafica (GUI) con l'espansione del componente Site Selector visualizzata nella struttura ad albero.	458
17. Esempio di CBR configurato con un unico cluster e 2 porte.	100	44. L'interfaccia utente grafica (GUI) con l'espansione del componente Cisco CSS Controller visualizzata nella struttura ad albero	459
18. Esempio di CBR configurato con due cluster, una porta ciascuno.	101	45. L'interfaccia utente grafica (GUI) con l'espansione del componente Nortel Alteon Controller visualizzata nella struttura ad albero	460
19. Esempio di CBR configurato con 2 cluster, 2 porte ciascuno	102	46. Esempio di configurazione di disponibilità elevata a due livelli con Dispatcher, CBR e Caching Proxy	477
20. File di configurazione di CBR su sistemi AIX, Linux e Solaris	112		
21. File di configurazione di CBR per sistemi HP-UX.	112		
22. File di configurazione di CBR su sistemi Windows	113		
23. Una configurazione Site Selector semplice	119		
24. Esempio di un ambiente DNS	124		
25. Una configurazione Cisco CSS Controller semplice	135		
26. Esempio di un consultant connesso dietro gli switch	141		
27. Esempio di consultant (con partner di disponibilità elevata facoltativo), configurato dietro lo switch con l'interfaccia utente davanti allo switch.	142		

Informazioni su questa guida

Questa guida illustra come pianificare, installare, configurare, utilizzare e risolvere i problemi di IBM WebSphere Application Server Load Balancer nei sistemi operativi AIX, HP-UX, Linux, Solaris e Windows. Precedentemente, questo prodotto era chiamato Edge Server Network Dispatcher, SecureWay Network Dispatcher, eNetwork Dispatcher, and Interactive Network Dispatcher.

Destinatari di questa guida

La presente *Guida alla gestione per Load Balancer* è destinata ad amministratori di rete e di sistema esperti, con una buona conoscenza dei propri sistemi operativi e della fornitura di servizi Internet. Non è richiesta alcuna precedente esperienza con Load Balancer.

Questa guida non è destinata a supportare release precedenti di Load Balancer.

Informazioni di riferimento

Il sito Web del centro informazioni Edge Components contiene un collegamento alla versione corrente di questa guida in formato HTML e PDF.

Per gli aggiornamenti più recenti di Load Balancer, visitare la pagina di assistenza del sito Web e collegarsi al sito Technote.

Per accedere a queste pagine Web e alle pagine correlate, utilizzare gli URL elencati in "Documenti correlati e siti Web" a pagina xix.

Accessibilità

Le funzioni di accessibilità consentono a un utente con invalidità fisica, ad esempio con mobilità o vista limitata, di utilizzare agevolmente i prodotti software. Di seguito sono riportate le principali funzioni di accessibilità in Load Balancer:

- è possibile utilizzare un software di lettura dello schermo e un sintetizzatore vocale digitale per ascoltare ciò che viene visualizzato sullo schermo. Inoltre, è possibile utilizzare un software di riconoscimento vocale, IBM ViaVoice, per immettere dati e per spostarsi all'interno dell'interfaccia utente.
- È possibile utilizzare le funzioni tramite la tastiera piuttosto che tramite il mouse.
- È possibile configurare e gestire le funzioni di Load Balancer utilizzando le interfacce della riga comandi o gli editor di testo standard forniti, anziché le interfacce utente fornite. Per ulteriori informazioni sull'accessibilità di funzioni particolari, fare riferimento alla documentazione relativa a tali funzioni.

Come inviare i propri commenti

I vostri commenti risultano di estrema importanza poiché consentono di fornire informazioni della massima accuratezza e qualità. Per fornire commenti su questa guida o su qualsiasi altra documentazione relativa ai componenti Edge:

- Inviare i commenti tramite email all'indirizzo fsdoc@us.ibm.com. Accertarsi di includere il nome del manuale, il numero di parte, la versione e, se il caso, il punto specifico del testo che si sta commentando, quale un numero di pagina o un numero di tabella.

Documenti correlati e siti Web

- *Concetti, pianificazione e installazione per Edge Components* GC13-3367-02
- *Guida alla programmazione per Edge Components* GC13-3368-02
- *Guida alla gestione per Caching Proxy* GC13-3366-02
- Home page del sito Web di IBM: www.ibm.com/
- Prodotto IBM WebSphere Application Server: www.ibm.com/software/webservers/appserv/
- Sito Web librerie di IBM WebSphere Application Server: www.ibm.com/software/webservers/appserv/was/library/
- Sito Web supporto di IBM WebSphere Application Server: www.ibm.com/software/webservers/appserv/was/support/
- Centro informazioni per IBM WebSphere Application Server: www.ibm.com/software/webservers/appserv/infocenter.html
- Centro informazioni per IBM WebSphere Application Server Edge Components: www.ibm.com/software/webservers/appserv/ecinfocenter.html

Parte 1. Introduzione a Load Balancer

Questa sezione presenta una panoramica di Load Balancer e dei suoi componenti, una descrizione dettagliata delle funzioni di configurazione disponibili, un elenco dei requisiti hardware e software e istruzioni di installazione. Contiene i seguenti capitoli:

- Capitolo 1, "Panoramica di Load Balancer", a pagina 3
- Capitolo 2, "Panoramica dei componenti di Load Balancer", a pagina 9
- Capitolo 3, "Gestione della rete: determinazione delle funzioni di Load Balancer da utilizzare", a pagina 19
- Capitolo 4, "Installazione di Load Balancer", a pagina 29

Capitolo 1. Panoramica di Load Balancer

Questo capitolo fornisce una panoramica di Load Balancer e comprende le seguenti sezioni:

- “Descrizione di Load Balancer”
- “Componenti di Load Balancer disponibili per l’uso”
- “Vantaggi di Load Balancer” a pagina 4
- “Disponibilità elevata di Load Balancer” a pagina 6
- “Nuove opzioni” a pagina 6

Per un elenco dettagliato delle opzioni di configurazione fornite da ciascun componente di Load Balancer e decidere quali di esse devono essere utilizzate per la gestione della rete, vedere Capitolo 3, “Gestione della rete: determinazione delle funzioni di Load Balancer da utilizzare”, a pagina 19.

Descrizione di Load Balancer

Load Balancer è una soluzione software che consente di distribuire le richieste entranti dei client tra diversi server. Quindi migliora le prestazioni dei server indirizzando le richieste delle sessioni TCP/IP a server diversi nell’ambito di un gruppo; in tal modo le richieste vengono bilanciate tra tutti i server. Questo bilanciamento del carico è trasparente agli utenti e alle altre applicazioni. Load Balancer è utile per applicazioni come i server di posta elettronica, i server World Wide Web, le query distribuite su database paralleli e altre applicazioni TCP/IP.

Quando viene utilizzato con i server Web, Load Balancer consente di ottimizzare le prestazioni di un sito dal momento che fornisce una soluzione potente, flessibile e scalabile per far fronte ai picchi di domanda. Se un sito Web non è in grado di gestire tutti i visitatori nei momenti di picco di domanda, utilizzare Load Balancer per individuare automaticamente il server migliore in grado di gestire le richieste entranti, migliorando la soddisfazione dei clienti e i profitti dell’azienda.

Componenti di Load Balancer disponibili per l’uso

IMPORTANTE: se si sta utilizzando Load Balancer per IPv4 e IPv6, solo il componente Dispatcher è disponibile. Per ulteriori informazioni, consultare Capitolo 8, “Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6”, a pagina 79.

Load Balancer è composto dai seguenti cinque componenti che possono essere usati separatamente o insieme per ottenere un bilanciamento del carico ottimale.

- È possibile utilizzare il componente **Dispatcher** per bilanciare il carico sui server di una rete locale (LAN, Local Area Network) o di una rete geografica (WAN, Wide Area Network) utilizzando un certo numero di pesi e misure impostati dinamicamente da Dispatcher. Questo componente fornisce un bilanciamento del carico a livello di servizi specifici, tipo HTTP, FTP, SSL, NNTP, IMAP, POP3, SMTP, SIP e Telnet. Non utilizza un DNS (Domain Name Server) per associare i nomi di dominio agli indirizzi IP.

Per il protocollo HTTP, è possibile utilizzare la funzione Instradamento basato sul contenuto di Dispatcher per bilanciare il carico in base al contenuto delle

richieste dei client. Il server verrà scelto associando l'URL a una regola specifica. L'instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr) *non* richiede Caching Proxy.

- Per entrambi i protocolli HTTP e HTTPS (SSL), è possibile utilizzare il componente **Content Based Routing** (CBR) per il bilanciamento del carico basato sul contenuto delle richieste dei client. Un client invia una richiesta a Caching Proxy, e Caching Proxy la inoltra al server appropriato. Il server verrà scelto associando l'URL a una regola specifica.

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l'uso di Caching Proxy. Per ulteriori informazioni, vedere "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

- È possibile utilizzare il componente **Site Selector** per bilanciare il carico sui server all'interno di una rete locale (LAN, Local Area Network) o di una rete geografica (WAN, Wide Area Network) utilizzando un approccio di tipo DNS round-robin o un approccio più avanzato specificato dall'utente. Site Selector interagisce con un server dei nomi per associare i nomi DNS agli indirizzi IP.
- È possibile utilizzare il componente **Controller Cisco CSS** o il componente **Controller Nortel Alteon** per generare pesi dei server che vengono quindi inviati allo Switch Cisco CSS o allo Switch Nortel Alteon Web per scegliere il server migliore, ottimizzare il carico e ottenere una buona tolleranza agli errori.

Per ulteriori informazioni sui componenti Dispatcher, CBR, Site Selector, Controller Cisco CSS, e Controller Nortel Alteon, vedere "Componenti di Load Balancer" a pagina 9.

Vantaggi di Load Balancer

Il numero di utenti e di reti che utilizzano Internet sta crescendo in misura esponenziale. Questa crescita causa problemi di scala che possono limitare l'accesso degli utenti ai siti più popolari.

Attualmente, gli amministratori dei siti utilizzano diversi metodi per ottimizzare gli accessi. Alcuni di questi metodi consentono agli utenti di scegliere un server diverso a caso, se la scelta precedente non ha consentito l'accesso o in caso di operazioni eccessivamente lente. Questo approccio è scomodo, noioso e inefficace. Un altro metodo è il round-robin standard, che prevede che sia il server dei nomi di dominio (DNS) a scegliere di volta in volta i server che devono gestire le richieste. Questo approccio è migliore, ma ancora inefficace, poiché inoltra il traffico alla cieca, senza prendere in considerazione in alcun modo il carico di lavoro dei server. Inoltre, se un server subisce un guasto, il DNS continuerà a inviargli richieste.

La necessità di sviluppare una soluzione più potente ha prodotto Load Balancer. Questo prodotto offre numerosi benefici rispetto alle soluzioni precedenti e alla concorrenza.

Scalabilità

Man mano che le richieste dei client aumentano, è possibile aggiungere dinamicamente altri server, consentendo quindi di supportare decine di milioni di richieste al giorno attraverso decine o centinaia di server.

Uso efficiente delle apparecchiature

Il bilanciamento del carico consente di ottimizzare l'uso dell'hardware di ciascun gruppo di server, riducendo al minimo le aree sensibili (hot-spot) che si vengono a creare frequentemente con il metodo round-robin standard.

Facile integrazione

Load Balancer utilizza i protocolli standard TCP/IP o UDP/IP. È possibile aggiungerlo alla rete esistente senza doverla modificare in alcun modo. È semplice da installare e configurare.

Basso sovraccarico

Utilizzando il metodo di inoltro del livello MAC, il componente Dispatcher controlla soltanto il traffico entrante dai client verso i server. Esso non gestisce il traffico uscente dai server verso i client. Ciò riduce significativamente il suo impatto sull'applicazione, confrontato con gli altri approcci, e migliora le prestazioni della rete.

Disponibilità elevata

I componenti Dispatcher, Controller Cisco CSS e Controller Nortel Alteon offrono una disponibilità elevata grazie all'uso di una macchina di backup sempre pronta a entrare in funzione per gestire il bilanciamento del carico in caso di guasto al server principale. In caso di guasto a uno dei server, le richieste continueranno a essere soddisfatte dall'altro server. Ciò elimina la possibilità che qualsiasi server diventi un "single point of failure" e rende il sito altamente disponibile.

Per ulteriori informazioni, vedere "Disponibilità elevata di Load Balancer" a pagina 6

Instradamento basato sul contenuto (utilizzando il componente CBR o Dispatcher)

Insieme al Caching Proxy, il componente CBR può funzionare da proxy per le richieste HTTP e HTTPS (SSL) indirizzati a server specifici in base al contenuto richiesto. Ad esempio, se una richiesta contiene la stringa "/cgi-bin/" nella sezione directory dell'URL, e il nome del server indica un server locale, il componente CBR può indirizzare la richiesta al server migliore di un gruppo di server dedicati specificatamente alla gestione di richieste cgi.

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l'uso di Caching Proxy. Per ulteriori informazioni, vedere "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

Il componente Dispatcher fornisce inoltre un instradamento basato sul contenuto, ma non richiede che sia installato il Caching Proxy. Poiché l'instradamento basato sul contenuto fornito dal componente Dispatcher viene eseguito nel kernel man mano che i pacchetti vengono ricevuti, questa funzione risulta *più veloce* rispetto a quella fornita dal componente CBR. Il componente Dispatcher esegue l'instradamento basato sul contenuto per HTTP (utilizzando la regola di tipo "contenuto") e per HTTPS (utilizzando l'affinità ID di sessione SSL).

Nota: Solo il componente CBR può utilizzare la regola di tipo contenuto per HTTPS (SSL) durante le operazioni di bilanciamento del carico del traffico basato sul contenuto delle richieste HTTP, che richiede la decodifica e la successiva codifica dei messaggi.

Disponibilità elevata di Load Balancer

Dispatcher

Il componente Dispatcher offre opzioni incorporate di disponibilità elevata, evitando di diventare un "single point of failure" della rete. Ciò viene realizzato grazie all'uso di una seconda macchina Dispatcher che controlla costantemente la macchina principale ed è sempre pronta a entrare in funzione in caso di guasto a quest'ultima. La disponibilità offerta dal componente Dispatcher è ancora più elevata se si considera che le due macchine possono fungere contemporaneamente da principale e da secondaria (backup). Vedere "Configurazione della disponibilità elevata" a pagina 199.

CBR

Utilizzando la configurazione a due livelli con una macchina Dispatcher che bilancia il carico del traffico tra più server equipaggiati con CBR, è possibile ottenere un livello di disponibilità elevata per questi componenti.

Controller Cisco CSS o Controller Nortel Alteon

I controller sono caratterizzati da disponibilità elevata dal momento che è stata eliminata la possibilità di diventare un "single point of failure". Un controller su una macchina può essere configurato come principale e un altro, su una macchina diversa, può essere configurato come secondario o di backup. Il controller di backup controlla costantemente il controller principale e si tiene sempre pronto a fornire agli switch i pesi dei server, in caso di guasto alla macchina principale. Per ulteriori informazioni, consultare "Disponibilità elevata" a pagina 235.

Nuove opzioni

Load Balancer per IBM WebSphere Application Server Versione 6.1 contiene un certo numero di nuove opzioni. Le nuove opzioni più importanti sono elencate qui di seguito.

- **Supporto per l'esecuzione di processi di bilanciamento del carico nello spazio utente su sistemi Linux**

Il supporto è stato aggiunto alle installazioni Load Balancer per IPv4 e IPv6 per eseguire i processi di bilanciamento del carico nello spazio utente piuttosto che nello spazio kernel. Per sistemi Linux, non esiste alcuna dipendenza dal modulo kernel.

Per le informazioni più aggiornate sulle piattaforme che supportano il bilanciamento del carico nello spazio utente (senza kernel), fare riferimento al seguente sito Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

Per ulteriori informazioni, vedere "Piattaforme supportate per Load Balancer per IPv4 e IPv6" a pagina 80.

- **Supporto per HP 11iv2 su PA-RISC (supporto rimosso per HP 11iv1)**

Per informazioni sui requisiti di sistema hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

- **Supporto per sistemi Linux su zSeries 64-bit**

Il supporto per i sistemi Linux su zSeries a 64-bit è fornito solo per le installazioni Load Balancer per IPv4 e IPv6.

Per ulteriori informazioni su Load Balancer per IPv4 e IPv6 e sulle considerazioni speciali per l'esecuzione di sistemi Linux su zSeries a 64-bit, fare riferimento a Capitolo 8, "Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6", a pagina 79.

Per informazioni sui requisiti di sistema hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web:
<http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

- **Supporto per l'advisor SIP**

Il supporto per un advisor Session Initiation Protocol (SIP) è stato aggiunto. L'advisor SIP supportato viene eseguito solo sul protocollo TCP.

Per ulteriori informazioni, fare riferimento a 184.

- **Per sistemi Linux, supporto di configurazioni client posizionate**

Questa funzione si applica a tutti i componenti di Load Balancer.

I client che si trovano sulla stessa macchina di Load Balancer sono supportati solo su sistemi Linux.

Per ulteriori informazioni, vedere "Utilizzo di un client posizionato" a pagina 234.

- **Supporto per il browser Firefox**

Per informazioni sulle versioni supportate di Firefox e su tutti i browser supportati, fare riferimento al seguente sito Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

Capitolo 2. Panoramica dei componenti di Load Balancer

Questo capitolo fornisce una panoramica dei componenti di Load Balancer e comprende le seguenti sezioni:

- “Componenti di Load Balancer”
- “Panoramica del componente Dispatcher”
- “Panoramica del componente CBR (Content Based Routing)” a pagina 12
- “Panoramica del componente Site Selector” a pagina 13
- “Panoramica del componente Controller Cisco CSS” a pagina 15
- “Panoramica del componente Controller Nortel Alteon” a pagina 16

Per un elenco dettagliato delle opzioni di configurazione fornite da ciascun componente di Load Balancer e decidere quali di esse devono essere utilizzate per la gestione della rete, vedere Capitolo 3, “Gestione della rete: determinazione delle funzioni di Load Balancer da utilizzare”, a pagina 19.

Componenti di Load Balancer

I cinque componenti di Load Balancer sono: Dispatcher, Content Based Routing (CBR), Site Selector, Controller Cisco CSS e Controller Nortel Alteon. Load Balancer è un prodotto flessibile che consente di utilizzare i componenti separatamente o insieme a seconda della configurazione del sito. Questa sezione descrive brevemente ciascuno di questi componenti.

IMPORTANTE: se si utilizza Load Balancer per IPv4 e IPv6, solo il componente Dispatcher è disponibile. Per ulteriori informazioni, vedere Capitolo 8, “Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6”, a pagina 79.

Panoramica del componente Dispatcher

Il componente Dispatcher bilancia il traffico tra i server tramite un'efficace combinazione di bilanciamento del carico e software di gestione. Inoltre, Dispatcher è in grado di rilevare un server che non funziona e di deviare il traffico a lui indirizzato. Dispatcher supporta i protocolli HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3, Telnet, SIP e ogni altra applicazione basata sul protocollo TCP o UDP senza informazioni di stato.

Tutte le richieste client inviate alla macchina Dispatcher sono indirizzate al server considerato più adatto in base ai pesi che vengono impostati dinamicamente. È possibile utilizzare i valori predefiniti per questi pesi o attribuire loro dei valori diversi durante il processo di configurazione.

Dispatcher offre tre metodi di inoltro (specificati sulla porta):

- Metodo di inoltro MAC (**mac**). Utilizzando questo metodo di inoltro, Dispatcher bilancia il carico delle richieste in entrata sul server. Il server restituisce poi la risposta direttamente al client senza coinvolgere Dispatcher.
- Metodo di inoltro NAT/NAPT (**nat**). La funzione NAT (Network Address Translation)/ NAPT (Network Address Port Translation) consente di superare il limite di dover collegare i server di backend localmente in rete. Se si desidera collegare server situati in ubicazioni remote, è possibile utilizzare la tecnica NAT anziché la tecnica GRE (Generic Routing Encapsulation)/WAN (Wide Area

Network). Utilizzando il metodo di inoltro NAT, Dispatcher bilancia il carico delle richieste in entrata sul server. Il server restituisce la risposta a Dispatcher. La macchina Dispatcher restituisce a sua volta la risposta al client.

- Metodo di inoltro cbr (instradamento basato sul contenuto) (**cbr**). Senza Caching Proxy, il componente Dispatcher consente di eseguire l'instradamento basato sul contenuto per HTTP (utilizzando la regola di tipo "contenuto") e per HTTPS (utilizzando l'affinità ID di sessione SSL). Per il traffico HTTP e HTTPS, il componente Dispatcher può offrire un instradamento basato sul contenuto *più rapido* di quello offerto dal componente CBR. Utilizzando il metodo di inoltro cbr, Dispatcher bilancia il carico delle richieste in entrata sul server. Il server restituisce la risposta a Dispatcher. La macchina Dispatcher restituisce a sua volta la risposta al client.

Il componente Dispatcher è il fattore chiave che consente di gestire in modo stabile ed efficiente una rete ampia e scalabile di server. Dispatcher consente di collegare molti server singoli in modo da farli sembrare un solo server virtuale. Quindi il sito sembrerà avere un unico indirizzo IP. Dispatcher funziona indipendentemente da un DNS (Domain Name Server); tutte le richieste vengono inviate all'indirizzo IP della macchina Dispatcher.

Dispatcher offre considerevoli vantaggi nel bilanciamento del carico di traffico sui server organizzati in cluster consentendo di gestire i siti in modo stabile ed efficace.

Gestione dei server locali con Dispatcher

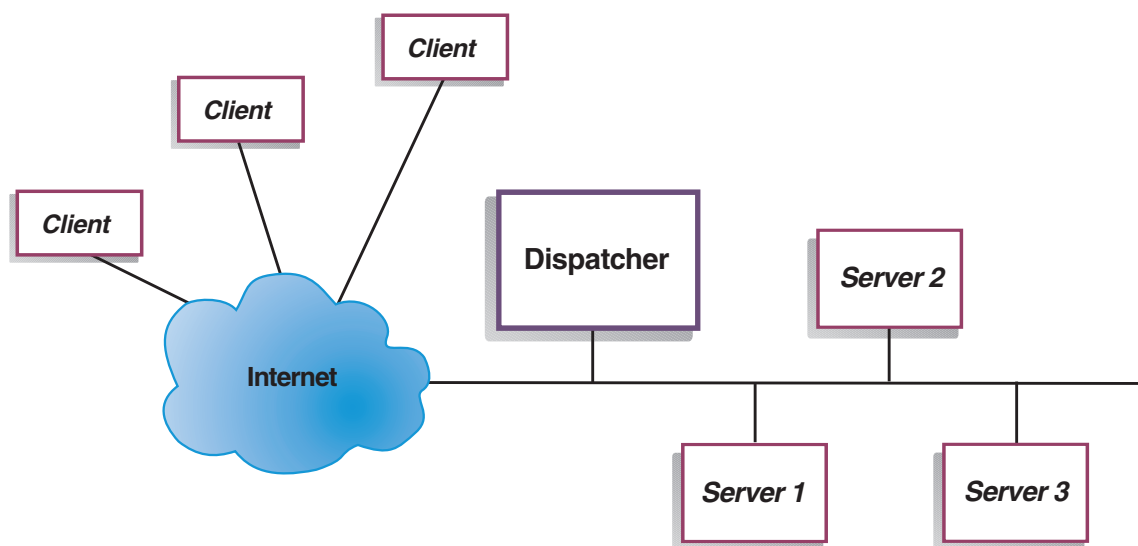


Figura 1. Esempio di rappresentazione fisica di un sito dove i server locali sono gestiti da Dispatcher

La Figura 1 mostra una rappresentazione fisica del sito che utilizza una configurazione di rete Ethernet. È possibile installare la macchina Dispatcher senza dover apportare modifiche fisiche alla rete. Dopo che Dispatcher ha indirizzato la richiesta client al server più adatto, se si utilizza il metodo di inoltro MAC, la risposta viene inviata direttamente dal server al client senza coinvolgere Dispatcher.

Gestione dei server con Dispatcher e Metric Server

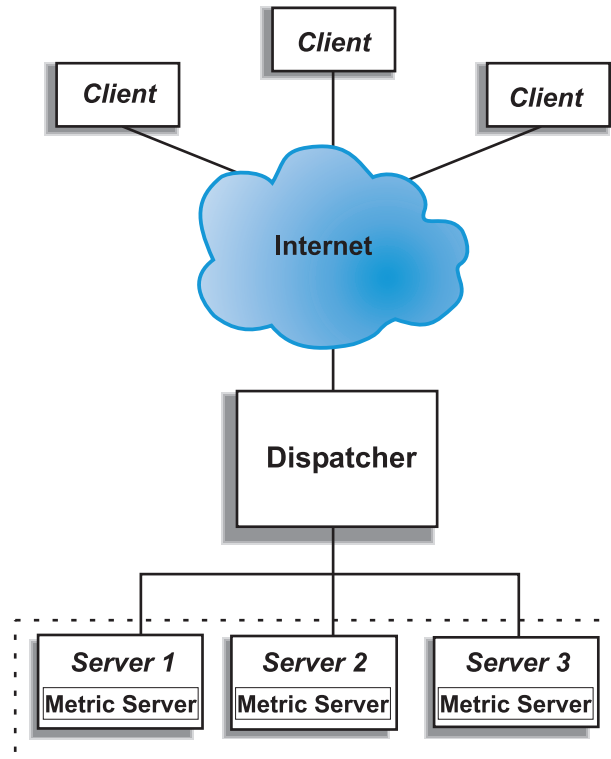


Figura 2. Esempio di un sito dove i server sono gestiti da Dispatcher e Metric Server

La Figura 2 illustra un sito in cui tutti i server risiedono in una rete locale. Il componente Dispatcher viene utilizzato per inoltrare le richieste; Metric Server viene utilizzato per fornire alla macchina Dispatcher le informazioni relative al carico del sistema.

In questo esempio, il daemon di Metric Server viene installato su ciascun server di backend. È possibile utilizzare Metric Server con il componente Dispatcher o con un altro componente di Load Balancer.

Gestione di server locali e remoti con Dispatcher

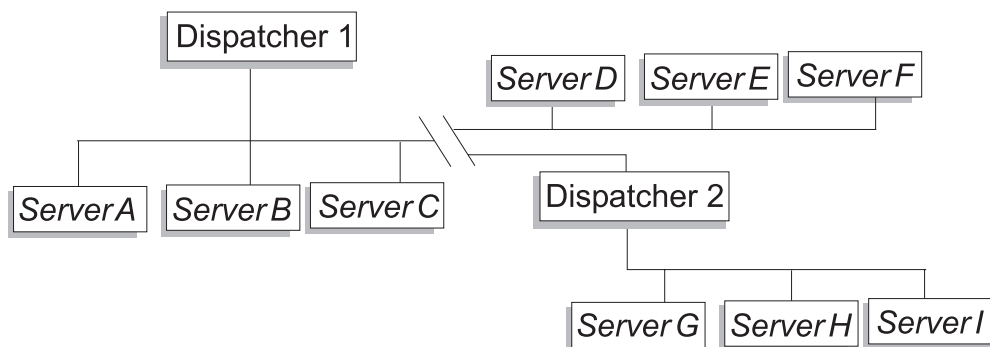


Figura 3. Esempio di un sito dove i server locali e remoti sono gestiti da Dispatcher

Il supporto per rete geografica di Dispatcher consente di utilizzare sia i server locali che i server remoti (server situati su sottoreti diverse). La Figura 3 a pagina 11 mostra una configurazione dove un Dispatcher locale (Dispatcher 1) funge da punto d'ingresso di tutte le richieste. Il Dispatcher locale distribuisce le richieste tra i server locali (ServerA, ServerB, ServerC) e sul Dispatcher remoto (Dispatcher 2), che a sua volta bilancerà il carico tra i server locali di sua competenza (ServerG, ServerH, ServerI).

Quando si usa il metodo di inoltro NAT di Dispatcher o il supporto GRE, è possibile realizzare il supporto per rete geografica anche senza utilizzare un Dispatcher sul sito remoto (dove si trovano ServerD, ServerE e ServerF). Per ulteriori informazioni, vedere "NAT/NAPT del Dispatcher (metodo di inoltro nat)" a pagina 51 e "Supporto GRE (Generic Routing Encapsulation)" a pagina 227.

Panoramica del componente CBR (Content Based Routing)

CBR funziona con Caching Proxy per inviare le richieste ai server HTTP o HTTPS (SSL) specificati tramite proxy. Consente di gestire i dettagli di memorizzazione nella cache per recuperare più rapidamente i documenti Web con una larghezza di banda della rete inferiore. CBR con Caching Proxy esamina le richieste HTTP utilizzando tipi di regole specifici.

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l'uso di Caching Proxy. Per ulteriori informazioni, vedere "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

CBR consente di specificare un gruppo di server che gestisca una richiesta in base all'espressione regolare corrispondente al contenuto della richiesta. Poiché CBR consente di specificare più server per ciascun tipo di richiesta, il carico delle richieste può essere bilanciato per ottimizzare i tempi di risposta ai client. Inoltre, CBR rileva eventuali malfunzionamenti di un server del gruppo e interrompe l'instradamento delle richieste destinate a quel server. L'algoritmo di bilanciamento del carico utilizzato dal componente CBR è lo stesso dell'algoritmo utilizzato dal componente Dispatcher.

Quando Caching Proxy riceve una richiesta, questa viene confrontata con le regole che sono state definite nel componente CBR. Se viene rilevata una corrispondenza, uno dei server associati a quella regola viene scelto per gestire la richiesta. Quindi, Caching Proxy esegue la propria abituale elaborazione per inviare la richiesta al server prescelto tramite proxy.

CBR dispone delle stesse funzioni di Dispatcher, eccetto la funzione di disponibilità elevata, l'agente secondario SNMP, il supporto per rete geografica e alcuni altri comandi di configurazione.

Caching Proxy deve essere in esecuzione prima che il componente CBR possa iniziare a bilanciare il carico delle richieste client.

Gestione di server locali con CBR

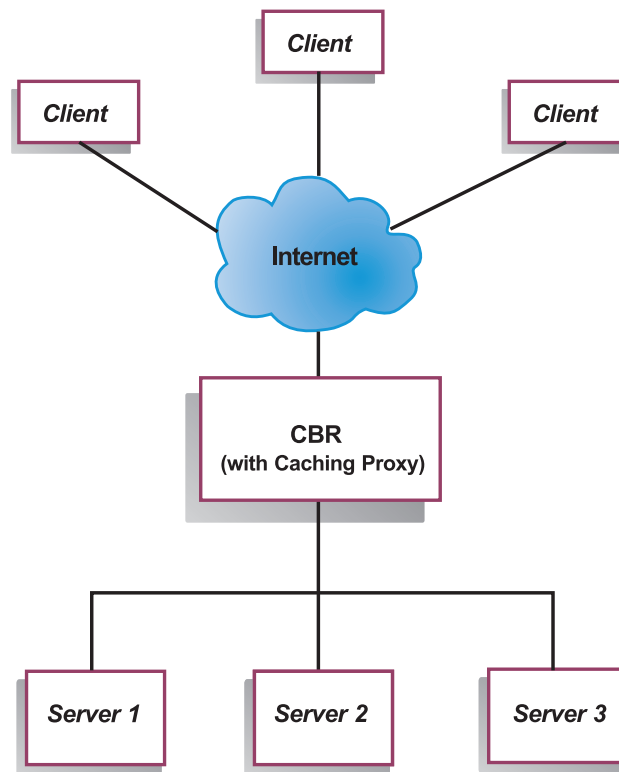


Figura 4. Esempio di un sito dove i server locali sono gestiti da CBR

La Figura 4 mostra la rappresentazione logica di un sito in cui CBR viene utilizzato come proxy per gestire alcuni tipi di contenuti provenienti dai server locali. Il componente CBR utilizza Caching Proxy per inoltrare le richieste client (HTTP o HTTPS) ai server in base al contenuto dell'URL.

Panoramica del componente Site Selector

Site Selector agisce come un server dei nomi che funziona in associazione con altri server dei nomi in un DNS per eseguire il bilanciamento del carico tra un gruppo di server utilizzando le misure e i pesi raccolti. È possibile creare una configurazione del sito per consentire il bilanciamento del carico del traffico tra un gruppo di server basato sul nome dominio utilizzato per una richiesta del client.

Un client invia una richiesta di risoluzione di un nome dominio a un server dei nomi presente nella rete. Il server dei nomi inoltra la richiesta alla macchina Site Selector. Quindi, Site Selector risolve il nome dominio nell'indirizzo IP di uno dei server configurati per quel nome del sito. Site Selector restituisce l'indirizzo IP del server selezionato al server dei nomi. Il server dei nomi restituisce l'indirizzo IP al client.

Metric Server è un componente di monitoraggio del sistema di Load Balancer che deve essere installato su ciascun server della configurazione che si intende sottoporre a bilanciamento del carico. Insieme a Metric Server, Site Selector può monitorare il livello di attività su un server, rilevare un server che sta elaborando un carico inferiore rispetto agli altri e individuare un server in errore. Il carico misura il traffico sul server. La personalizzazione dei file di script delle metriche del sistema consente di controllare il tipo di misurazioni utilizzate per valutare il calcolo. È possibile configurare Site Selector in base all'ambiente, prendendo in

considerazione fattori quali la frequenza degli accessi, il numero totale degli utenti e i tipi di accesso (ad esempio, query brevi e lunghe oppure carichi che richiedono molto spazio sulla CPU).

Gestione dei server locali e remoti con Site Selector e Metric Server

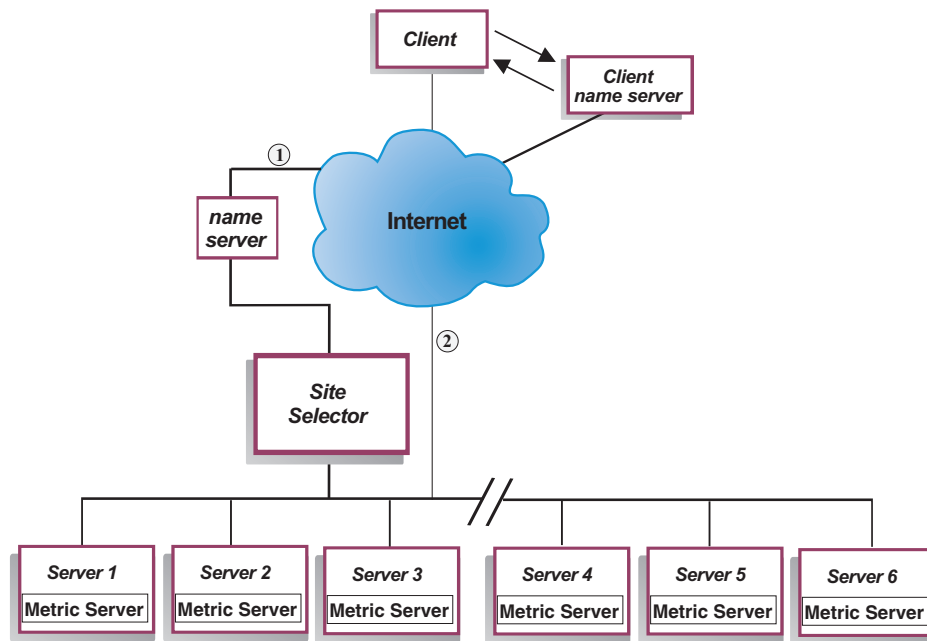


Figura 5. Esempio di un sito dove i server locali e remoti sono gestiti da Site Selector e Metric Server

La Figura 5 illustra un sito in cui il componente Site Selector viene utilizzato per rispondere alle richieste. Server1, Server2 e Server3 sono server locali. Server4, Server5 e Server6 sono server remoti.

Un client invia una richiesta di risoluzione di un nome dominio a un server dei nomi client. Il server dei nomi client inoltra la richiesta tramite DNS alla macchina Site Selector (percorso 1). Quindi, Site Selector risolve il nome dominio nell'indirizzo IP di uno dei server. Site Selector restituisce l'indirizzo IP del server selezionato al server dei nomi client. Il server dei nomi restituisce l'indirizzo IP al client.

Dopo che il client ha ricevuto l'indirizzo IP del server, instrada le richieste dell'applicazione direttamente al server selezionato (percorso 2).

Nota: in questo esempio, Metric Server fornisce informazioni sul carico del sistema alla macchina Site Selector. L'agente Metric Server viene installato su ciascun server di backend. Utilizzare Metric Server insieme a Site Selector; in caso contrario, per il bilanciamento del carico Site Selector può utilizzare solo un metodo di selezione del tipo round-robin.

Panoramica del componente Controller Cisco CSS

Controller Cisco CSS forma una soluzione complementare insieme agli switch della serie CSS 11000 di Cisco. La soluzione combinata unisce le funzioni di instradamento basato sul contenuto e di inoltro del potente pacchetto CSS serie 11000 con i sofisticati algoritmi di raccolta delle informazioni di Load Balancer per determinare i dati sul carico e la disponibilità del *servizio* (database o applicazione del server di backend). La funzione Controller Cisco CSS utilizza l'algoritmo di calcolo dei pesi, gli advisor standard e personalizzati di Load Balancer e Metric Server per determinare le metriche, lo stato e il carico del servizio. Queste informazioni vengono utilizzate da Controller Cisco CSS per generare i pesi del servizio che vengono poi inviati a Switch Cisco CSS per la selezione del servizio più adatto, per l'ottimizzazione del carico e per la tolleranza agli errori.

Controller Cisco CSS utilizza molti criteri, tra cui:

- Connessioni attive e frequenza di connessione (il numero di nuove connessioni in un ciclo di calcolo dei pesi)
- Disponibilità delle applicazioni e dei database, facilitata dall'uso di advisor standard e personalizzati, e agenti residenti nel servizio personalizzati sull'applicazione specifica
- Utilizzo della CPU
- Utilizzo della memoria
- Metriche del sistema personalizzabili

Quando Switch Cisco CSS, senza Controller Cisco CSS, determina lo stato di un servizio che fornisce contenuti, utilizza i tempi di risposta per le richieste di contenuto o altre misurazioni della rete. Al contrario, con Controller Cisco CSS, queste attività vengono trasferite da Switch Cisco CSS su Controller Cisco CSS. Controller Cisco CSS influenza il peso del servizio o la capacità di trasferire contenuti e attiva o sospende un servizio quando il servizio diventa di nuovo disponibile o non è più disponibile.

Controller Cisco CSS:

- Utilizza un'interfaccia SNMP pubblicata per ottenere le informazioni sulla connessione da Switch Cisco CSS
- Utilizza l'input dell'advisor per analizzare la disponibilità del servizio e i tempi di risposta
- Utilizza le informazioni raccolte da Metric Server per analizzare il carico del sistema
- Genera i pesi per ciascun servizio della configurazione

I pesi vengono applicati a tutti i servizi su una porta. Per ogni particolare porta, le richieste vengono distribuite tra i servizi in base ai loro pesi rispettivi. Ad esempio, se un servizio è impostato su un peso pari a 10 e l'altro su un peso pari a 5, il servizio impostato a 10 riceverà il doppio delle richieste del service impostato a 5. Questi pesi vengono forniti a Switch Cisco CSS tramite SNMP. Quando il peso di un servizio è impostato su un valore superiore, Switch Cisco CSS indirizza più richieste a quel servizio.

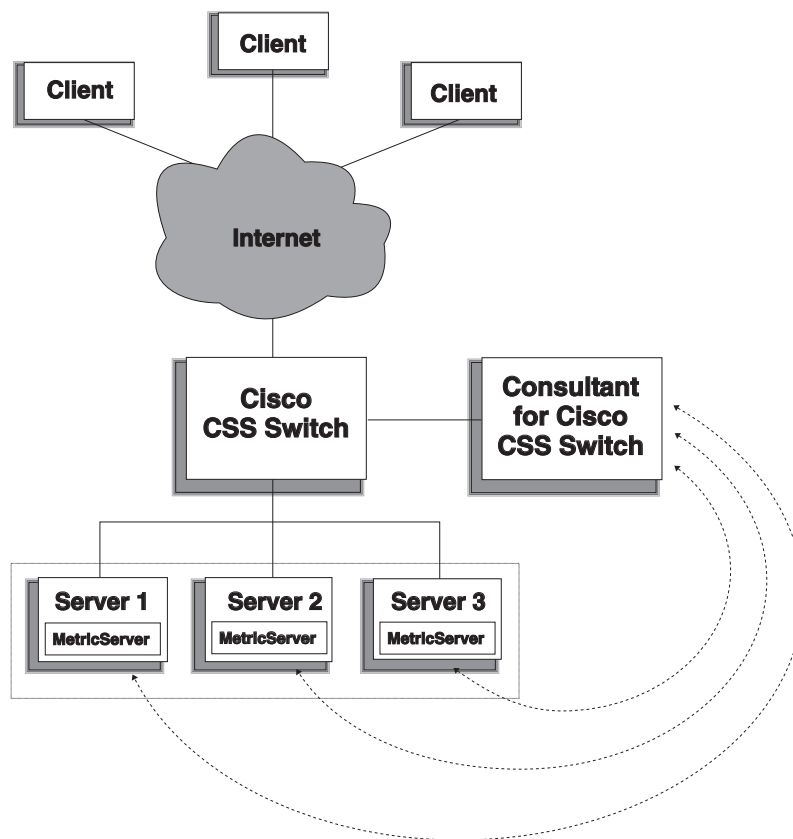


Figura 6. Esempio di un sito dove i server locali sono gestiti da Controller Cisco CSS e Metric Server

Controller Cisco CSS, insieme a Switch Cisco CSS, offre la migliore soluzione possibile che combina la funzione di scambio dei contenuti in base alla velocità di connessione con un sistema di raccolta delle informazioni sulle applicazioni più sofisticato, tolleranza agli errori e ottimizzazione del carico del servizio. Controller Cisco CSS fa parte di una soluzione complementare globale tra Switch Cisco CSS e IBM WebSphere Application Server Load Balancer.

Panoramica del componente Controller Nortel Alteon

Controller Nortel Alteon insieme alla famiglia di switch Web di Nortel Alteon fornisce una soluzione complementare che combina le funzionalità e la velocità di inoltro del pacchetto degli switch con i sofisticati algoritmi per la raccolta delle informazioni di Load Balancer per determinare i pesi dei server.

Controller Nortel Alteon consente di sviluppare advisor personalizzati che siano in grado di eseguire valutazioni più intelligenti e consapevoli della disponibilità e del carico delle applicazioni utilizzate per distribuire i servizi.

Metric Server fornisce informazioni sul carico del sistema, quali le informazioni sull'utilizzo della CPU e della memoria e un framework per sviluppare le misurazioni di carico personalizzate del sistema.

Controller Nortel Alteon raccoglie molti tipi di informazioni metriche al fine di determinare i pesi per i server che verranno sottoposti al bilanciamento del carico da parte dei Switch Nortel Alteon Web, tra cui:

- Connessioni attive e nuove connessioni

- Disponibilità delle applicazioni e dei database, facilitata dall'uso di advisor standard e personalizzati, e agenti residenti nel server, personalizzati sull'applicazione specifica
- Utilizzo della CPU
- Utilizzo della memoria
- Metriche del server personalizzabili
- Accessibilità

Controller Nortel Alteon utilizza SNMP per comunicare con lo switch. Le informazioni sulla configurazione, sullo stato e sulla connessione vengono richiamate dallo switch. Una volta che i pesi dei server sono stati calcolati dal controller, vengono impostati sullo switch. Lo switch utilizza i pesi impostati dal controller per selezionare il server più adatto a gestire le richieste client per un servizio.

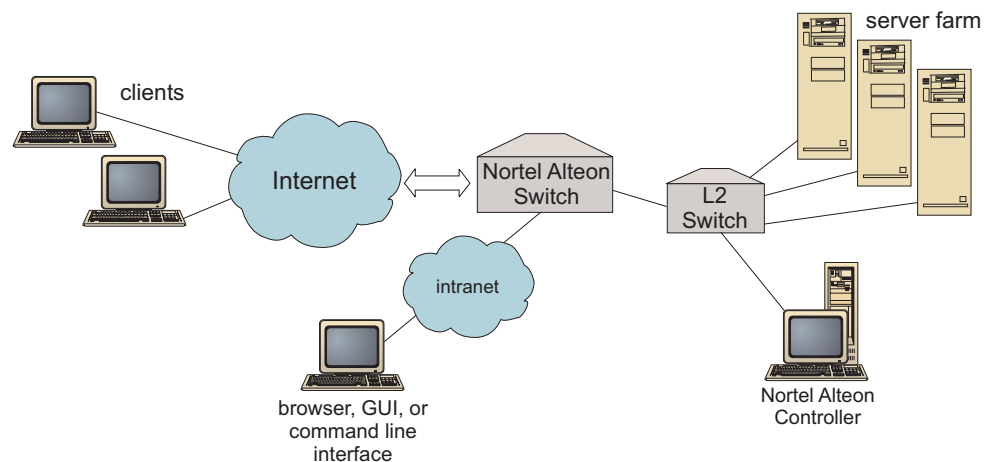


Figura 7. Esempio di un sito dove i server locali sono gestiti da Controller Nortel Alteon

È possibile gestire il controller tramite un'interfaccia browser, una GUI remota o una riga comandi remota.

Controller Nortel Alteon, insieme alla famiglia di switch Web di Nortel Alteon offre la migliore soluzione possibile che combina la funzione di scambio dei contenuti in base alla velocità di connessione con informazioni più sofisticate sulle applicazioni e un'ottimizzazione del carico dei server. Controller Nortel Alteon fa parte di una soluzione complementare tra la famiglia di switch Web di Nortel Alteon e IBM WebSphere.

Capitolo 3. Gestione della rete: determinazione delle funzioni di Load Balancer da utilizzare

Questo capitolo elenca le funzioni di configurazione dei componenti di Load Balancer per facilitare la scelta delle opzioni da utilizzare per la gestione della rete:

- “Funzioni del gestore, degli advisor e di Metric Server (per i componenti Dispatcher, CBR e Site Selector)”
- “Funzioni del componente Dispatcher”
- “Funzioni del componente CBR (Content Based Routing)” a pagina 23
- “Funzioni del componente Site Selector” a pagina 25
- “Funzioni del componente Controller Cisco CSS” a pagina 27
- “Funzioni del componente Controller Nortel Alteon” a pagina 28

IMPORTANTE: se si utilizza Load Balancer per IPv4 e IPv6, solo il componente Dispatcher è disponibile. Per ulteriori informazioni, consultare Capitolo 8, “Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6”, a pagina 79.

Funzioni del gestore, degli advisor e di Metric Server (per i componenti Dispatcher, CBR e Site Selector)

Per ottimizzare il bilanciamento del carico tra i server e garantire che venga scelto il server più adatto, vedere:

- “Ottimizzazione del bilanciamento del carico in Load Balancer” a pagina 176
- “Advisor” a pagina 181
- “Metric Server” a pagina 191

Funzioni del componente Dispatcher

Dispatcher supporta il bilanciamento del carico tra i server per HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3, Telnet, SIP e ogni altra applicazione basata sul protocollo TCP o UDP senza informazioni sullo stato.

Amministrazione remota

- Per eseguire la configurazione di Load Balancer da una macchina diversa da quella dove risiede Load Balancer, vedere “Amministrazione remota di Load Balancer” a pagina 253.
(Se si utilizza l’installazione di Load Balancer per IPv4 e IPv6, questa funzione non è disponibile.)

Posizionamento

- Per eseguire Dispatcher sulla stessa macchina di un server Web per cui si sta effettuando il bilanciamento del carico, vedere “Utilizzo dei server posizionati” a pagina 196.

Disponibilità elevata

- Per utilizzare Dispatcher per eliminare la limitazione che un server diventi un “single point-of-failure”, vedere “Disponibilità elevata di tipo semplice” a pagina 57 e “Disponibilità elevata reciproca” a pagina 58.

(Se si utilizza l'installazione di Load Balancer per IPv4 e IPv6, è disponibile solo la funzione semplice di disponibilità elevata e non la disponibilità elevata reciproca.)

Affinità client-server

Quando si esegue il bilanciamento del carico sul traffico SSL (HTTPS):

- Per garantire che il client utilizzi lo stesso server SSL per connessioni multiple, vedere “Funzionamento della funzione di affinità di Load Balancer” a pagina 214.
- Per garantire che il client utilizzi lo stesso server per il traffico HTTP e SSL, vedere “Affinità multiporta” a pagina 215.
(Se si utilizza l'installazione di Load Balancer per IPv4 e IPv6, la funzione di affinità multiporta non è disponibile.)
- Per garantire che il client utilizzi lo stesso server per connessioni multiple, vedere “Funzionamento della funzione di affinità di Load Balancer” a pagina 214.
- Per garantire che un gruppo di client utilizzi lo stesso server per connessioni multiple, vedere “Maschera indirizzo affinità (stickymask)” a pagina 216.
(Se si utilizza l'installazione di Load Balancer per IPv4 e IPv6, la funzione stickmask non è disponibile.)
- Per eliminare un server dalla configurazione (ad esempio, a scopi di gestione) senza interrompere il traffico client, vedere “Gestione della disattivazione delle connessioni server” a pagina 217.

Bilanciamento del carico basato sulle regole

Per indirizzare i client a gruppi di server diversi configurati per lo stesso indirizzo Web, è possibile aggiungere delle regole alla configurazione di Dispatcher. Per ulteriori informazioni, vedere “Configurazione del bilanciamento del carico in base alle regole” a pagina 205.

- Per indirizzare i client a gruppi di server diversi in base all'indirizzo IP origine del client, vedere “Utilizzo delle regole basate sull'indirizzo IP del client” a pagina 207.
- Per indirizzare i client a gruppi di server diversi in base alla porta del client, vedere “Utilizzo delle regole basate sulla porta client” a pagina 207.
- Per indirizzare i client a gruppi di server diversi in base all'ora, vedere “Utilizzo delle regole basate sull'ora del giorno” a pagina 207.
- Per indirizzare i client ai server in base ai bit TOS (Type of Service) dei pacchetti di rete, vedere “Utilizzo delle regole basate sul tipo di servizio (TOS, type of service)” a pagina 208.
- Per indirizzare i client a gruppi di server diversi in base al traffico del sito:
 - Utilizzando le connessioni al secondo, vedere “Utilizzo delle regole basate sulle connessioni al secondo” a pagina 208.
 - Utilizzando il totale delle connessioni attive, vedere “Utilizzo delle regole basate sul numero totale di connessioni attive” a pagina 208.
 - Riservando e condividendo la larghezza di banda per indirizzi Web diversi, vedere “Utilizzo delle regole basate sulla larghezza di banda riservata e condivisa” a pagina 209.
 - Garantendo che il traffico venga misurato correttamente per il proprio gruppo di server, vedere “Opzione di valutazione dei server per le regole” a pagina 213.

- Per indirizzare il sovraccarico di traffico a un gruppo di server predefinito (ad esempio, i server che avvertono che il sito è occupato), vedere “Utilizzo di regole il cui valore è sempre true” a pagina 212.
- Per escludere l’affinità di client e garantire che un client non rimanga aderente a un server sovraccarico, vedere “ignora affinità di porta” a pagina 213.

Se si utilizza l’installazione di Load Balancer per IPv4 e IPv6, il bilanciamento del carico basato sulle regole non è disponibile.

Instradamento basato sul contenuto con il metodo di inoltro cbr di Dispatcher

Per garantire che i client SSL ritornino sullo stesso server SSL, in base all’ID SSL della richiesta client

- Vedere a pagina 53.

Per indirizzare i client HTTP a gruppi di server diversi utilizzando le regole di corrispondenza dei contenuti URL della richiesta client, vedere “Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)” a pagina 53 e “Utilizzo delle regole basate sul contenuto delle richieste” a pagina 212 per ulteriori informazioni.

- Per distinguere tra i singoli URL e le relative applicazioni dei servizi, vedere “Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)” a pagina 55.
- Per garantire che i client ritornino allo stesso server quando le richieste contengono dei contenuti simili in più connessioni utilizzando i cookie creati dai propri server Web, vedere “Affinità cookie passivo” a pagina 219.
- Per bilanciare il carico del traffico Web sui server Caching Proxy che consentono la memorizzazione nella cache di contenuti univoci su ciascun server (aumentando quindi le dimensioni della cache del sito ed eliminando la memorizzazione ridondante di contenuti su più macchine), vedere “Affinità URI” a pagina 220.

(Se si utilizza l’installazione di Load Balancer per IPv4 e IPv6, il metodo di inoltro cbr di Dispatcher non è disponibile.)

Confronto tra il metodo di inoltro cbr del componente Dispatcher e il componente CBR

Il vantaggio del metodo di inoltro cbr di Dispatcher rispetto all’uso del componente CBR consiste nella rapidità di risposta alle richieste client. Inoltre, il metodo di inoltro cbr di Dispatcher *non* richiede l’installazione e l’uso di Caching Proxy.

Se la rete prevede traffico SSL totalmente protetto (client a server), il vantaggio di utilizzare il componente CBR (in combinazione con Caching Proxy) consiste nella possibilità di elaborare la codifica/decodifica richiesta al fine di eseguire l’instradamento basato sul contenuto. Per connessioni totalmente protette, il metodo di inoltro cbr di Dispatcher può essere configurato solo con l’affinità ID SSL in quanto non è in grado di elaborare la codifica/decodifica per eseguire l’instradamento basato sul contenuto sull’URL della richiesta client.

Bilanciamento del carico per una rete geografica

Il bilanciamento del carico per una rete geografica può essere ottenuto utilizzando metodi diversi.

- Per bilanciare il carico sui server remoti utilizzando la funzione per la rete geografica di Dispatcher, vedere: “Configurazione del supporto di Dispatcher per una rete geografica” a pagina 221 e “Supporto GRE (Generic Routing Encapsulation)” a pagina 227.

Nota: se GRE non è supportato sul sito remoto, è necessario aggiungere un altro Dispatcher sul sito remoto.

- Per bilanciare il carico sui server remoti utilizzando il metodo di inoltro nat di Dispatcher, vedere “NAT/NAPT del Dispatcher (metodo di inoltro nat)” a pagina 51.

Nota: *non* è necessario alcun Dispatcher aggiuntivo sul sito remoto, se viene utilizzato il metodo di inoltro nat.

(Se si utilizza l’installazione di Load Balancer per IPv4 e IPv6, la funzione di bilanciamento del carico per una rete geografica non è disponibile.)

Mappatura delle porte

- Per bilanciare il carico di un indirizzo Web su più server daemon sulla stessa macchina, dove ciascun daemon rimane in ascolto su una porta univoca, vedere “NAT/NAPT del Dispatcher (metodo di inoltro nat)” a pagina 51.

(Se si utilizza l’installazione di Load Balancer per IPv4 e IPv6, questa funzione non è disponibile.)

Configurazione di Dispatcher su una rete privata

- Per indirizzare il traffico di Dispatcher su una rete diversa da quella su cui viene indirizzato il traffico dei client (per migliorare le prestazioni riducendo i conflitti sulla rete esterna), vedere “Utilizzo di una configurazione di rete privata” a pagina 228.

Cluster e porta jolly

- Per combinare indirizzi Web multipli in un’unica configurazione, vedere “Utilizzo del cluster jolly per combinare le configurazioni di server” a pagina 229.
- Per bilanciare il carico dei firewall, vedere “Utilizzo di cluster jolly per bilanciare il carico dei firewall” a pagina 230.
- Per indirizzare il traffico a tutte le porte di destinazione, vedere “Utilizzo della porta jolly per indirizzare il traffico per una porta non configurata” a pagina 231.

Rilevamento di attacchi “Denial of service”

- Per individuare possibili attacchi “denial of service”, vedere “Rilevamento attacco di tipo Denial of service” a pagina 231.

Registrazione binaria

- Per analizzare il traffico dei server, vedere “Uso della registrazione binaria per analizzare le statistiche dei server” a pagina 232.

Avvisi

- Per generare avvisi quando i server vengono contrassegnati come attivi o inattivi, vedere “Uso degli script per generare un avviso o registrare un malfunzionamento dei server” a pagina 180.

Funzioni del componente CBR (Content Based Routing)

CBR integra il bilanciamento del carico con Caching Proxy di WebSphere Application Server per inviare le richieste dei client ai server HTTP o HTTPS (SSL) specificati attraverso un server proxy. Per utilizzare CBR, Caching Proxy deve essere installato e configurato sulla stessa macchina. Per informazioni su come configurare Caching Proxy perché utilizzi CBR, vedere “Fase 1. Configurazione di Caching Proxy per l’uso di CBR” a pagina 111.

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l’uso di Caching Proxy. Per ulteriori informazioni, vedere “Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)” a pagina 53.

Il componente CBR (o il metodo di inoltro cbr di Dispatcher) consente di offrire i seguenti vantaggi ai client:

- Bilanciare il carico delle richieste client per tipi diversi di contenuti su gruppi di server. (Vedere “Bilanciamento del carico di richieste per tipi diversi di contenuto” a pagina 104.)
- Migliorare il tempo di risposta dividendo in maniera ottimale i contenuti del sito tra i server Web. (Vedere “Suddivisione del contenuto del sito per ottimizzare i tempi di risposta” a pagina 104.)
- Garantire un traffico client ininterrotto in caso di malfunzionamento di un server assegnando ciascun tipo di contenuto a più server. (Vedere “Backup del contenuto del server Web” a pagina 105.)

Confronto tra il componente CBR e il metodo di inoltro cbr del componente Dispatcher

Se la rete richiede la gestione di traffico SSL totalmente protetto (client a server), il vantaggio di utilizzare il componente CBR (in combinazione con Caching Proxy) consiste nella possibilità di elaborare la codifica/decodifica SSL al fine di eseguire l’instradamento basato sul contenuto.

Per connessioni SSL totalmente protette, il metodo di inoltro cbr di Dispatcher può essere configurato solo con l’affinità ID SSL in quanto non è in grado di elaborare la codifica/decodifica per eseguire l’instradamento basato sul contenuto sull’URL della richiesta client.

Per il traffico HTTP, il vantaggio del metodo di inoltro cbr di Dispatcher rispetto all’uso del componente CBR consiste nella rapidità di risposta alle richieste client. Inoltre, il metodo di inoltro cbr di Dispatcher *non* richiede l’installazione e l’uso di Caching Proxy.

Amministrazione remota

- Per eseguire la configurazione di Load Balancer da una macchina diversa da quella dove risiede Load Balancer, vedere “Amministrazione remota di Load Balancer” a pagina 253.

Posizionamento

- È possibile eseguire il componente CBR sulla stessa macchina di un server per cui si sta effettuando il bilanciamento del carico. Per ulteriori informazioni, vedere “Utilizzo dei server posizionati” a pagina 196.

CBR con più istanze di Caching Proxy

- Per migliorare l'utilizzo della CPU utilizzando più processi Caching Proxy, vedere “Uso di più processi Caching Proxy per migliorare l'utilizzo della CPU” a pagina 105.

Instradamento basato sul contenuto per le connessioni SSL

Per consentire l'instradamento basato sul contenuto per il traffico SSL:

- Utilizzando connessioni protette su entrambi i lati (client-proxy e proxy-server), vedere “Bilanciamento del carico tra connessioni protette (SSL)” a pagina 105.
- Utilizzando le connessioni protette solo sul lato client-proxy, vedere “Bilanciamento del carico client-proxy in SSL e proxy-server in HTTP” a pagina 106.

Suddivisione in partizioni dei server

- Per distinguere tra i singoli URL e le relative applicazioni dei servizi, vedere “Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)” a pagina 55.

Bilanciamento del carico basato sulle regole

Per indirizzare i client a gruppi di server diversi configurati per lo stesso indirizzo Web, è possibile aggiungere delle regole alla configurazione di CBR. Per ulteriori informazioni, vedere “Configurazione del bilanciamento del carico in base alle regole” a pagina 205.

- Per indirizzare i client a gruppi di server diversi in base al contenuto dell'URL richiesto, vedere “Utilizzo delle regole basate sul contenuto delle richieste” a pagina 212.
- Per indirizzare i client a gruppi di server diversi in base all'indirizzo IP origine del client, vedere “Utilizzo delle regole basate sull'indirizzo IP del client” a pagina 207.
- Per indirizzare i client a gruppi di server diversi in base all'ora, vedere “Utilizzo delle regole basate sull'ora del giorno” a pagina 207.
- Per indirizzare i client a gruppi di server diversi in base al traffico del sito:
 - Utilizzando le connessioni al secondo, vedere “Utilizzo delle regole basate sulle connessioni al secondo” a pagina 208.
 - Utilizzando il totale delle connessioni attive, vedere “Utilizzo delle regole basate sul numero totale di connessioni attive” a pagina 208.
- Per indirizzare il sovraccarico di traffico a un gruppo di server predefinito (ad esempio, i server che avvertono che il sito è occupato) vedere “Utilizzo di regole il cui valore è sempre true” a pagina 212.

- Per escludere l'affinità dei client e garantire che un client non rimanga aderente a un server sovraccarico, vedere "ignora affinità di porta" a pagina 213.

Affinità client-server

- Per garantire che il client ritorni allo stesso server in caso di connessioni multiple, vedere "Funzionamento della funzione di affinità di Load Balancer" a pagina 214.
- Per eliminare un server dalla configurazione (ad esempio, a scopi di gestione) senza interrompere il traffico client, vedere "Gestione della disattivazione delle connessioni server" a pagina 217.
- Per garantire che i client ritornino allo stesso server quando le richieste contengono dei contenuti simili in più connessioni senza fare affidamento sui cookie creati dai propri server Web, vedere "Affinità cookie attivo" a pagina 218.
- Per garantire che i client ritornino allo stesso server quando le richieste contengono dei contenuti simili in più connessioni utilizzando i cookie creati dai propri server Web, vedere "Affinità cookie passivo" a pagina 219.
- Per bilanciare il carico del traffico Web sui server Caching Proxy che consentono la memorizzazione nella cache di contenuti univoci su ciascun server (aumentando quindi le dimensioni della cache del sito ed eliminando la memorizzazione ridondante di contenuti su più macchine), vedere "Affinità URI" a pagina 220.

Disponibilità elevata con Dispatcher e CBR

- Per eliminare le limitazioni "single point of failure" nella rete utilizzando Dispatcher in una configurazione a due livelli con CBR, vedere "Disponibilità elevata di Load Balancer" a pagina 6.

Registrazione binaria

- Per analizzare il traffico dei server, vedere "Uso della registrazione binaria per analizzare le statistiche dei server" a pagina 232.

Avvisi

- Per generare avvisi quando i server vengono contrassegnati come attivi o inattivi, vedere "Uso degli script per generare un avviso o registrare un malfunzionamento dei server" a pagina 180.

Funzioni del componente Site Selector

Site Selector bilancia il carico di una richiesta di servizio dei nomi in un gruppo di server.

Amministrazione remota

- Per eseguire la configurazione di Load Balancer da una macchina diversa da quella dove risiede Load Balancer, vedere "Amministrazione remota di Load Balancer" a pagina 253.

Posizionamento

- È possibile eseguire il componente Site Selector sulla stessa macchina di un server per cui si sta effettuando il bilanciamento del carico, senza ulteriori fasi di configurazione.

Disponibilità elevata

- La funzione di disponibilità elevata è disponibile tramite le metodologie DNS (Domain Name System) utilizzando più Site Selector ridondanti, a condizione che siano presenti la corretta configurazione del server dei nomi parent e i normali metodi di ripristino DNS. Esempi dei normali metodi di ripristino DNS sono: nuova trasmissione delle query e nuovi tentativi di trasferimento zone.
- Per eliminare le limitazioni "single point of failure" nella rete utilizzando Dispatcher in una configurazione a due livelli con Site Selector, vedere "Disponibilità elevata di Load Balancer" a pagina 6.

Affinità client-server

- Per garantire che il client utilizzi lo stesso server per richieste di server dei nomi multiple, vedere "Funzionamento della funzione di affinità di Load Balancer" a pagina 214.
- Per garantire l'affinità dei client a un server utilizzando il metodo di impostazione DNS standard per il valore TTL (Time To Live), vedere "Considerazioni su TTL" a pagina 125.

Bilanciamento del carico basato sulle regole

Per indirizzare le richieste client a gruppi di server diversi per la risoluzione di un nome di dominio, è possibile aggiungere delle regole alla configurazione di Site Selector. Per ulteriori informazioni, vedere "Configurazione del bilanciamento del carico in base alle regole" a pagina 205.

- Per indirizzare i client a gruppi di server diversi in base all'indirizzo IP origine del client, vedere "Utilizzo delle regole basate sull'indirizzo IP del client" a pagina 207.
- Per indirizzare i client a gruppi di server diversi in base all'ora, vedere "Utilizzo delle regole basate sull'ora del giorno" a pagina 207.
- Per indirizzare i client a gruppi di server diversi in base ai valori metrici del carico del gruppo di server, vedere:
 - "Regola Metric all" a pagina 211
 - "Regola media metrica" a pagina 211
- Per indirizzare il sovraccarico di traffico a un gruppo di server predefinito (ad esempio, i server che avvisano che il sito è occupato) vedere "Utilizzo di regole il cui valore è sempre true" a pagina 212.

Bilanciamento del carico per una rete geografica

Site Selector può essere eseguito su una rete locale (LAN) o su una rete geografica (WAN).

In un ambiente WAN:

- Per bilanciare il carico di richieste dei server dei nomi client utilizzando un metodo di selezione round-robin, non sono necessarie ulteriori fasi di configurazione.

- Per prendere in considerazione la prossimità di rete del server dei nomi client ai server che forniscono l'applicazione richiesta (i server di destinazione), vedere "Uso della funzione di prossimità della rete" a pagina 126.

Avvisi

- Per generare avvisi quando i server vengono contrassegnati come attivi o inattivi, vedere "Uso degli script per generare un avviso o registrare un malfunzionamento dei server" a pagina 180.

Funzioni del componente Controller Cisco CSS

Controller Cisco CSS potenzia la funzione di bilanciamento del carico dei server eseguita dagli switch Cisco sulla base di informazioni più accurate sui sistemi e sulle applicazioni. Il controller utilizza metriche più sensibili alle applicazioni e al sistema per calcolare i pesi dei server dinamicamente. I pesi vengono forniti allo switch tramite SNMP. Lo switch utilizza i pesi durante l'elaborazione delle richieste client con conseguente ottimizzazione del carico dei server e una maggiore tolleranza agli errori.

Per ottimizzare il bilanciamento del carico tra i server e garantire che venga scelto il server più adatto, vedere:

- "Ottimizzazione del bilanciamento del carico in Load Balancer" a pagina 238
- "Advisor" a pagina 240 e "Creazione di advisor personalizzati" a pagina 242
- "Metric Server" a pagina 245

Amministrazione remota

- Per eseguire la configurazione di Load Balancer da una macchina diversa da quella dove risiede Load Balancer, vedere "Amministrazione remota di Load Balancer" a pagina 253.

Posizionamento

- È possibile eseguire il componente Controller Cisco CSS sulla stessa macchina di un server per cui si sta effettuando il bilanciamento del carico, senza ulteriori fasi di configurazione.

Disponibilità elevata

- Per eliminare limitazioni "single point of failure" nella rete, Switch Cisco CSS e Cisco CSS Controller dispongono della funzione di disponibilità elevata. Per lo switch, le funzioni di disponibilità elevata sono rese possibili dal protocollo di ridondanza CSS. Per Cisco CSS Controller, viene utilizzato un protocollo proprietario che consente la configurazione hot-standby di due controller.
Per ulteriori informazioni sulla configurazione della funzione di disponibilità elevata, vedere "Disponibilità elevata" a pagina 142.

Registrazione binaria

- Per analizzare il traffico dei server, vedere "Uso della registrazione binaria per analizzare le statistiche dei server" a pagina 247.

Avvisi

- Per generare avvisi quando i server vengono contrassegnati come attivi o inattivi, vedere “Uso degli script per generare un avviso o registrare un malfunzionamento dei server” a pagina 249.

Funzioni del componente Controller Nortel Alteon

Controller Nortel Alteon potenzia la funzione di bilanciamento del carico dei server eseguita dagli switch Nortel Alteon sulla base di informazioni più accurate sui sistemi e sulle applicazioni. Il controller utilizza metriche più sensibili alle applicazioni e al sistema per calcolare i pesi dei server dinamicamente. I pesi vengono forniti allo switch tramite SNMP. Lo switch utilizza i pesi durante l'elaborazione delle richieste client con conseguente ottimizzazione del carico dei server e una maggiore tolleranza agli errori.

Per ottimizzare il bilanciamento del carico tra i server e garantire che venga scelto il server più adatto, vedere:

- “Ottimizzazione del bilanciamento del carico in Load Balancer” a pagina 238
- “Advisor” a pagina 240 e “Creazione di advisor personalizzati” a pagina 242
- “Metric Server” a pagina 245

Amministrazione remota

- Per eseguire la configurazione di Load Balancer da una macchina diversa da quella dove risiede Load Balancer, vedere “Amministrazione remota di Load Balancer” a pagina 253.

Posizionamento

- È possibile eseguire il componente Controller Nortel Alteon sulla stessa macchina di un server per cui si sta effettuando il bilanciamento del carico, senza ulteriori fasi di configurazione.

Disponibilità elevata

- Per eliminare limitazioni “single point of failure” nella rete, Nortel Alteon Web Switch e Nortel Alteon Controller dispongono della funzione di disponibilità elevata. Per utilizzare la funzione di disponibilità elevata con lo switch, è necessario utilizzare il protocollo di ridondanza per le connessioni ai server e per i servizi. Nortel Alteon Controller fornisce la funzione di disponibilità elevata utilizzando un protocollo proprietario che consente una configurazione hot-standby di due controller.
Per ulteriori informazioni sulla configurazione della funzione di disponibilità elevata, vedere “Disponibilità elevata” a pagina 162.

Registrazione binaria

- Per analizzare il traffico dei server, vedere “Uso della registrazione binaria per analizzare le statistiche dei server” a pagina 247.

Avvisi

- Per generare avvisi quando i server vengono contrassegnati come attivi o inattivi, vedere “Uso degli script per generare un avviso o registrare un malfunzionamento dei server” a pagina 249.

Capitolo 4. Installazione di Load Balancer

Questo capitolo descrive come installare Load Balancer utilizzando gli strumenti di assemblaggio del sistema e i requisiti di tutti i sistemi operativi supportati.

- “Requisiti di sistema e installazione in AIX”
- “Requisiti di sistema e installazione in HP-UX” a pagina 33
- “Requisiti di sistema e installazione in Linux” a pagina 34
- “Requisiti di sistema e installazione in Solaris” a pagina 36
- “Requisiti di sistema e installazione in Windows” a pagina 38

Per le istruzioni di installazione con il programma di configurazione del prodotto, fare riferimento al documento *Informazioni di base, pianificazione e installazione per Edge Components*.

Java 2 SDK viene installato automaticamente con Load Balancer su tutte le piattaforme.

Se si sta eseguendo la migrazione da una precedente versione di Load Balancer, o se si sta reinstallando un sistema operativo, prima di procedere all'installazione, salvare tutti i file di configurazione o i file script precedenti di Load Balancer.

- Completata l'installazione, collocare i file di configurazione nella directory `.../ibm/edge/lb/servers/configurations/componente` (dove per *componente* si intende dispatcher, cbr, ss, cco o nal).
- Completata l'installazione, collocare i file script (come goIdle e goStandby) nella directory `.../ibm/edge/lb/servers/bin`, per eseguirli.

In base al tipo di installazione, non sono forniti tutti i pacchetti di Load Balancer elencati in questa sezione.

- Per le installazioni di Edge Component che forniscono sia Load Balancer che Caching Proxy, tutti i pacchetti dei componenti di installazione di Load Balancer sono disponibili.
- Per le installazioni di Edge Component che forniscono Load Balancer ma non Caching Proxy, il pacchetto del componente CBR non è incluso con Load Balancer.
- Per installazioni di Edge Component per IPv6 (Load Balancer per IPv4 e IPv6), il pacchetto del componente Dispatcher è incluso con Load Balancer. I pacchetti dei componenti CBR, Site Selector e Controller non sono inclusi. Per l'ordine di installazione consigliato dei pacchetti Load Balancer per IPv4 e IPv6, fare riferimento a “Installazione di Load Balancer per IPv4 e IPv6” a pagina 81.

Requisiti di sistema e installazione in AIX

Requisiti per i sistemi AIX

Per i requisiti hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Installazione di sistemi AIX

Tabella 1 riporta le immagini di installp per Load Balancer e l'ordine di installazione consigliato mediante lo strumento di installazione dei pacchetti del sistema.

Tabella 1. immagini installp in AIX

Base	ibmlb.base.rte
Amministrazione (con i messaggi)	<ul style="list-style-type: none">• ibmlb.admin.rte• ibmlb.msg.language.admin
Driver unità	ibmlb.lb.driver
Licenza	ibmlb.lb.license
Componenti Load Balancer (con messaggi)	<ul style="list-style-type: none">• ibmlb.componente.rte• ibmlb.msg.language.lb
Documentazione (con messaggi)	<ul style="list-style-type: none">• ibmlb.doc.rte• ibmlb.msg.en_US.doc
Metric Server	ibmlb.ms.rte

Dove *component* può essere: disp (Dispatcher), cbr (CBR), ss (Site Selector), cco (Cisco CSS Controller) o nal (Nortel Alteon Controller). Selezionare facoltativamente i componenti che si desidera installare.

Dove *language* può essere:

- en_US
- de_CH
- de_DE
- es_ES
- fr_CA
- fr_CH
- fr_FR
- it_CH
- it_IT
- ja_JP
- Ja_JP
- ko_KR
- pt_BR
- zh_CN
- ZH_CN
- zh_TW
- Zh_TW

Il pacchetto della documentazione contiene soltanto la lingua Inglese. Le versioni tradotte della documentazione di Load Balancer si trovano sul sito Web al seguente indirizzo: www.ibm.com/software/webservers/appserv/ecinfocenter.html.

Prima dell'installazione

Se è già stata installata una precedente versione, disinstallarne la copia prima di installare la versione aggiornata. In primo luogo, accertarsi che tutti gli executor e i

server siano stati arrestati. Quindi, disinstallare l'intero prodotto, immettere **installp -u ibmlb** (o il nome precedente, ad esempio, **intnd**). Per disinstallare determinati fileset, elencarli invece di indicare il nome del pacchetto.

Nel momento in cui si disinstalla il prodotto, è possibile scegliere di installare uno o tutti i componenti elencati di seguito:

- Base
- Amministrazione (con messaggi)
- Driver unità (obbligatorio)
- Licenza (obbligatoria)
- Componente Dispatcher (con messaggi)
- Componente CBR (con messaggi)
- Componente Site Selector (con messaggi)
- Componente Cisco CSS Controller (con messaggi)
- Componente Nortel Alteon Controller (con messaggi)
- Documentazione (con messaggi)
- Metric Server

Fasi di installazione

Attenersi alla procedura elencata di seguito per installare Load Balancer in AIX:

1. Accedere come utente root.
2. Inserire il supporto contenente il prodotto oppure, se si sta eseguendo l'installazione dal Web, copiare le immagini di installazione su una directory.
3. Installare l'immagine di installazione. Per installare Load Balancer per AIX si consiglia di utilizzare SMIT, dal momento che questo garantisce l'installazione automatica di tutti i messaggi.

Uso di **SMIT**:

Selezionare

Software Installation and Maintenance

Selezionare

Install and Update Software

Selezionare

Install and update from latest Available Software

Immettere

Il dispositivo o la directory contenente le immagini installp

Immettere

Nella riga *SOFTWARE to Install, inserire le informazioni appropriate per specificare le opzioni (o selezionare List)

Premere

OK

Una volta completato il comando, premere **Done**, quindi selezionare **Exit Smit** dal menu Exit oppure premere **F12**. Se si utilizza SMITTY, premere **F10** per uscire dal programma.

Uso della riga comandi:

Se si esegue l'installazione da un CD, immettere il seguente comando per caricarlo:

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

Fare riferimento alla tabella riportata di seguito per determinare i comandi da immettere per installare i pacchetti Load Balancer desiderati per AIX:

Tabella 2. Comandi di installazione AIX

Base	<code>installp -acXgd device ibmlb.base.rte</code>
Amministrazione (con messaggi)	<code>installp -acXgd device ibmlb.admin.rte</code> <code>ibmlb.msg.language.admin</code>
Driver unità	<code>installp -acXgd device ibmlb.lb.driver</code>
Licenza	<code>installp -acXgd device ibmlb.lb.license</code>
Componenti di Load Balancer (con msg). Tra i componenti sono inclusi: Dispatcher, CBR, Site Selector, Controller Cisco CSS e Controller Nortel Alteon	<code>installp -acXgd device ibmlb.component.rte</code> <code>ibmlb.msg.language.lb</code>
Documenti (con messaggi)	<code>installp -acXgd unità ibmlb.doc.rte</code> <code>ibmlb.msg.en_US.lb</code>
Metric Server	<code>installp -acXgd device ibmlb.ms.rte</code>

dove per *device* si intende:

- `/cdrom` se l'installazione avviene da un CD.
- `/dir` (la directory contenente le immagini installp) se l'installazione avviene da un file system.

Accertarsi che la colonna dei risultati del riepilogo contenga SUCCESS per ciascun componente di Load Balancer che si sta installando (APPLYing). Non proseguire finché tutti i componenti desiderati non verranno installati.

Nota: per creare un elenco di fileset in un'immagine installp, tra cui tutti i cataloghi messaggi disponibili, immettere
`installp -ld device`

dove per *device* si intende:

- `/cdrom` se l'installazione avviene da un CD.
- `/dir` (la directory contenente le immagini installp) se l'installazione avviene da un file system.

Per disinstallare il CD, immettere:

`umount /cdrom`

4. Verificare che il prodotto sia installato. Immettere il seguente comando:

```
lsllpp -h | grep ibmlb
```

Se il prodotto è stato installato completamente, questo comando restituisce quanto segue:

```
ibmlb.base.rte
ibmlb.admin.rte
ibmlb.lb.driver
ibmlb.lb.license
ibmlb.<component>.rte
ibmlb.doc.rte
ibmlb.ms.rte
ibmlb.msg.language.admin
ibmlb.msg.en_US.doc
ibmlb.msg.language.lb
```

I percorsi di installazione di Load Balancer includono quanto segue:

- Amministrazione - `/opt/ibm/edge/lb/admin`
- Componenti di Load Balancer - `/opt/ibm/edge/lb/servers`

- Metric Server - `/opt/ibm/edge/lb/ms`
- Documentazione (*Guida alla gestione*) - `/opt/ibm/edge/lb/documentation`

Per l'amministrazione remota di Load Balancer, utilizzando il metodo RMI (Remote Method Invocation), è necessario installare i pacchetti amministrazione, base, componenti e licenza sul client. Per informazioni sul metodo RMI, vedere "RMI (Remote Method Invocation)" a pagina 254.

Requisiti di sistema e installazione in HP-UX

>Requisiti per i sistemi HP-UX

Per i requisiti hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Installazione di sistemi HP-UX

In questa sezione viene illustrato come installare Load Balancer su HP-UX mediante il CD del prodotto.

Prima dell'installazione

Prima di avviare la procedura di installazione, verificare di essere in possesso dell'autorizzazione root per installare il software.

Se è già stata installata una precedente versione, disinstallarne la copia prima di installare la versione aggiornata. Per prima cosa, accertarsi di avere arrestato sia l'executor che il server. Quindi, per disinstallare Load Balancer, consultare "Istruzioni per la disinstallazione dei pacchetti" a pagina 34.

Fasi di installazione

La Tabella 3 visualizza un elenco di nomi di pacchetti di installazione per Load Balancer e l'ordine necessario per installarli mediante lo strumento di installazione pacchetto del sistema.

Tabella 3. Dettagli sull'installazione del pacchetto HP-UX per Load Balancer

Descrizione pacchetto	Nome pacchetto HP-UX
Base	ibmlb.base
Amministrazione e messaggi	ibmlb.admin ibmlb.nlv- <i>lang</i>
Licenza di Load Balancer	ibmlb.lic
Componenti Load Balancer	ibmlb. <i>component</i>
Documentazione	ibmlb.doc
Metric Server	ibmlb.ms
Note: <ol style="list-style-type: none"> 1. La variabile <i>lang</i> si riferisce alla sostituzione di uno dei seguenti codici specifici della lingua: de_DE, en_US, es_ES, fr_FR, it_IT, ja_JP, ko_KR, zh_CN, zh_TW. 2. La variabile <i>component</i> fa riferimento alla sostituzione di: disp (dispatcher), cbr (CBR), ss (Site Selector), cco (Cisco CSS Controller) o nal (Nortel Alteon Controller). 3. Il pacchetto della documentazione (ibmlb.doc) contiene soltanto la lingua Inglese. Le versioni tradotte della documentazione di Load Balancer si trovano sul sito Web al seguente indirizzo: www.ibm.com/software/webervers/appserv/ecinfocenter.html. 	

Nota: I sistemi HP-UX non supportano la locale Portoghese brasaliano (pt_BR). Le locali supportate su sistemi HP-UX sono:

- de_DE.iso88591
- en_US.iso88591
- es_ES.iso88591
- fr_FR.iso88591
- it_IT.iso88591
- ja_JP.SJIS
- ko_KR.eucKR
- zh_CN.hp15CN
- zh_TW.big5

Istruzioni per l'installazione dei pacchetti

La procedura riportata di seguito illustra le operazioni necessarie al completamento di questa attività.

1. Utilizzare root superuser locale.

```
su - root
Password: password
```

2. Emettere il comando `install` per installare i pacchetti:

```
swinstall -s /origine nome_pacchetto
```

in cui *origine* è il percorso directory assoluto di ubicazione del pacchetto e *nome_pacchetto* è il nome del pacchetto.

Il comando riportato di seguito installa il pacchetto di base di Load Balancer (ibmlb.base), se l'installazione avviene dalla root del CD:

```
swinstall -s /origine ibmlb.base
```

Per installare tutti i pacchetti per Load Balancer emettere il seguente comando, se l'installazione avviene dalla directory root del CD:

```
swinstall -s /origine ibmlb
```

3. Verificare l'installazione dei pacchetti Load Balancer

Emettere il comando **swlist** per elencare tutti i pacchetti installati. Ad esempio,

```
swlist -l fileset ibmlb
```

Istruzioni per la disinstallazione dei pacchetti

Utilizzare il comando **swremove** per disinstallare i pacchetti. I pacchetti devono essere rimossi nell'ordine inverso rispetto all'installazione. Ad esempio, emettere i seguenti comandi:

- Per disinstallare tutti i pacchetti Load Balancer:

```
swremove ibmlb
```

Per disinstallare un singolo pacchetto, ad esempio il componente Dispatcher:

```
swremove ibmlb.disp
```

Requisiti di sistema e installazione in Linux

Requisiti per i sistemi Linux

Per i requisiti hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Installazione per i sistemi Linux

Questa sezione illustra come installare Load Balancer in Linux mediante un CD del prodotto.

Prima dell'installazione

Prima di avviare la procedura di installazione, verificare di essere in possesso dell'autorizzazione root per installare il software.

Se è già stata installata una precedente versione, disinstallarne la copia prima di installare la versione aggiornata. In primo luogo, accertarsi che tutti gli executor e i server siano stati arrestati. Quindi per disinstallare completamente il prodotto, immettere **rpm -e pkgname**. Durante la disinstallazione, invertire l'ordine utilizzato per l'installazione, verificando che i pacchetti di amministrazione vengano disinstallati per ultimi.

Fasi di installazione

Per installare Load Balancer:

1. Preparare l'installazione.

- Accedere come utente root.
- Inserire il supporto del prodotto o scaricare il prodotto dal sito Web e installare l'immagine di installazione utilizzando RPM (Red Hat Packaging Manager).

L'immagine di installazione è un file nel formato **eLBLX-version:tar.z**.

- Decomprimere il file tar in una directory temporanea digitando: **tar -xf eLBLX-version:tar.z**. Il risultato sarà un gruppo di file con estensione .rpm.

Di seguito è riportato un elenco dei pacchetti RPM installabili.

- *ibmlb-base-versione-release.hardw.rpm* (Base)
- *ibmlb-admin-versione-release.hardw .rpm* (Amministrazione)
- *ibmlb-lic-versione-release.hardw.rpm* (Licenza)
- *ibmlb-componente-release-version.hardw.rpm* (Componente di Load Balancer)
- *ibmlb-doc-versione-release.hardw.rpm* (Documentazione)
- *ibmlb-ms-versione-release.hardw.rpm* (Metric Server)

Dove —

- *versione-release* è il rilascio corrente, ad esempio 6.1-0
- *hardw* è uno dei seguenti valori: i386, ppc64, ppc, s390, s390x, x86_64
- *componente* indica uno dei seguenti valori: disp (componente Dispatcher), cbr (componente CBR), ss (componente Site Selector), cco (Cisco CSS Controller), nal (Nortel Alteon Controller)

Il pacchetto della documentazione contiene soltanto la lingua Inglese. Le versioni tradotte della documentazione di Load Balancer si trovano sul sito Web al seguente indirizzo: www.ibm.com/software/webservers/appserv/ecinfocenter.html.

- L'ordine di installazione dei pacchetti è importante. Di seguito viene riportato un elenco di pacchetti necessari e l'ordine in cui dovrebbero essere installati:
 - Base (base)
 - Amministrazione (admin)
 - Licenza (lic)
 - Componenti di Load Balancer (disp, cbr, ss, cco, nal)

- Metric Server (ms)
- Documentazione (doc)

Il comando di installazione dei pacchetti deve essere immesso dalla stessa directory in cui risiedono i file RPM. Per installare ciascun pacchetto, immettere il seguente comando: **rpm -i *package.rpm***.

Sistemi Red Hat Linux: a causa di un problema noto con Red Hat Linux, sarà necessario eliminare i file RPM `_db*` o si verificherà un errore.

- I percorsi di installazione di Load Balancer includono quanto segue:
 - Amministrazione - **/opt/ibm/edge/lb/admin**
 - Componenti di Load Balancer - **/opt/ibm/edge/lb/servers**
 - Metric Server- **/opt/ibm/edge/lb/ms**
 - Documentazione - **/opt/ibm/edge/lb/documentation**
 - Per disinstallare i pacchetti, invertire l'ordine utilizzato per l'installazione, verificando che i pacchetti di amministrazione vengano disinstallati per ultimi.
2. Verificare che il prodotto sia installato. Immettere il seguente comando:

rpm -qa | grep ibmlb

L'installazione del prodotto completo genera un elenco analogo al seguente:

- *ibmlb-base-versione-release*
- *ibmlb-admin-versione-release*
- *ibmlb-lic-versione-release*
- *ibmlb-dsp-versione-release*
- *ibmlb-cbr-versione-release*
- *ibmlb-ss-versione-release*
- *ibmlb-cco-versione-release*
- *ibmlb-nal-versione-release*
- *ibmlb-doc-versione-release*
- *ibmlb-ms-versione-release*

Per l'amministrazione remota di Load Balancer, utilizzando il metodo RMI (Remote Method Invocation), È necessario installare i pacchetti amministrazione, base, componenti e licenza sul client. Per informazioni sul metodo RMI, vedere "RMI (Remote Method Invocation)" a pagina 254.

Requisiti di sistema e installazione in Solaris

Requisiti in Solaris

Per i requisiti hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Installazione in Solaris

Questa sezione illustra come installare Load Balancer su sistemi Solaris mediante il CD del prodotto.

Prima dell'installazione

Prima di avviare la procedura di installazione, verificare di essere in possesso dell'autorizzazione root per installare il software.

Se è già stata installata una precedente versione, disinstallarne la copia prima di installare la versione aggiornata. In primo luogo, verificare di aver arrestato tutti gli *executor* e i *server*. Quindi, per disinstallare Load Balancer, immettere **pkgrm pkgname**.

Fasi di installazione

Per installare Load Balancer:

1. Preparare l'installazione.

- Accedere come utente *root*.
- Inserire il CD-ROM contenente il software Load Balancer nell'apposita unità.

Sul prompt dei comandi, immettere **pkgadd -d pathname**, dove per *pathname* si intende il nome dell'unità CD-ROM o la directory sul disco rigido dove risiede il pacchetto, ad esempio: **pkgadd -d /cdrom/cdrom0/**.

Di seguito è riportato un elenco dei pacchetti visualizzati e l'ordine di installazione consigliato.

- *ibmlbbase* (Base)
- *ibmlbadm* (Amministrazione)
- *ibmlblic* (Licenza)
- *ibmlbdisp* (componente Dispatcher)
- *ibmlbcbr* (componente CBR)
- *ibmlbss* (componente Site Selector)
- *ibmlbcc* (componente Cisco CSS Controller)
- *ibmlbna* (componente Nortel Alteon Controller)
- *ibmlbdoc* (Documentazione)
- *ibmlbms* (Metric Server)

Il pacchetto della documentazione (*ibmlbdoc*) contiene soltanto la lingua Inglese. Le versioni tradotte della documentazione di Load Balancer si trovano sul sito Web al seguente indirizzo: www.ibm.com/software/web servers/appserv/ecinfo center.html.

Se si desidera installare tutti i pacchetti, è sufficiente immettere "all" e premere Invio. Se si desidera installare solo alcuni componenti, immettere i nomi corrispondenti ai pacchetti da installare, separati da uno spazio o da una virgola, quindi premere Invio. Potrebbe essere richiesto di modificare le autorizzazioni sulle directory o file esistenti. Premere Invio o rispondere "yes". È necessario installare i pacchetti dei prerequisiti (l'installazione rispetta l'ordine alfabetico anziché l'ordine dei prerequisiti). Se si sceglie l'opzione "all", rispondere affermativamente ("yes") a tutti i prompt visualizzati per completare l'installazione correttamente.

Se si desidera installare soltanto il componente Dispatcher con la documentazione e Metric Server, è necessario installare i seguenti pacchetti: *ibmlbbase*, *ibmlbadm*, *ibmlblic*, *ibmlbdisp*, *ibmlbdoc* e *ibmlbms*.

Per l'amministrazione remota di Load Balancer, utilizzando il metodo RMI (Remote Method Invocation), è necessario installare i pacchetti amministrazione, base, componenti e licenza sul client. Per informazioni sul metodo RMI, vedere "RMI (Remote Method Invocation)" a pagina 254.

I percorsi di installazione di Load Balancer sono:

- I componenti di Load Balancer risiedono nella directory di installazione **/opt/ibm/edge/lb/servers**.
- Il pacchetto Amministrazione installato risiede nella directory **/opt/ibm/edge/lb/admin**.

- Metric Server installato risiede nella directory `/opt/ibm/edge/lb/ms`.
 - La documentazione installata risiede nella directory `/opt/ibm/edge/lb/documentation`.
2. Verificare che il prodotto sia installato. Immettere il seguente comando: `pkginfo | grep ibm`.

Requisiti di sistema e installazione in Windows

Requisiti per i sistemi Windows

Per i requisiti hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Installazione di sistemi Windows

Questa sezione illustra come installare Load Balancer su sistemi Windows mediante un CD del prodotto.

Pacchetti di installazione

Viene fornita una scelta di pacchetti da installare:

- Amministrazione
- Licenza
- Dispatcher
- Content Based Routing
- Site Selector
- Cisco CSS Controller
- Nortel Alteon Controller
- Documentazione
- Metric Server

Per l'amministrazione remota di Load Balancer, utilizzando il metodo RMI (Remote Method Invocation), è necessario installare i pacchetti amministrazione, base, componenti e licenza sul client. Per informazioni sul metodo RMI, vedere "RMI (Remote Method Invocation)" a pagina 254.

Prima dell'installazione

Limitazioni: La versione Windows di Load Balancer non può essere installata sulla stessa macchina di IBM Firewall.

Prima di iniziare la procedura di installazione, verificare di aver effettuato il collegamento come amministratore o come utente con privilegi amministrativi.

Se è già stata installata una precedente versione, disinstallarne la copia prima di installare la versione aggiornata. Per effettuare la disinstallazione utilizzando **Installazione applicazioni**, attenersi alla seguente procedura:

1. Fare clic su **Start > Impostazioni** (in Windows 2000) > **Pannello di controllo**
2. Fare doppio clic su **Installazione applicazioni**
3. Selezionare *IBM WebSphere Edge Components* (o il nome precedente, ad esempio *IBM Edge Server*)
4. Fare clic sul pulsante **Cambia/Rimuovi**

Fasi di installazione

Per installare Load Balancer:

1. Inserire il CD-ROM di Load Balancer nell'apposita unità, la finestra di installazione viene visualizzata automaticamente.
2. Le operazioni seguenti sono necessarie solo se l'esecuzione automatica del CD non funziona. Utilizzare il pulsante 1 del mouse per effettuare le seguenti attività:
 - Fare clic su **Start**.
 - Selezionare **Esegui**.
 - Specificare l'unità CD-ROM seguita da setup.exe, ad esempio:
`E:\setup`
3. Selezionare la **lingua** in cui leggere le istruzioni del processo di installazione.
4. Fare clic su **OK**.
5. Seguire le istruzioni del programma di installazione.
6. Per modificare l'unità o la directory di destinazione, fare clic su **Sfoglia**.
7. È possibile scegliere di installare "tutti i componenti di Load Balancer" o "solo alcuni componenti".
8. Terminata l'installazione, un messaggio richiede di riavviare il sistema prima di utilizzare Load Balancer. Il riavvio è necessario per garantire che tutti i file vengano installati e che la variabile d'ambiente IBMLBPATH sia aggiunta al registro.

I percorsi di installazione di Load Balancer includono quanto segue:

- Amministrazione – `C:\Program Files\IBM\edge\lb\admin`
- Componenti di Load Balancer – `C:\Program Files\IBM\edge\lb\servers`
- Metric Server – `C:\Program Files\IBM\edge\lb\ms`
- Documentazione (Guida alla gestione) – `C:\Program Files\IBM\edge\lb\documentation`

Nota: Il pacchetto della documentazione nella directory install contiene soltanto la lingua Inglese. Le versioni tradotte della documentazione di Load Balancer si trovano sul sito Web al seguente indirizzo:
www.ibm.com/software/webservers/appserv/ecinfocenter.html.

Parte 2. Componente Dispatcher

Questa sezione fornisce informazioni per una rapida configurazione, considerazioni sulla pianificazione e descrive i metodi di configurazione del componente Dispatcher di Load Balancer. Contiene i seguenti capitoli:

- Capitolo 5, "Configurazione rapida", a pagina 43
- Capitolo 6, "Pianificazione del Dispatcher", a pagina 49
- Capitolo 7, "Configurazione del Dispatcher", a pagina 61
- Capitolo 8, "Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6", a pagina 79

Capitolo 5. Configurazione rapida

Questo esempio di configurazione rapida mostra, appunto, come configurare tre stazioni di lavoro collegate localmente mediante il metodo di inoltro mac del componente Dispatcher, per bilanciare il traffico tra i due server Web. La configurazione è essenzialmente la stessa di quella utilizzata per bilanciare il traffico di altre applicazioni UDP stateless o TCP.

IMPORTANTE: se si sta utilizzando Load Balancer per IPv4 e IPv6, vedere anche Capitolo 8, “Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6”, a pagina 79.

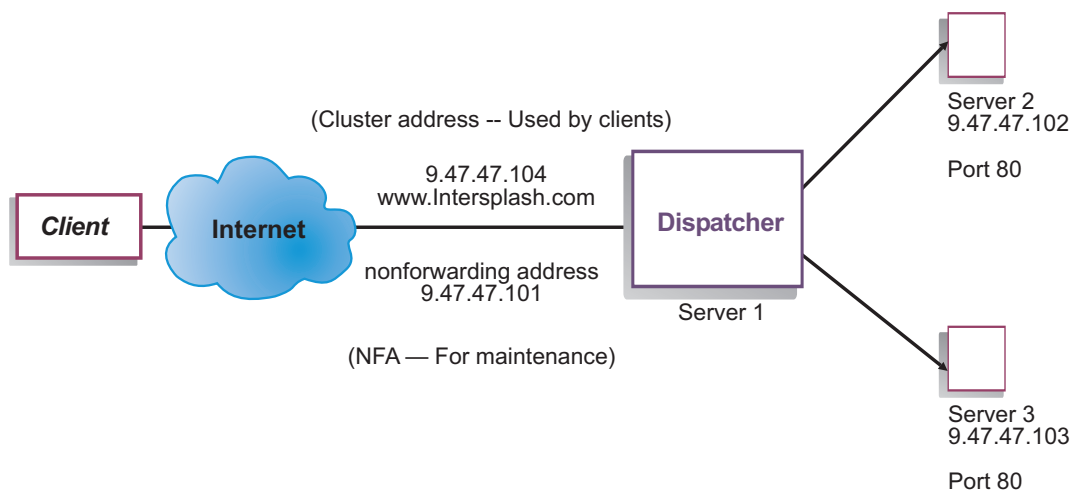


Figura 8. Una semplice configurazione Dispatcher locale

Il metodo di inoltro mac è il metodo predefinito con cui Dispatcher bilancia il carico delle richieste in entrata sul server e il server restituisce la risposta direttamente al client. Per ulteriori informazioni sul metodo di inoltro MAC del componente Dispatcher, consultare “Instradamento a livello MAC del Dispatcher (metodo di inoltro mac)” a pagina 51.

Nota: Questa configurazione può essere completata utilizzando solo due stazioni di lavoro con il Dispatcher collocato su una delle stazioni di lavoro del server Web. Questa configurazione rappresenta una configurazione collocata. Le procedure per l'impostazione di configurazioni più complesse si trovano in “Configurazione della macchina Dispatcher” a pagina 64.

Elementi richiesti

Per l'esempio di avvio rapido, è necessario disporre di tre stazioni di lavoro e di quattro indirizzi IP. Una stazione di lavoro è la macchina del Dispatcher mentre le altre due sono i server Web. Ciascun server Web richiede un indirizzo IP. La stazione di lavoro Dispatcher richiede due indirizzi: l'indirizzo di non inoltro (NFA) e l'indirizzo cluster (l'indirizzo su cui effettuare il bilanciamento del carico) che verranno forniti ai client per poter accedere al sito Web.

Nota: NFA è l'indirizzo restituito dal comando **hostname**. Questo indirizzo viene utilizzato per scopi di gestione, come ad esempio la configurazione remota.

Preparazione

1. Per questo esempio di configurazione di stazioni collegate localmente, impostare le stazioni di lavoro in modo da inserirle nello stesso segmento LAN. Verificare che il traffico di rete tra le tre macchine non debba attraversare router o bridge. Per le configurazioni con server remoti, vedere "Configurazione del supporto di Dispatcher per una rete geografica" a pagina 221).
2. Configurare gli adattatori di rete delle tre stazioni di lavoro. Ad esempio, con la seguente configurazione di rete:

Stazione di lavoro	Nome	Indirizzo IP
1	server1.Intersplashx.com	9.47.47.101
2	server2.Intersplashx.com	9.47.47.102
3	server3.Intersplashx.com	9.47.47.103
Netmask = 255.255.255.0		

Ciascuna stazione di lavoro contiene solo una scheda interfaccia di rete Ethernet standard.

3. Verificare che server1.Intersplashx.com possa eseguire il ping su server2.Intersplashx.com e server3.Intersplashx.com.
4. Verificare che server2.Intersplashx.com e server3.Intersplashx.com possano eseguire il ping su server1.Intersplashx.com.
5. Accertarsi che il contenuto sui due server Web (Server 2 e Server 3) sia identico. Ciò può essere eseguito replicando i dati su entrambe le stazioni di lavoro, utilizzando un file system condiviso, ad esempio NFS, AFS o DFS oppure mediante altri strumenti adatti al sito.
6. Verificare che i server Web su server2.Intersplashx.com e server3.Intersplashx.com siano operativi. Utilizzare un browser Web per richiedere le pagine direttamente da **http://server2.Intersplashx.com** e **http://server3.Intersplashx.com**.
7. Acquisire un indirizzo IP valido per questo segmento LAN. Si tratta dell'indirizzo fornito ai clienti che intendono accedere al sito. In questo esempio si utilizza:

Name= www.Intersplashx.com
IP=9.47.47.104

8. Configurare le due stazioni di lavoro del server Web in modo che accettino il traffico di www.Intersplashx.com.

Aggiungere un alias www.Intersplashx.com all'interfaccia **loopback** su server2.Intersplashx.com e server3.Intersplashx.com.

- Per sistemi AIX:

ifconfig lo0 alias www.Intersplashx.com netmask 255.255.255.0

- Per sistemi Solaris 9:

ifconfig lo0:1 plumb www.Intersplashx.com netmask 255.255.255.0 up

- Per altri sistemi operativi, vedere Tabella 5 a pagina 71.

9. Eliminare eventuali instradamenti supplementari che potrebbero essere stati prodotti come risultato dell'aggiunta dell'alias all'interfaccia loopback. Vedere "Fase 2. Ricerca di un instradamento supplementare" a pagina 74.

A questo punto, tutte le fasi di configurazione necessarie sulle stazioni di lavoro del server Web sono state portate a termine.

Configurazione del componente Dispatcher

Con il Dispatcher, è possibile creare una configurazione dalla riga comandi, con la configurazione guidata o mediante l'interfaccia utente grafica (GUI).

Nota: i valori dei parametri devono essere immessi utilizzando l'alfabeto inglese. Le uniche eccezioni sono rappresentate dai nomi host e dai nomi file.

Configurazione mediante la riga comandi

Se si utilizza la riga comandi:

1. Avviare dsserver sul Dispatcher:
 - Per sistemi AIX, HP-UX, Linux o Solaris, emettere il seguente comando come utente root: **dsserver**
 - Per sistemi Windows, dsserver è in esecuzione come servizio e si avvia automaticamente.
2. Avviare la funzione executor del Dispatcher:
dscontrol executor start
3. Aggiungere l'indirizzo cluster alla configurazione del Dispatcher:
dscontrol cluster add www.Intersplashx.com
4. Aggiungere la porta del protocollo HTTP alla configurazione del Dispatcher:
dscontrol port add www.Intersplashx.com:80
5. Aggiungere ciascun server Web alla configurazione del Dispatcher:
dscontrol server add www.Intersplashx.com:80:server2.Intersplashx.com
dscontrol server add www.Intersplashx.com:80:server3.Intersplashx.com
6. Configurare la stazione di lavoro in modo che accetti il traffico dell'indirizzo cluster:
dscontrol executor configure www.Intersplashx.com
7. Avviare la funzione gestore del Dispatcher:
dscontrol manager start
Dispatcher a questo punto esegue il bilanciamento del carico in base alla prestazioni del server.
8. Avviare la funzione advisor del Dispatcher:
dscontrol advisor start http 80
Il Dispatcher garantisce, a questo punto, che le richieste client non verranno inviate a un server Web in errore.

La configurazione di base, con i server collegati localmente, è ora completa.

Verifica della configurazione

Verificare se la configurazione è in esecuzione:

1. Da un browser Web, andare all'indirizzo **http://www.Intersplashx.com**. Se viene visualizzata una pagina, allora la configurazione funziona correttamente.
2. Ricaricare la pagina nel browser Web.
3. Controllare i risultati del seguente comando: **dscontrol server report www.Intersplashx.com:80:**. La somma totale della colonna connessioni dei due server deve essere "2."

Configurazione mediante l'interfaccia utente grafica (GUI)

Per informazioni sull'uso della GUI di Dispatcher, vedere "GUI" a pagina 63 e Appendice A, "GUI: istruzioni generali", a pagina 455.

Configurazione guidata

Per informazioni sulla configurazione guidata, vedere "Configurazione mediante la procedura guidata" a pagina 64.

Tipi di configurazione cluster, port e server

Esistono molti modi con cui configurare Load Balancer per supportare il sito. Se si dispone di un solo nome host per il sito a cui tutti i clienti vorranno connettersi, è possibile definire un unico cluster di server. Per ognuno di questi server configurare una porta attraverso la quale Load Balancer comunica. Vedere Figura 9.

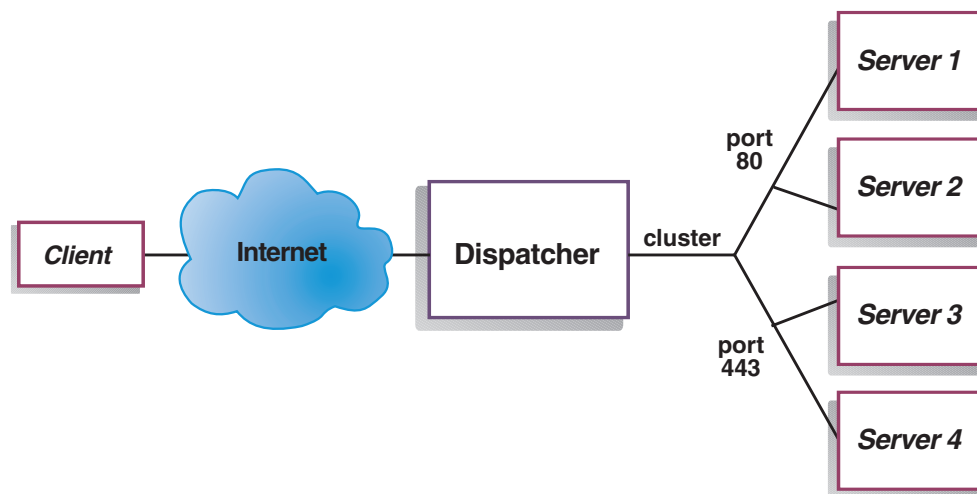


Figura 9. Esempio di Dispatcher configurato con un unico cluster e 2 porte

In questo esempio relativo al componente Dispatcher, un cluster viene definito all'indirizzo `www.productworks.com`. Questo cluster ha due porte: la porta 80 per HTTP e la porta 443 per SSL. Un client che effettua una richiesta all'indirizzo `http://www.productworks.com` (porta 80) viene indirizzato a un server diverso da quello di un client che effettua la richiesta all'indirizzo `https://www.productworks.com` (porta 443).

Se il sito da gestire è molto grande, con un gran numero di server dedicati a ciascun protocollo supportato, potrebbe essere indicato un altro tipo di configurazione di Load Balancer. In tal caso, è possibile definire un cluster per ogni protocollo, con una singola porta ma con molti server, come illustrato in Figura 10 a pagina 47.

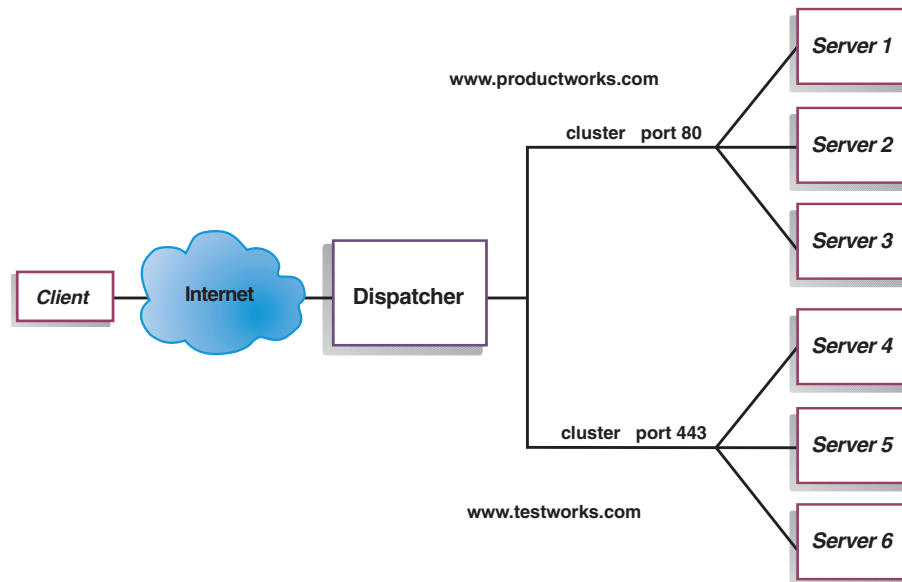


Figura 10. Esempio di Dispatcher configurato con due cluster, ognuno con una porta

In questo esempio relativo al componente Dispatcher, vengono definiti due cluster: `www.productworks.com` per la porta 80 (HTTP) e `www.testworks.com` per la porta 443 (SSL).

È necessario ricorrere a un terzo tipo di configurazione di Load Balancer se il sito gestito deve ospitare i contenuti di più aziende o dipartimenti, a ciascuno dei quali i client accedono utilizzando URL diversi. In questo caso, è possibile definire un cluster per ogni società o dipartimento e, di conseguenza, decidere le porte su cui ricevere le connessioni a quell'URL, come illustrato in Figura 11 a pagina 48.

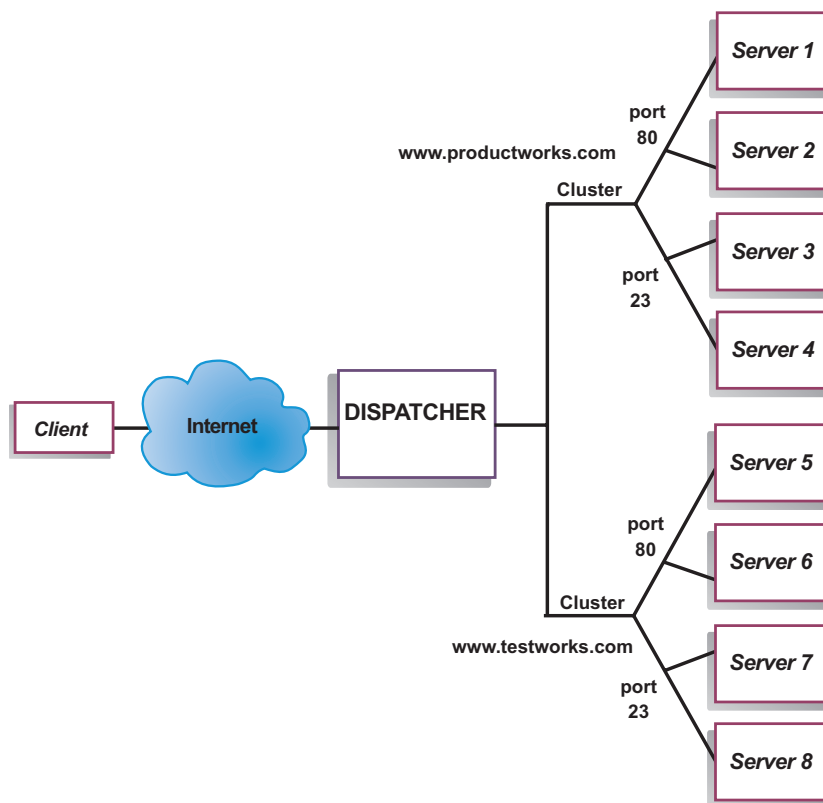


Figura 11. Esempio di Dispatcher configurato con 2 cluster, ognuno con 2 porte

In questo esempio relativo al componente Dispatcher, vengono definiti due cluster con la porta 80 per HTTP e la porta 23 per Telnet per ogni sito all'indirizzo www.productworks.com e www.testworks.com.

Capitolo 6. Pianificazione del Dispatcher

Questo capitolo descrive i fattori che un responsabile della pianificazione di rete deve considerare prima di installare e configurare il componente Dispatcher.

- Vedere Capitolo 3, “Gestione della rete: determinazione delle funzioni di Load Balancer da utilizzare”, a pagina 19, per una panoramica delle opzioni disponibili per la gestione della rete.
- Vedere Capitolo 7, “Configurazione del Dispatcher”, a pagina 61 per informazioni sulla configurazione dei parametri di bilanciamento del carico del Dispatcher.
- Vedere Capitolo 8, “Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6”, a pagina 79, se si sta utilizzando Load Balancer per IPv4 e IPv6.
- Vedere Capitolo 22, “Funzioni avanzate di Dispatcher, CBR e Site Selector”, a pagina 195, per informazioni su come configurare Load Balancer per funzioni più avanzate.
- Vedere Capitolo 24, “Funzionamento e gestione di Load Balancer”, a pagina 253 per informazioni sull’amministrazione autenticata remota, sui log di Load Balancer e sull’uso dei componenti di Load Balancer.

Questo capitolo include le seguenti sezioni:

- “Considerazioni sulla pianificazione”
- “Instradamento a livello MAC del Dispatcher (metodo di inoltro mac)” a pagina 51
- “NAT/NAPT del Dispatcher (metodo di inoltro nat)” a pagina 51
- “Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)” a pagina 53
- “Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)” a pagina 55
- “Disponibilità elevata” a pagina 57

Nota: per le versioni precedenti, quando il prodotto era noto come Network Dispatcher, il nome del comando per il controllo del Dispatcher era `ndcontrol`. Il nome del comando per il controllo del Dispatcher è ora `dscontrol`.

Considerazioni sulla pianificazione

IMPORTANTE: se si sta utilizzando Load Balancer per IPv4 e IPv6, vedere anche Capitolo 8, “Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6”, a pagina 79.

Dispatcher è composto dalle seguenti funzioni:

- **dsserver** gestisce le richieste provenienti dalla riga comandi all’**executor**, al gestore e agli advisor.
- L’**executor** supporta il bilanciamento del carico basato su porte delle connessioni TCP e UDP ed è in grado di inoltrare connessioni ai server in base al tipo di richiesta ricevuta (ad esempio, HTTP, FTP, SSL, ecc.). L’**executor** è sempre in esecuzione quando il componente Dispatcher viene utilizzato per il bilanciamento del carico.
- Il **gestore** imposta i pesi utilizzati dall’**executor** in base a:

- Contatori interni nell’executor
- Informazioni restituite dai server fornite dagli advisor
- Informazioni restituite da un programma di monitoraggio del sistema, ad esempio Metric Server o WLM.

L’uso del gestore è facoltativo. Tuttavia, se il gestore non viene utilizzato, il bilanciamento del carico verrà eseguito utilizzando la pianificazione con il metodo round-robin basata sui pesi dei server correnti, mentre gli advisor non saranno disponibili.

- Gli **advisor** interrogano i server e analizzano i risultati per protocollo prima di interpellare il gestore affinché imposti i pesi in modo appropriato. Al momento, sono disponibili degli advisor per i seguenti protocolli: HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3, SIP e Telnet.

Il Dispatcher fornisce inoltre degli advisor che non scambiano informazioni specifiche sul protocollo, come l’advisor DB2 che riporta lo stato dei server DB2 e l’advisor ping che comunica se il server risponde o meno a un ping. Per un elenco completo degli advisor, vedere “Elenco di advisor” a pagina 184.

È possibile anche scrivere advisor personalizzati (vedere “Creazione di advisor personalizzati” a pagina 188).

L’uso degli advisor è facoltativo ma consigliato.

- Per configurare e gestire l’executor, gli advisor e il gestore, utilizzare la riga comandi (**dscontrol**) o l’interfaccia utente grafica (**lbadmin**).
- È disponibile un **file di configurazione di esempio**, da utilizzare per la configurazione e la gestione della macchina Dispatcher. Vedere Appendice C, “File di configurazione di esempio”, a pagina 467. Dopo aver installato il prodotto, questo file è disponibile nella directory secondaria **...ibm/edge/lb/servers/samples** in cui risiede Load Balancer.
- L’**agente secondario SNMP** consente a un’applicazione di gestione basata su SNMP di monitorare lo stato del Dispatcher.

Le tre funzioni chiave del Dispatcher (executor, gestore e advisor interagiscono per bilanciare e distribuire le richieste in entrata tra i server. Insieme al bilanciamento del carico delle richieste, l’executor controlla il numero delle nuove connessioni, delle connessioni attive e delle connessioni terminate. L’executor esegue inoltre la raccolta di dati inutili di connessioni completate o ripristinate e comunica tali informazioni al gestore.

Il gestore raccoglie le informazioni provenienti dall’executor, dagli advisor e da un programma di monitoraggio del sistema, quale Metric Server. In base alle informazioni ricevute, il gestore regola il peso delle macchine server su ciascuna porta e comunica all’executor i nuovi pesi da utilizzare nel bilanciamento delle nuove connessioni.

Gli advisor controllano ciascun server sulla porta assegnata, per determinare il tempo di risposta del server e la disponibilità, quindi, comunicano queste informazioni al gestore. Anche gli advisor controllano se un server è attivo o meno. Senza il gestore e gli advisor, l’executor esegue una pianificazione con il metodo round-robin basata sui pesi attuali dei server.

Metodi di inoltro

Con il Dispatcher, è possibile selezionare uno dei tre metodi di inoltro specificati a livello di porta: inoltro MAC, NAT/NAPT o CBR (content-based routing).

Instradamento a livello MAC del Dispatcher (metodo di inoltro mac)

Utilizzando il metodo di inoltro MAC del Dispatcher (il metodo di inoltro predefinito), il Dispatcher bilancia il carico delle richieste in entrata al server selezionato e il server restituisce la risposta *direttamente* al client senza coinvolgere il Dispatcher. Con questo metodo di inoltro, il Dispatcher controlla soltanto il traffico entrante dai client verso i server e non gestisce il traffico uscente dai server verso i client. Ciò riduce significativamente il suo impatto sull'applicazione e migliora le prestazioni della rete.

Il metodo di inoltro può essere selezionato quando si aggiunge una porta con il comando **dscontrol port add cluster:port method value**. Il valore del metodo di inoltro predefinito è **mac**. Il parametro **method** può essere specificato solo quando si aggiunge la porta. Dopo aver aggiunto la porta, non è possibile modificare l'impostazione del metodo di inoltro. Per ulteriori informazioni, consultare "dscontrol port — configura le porte" a pagina 369.

Limitazione per Linux: Linux impiega un modello basato su host per comunicare gli indirizzi hardware agli indirizzi IP utilizzando ARP. Questo modello non è compatibile con i requisiti del server backend o del server con disponibilità elevata, per quel che riguarda il metodo di inoltro mac di Load Balancer. Vedere "Alternative per l'aggiunta dell'alias loopback Linux quando si utilizza il metodo di inoltro mac di Load Balancer" a pagina 76, che contiene un numero di soluzioni per modificare il funzionamento del sistema Linux in modo da renderlo compatibile con l'inoltro mac di Load Balancer.

Su Linux, esistono delle limitazioni quando si utilizzano server zSeries o S/390 che hanno schede Open System Adapter (OSA). Fare riferimento a "Problema: su Linux, esistono delle limitazioni alla configurazione del Dispatcher quando si utilizzano server zSeries o S/390 che utilizzano schede Open System Adapter (OSA)" a pagina 312 per le eventuali soluzioni alternative.

NAT/NAPT del Dispatcher (metodo di inoltro nat)

Utilizzando la capacità NAT (Network Address Translation) o NAPT (Network Address Port Translation) del Dispatcher si elimina la limitazione che prevede di dover posizionare i server sottoposti a bilanciamento del carico su una rete collegata localmente. Se si desidera collegare server situati in ubicazioni remote, è possibile utilizzare la tecnica del metodo di inoltro NAT anziché la tecnica di incapsulamento GRE/WAN. È anche possibile utilizzare la funzione NAPT per accedere a più daemon server che risiedono su ciascuna macchina sottoposta a bilanciamento del carico, dove ogni daemon è in ascolto su una specifica porta.

È possibile configurare un server con più daemon in due modi differenti:

- Con NAT, è possibile configurare più daemon server per rispondere alle richieste su indirizzi IP differenti. Questa procedura è nota come collegamento di un daemon server a un indirizzo IP.
- Con NAPT, è possibile configurare più daemon server (in esecuzione sullo stesso server fisico) per essere in ascolto su numeri di porta differenti.

Questa applicazione funziona bene con protocolli di applicazioni di livello superiore come HTTP, SSL, IMAP, POP3, NNTP, SMTP, Telnet, ecc.

Limitazioni:

- L'implementazione di NAT/NAPT nel Dispatcher è un'implementazione *semplice* di questa funzione. Essa analizza e funziona solo sui contenuti delle intestazioni dei pacchetti TCP/IP. Non analizza i contenuti della parte dati dei pacchetti. Per il Dispatcher, NAT/NAPT non funziona con protocolli di applicazioni, quali FTP, che incorporano gli indirizzi o i numeri di porta nella parte dati dei messaggi. Si tratta di una limitazione ben nota dei metodi NAT/NAPT basati su intestazioni.
- I metodi NAT/NAPT del Dispatcher non possono funzionare insieme alla funzione cluster o porta jolly.

Saranno necessari tre indirizzi IP per la macchina Dispatcher – indirizzo nfa, cluster e mittente. Per implementare NAT/NAPT, effettuare quanto segue (vedere anche “Operazioni di esempio per configurare i metodi di inoltro nat o cbr del Dispatcher” a pagina 54):

- Impostare il parametro **clientgateway** sul comando **dscontrol executor set**. Il parametro **clientgateway** è un indirizzo IP utilizzato come indirizzo router attraverso cui il traffico in direzione di ritorno viene inoltrato da Load Balancer ai client. Prima di poter utilizzare NAT/NAPT, è necessario impostare questo valore su un indirizzo IP diverso da zero. Per ulteriori informazioni, consultare “dscontrol executor — controlla l’executor” a pagina 349.
- Aggiungere una porta utilizzando il comando **dscontrol port add cluster:port method value**. Il valore del metodo di inoltro dovrebbe essere impostato su **nat**. Il parametro **method** può essere specificato solo quando si aggiunge la porta. Dopo aver aggiunto la porta, non è possibile modificare l'impostazione del metodo di inoltro. Per ulteriori informazioni, consultare “dscontrol port — configura le porte” a pagina 369.

Nota: se non si imposta un indirizzo gateway del client su un valore diverso da zero, il metodo di inoltro potrà essere solo **mac** (metodo di inoltro basato su MAC).

- Aggiungere un server utilizzando i parametri **mapport**, **returnaddress** e **router** con il comando **dscontrol**. Ad esempio:

```
dscontrol server add cluster:port:server mapport value returnaddress  
rtrnaddress router rtraddress
```

– **mapport** (facoltativo)

Mappa il numero di porta (specifico per il Dispatcher) di destinazione della richiesta client sul numero di porta del server che il Dispatcher utilizza per bilanciare il carico delle richieste del client. Il parametro **mapport** consente a Load Balancer di ricevere una richiesta del client su una porta e di trasmetterla a una porta differente sulla macchina server. Con il parametro **mapport** è possibile bilanciare il carico delle richieste di un client su una macchina server che potrebbe disporre di più daemon server attivi. Il valore predefinito per **mapport** è il numero di porta di destinazione della richiesta client.

– **returnaddress**

L'indirizzo mittente è un indirizzo univoco o un nome host configurato sulla macchina Dispatcher. Il Dispatcher utilizza l'indirizzo mittente come indirizzo di origine quando bilancia il carico delle richieste del client al server. In questo modo, il server restituisce il pacchetto alla macchina Dispatcher, anziché inviarlo direttamente al client. (Il Dispatcher inoltra quindi il pacchetto IP al client.) Quando si aggiunge il server, è necessario specificare il valore dell'indirizzo mittente. Non è possibile modificare l'indirizzo mittente, a meno il server non venga prima rimosso quindi riaggiunto. L'indirizzo mittente non può essere uguale all'indirizzo cluster, server o NFA.

– **router**

L'indirizzo del router al server remoto. Se questo è un server collegato in locale, immettere l'indirizzo del server, a meno che questo non si trovi sulla stessa macchina di Load Balancer. In tal caso, continuare a utilizzare l'indirizzo reale del router.

Per ulteriori informazioni sul comando **dscontrol server** con i parametri **mapport**, **returnaddress** e **router**, vedere “dscontrol server — configura i server” a pagina 381.

Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)

Il componente Dispatcher consente di eseguire l'instradamento basato sul contenuto per HTTP (utilizzando la regola di tipo "contenuto") e HTTPS (utilizzando l'affinità ID di sessione SSL) senza la necessità di utilizzare Caching Proxy. Per il traffico HTTP e HTTPS, il metodo di inoltro cbr del componente Dispatcher può offrire un instradamento basato sul contenuto più rapido rispetto a quello offerto dal componente CBR, che richiede Caching Proxy.

Per HTTP: la selezione del server per l'Instradamento basato sul contenuto di Dispatcher è basata sui contenuti di un'intestazione URL o HTTP. La configurazione avviene utilizzando la regola di tipo "contenuto". Quando si configura la regola contenuto, specificare il "modello" della stringa di ricerca e un insieme di server per la regola. Durante l'elaborazione di una nuova richiesta in entrata, questa regola confronta la stringa specificata con l'URL del client o con l'intestazione HTTP specificata nella richiesta client.

Se il Dispatcher trova la stringa nella richiesta client, inoltra la richiesta a uno dei server nella regola. Il Dispatcher trasmette quindi i dati della risposta dal server al client (metodo di inoltro "cbr").

Se il Dispatcher non trova la stringa nella richiesta client, *non* seleziona alcun server dall'insieme dei server nella regola.

Nota: la regola contenuto viene configurata nella stessa maniera, sia per il componente Dispatcher che per il componente CBR. Il Dispatcher può utilizzare la regola contenuto per il traffico HTTP. Tuttavia, il componente CBR può utilizzare la regola contenuto *sia* per il traffico HTTP che HTTPS (SSL).

Per HTTPS (SSL): l'instradamento basato sul contenuto (cbr) del Dispatcher bilancia il carico in base al campo sessione ID SSL della richiesta client. Con SSL, una richiesta client contiene l'ID sessione SSL di una sessione precedente e i server mantengono una memoria cache delle connessioni SSL precedenti. L'affinità di sessione ID SSL del Dispatcher consente al client e al server di stabilire una nuova connessione utilizzando i parametri di sicurezza della precedente connessione al server. Eliminando la rinegoziazione dei parametri di sicurezza SSL, come le chiavi condivise e gli algoritmi di codifica, i server salvano i cicli della CPU e il client riceve una risposta più velocemente. Per abilitare l'affinità ID di sessione SSL: il tipo **protocol** specificato per la porta deve essere **SSL** e la porta **stickytime** deve essere impostata su un valore diverso da zero. Quando il valore di stickytime viene superato, il client potrebbe essere inviato a un server diverso dal precedente.

Saranno necessari tre indirizzi IP per la macchina Dispatcher – indirizzo nfa, cluster e mittente. Per implementare l'Instradamento basato sul contenuto di

Dispatcher (vedere anche “Operazioni di esempio per configurare i metodi di inoltro nat o cbr del Dispatcher”):

- Impostare il parametro **clientgateway** sul comando **dscontrol executor set**. Il parametro **clientgateway** è un indirizzo IP utilizzato come indirizzo router attraverso cui il traffico in direzione di ritorno viene inoltrato dal Dispatcher ai client. Il parametro **clientgateway** assume il valore zero. Questo valore deve essere impostato su un indirizzo IP diverso da zero prima di poter aggiungere un metodo di inoltro cbr (instradamento basato sul contenuto). Per ulteriori informazioni, consultare “dscontrol executor — controlla l’executor” a pagina 349.
- Aggiungere una porta utilizzando il parametro **method** e il parametro **protocol** sul comando **dscontrol port add**. Il valore del metodo di inoltro dovrebbe essere impostato su **cbr**. Il tipo di protocollo della porta può essere HTTP o SSL. Per ulteriori informazioni, consultare “dscontrol port — configura le porte” a pagina 369.

Nota: se non si imposta un indirizzo gateway del client su un valore diverso da zero, il metodo di inoltro potrà essere solo **mac**.

- Aggiungere un server utilizzando i parametri **mapport**, **returnaddress** e **router**
dscontrol server add cluster:port:server mapport value returnaddress rtraddress router rtraddress

Nota: per informazioni sulla configurazione del server utilizzando i parametri **mapport** (facoltativo), **returnaddress** e **router**, vedere a pagina 52.

- **Per HTTP:** eseguire la configurazione utilizzando le regole basate sul contenuto della richiesta client (tipo di regola **content**). Ad esempio,

dscontrol rule 125.22.22.03:80:contentRule1 type content pattern pattern

Dove *pattern* specifica il modello da utilizzare per il tipo di regola **content**. Per ulteriori informazioni sul tipo di regola **content**, vedere “Utilizzo delle regole basate sul contenuto delle richieste” a pagina 212. Per ulteriori informazioni sulle espressioni valide per *pattern*, vedere Appendice B, “Sintassi della regola di contenuto (modello)”, a pagina 463.

Nota: la funzione di disponibilità elevata per la replica del record delle connessioni (che garantisce che una connessione del client non venga interrotta quando una macchina Dispatcher secondaria assume il controllo al posto della macchina principale) *non* è supportata con l’instradamento basato sul contenuto (cbr) del Dispatcher.

Operazioni di esempio per configurare i metodi di inoltro nat o cbr del Dispatcher

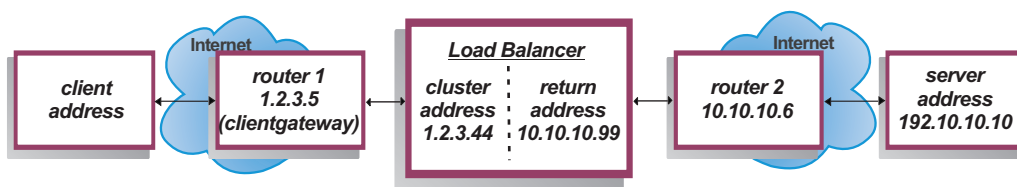


Figura 12. Esempio d'uso dei metodi di inoltro nat o cbr del Dispatcher

Saranno necessari almeno tre indirizzi IP per la macchina Dispatcher. Per la Figura 12 a pagina 54, le operazioni riportate di seguito sono indispensabili per configurare al minimo i metodi di inoltro nat o cbr del Dispatcher:

1. Avviare l'executor
`dscontrol executor start`
2. Definire il gateway client
`dscontrol executor set clientgateway 1.2.3.5`
NOTA: se la sottorete non dispone di un router locale, è necessario configurare una macchina per eseguire l'inoltro IP e utilizzarla come clientgateway. Consultare la documentazione del sistema operativo per determinare come attivare l'inoltro IP.
3. Definire l'indirizzo cluster
`dscontrol cluster add 1.2.3.44`
4. Configurare l'indirizzo cluster
`dscontrol executor configure 1.2.3.44`
5. Definire la porta con un metodo nat o cbr
`dscontrol port add 1.2.3.44:80 method nat`
o
`dscontrol port add 1.2.3.44:80 method cbr protocol http`
6. Configurare un indirizzo mittente alias su Load Balancer (utilizzando la scheda ethernet 0)
NOTA: su sistemi Linux, non è necessario creare un alias per l'indirizzo di restituzione se si u

`dscontrol executor configure 10.10.10.99`

o utilizzare il comando `ifconfig` (solo per Linux o UNIX):
AIX: `ifconfig en0 alias 10.10.10.99 netmask 255.255.255.0`
HP-UX: `ifconfig lan0:1 10.10.10.99 netmask 255.255.255.0 up`
Linux: `ifconfig eth0:1 10.10.10.99 netmask 255.255.255.0 up`
Solaris: `ifconfig eri0 addif 10.10.10.99 netmask 255.255.255.0 up`
7. Definire i server backend
`dscontrol server add 1.2.3.4:80:192.10.10.10`
`router 10.10.10.6 returnaddress 10.10.10.99`

Il gateway client (1.2.3.5) è l'indirizzo router 1 tra Load Balancer e il client. Il router (10.10.10.6) è l'indirizzo router 2 tra Load Balancer e il server backend. In caso di dubbi sull'indirizzo clientgateway o router 2, è possibile utilizzare un programma denominato `tracert` con l'indirizzo client (o server) per determinare l'indirizzo router. La sintassi esatta di questo programma differisce in base al sistema operativo utilizzato. È preferibile consultare la documentazione del sistema operativo per ulteriori informazioni circa questo programma.

Se il server si trova sulla stessa rete di Load Balancer (ossia, non vengono restituiti router mediante `tracert`), specificare l'indirizzo server come indirizzo router. Tuttavia, se il server si trova sulla stessa macchina di Load Balancer, nel campo del router va immesso l'indirizzo del router e non l'indirizzo del server. L'indirizzo router è l'indirizzo utilizzato nel comando "server add" sulla macchina Load Balancer al punto 7.

Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)

Con la suddivisione in partizioni del server, è possibile distinguere ulteriormente tra URL particolari e relative applicazioni specifiche. Ad esempio, un server Web può supportare pagine JSP, pagine HTML, file GIF, richieste database e così via. Load Balancer consente ora di suddividere in partizioni un server specifico di una

porta o di un cluster in più server logici. In questo modo, l'utente può fornire informazioni su uno specifico servizio su una macchina per rilevare se un motore servlet o una richiesta database è in esecuzione più velocemente o non lo è affatto.

La suddivisione in partizioni del server consente a Load Balancer di individuare, ad esempio, se il servizio HTML sta servendo le pagine velocemente ma la connessione al database è interrotta. Ciò consente di distribuire il carico in base a un carico di lavoro differenziando i diversi servizi, piuttosto che calcolare solo i pesi dei vari server.

Suddivisione in partizioni del server mediante advisor HTTP o HTTPS

La suddivisione in partizioni del server può essere utile se utilizzata insieme agli advisor HTTP e HTTPS. Ad esempio, con un server HTML che gestisce pagine HTML, GIF e JSP, se si definisce una volta (mediante aggiunta) il server nella porta 80, si riceve solo un valore di carico per l'intero server HTTP. Ciò può essere fuorviante in quanto è possibile che il servizio GIF non sia operativo sul server. Il Dispatcher continua a inoltrare pagine GIF al server ma il client riscontra un timeout o un errore.

Se si definisce il server tre volte (ad esempio, ServerHTML, ServerGIF, ServerJSP) nella porta e si definisce il parametro **advisorrequest** del server con una stringa differente per ciascun server logico, è possibile eseguire una query relativa allo stato di uno specifico servizio sul server. ServerHTML, ServerGIF e ServerJSP rappresentano tre server logici che sono stati suddivisi in partizioni da un unico server fisico. Per ServerJSP, è possibile definire la stringa **advisorrequest** per eseguire una query relativa al servizio sulla macchina che gestisce le pagine JSP. Per ServerGIF, è possibile definire la stringa **advisorrequest** per eseguire la query relativa al servizio GIF. Infine, per ServerHTML, si definisce la stringa **advisorrequest** per eseguire una query relativa al servizio HTML. In questo modo, se il client non riceve risposta da **advisorrequest** alla query relativa al servizio GIF, il Dispatcher contrassegnerà il server logico (ServerGIF) come inattivo, mentre gli altri due potrebbero essere attivi. Il Dispatcher non inoltra altre pagine GIF al server fisico ma può ancora inviare richieste JSP e HTML al server.

Per ulteriori informazioni sul parametro **advisorrequest**, vedere "Configurazione dell'advisor HTTP o HTTPS utilizzando l'opzione richiesta/risposta (URL)" a pagina 186.

Esempio di configurazione di un server fisico in server logici

All'interno della configurazione del Dispatcher, è possibile rappresentare un server fisico o un server logico utilizzando la gerarchia *cluster:port:server*. Il server può essere un indirizzo IP univoco della macchina (server fisico) espresso come nome simbolico o in formato indirizzo IP. Altrimenti, se si definisce il server per rappresentare un server suddiviso in partizioni, è necessario specificare un indirizzo server risolvibile per il server fisico sul parametro **address** del comando **dscontrol server add**. Per ulteriori informazioni, consultare "dscontrol server — configura i server" a pagina 381.

Segue un esempio di suddivisione in partizioni di server fisici in server logici, per gestire differenti tipi di richieste.

```
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 questo esempio, il server 1.1.1.2 è suddiviso in 2 server logici: "A" (che gestisce le richieste HTML) e "B" (che gestisce le richieste GIF). Il server 1.1.1.3 è suddiviso in 2 server logici: "C" (che gestisce le richieste HTML) e "D" (che gestisce le richieste JSP). Il server 1.1.1.4 è suddiviso in 2 server logici: "E" (che gestisce le richieste GIF) e "F" (che gestisce le richieste JSP).

Disponibilità elevata

Disponibilità elevata di tipo semplice

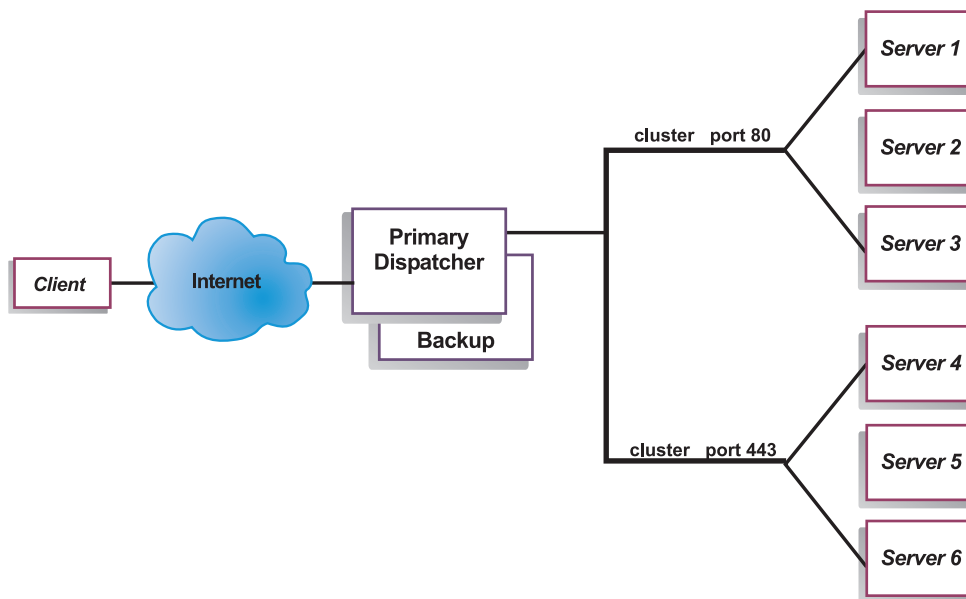


Figura 13. Esempio di un Dispatcher che utilizza la disponibilità elevata di tipo semplice

La funzione di disponibilità elevata implica l'uso di una seconda macchina Dispatcher. La prima macchina Dispatcher esegue il bilanciamento del carico per tutto il traffico client, come in una configurazione a un solo Dispatcher. La seconda macchina Dispatcher controlla lo "stato" della prima e assume il controllo delle attività di bilanciamento del carico se rileva un malfunzionamento sulla prima macchina Dispatcher.

A ciascuna delle due macchine viene assegnato un ruolo specifico, ossia *primary* (principale) o *backup* (secondario). La macchina principale invia continuamente i dati di connessione alla macchina secondaria. Mentre la macchina principale è *attiva* (ed esegue il bilanciamento del carico), la macchina secondaria si trova in *standby*, aggiornata di continuo e pronta ad assumere il controllo, se necessario.

Le sessioni di comunicazione tra le due macchine vengono denominate *heartbeat*. Gli heartbeat consentono a ciascuna macchina di controllare lo stato dell'altra.

Se la macchina secondaria rileva un malfunzionamento della macchina attiva, assumerà il controllo e inizierà a eseguire il bilanciamento del carico. A quel punto, gli *stati* delle due macchine si invertono: la macchina secondaria diventa *attiva* mentre la macchina principale passa in *standby*.

Nella configurazione a disponibilità elevata, sia la macchina principale che quella secondaria si trovano sulla stessa sottorete con configurazione identica.

Per informazioni sulla configurazione della disponibilità elevata, vedere "Disponibilità elevata" a pagina 198.

Disponibilità elevata reciproca

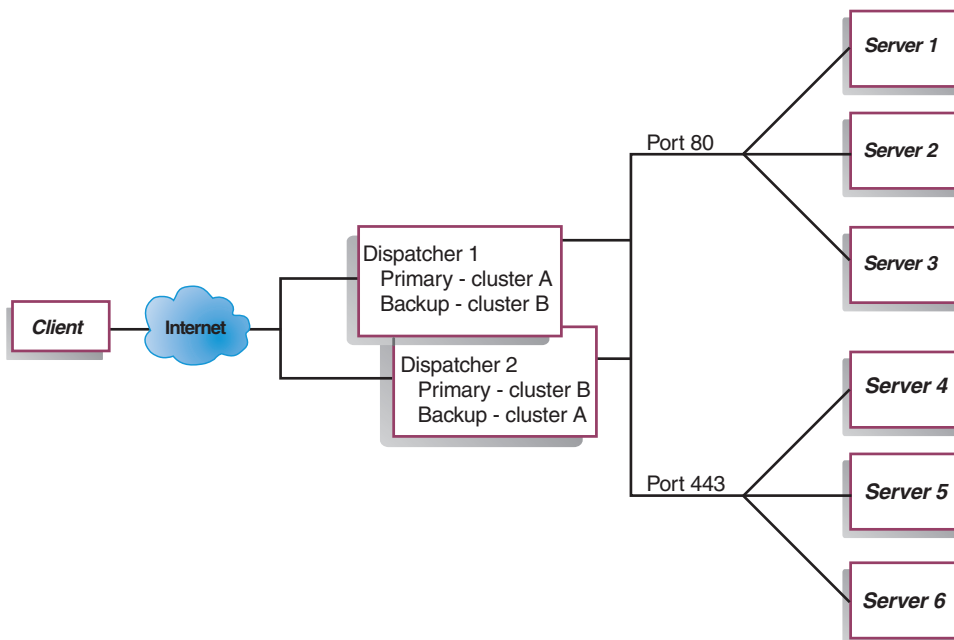


Figura 14. Esempio di un Dispatcher che utilizza la disponibilità elevata reciproca

La funzione di disponibilità elevata reciproca implica l'uso di due macchine Dispatcher. Entrambe le macchine eseguono attivamente il bilanciamento del carico del traffico client e fungono da backup l'una per l'altra. In una configurazione a disponibilità elevata di tipo semplice, solo una macchina esegue il bilanciamento del carico. In una configurazione a disponibilità elevata reciproca, entrambe le macchine eseguono il bilanciamento del carico di una parte del traffico client.

Per la disponibilità elevata reciproca, il traffico client viene assegnato a ciascuna macchina Dispatcher in base all'indirizzo cluster. Ciascun cluster può essere configurato con l'NFA (nonforwarding address) del Dispatcher principale. La

macchia Dispatcher principale normalmente esegue il bilanciamento del carico per quel cluster. Nel caso di un malfunzionamento, l'altra macchina eseguirà il bilanciamento del carico sia per il proprio cluster che per il cluster del Dispatcher malfunzionante.

Per un'illustrazione di una configurazione a disponibilità elevata reciproca con il "gruppo di cluster A" e il "gruppo di cluster B" condivisi, vedere Figura 14 a pagina 58. Ciascun Dispatcher può attivamente instradare pacchetti per il proprio cluster *principale*. Se uno dei Dispatcher ha riscontrato un errore e non può più inviare attivamente pacchetti per il proprio cluster principale, l'altro Dispatcher può assumere il controllo e instradare pacchetti per il proprio cluster *secondario*.

Nota: in entrambe le macchine, la configurazione dei gruppi di cluster condivisi deve essere identica. Ossia, le porte utilizzate e i server in ciascuna porta devono essere identici nelle due configurazioni.

Per informazioni sulla configurazione della disponibilità elevata semplice e reciproca, vedere "Disponibilità elevata" a pagina 198.

Capitolo 7. Configurazione del Dispatcher

Prima di eseguire le operazioni riportate in questo capitolo, vedere Capitolo 6, “Pianificazione del Dispatcher”, a pagina 49. Questo capitolo illustra come creare una configurazione di base per il componente Dispatcher di Load Balancer.

- Vedere Capitolo 8, “Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6”, a pagina 79, se si sta utilizzando Load Balancer per IPv4 e IPv6.
- Vedere Capitolo 21, “Funzioni gestore, advisor e Metric Server per Dispatcher, CBR e Site Selector”, a pagina 175 e Capitolo 22, “Funzioni avanzate di Dispatcher, CBR e Site Selector”, a pagina 195 per configurazioni più complesse di Load Balancer.
- Vedere Capitolo 24, “Funzionamento e gestione di Load Balancer”, a pagina 253 per informazioni sull’amministrazione autenticata remota, sui log di Load Balancer e sull’uso dei componenti di Load Balancer.

Nota: per le versioni precedenti, quando il prodotto era noto come Network Dispatcher, il nome del comando per il controllo del Dispatcher era `ndcontrol`. Il nome del comando per il controllo del Dispatcher è ora `dscontrol`.

Panoramica delle attività di configurazione

IMPORTANTE: se si sta utilizzando Load Balancer per IPv4 e IPv6, vedere Capitolo 8, “Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6”, a pagina 79.

Prima di iniziare le procedure di configurazione contenute nella tabella, verificare che la macchina Dispatcher e tutte le macchine server siano collegate in rete, abbiano indirizzi IP validi e siano in grado di eseguire il ping reciprocamente.

Tabella 4. Attività di configurazione per la funzione Dispatcher

Attività	Descrizione	Informazioni correlate
Configurazione della macchina Dispatcher.	Configurazione del bilanciamento del carico.	“Configurazione della macchina Dispatcher” a pagina 64
Configurazione delle macchine da sottoporre a bilanciamento del carico.	Creazione dell’alias dell’unità loopback, ricerca di instradamenti supplementari ed eventuale eliminazione di questi ultimi.	“Configurazione delle macchine server per il bilanciamento del carico” a pagina 70

Metodi di configurazione

Per configurare il Dispatcher, sono disponibili quattro metodi di base:

- Riga comandi
- Script
- Interfaccia utente grafica (GUI)
- Configurazione guidata

Riga comandi

Si tratta del metodo più diretto per configurare il Dispatcher. I valori dei parametri dei comandi devono essere immessi utilizzando l'alfabeto inglese. Le uniche eccezioni sono i nomi host (utilizzati in cluster, server e comandi highavailability) e i nomi file (utilizzati in comandi file).

Per avviare il Dispatcher dalla riga comandi:

1. Emettere **dsserver** dal prompt dei comandi. Per arrestare il servizio, immettere: **dsserver stop**

Nota: Su sistemi Windows, fare clic su **Start > Impostazioni** (per Windows 2000)> **Pannello di controllo > Strumenti di amministrazione > Servizi**. Fare clic con il tasto destro del mouse su **IBM Dispatcher**, quindi selezionare **Avvia**. Per arrestare il servizio, effettuare le stesse operazioni e selezionare **Arresta**.

2. Quindi, emettere i comandi di controllo del Dispatcher desiderati per impostare la propria configurazione. Le procedure descritte nel presente manuale presumono l'uso della riga comandi. Il comando è **dscontrol**. Per ulteriori informazioni sui comandi, vedere Capitolo 27, "Riferimenti sui comandi per Dispatcher e CBR", a pagina 337.

È possibile utilizzare una versione ridotta dei parametri del comando **dscontrol**, immettendo le lettere che designano in modo univoco i parametri. Ad esempio, per visualizzare la guida del comando di salvataggio file, è possibile immettere **dscontrol he f** anziché **dscontrol help file**.

Per attivare l'interfaccia della riga comandi: emettere **dscontrol** per ricevere un prompt dei comandi **dscontrol**.

Per chiudere l'interfaccia della riga comandi: emettere **exit** o **quit**.

Script

È possibile immettere i comandi per la configurazione di Dispatcher in un file script di configurazione per eseguirli tutti insieme. Vedere "File di configurazione di Load Balancer di esempio" a pagina 467.

Nota: Per eseguire rapidamente il contenuto di un file di script (ad esempio, *myscript*), utilizzare uno dei seguenti comandi:

- Per aggiornare la configurazione corrente, eseguire i comandi eseguibili dal proprio file di script:

dscontrol file appendload *myscript*

- Per sostituire completamente la configurazione corrente, eseguire i comandi eseguibili dal proprio file di script:

dscontrol file newload *myscript*

Per salvare la configurazione corrente nel file di script (ad esempio, *savescript*), eseguire il comando:

dscontrol file save *savescript*

Questo comando salva il file di script della configurazione nella directory **...ibm/edge/lb/servers/configurations/dispatcher**.

GUI

Per istruzioni generali e un esempio della GUI, vedere Figura 41 a pagina 456.

Per avviare la GUI, effettuare quanto segue:

1. Verificare che **dsserver** sia in esecuzione
 - Su sistemi AIX, HP-UX, Linux o Solaris, emettere il seguente comando come root:
dsserver
 - Su sistemi Windows, **dsserver** viene eseguito come servizio che viene avviato automaticamente.
2. A seconda del sistema operativo utilizzato, effettuare una delle seguenti operazioni:
 - Su sistemi AIX, HP-UX, Linux o Solaris immettere **lbadm**
 - Su sistemi Windows fare clic su **Start > Programmi > IBM WebSphere > Edge Components > IBM Load Balancer > Load Balancer**

Per configurare il componente Dispatcher dalla GUI, è necessario anzitutto selezionare **Dispatcher** nella struttura ad albero. È possibile avviare l'executor e il gestore dopo essersi collegati a un host. Inoltre, è possibile creare cluster contenenti porte e server e avviare gli advisor per il gestore.

La GUI può essere utilizzata per eseguire le operazioni che verrebbero effettuate con il comando **dscontrol**. Ad esempio, per definire un cluster utilizzando la riga comandi, si deve immettere il comando **dscontrol cluster add cluster**. Per definire un cluster dalla GUI, fare clic con il tasto destro del mouse su **Executor**, quindi nel menu a comparsa fare clic con il tasto sinistro del mouse su **Add Cluster**. Immettere l'indirizzo del cluster nella finestra a comparsa, quindi fare clic su **OK**.

I file di configurazione Dispatcher esistenti possono essere caricati utilizzando l'opzione **Load New Configuration** (per sostituire completamente la configurazione corrente) e l'opzione **Append to Current Configuration** (per aggiornare la configurazione corrente), contenute nel menu a comparsa **Host**. Salvare periodicamente la configurazione Dispatcher su un file utilizzando l'opzione **Save Configuration File As** contenuta nel menu a comparsa **Host**. Il menu **File** situato sulla parte superiore della GUI consente di salvare le connessioni host correnti in un file o di ripristinare le connessioni nei file esistenti per tutti i componenti di Load Balancer.

I comandi di configurazione possono essere eseguiti anche da remoto. Per ulteriori informazioni, vedere "RMI (Remote Method Invocation)" a pagina 254.

Per eseguire un comando dalla GUI: evidenziare il nodo Host dalla struttura ad albero della GUI e selezionare **Send command....** dal menu a comparsa Host. Nel campo di immissione dei comandi, digitare il comando che si desidera eseguire, ad esempio: **executor report**. I risultati e la cronologia dei comandi in esecuzione nella sessione corrente vengono visualizzati nella finestra fornita.

È possibile accedere alla guida (**Help**) facendo clic sull'icona punto interrogativo nell'angolo in alto a destra della finestra di Load Balancer.

- **Help: Field level** — descrive i valori predefiniti di ciascun campo
- **Help: How do I** — elenca le attività possibili da questa schermata
- **InfoCenter** — consente l'accesso centralizzato alle informazioni sul prodotto

Per ulteriori informazioni sull'uso della GUI, vedere Appendice A, "GUI: istruzioni generali", a pagina 455.

Configurazione mediante la procedura guidata

Se si utilizza la configurazione guidata, effettuare quanto segue:

1. Avviare dserver sul Dispatcher:
 - Su sistemi AIX, HP-UX, Linux o Solaris, emettere quanto riportato di seguito come utente root:
dserver
 - Per sistemi Windows, dserver è in esecuzione come servizio e si avvia automaticamente.
2. Avviare la funzione della procedura guidata del Dispatcher, **dswizard**.

La procedura guidata illustra nei dettagli come creare una configurazione di base del componente Dispatcher. L'utente dovrà rispondere ad alcune domande circa la rete e riceverà tutte le informazioni necessarie per impostare un cluster del Dispatcher per bilanciare il traffico tra un gruppo di server.

Configurazione della macchina Dispatcher

Per poter configurare la macchina Dispatcher, è necessario disporre dei diritti utente root (per AIX, HP-UX, Linux o Solaris) o amministratore su Windows.

Su tutte le piattaforme supportate, Load Balancer può disporre di un server **posizionato**. Ciò significa che Load Balancer può fisicamente risiedere su una macchina server su cui sta eseguendo il bilanciamento del carico.

Per la macchina Dispatcher, quando si utilizza il metodo di inoltro mac, saranno necessari almeno due indirizzi IP validi. Per il metodo di inoltro cbr o nat, saranno necessari almeno tre indirizzi IP validi:

- Un indirizzo IP specifico per la macchina Dispatcher
Si tratta dell'indirizzo IP principale della macchina Dispatcher, noto come NFA (nonforwarding address, indirizzo non inoltrabile). Per impostazione predefinita, questo indirizzo è identico a quello restituito dal comando **hostname**. Utilizzare questo indirizzo per collegarsi alla macchina per scopi di gestione, ad esempio, per eseguire una configurazione remota using Telnet o per accedere all'agente secondario SNMP. Se la macchina Dispatcher può già eseguire il ping su altre macchine sulla rete, non sono necessarie ulteriori operazioni per impostare l'indirizzo di non inoltro.
- Un indirizzo IP per ciascun cluster
Un indirizzo cluster è un indirizzo associato a un nome host (ad esempio, www.yourcompany.com). Questo indirizzo IP viene utilizzato da un client per collegarsi ai server di un cluster. Si tratta dell'indirizzo sottoposto a bilanciamento del carico dal Dispatcher.
- Per il metodo di inoltro cbr o nat, un indirizzo IP per l'indirizzo mittente
Il Dispatcher utilizza l'indirizzo mittente come indirizzo di origine quando bilancia il carico delle richieste del client al server. In questo modo, il server restituisce il pacchetto alla macchina Dispatcher, anziché inviarlo direttamente al client. (Il Dispatcher inoltra quindi il pacchetto IP al client.) Quando si aggiunge il server, è necessario specificare il valore dell'indirizzo mittente. Non è possibile modificare l'indirizzo mittente, a meno il server non venga prima rimosso quindi riaggiunto.

Solo su sistemi Solaris:

- Per impostazione predefinita, il Dispatcher è configurato per bilanciare il carico del traffico su schede di interfaccia di rete (NIC) Ethernet 100Mbps. La scheda Ethernet 100Mbps predefinita viene specificata in `ibmlb.conf` come `eri`. Tuttavia, è fornito un supporto anche per altri tipi di schede, quali `le`, `ce`, `ge`, `hme`, `eri`, `bge`, `vge`, `qfe`, `dfme`, `fjgi` e `fjge`.

Ad esempio, per modificare le impostazioni predefinite, modificare il file `/opt/ibm/edge/lb/servers/ibmlb.conf` come segue:

- Per utilizzare una scheda Ethernet 10 Mbps, sostituire `eri` con `le`.
- Per utilizzare una scheda Ethernet 1Gbps, sostituire `eri` con `ge`.
- Per utilizzare una scheda multiport, sostituire `eri` con `qfe`.

Per supportare più tipi di schede, replicare la riga nel file `ibmlb.conf` e modificare ciascuna riga in modo che corrisponda al tipo di unità.

Ad esempio, se si desidera utilizzare due schede Ethernet da 100Mbps, è necessario inserire un'unica riga nel file `ibmlb.conf` specificando la scheda `eri`.

Se invece si intende utilizzare una scheda Ethernet 10Mbps e una scheda Ethernet 100Mbps, il file `ibmlb.conf` conterrà due righe: una che specifica l'unità `le` e l'altra che specifica l'unità `eri`.

Nota: Il file `ibmlb.conf` fornisce l'input per il comando `autopush` Solaris e deve essere compatibile con il comando `autopush`.

- Per determinare il tipo di interfaccia di rete Ethernet in uso sulla macchina, emettere il seguente comando dal prompt di Solaris:

```
ifconfig -a
```

Se viene visualizzato il seguente output:

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL>
    mtu 8232 index 1 inet 127.0.0.1 netmask ff000000
eri0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
    mtu 1500 index 2 inet 9.42.93.208
    netmask fffffc00 broadcast 9.42.95.255 ether 0:3:ba:2d:24:45
```

allora è necessario modificare il file `ibmlb.conf` come riportato di seguito:

```
eri -1 0 ibmlb
```

- L'avvio e l'arresto dell'executor Dispatcher deconfigura tutti gli alias sulle schede elencate nel file `ibmlb.conf`. Per riconfigurare automaticamente gli alias sulle schede suddette (ad eccezione di quelle destinate a essere utilizzate dal componente Dispatcher di Load Balancer) utilizzare il file script `goAliases`. Uno script di esempio è disponibile nella directory `...ibm/edge/lb/servers/samples` e deve essere spostato in `...ibm/edge/lb/servers/bin` prima di poterlo eseguire. Lo script `goAliases` viene eseguito automaticamente al momento dell'avvio o dell'arresto dell'executor Dispatcher.

Ad esempio, se i cluster X e Y sono configurati per essere utilizzati dal componente CBR su una delle schede elencate in `ibmlb.conf`, i cluster X e Y vengono deconfigurati nel momento in cui vengono emessi i comandi `dscontrol executor start` o `dscontrol executor stop`. Questo potrebbe non essere il risultato desiderato. Quando i cluster X e Y vengono configurati nello script `goAliases`, i cluster vengono automaticamente riconfigurati dopo l'avvio o l'arresto dell'executor Dispatcher.

Verificare che l'inoltro IP non sia abilitato per il protocollo TCP/IP.

La Figura 15 mostra un esempio di Dispatcher impostato con un cluster, due porte e tre server.

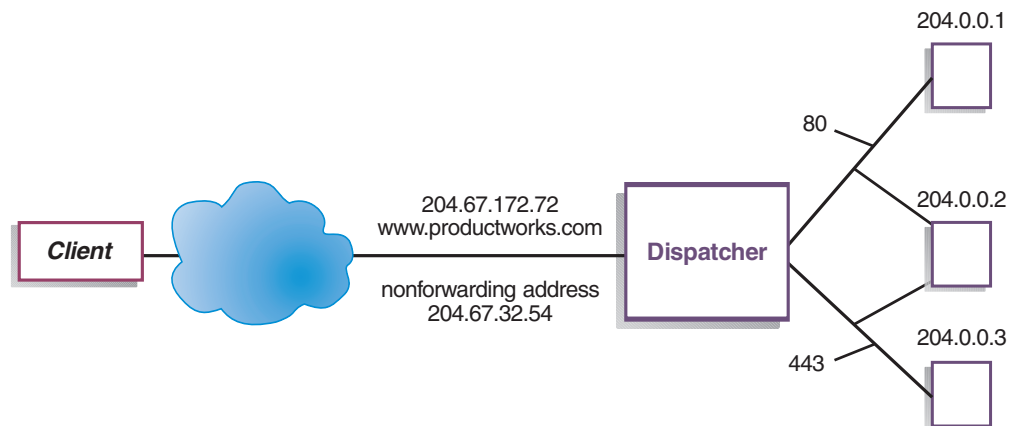


Figura 15. Esempio degli indirizzi IP necessari per la macchina Dispatcher

Per la guida dei comandi utilizzati in questa procedura, vedere Capitolo 27, “Riferimenti sui comandi per Dispatcher e CBR”, a pagina 337.

Per un file di configurazione di esempio, vedere “File di configurazione di Load Balancer di esempio” a pagina 467.

Fase 1. Avvio della funzione server

Su sistemi **AIX**, **HP-UX**, **Linux** o **Solaris**: per avviare la funzione server, immettere **dsserver**.

Su sistemi **Windows**: la funzione server viene avviata automaticamente come servizio.

Nota: un file di configurazione predefinito (default.cfg) viene automaticamente caricato all’avvio di **dsserver**. Se l’utente decide di salvare la configurazione Dispatcher in default.cfg, tutto quello che è stato salvato in questo file verrà automaticamente caricato al successivo avvio di **dsserver**.

Fase 2. Avvio della funzione executor

Per avviare la funzione executor, immettere il comando **dscontrol executor start**. In questa fase, è possibile anche modificare le varie impostazioni dell’executor. Vedere Capitolo 27, “Riferimenti sui comandi per Dispatcher e CBR”, a pagina 337.

Fase 3. Definizione dell’indirizzo non inoltrabile (se diverso dal nome host)

L’indirizzo non inoltrabile viene adoperato per collegarsi alla macchina per scopi di gestione, ad esempio per utilizzare Telnet o SMTP. Per impostazione predefinita, questo indirizzo è il nome host.

Per definire l’indirizzo non inoltrabile, immettere il comando **dscontrol executor set nfa IP_address** o modificare il file di configurazione di esempio. Per **IP_address** è possibile specificare il nome simbolico o l’indirizzo IP.

Fase 4. Definizione di un cluster e impostazione delle relative opzioni

Il Dispatcher esegue il bilanciamento del carico delle richieste inviate all'indirizzo cluster per i server configurati sulle porte del cluster specificato.

Il cluster può essere il nome simbolico, l'indirizzo in formato decimale puntato o l'indirizzo speciale 0.0.0.0, che definisce un cluster jolly. Per definire un cluster, emettere il comando **dscontrol cluster add**. Per impostare le opzioni del cluster, emettere il comando **dscontrol cluster set** oppure utilizzare la GUI per emettere i comandi. I cluster jolly possono essere utilizzati per individuare più indirizzi IP per i pacchetti in entrata su cui eseguire il bilanciamento del carico. Consultare "Utilizzo del cluster jolly per combinare le configurazioni di server" a pagina 229, "Utilizzo di cluster jolly per bilanciare il carico dei firewall" a pagina 230 e "Utilizzo del cluster jolly con Caching Proxy per proxy trasparente" a pagina 230, per ulteriori informazioni.

Fase 5. Creazione dell'alias della scheda di interfaccia di rete (NIC)

Normalmente, dopo aver definito il cluster, è necessario configurare l'indirizzo cluster su una delle schede di interfaccia di rete della macchina Dispatcher. A tale scopo, emettere il comando **dscontrol executor configure cluster_address**. In questo modo, verrà ricercata una scheda con un indirizzo esistente che appartiene alla stessa sottorete dell'indirizzo cluster. Verrà quindi emesso il comando di configurazione della scheda del sistema operativo per l'indirizzo cluster, utilizzando la scheda individuata e la maschera di rete dell'indirizzo esistente di quella scheda. Ad esempio:

```
dscontrol executor configure 204.67.172.72
```

In alcuni casi, che prevedono cluster aggiunti a un server in standby in modalità a disponibilità elevata o cluster aggiunti a un dispatcher all'interno di una rete geografica che funge da server remoto, è preferibile non configurare l'indirizzo cluster. Inoltre, non è necessario eseguire il comando **executor configure** se, in modalità autonoma, si utilizza lo script di esempio **goldle**. Per informazioni sullo script **goldle**, vedere "Utilizzo di script" a pagina 202.

In rari casi, l'indirizzo cluster a disposizione potrebbe non coincidere con nessuna delle sottoreti degli indirizzi esistenti. In questo caso, utilizzare il secondo formato del comando **executor configure** e specificare in modo esplicito il nome dell'interfaccia e la maschera di rete. Utilizzare **dscontrol executor configure cluster_address interface_name netmask**.

Di seguito sono riportati alcuni esempi:

```
dscontrol executor configure 204.67.172.72 en0 255.255.0.0
(sistemi AIX)
dscontrol executor configure 204.67.172.72 eth0:1 255.255.0.0
(sistemi Linux)
dscontrol executor configure 204.67.172.72 eri0 255.255.0.0
(sistemi Solaris)
dscontrol executor configure 204.67.172.72 en1 255.255.0.0
(sistemi Windows)
```

Sistemi Windows

Per utilizzare il secondo formato del comando **executor configure** su Windows, è necessario determinare il nome dell'interfaccia da utilizzare. Se si dispone solo di una scheda Ethernet nella macchina, il nome dell'interfaccia sarà **en0**. Se si dispone

solo di una scheda Token Ring nella macchina, il nome dell'interfaccia sarà tr0. In presenza di più schede di entrambi i tipi, sarà necessario determinare la mappatura delle schede. Effettuare quanto segue:

1. Dalla riga comandi avviare l'executor: `dscontrol executor start`
2. Eseguire il comando: `dscontrol executor xm 1`

L'output verrà visualizzato sullo schermo. Per determinare l'interfaccia da utilizzare per la configurazione di Load Balancer, ricercare l'indirizzo IP della macchina Load Balancer nelle righe che seguono Number of NIC records.

L'indirizzo IP della macchina Load Balancer verrà riportato come: `ia->ia_addr`. Il nome dell'interfaccia associata sarà riportato come `ifp->if_name`.

I nomi delle interfacce assegnate dal comando `executor configure` vengono associati ai nomi delle interfacce riportati in questo comando.

Dopo aver ottenuto le informazioni sulla mappatura, è possibile creare un alias sull'interfaccia di rete all'indirizzo cluster.

Utilizzo dei comandi `ifconfig` per configurare gli alias cluster

Su sistemi Linux o UNIX, il comando `executor configure` esegue i comandi `ifconfig`.

Sistemi Solaris e HP-UX: Quando si utilizzano applicazioni server specifiche del collegamento che si collegano a un elenco di indirizzi IP che non contengono l'IP del server, utilizzare il comando **arp publish** al posto di `ifconfig` per impostare dinamicamente un indirizzo IP sulla macchina Load Balancer. Ad esempio:

```
arp -s <cluster> <Load Balancer MAC address> pub
```

Fase 6. Definizione delle porte e impostazioni delle relative opzioni

Per definire una porta, immettere il comando **dscontrol port add** *cluster:port*, modificare il file di configurazione di esempio o utilizzare la GUI. Per *cluster* è possibile specificare il nome simbolico o l'indirizzo IP. Per *port* specificare il numero della porta che si sta utilizzando per il protocollo. In questa fase, è possibile anche modificare varie impostazioni di porta. È necessario definire e configurare tutti i server di una porta. Vedere Capitolo 27, "Riferimenti sui comandi per Dispatcher e CBR", a pagina 337.

Il numero di porta 0 (zero) viene utilizzato per specificare una porta jolly. Questa porta accetta il traffico di una porta non destinato ad alcuna porta definita sul cluster. La porta jolly verrà utilizzata per configurare regole e server per qualsiasi porta. Questa funzione può essere utilizzata anche in caso di una configurazione server/regola identica per più porte. Il traffico su una porta può quindi influire sulle decisioni inerenti il bilanciamento del carico del traffico su altre porte. Vedere "Utilizzo della porta jolly per indirizzare il traffico per una porta non configurata" a pagina 231, per ulteriori informazioni sui casi in cui è opportuno utilizzare una porta jolly.

Fase 7. Definizione delle macchine server con bilanciamento del carico

Per definire una macchina server con bilanciamento del carico, immettere il comando **dscontrol server add** *cluster:port:server*, modificare il file di configurazione di esempio o utilizzare la GUI. Per *cluster* e *server*, è possibile specificare il nome simbolico o l'indirizzo IP. Per *port* specificare il numero della porta che si sta

utilizzando per il protocollo. Per poter effettuare un bilanciamento del carico, è necessario definire più di un server per una porta su un cluster.

Server specifici del collegamento: Se il componente Dispatcher sta eseguendo il bilanciamento del carico su server specifici del collegamento, i server *devono* essere configurati per collegarsi all'indirizzo cluster. Poiché il Dispatcher inoltra i pacchetti senza modificare l'indirizzo IP di destinazione, quando i pacchetti raggiungono il server, conterranno ancora l'indirizzo cluster come destinazione. Se un server è stato configurato per collegarsi a un indirizzo IP diverso dall'indirizzo cluster, il server non sarà in grado di accettare pacchetti/richieste destinati al cluster.

Per determinare se il server è bind specifico, emettere il comando `netstat -an` e ricercare `server:porta`. Se il server non è bind specifico, il risultato di questo comando sarà `0.0.0.0:80`. Se invece il server è bind specifico, verrà visualizzato un indirizzo del tipo `192.168.15.103:80`.

Nota: Per sistemi Solaris e Linux: quando si utilizzano gli advisor, i server specifici del collegamento non devono essere posizionati.

Posizionamento con più indirizzi: In una configurazione posizionata, l'indirizzo della macchina server posizionata *non* deve essere identico all'indirizzo di non inoltro (NFA). Se la macchina è stata definita con più indirizzi IP, è possibile utilizzare un altro indirizzo. Per il componente Dispatcher, la macchina server posizionata deve essere definita come **posizionata** tramite il comando **dscontrol server**. Per ulteriori informazioni sui server posizionati, vedere "Utilizzo dei server posizionati" a pagina 196.

Per ulteriori informazioni sulla sintassi del comando `dscontrol server`, vedere "`dscontrol server` — configura i server" a pagina 381.

Fase 8. Avvio della funzione gestore (facoltativo)

La funzione gestore migliora il bilanciamento del carico. Per avviare il gestore, immettere il comando **dscontrol manager start**, modificare il file di configurazione di esempio o utilizzare la GUI.

Fase 9. Avvio della funzione advisor (facoltativo)

Gli advisor forniscono al gestore ulteriori informazioni sulla capacità delle macchine server con bilanciamento del carico di rispondere alle richieste. Un advisor è specifico di un protocollo. Ad esempio, per avviare l'advisor HTTP, immettere il seguente comando:

```
dscontrol advisor start http port
```

Per un elenco degli advisor e delle relative porte predefinite, vedere Capitolo 27, "Riferimenti sui comandi per Dispatcher e CBR", a pagina 337. Per una descrizione di ciascun advisor, vedere "Elenco di advisor" a pagina 184.

Fase 10. Impostazione delle proporzioni dei cluster secondo necessità

Se si avviano gli advisor, è possibile modificare le proporzioni di importanza attribuite alle informazioni raccolte dall'advisor che devono essere incluse nelle decisioni relative al bilanciamento del carico. Per impostare le proporzioni del

cluster, immettere il comando **dscontrol cluster set cluster proportions**. Per ulteriori informazioni, vedere “Proporzione di importanza attribuita alle informazioni sullo stato” a pagina 176.

Configurazione delle macchine server per il bilanciamento del carico

Effettuare le operazioni riportate di seguito in presenza di una delle seguenti condizioni:

- Se si sta utilizzando il metodo di inoltro mac e la macchina utilizzata è un server backend.
- Se si sta utilizzando il metodo di inoltro mac e la macchina utilizzata è un server posizionato, configurato come macchina in standby con disponibilità elevata.

Note:

1. Le procedure per eliminare l’alias del loopback dovranno essere inserite negli script go*, nel caso in cui la macchina passi allo stato attivo.
2. Se la macchina è stata configurata come attiva e con disponibilità elevata, le procedure per l’aggiunta dell’alias all’unità loopback dovranno essere inserite negli script go*, nel caso in cui la macchina passi allo stato standby.

Quando si utilizza il metodo di inoltro mac, il Dispatcher bilancerà il carico solo tra i server che consentono di configurare la scheda loopback con un indirizzo IP supplementare, per cui il server backend non risponderà mai alle richieste ARP (address resolution protocol). Attenersi alle operazioni descritte in questa sezione per configurare le macchine server sottoposte a bilanciamento del carico.

Fase 1. Creazione dell’alias dell’unità loopback

Per far funzionare macchine server sottoposte a bilanciamento del carico, è necessario impostare l’unità loopback (spesso denominata lo0) (o, preferibilmente, crearne l’alias) per l’indirizzo cluster. Quando si utilizza il metodo di inoltro mac, il componente Dispatcher non modifica l’indirizzo IP di destinazione nel pacchetto TCP/IP prima di inoltrare il pacchetto a una macchina server TCP. Configurando l’unità loopback sull’indirizzo cluster, o aggiungendovi l’alias, le macchine server sottoposte a bilanciamento del carico accettano un pacchetto destinato all’indirizzo cluster.

Con un sistema operativo che supporta l’aggiunta dell’alias delle interfacce di rete (come AIX, HP-UX, Linux, Solaris o Windows), si dovrebbe creare l’alias dell’unità loopback per l’indirizzo cluster. Il vantaggio derivante dall’uso di un sistema operativo che supporta gli alias è la possibilità di configurare macchine server sottoposte a bilanciamento del carico destinate a servire più indirizzi cluster.

IMPORTANTE: per i sistemi Linux, consultare “Alternative per l’aggiunta dell’alias loopback Linux quando si utilizza il metodo di inoltro mac di Load Balancer” a pagina 76.

Se si dispone di un server con un sistema operativo che non supporta gli alias, è necessario impostare l’unità loopback per l’indirizzo cluster.

Utilizzare il comando del sistema operativo a disposizione, come illustrato nella Tabella 5 a pagina 71, per impostare o creare l’alias dell’unità loopback.

Tabella 5. Comandi per creare l'alias dell'unità loopback (lo0) per Dispatcher

AIX 4.3 o versione precedente	ifconfig lo0 alias cluster_address netmask netmask Nota: utilizzare la maschera di rete della scheda principale
AIX 5.x	ifconfig lo0 alias cluster_address netmask 255.255.255.255
HP-UX	ifconfig lo0:1 cluster_address up
Linux	<p>Selezionare uno dei seguenti comandi:</p> <ul style="list-style-type: none"> • ip -4 addr add indirizzo_cluster/32 dev lo • ifconfig lo:1 cluster_address netmask 255.255.255.255 up <p>IMPORTANTE: una volta emesso uno dei comandi di configurazione sulla macchina, utilizzare sempre lo stesso comando (ip or ifconfig) altrimenti si verificheranno degli errori.</p>
OS/2	ifconfig lo cluster_address
OS/390	<p>Configurazione di un alias loopback sul sistema OS/390</p> <ul style="list-style-type: none"> • Nel membro del parametro IP (file), un amministratore dovrà creare una voce nell'elenco indirizzi Home. Ad esempio <pre>HOME ;Address Link 192.168.252.11 tr0 192.168.100.100 1tr1 192.168.252.12 loopback</pre> <ul style="list-style-type: none"> • Per il loopback è possibile definire molti indirizzi. • L'indirizzo loopback 127.0.0.1 è configurato per impostazione predefinita.
Solaris 7	ifconfig lo0:1 cluster_address 127.0.0.1 up
Solaris 8, Solaris 9 e Solaris 10	ifconfig lo0:1 plumb cluster_address netmask netmask up

Tabella 5. Comandi per creare l'alias dell'unità loopback (lo0) per Dispatcher (Continua)

Windows Server 2003	<ol style="list-style-type: none"> 1. Fare clic su Start, quindi su Pannello di controllo. 2. Aggiungere il driver scheda MS Loopback, nel caso l'operazione non fosse stata ancora eseguita. <ol style="list-style-type: none"> a. Fare clic su Installa hardware per avviare l'installazione guidata dell'hardware. b. Fare clic su Avanti c. Selezionare Sì, quindi fare clic su Avanti. d. Se la scheda MS Loopback è nell'elenco, allora è già installata — fare clic su Annulla per uscire. e. Se la scheda MS Loopback <i>non</i> è in elenco — selezionare Aggiungi nuova periferica, quindi fare clic su Avanti. f. Per selezionare l'hardware da un elenco, per il pannello Trova nuovo hardware, fare clic su No, quindi su Avanti. g. Selezionare Schede di rete, quindi fare clic su Avanti. h. Sul pannello Seleziona scheda di rete, selezionare Microsoft nell'elenco Produttori, quindi Scheda Microsoft Loopback. i. Fare clic su Avanti, quindi di nuovo su Avanti per installare le impostazioni predefinite (o selezionare Disco driver, quindi inserire il CD e procedere all'installazione). j. Fare clic su Fine per completare l'installazione. 3. Dal Pannello di controllo, fare doppio clic su Rete e connessioni remote. 4. Selezionare la connessione con Nome periferica "Scheda Microsoft Loopback". 5. Selezionare Proprietà dall'elenco a discesa. 6. Selezionare Protocollo Internet (TCP/IP), quindi fare clic su Proprietà. 7. Fare clic su Utilizza il seguente indirizzo IP. Nel campo <i>Indirizzo IP</i> inserire l'indirizzo cluster e nel campo <i>Subnet mask</i> inserire la subnet mask del server back-end. Nota: Non inserire un indirizzo router. Utilizzare l'host locale come server DNS predefinito.
---------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tabella 5. Comandi per creare l'alias dell'unità loopback (lo0) per Dispatcher (Continua)

Windows 2000	<ol style="list-style-type: none"> 1. Fare clic su Start, Impostazioni, Pannello di controllo. 2. Aggiungere il driver scheda MS Loopback, nel caso l'operazione non fosse stata ancora eseguita. <ol style="list-style-type: none"> a. Fare doppio clic su Installazione guidata hardware per avviare l'installazione guidata dell'hardware. b. Fare clic su Avanti, selezionare Aggiungi/risolvi i problemi (periferica), quindi fare clic su Avanti. c. Lo schermo si accende e si spegne a intermittenza, quindi visualizza il pannello Scegli periferica hardware. d. Se la scheda MS Loopback è nell'elenco, allora è già installata — fare clic su Annulla per uscire. e. Se la scheda MS Loopback <i>non</i> è in elenco — selezionare Aggiungi nuova periferica, quindi fare clic su Avanti. f. Per selezionare l'hardware da un elenco, per il pannello Trova nuovo hardware, fare clic su No, quindi su Avanti. g. Selezionare Schede di rete, quindi fare clic su Avanti. h. Sul pannello Seleziona scheda di rete, selezionare Microsoft nell'elenco Produttori, quindi Scheda Microsoft Loopback. i. Fare clic su Avanti, quindi di nuovo su Avanti per installare le impostazioni predefinite (o selezionare Disco driver, quindi inserire il CD e procedere all'installazione). j. Fare clic su Fine per completare l'installazione. 3. Dal Pannello di controllo, fare doppio clic su Rete e connessioni remote. 4. Selezionare la connessione con Nome periferica "Scheda Microsoft Loopback", quindi fare clic con il tasto destro del mouse. 5. Selezionare Proprietà dall'elenco a discesa. 6. Selezionare Protocollo Internet (TCP/IP), quindi fare clic su Proprietà. 7. Fare clic su Utilizza il seguente indirizzo IP. Nel campo <i>Indirizzo IP</i> inserire l'indirizzo cluster e nel campo <i>Subnet mask</i> inserire la subnet mask predefinita (255.0.0.0). Nota: Non inserire un indirizzo router. Utilizzare l'host locale come server DNS predefinito.
Windows NT	<ol style="list-style-type: none"> 1. Fare clic su Start, quindi su Impostazioni. 2. Fare clic su Pannello di controllo, quindi doppio clic su Rete. 3. Aggiungere il driver scheda MS Loopback, nel caso l'operazione non fosse stata ancora eseguita. <ol style="list-style-type: none"> a. Nella finestra Rete, fare clic su Schede. b. Selezionare Scheda MS Loopback, quindi fare clic su OK. c. Quando richiesto, inserire il CD o i dischi di installazione. d. Nella finestra Rete, fare clic su Protocolli. e. Selezionare Protocollo TCP/IP, quindi fare clic su Proprietà. f. Selezionare Scheda MS Loopback, quindi fare clic su OK. 4. Impostare l'indirizzo loopback sull'indirizzo cluster. Confermare la subnet mask predefinita (255.0.0.0) e non inserire un indirizzo gateway. Nota: potrebbe essere necessario chiudere e riaprire il pannello Impostazioni di rete prima di poter visualizzare il driver MS Loopback nella configurazione TCP/IP.

Fase 2. Ricerca di un instradamento supplementare

Su alcuni sistemi operativi, potrebbe essere stato creato un instradamento predefinito che deve essere rimosso.

- Ricercare un instradamento supplementare sul sistema operativo Windows con il seguente comando:

```
route print
```

IMPORTANTE: qualsiasi instradamento aggiuntivo deve essere ignorato su Windows 2003. Se si verificano dei problemi con l'instradamento in seguito alla creazione dell'alias, rimuovere l'alias e aggiungerlo di nuovo utilizzando una netmask differente.

- Ricercare un instradamento predefinito su tutti i Sistemi Linux e UNIX con il seguente comando:

```
netstat -nr
```

Esempio **Windows**:

1. Una volta immesso **route print**, verrà visualizzata una tabella simile a quella riportata nell'esempio seguente. (Questo esempio illustra la ricerca e la rimozione di un instradamento supplementare al cluster 9.67.133.158 con una maschera di rete predefinita 255.0.0.0.)

Active Routes:

Network Address	Netmask	Gateway Address	Interface	Metric
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

2. Ricercare l'indirizzo cluster nella colonna "Gateway Address". In presenza di un instradamento supplementare, l'indirizzo cluster verrà visualizzato due volte. Nell'esempio riportato, l'indirizzo cluster (9.67.133.158) viene visualizzato nella riga 2 e nella riga 8.
3. Ricercare l'indirizzo di rete in ciascuna riga in cui compare l'indirizzo cluster. L'utente deve conservare uno di questi instradamenti ed eliminare l'altro, che non è pertinente. L'instradamento supplementare da eliminare sarà quello il cui indirizzo di rete inizia con la prima cifra dell'indirizzo cluster, seguita da tre zero. Nell'esempio riportato, l'instradamento supplementare è quello che si trova alla riga due, con indirizzo di rete **9.0.0.0**:

```
9.0.0.0    255.0.0.0    9.67.133.158    9.67.133.158    1
```

Fase 3. Rimozione di un instradamento supplementare

È necessario rimuovere l'instradamento supplementare. Utilizzare il comando del sistema operativo illustrato nella Tabella 6 a pagina 75 per rimuovere l'instradamento supplementare.

Esempio: per eliminare un instradamento supplementare come illustrato nella tabella di esempio "Active Routes" della fase 2, immettere:

```
route delete 9.0.0.0 9.67.133.158
```


Tabella 6. Comandi per eliminare instradamenti supplementari per il Dispatcher

HP-UX	route delete <i>cluster_address cluster_address</i>
Windows	<p>route delete <i>network_address cluster_address</i> (a un prompt MS-DOS)</p> <p>Nota: è necessario eliminare l'instradamento supplementare ad ogni riavvio del server.</p> <p>Su Windows 2003, non è possibile eliminare gli instradamenti. Qualsiasi instradamento aggiuntivo deve essere ignorato su Windows 2003. Se si verificano dei problemi con l'instradamento in seguito alla creazione dell'alias, rimuovere l'alias e aggiungerlo di nuovo utilizzando una netmask differente.</p>

Se si utilizza l'esempio illustrato nella Figura 15 a pagina 66 e si configura una macchina server su cui è in esecuzione AIX, il comando sarà:

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

Fase 4. Verifica della corretta configurazione del server

Per verificare che un server backend sia correttamente configurato, effettuare le seguenti operazioni da una macchina differente sulla stessa sottorete, quando Load Balancer non è in esecuzione e il *cluster* non è configurato:

1. Emettere il comando:

```
arp -d cluster
```

2. Emettere il comando:

```
ping cluster
```

Non dovrebbe esserci risposta. Nel caso di risposta al ping, verificare di non aver eseguito il comando `ifconfig` per l'indirizzo *cluster* all'interfaccia. Accertarsi che non vi siano macchine che presentino una voce con `arp publish` nell'indirizzo *cluster*.

3. Eseguire il ping sul server backend, quindi emettere subito il comando:

```
arp -a
```

Nell'output del comando, dovrebbe essere visualizzato l'indirizzo MAC del server. Emettere il comando:

```
arp -s cluster server_mac_address
```

4. Eseguire il ping sul cluster. Si dovrebbe ricevere una risposta. Emettere una richiesta `http`, `telnet` o di altro tipo indirizzata al cluster che dovrebbe essere gestito dal server backend. Verificare che funzioni correttamente.
5. Emettere il comando:

```
arp -d cluster
```
6. Eseguire il ping sul cluster. Non dovrebbe esserci risposta.

Nota: in caso di risposta, emettere un'istruzione **arp *cluster*** per richiamare l'indirizzo MAC di una macchina non configurata correttamente. Quindi, ripetere le fasi da 1 a 6.

Alternative per l'aggiunta dell'alias loopback Linux quando si utilizza il metodo di inoltro mac di Load Balancer

Alcune versioni di Linux emettono delle risposte ARP per qualsiasi indirizzo IP configurato sulla macchina su ogni interfaccia presente sulla macchina stessa. Inoltre, è possibile selezionare un indirizzo IP di origine ARP per query ARP who-has basate su tutti gli indirizzi IP presenti sulla macchina, indipendentemente dalle interfacce su cui sono configurati quegli indirizzi. In questo modo, tutto il traffico cluster viene indirizzato a un unico server in maniera indeterminata.

Quando si utilizza il metodo di inoltro mac del Dispatcher, è necessario adoperare un meccanismo che assicuri che il traffico indirizzato al cluster venga accettato dagli stack dei server backend, compresa la macchina in standby con disponibilità elevata, se si utilizza sia la disponibilità elevata che il posizionamento.

Nella maggior parte dei casi, è necessario creare l'alias dell'indirizzo cluster sul loopback; perciò, per i server backend è obbligatorio creare l'alias del cluster sul loopback; inoltre, se si utilizza la disponibilità elevata e il posizionamento, per i server con bilanciamento del carico in standby, occorre creare l'alias del cluster sul loopback.

Per verificare che Linux non renda noti gli indirizzi sul loopback, è possibile utilizzare una delle seguenti soluzioni, per garantire la compatibilità tra Linux e il metodo di inoltro mac del Dispatcher.

1. Utilizzare un kernel che non renda noti gli indirizzi. Si tratta dell'opzione migliore, in quanto non incorre in un sovraccarico per ogni pacchetto e non richiede riconfigurazione per ciascun kernel.

- United Linux 1 / SLES8 con SP2(x86) o SP3 (tutte le altre architetture) e versioni successive contengono la patch nascosta ARP Julian. Accertarsi che questa sia sempre attiva prima di aggiungere l'alias all'indirizzo cluster con il comando:

```
# sysctl -w net.ipv4.conf.all.hidden=1 net.ipv4.conf.lo.hidden=1
```

Quindi, è possibile creare normalmente l'alias dei cluster, ad esempio:

```
# ifconfig lo:1 $CLUSTER_ADDRESS netmask 255.255.255.255 up
```

- Utilizzare `arp_ignore sysctl`, disponibile nelle versioni 2.4.25 e 2.6.5 e successive ma tenere presente che le distribuzioni a volte garantiscono la compatibilità delle funzioni con le versioni precedenti. Accertarsi che sia abilitato prima di aggiungere l'alias all'indirizzo cluster con i comandi:

```
# sysctl -w net.ipv4.conf.all.arp_ignore=3  
net.ipv4.conf.all.arp_announce=2
```

Quindi, è necessario creare l'alias dei cluster con il seguente comando:

```
# ip addr add $CLUSTER_ADDRESS/32 scope host dev lo
```

Un comando simile deve trovarsi negli script `go*` nelle configurazioni a disponibilità elevata.

- Nota: quando si utilizza `sysctl`, assicurarsi che queste impostazioni vengano conservate dopo il riavvio, mediante l'aggiunta delle impostazioni a `/etc/sysctl.conf`.
2. Utilizzare le tabelle IP per reindirizzare tutto il traffico cluster in entrata all'host locale. Se si utilizza questo metodo, non configurare la scheda loopback con un alias. Piuttosto, utilizzare il comando:

```
# iptables -t nat -A PREROUTING -d $CLUSTER_ADDRESS -j REDIRECT
```

In questo modo, Linux esegue la conversione degli indirizzi di rete (NAT, Network Address Translation) su ciascun pacchetto, sostituendo l'indirizzo del cluster con l'indirizzo dell'interfaccia di rete. Questo metodo penalizza la velocità delle connessioni al secondo del 6,4%. Il metodo funziona su qualsiasi distribuzione comune supportata; non sono necessari moduli kernel o patch+build+install del kernel.

3. Applicare un modulo noarp versione 1.2.0 o successiva. L'origine kernel deve essere disponibile e correttamente configurata; anche gli strumenti di sviluppo (gcc, gnu make, ecc.) devono essere disponibili. È necessario creare e installare i moduli ad ogni aggiornamento del kernel. Il modulo è disponibile all'indirizzo <http://www.masarlabs.com/noarp/>. Poiché il codice kernel in sé non viene modificato, è molto meno intrusivo della soluzione n. 4 (elencata di seguito) e meno incline a errori. Inoltre, esso deve essere configurato prima di creare l'alias di un indirizzo cluster sul loopback. Ad esempio:

```
# modprobe noarp
# noarpctl add $CLUSTER_ADDRESS nic-primary-addr
```

dove per *nic-primary-addr* si intende un indirizzo nella stessa sottorete dell'indirizzo cluster. Quindi, è possibile creare normalmente l'alias dei cluster, ad esempio:

```
# ifconfig lo:1 cluster address netmask 255.255.255.255 up
```

Nota: Per le configurazioni a disponibilità elevata, `noarpctl adds` e `dels` devono essere inseriti negli script `go*`. Ciò garantisce che il Load Balancer attivo possa eseguire l'ARP per l'indirizzo cluster e che il Load Balancer in standby, che funge da server, non inizi casualmente (ovvero, in modo indeterminato) a ricevere tutto il traffico cluster.

4. Richiedere una patch Julian dal sito Web riportato di seguito: <http://www.ssi.bg/~ja/#hidden>. Attenersi alle istruzioni relative alla distribuzione per applicare la patch e compilare un kernel adatto a essere utilizzato con la distribuzione. Se Load Balancer è inserito in una configurazione a disponibilità elevata, verificare che `uname -r` corrisponda al kernel fornito per la distribuzione e assicurarsi di iniziare con il file `.config` del kernel della distribuzione. Dopo aver creato, installato ed eseguito il kernel con la patch nascosta Julian, seguire le istruzioni contenute nella prima soluzione elencata per l'abilitazione della patch.

Nota: Per l'esecuzione di un kernel personalizzato ci potrebbero essere implicazioni associate alla distribuzione.

Capitolo 8. Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6

Il supporto per lo schema di indirizzamento IP esteso di IPv6 È disponibile con Load Balancer per IPv4 e IPv6. Load Balancer per IPv4 e IPv6 è un'immagine di installazione separata costituita esclusivamente dal componente Dispatcher. Questo tipo di installazione fornisce il bilanciamento del carico per il traffico IPv4 e IPv6 ai server configurati nella rete che utilizzano l'inoltro del pacchetto basato su MAC di Dispatcher.

Questo capitolo descrive le differenze di configurazione e le limitazioni di Dispatcher nell'installazione di Load Balancer per IPv4 e IPv6 di questo prodotto e comprende le seguenti sezioni:

- "Piattaforme supportate per Load Balancer per IPv4 e IPv6" a pagina 80
- "Installazione di Load Balancer per IPv4 e IPv6" a pagina 81
- "Considerazioni speciali e limitazioni per Load Balancer per IPv4 e IPv6" a pagina 81
- "Abilitazione dell'elaborazione dei pacchetti IPv6 in Load Balancer per IPv4 e IPv6" a pagina 85
- "Creazione dell'alias del dispositivo interfaccia in Load Balancer per IPv4 e IPv6" a pagina 86
- "Operazioni di configurazione del cluster per Linux suzSeries" a pagina 89
- "Comandi Dispatcher (dscontrol) in Load Balancer per IPv4 e IPv6" a pagina 89

Per informazioni generali sul componente Dispatcher, fare riferimento ai seguenti capitoli:

- Vedere "Funzioni del componente Dispatcher" a pagina 19 per una panoramica delle funzioni di Dispatcher disponibili per la gestione della rete.
- Vedere Capitolo 6, "Pianificazione del Dispatcher", a pagina 49 per informazioni sulla pianificazione dei parametri di bilanciamento del carico di Dispatcher.
- Vedere Capitolo 7, "Configurazione del Dispatcher", a pagina 61 per informazioni sulla configurazione dei parametri di bilanciamento del carico di Dispatcher.
- Vedere Capitolo 22, "Funzioni avanzate di Dispatcher, CBR e Site Selector", a pagina 195 per informazioni su come configurare Load Balancer per funzioni più avanzate.
- Vedere Capitolo 24, "Funzionamento e gestione di Load Balancer", a pagina 253 per informazioni sui log di Load Balancer e sull'uso dei componenti di Load Balancer.

È importante sottolineare che con l'installazione di Load Balancer per IPv4 e IPv6, la sintassi del comando Dispatcher (dscontrol) rimane la stessa, con un'unica eccezione. Il delimitatore dei comandi dscontrol è un simbolo at (@), anziché i due punti (:), quando si utilizza Load Balancer per IPv4 e IPv6. Quando negli altri capitoli del presente documento si fa riferimento ai comandi, ricordarsi di sostituire i due punti (:) con il simbolo @ come delimitatore nei comandi dscontrol.

Piattaforme supportate per Load Balancer per IPv4 e IPv6

L'installazione di Load Balancer per IPv4 e IPv6 È disponibile su tutte le piattaforme supportate ad eccezione di Windows 2000.

Per i requisiti di sistema hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Piattaforme supportate per il bilanciamento del carico nello spazio utente

Su alcune piattaforme supportate, come ad esempio tutte le architetture Linux, le installazioni Load Balancer per IPv4 e IPv6 eseguono i processi di bilanciamento del carico nello spazio utente anziché nello spazio del kernel. Per tali sistemi, non esiste alcuna dipendenza dal modulo kernel.

Per le informazioni più aggiornate sulle piattaforme che supportano il bilanciamento del carico nello spazio utente (senza kernel), fare riferimento al seguente sito Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

I sistemi supportati che eseguono i processi di bilanciamento del carico nello spazio utente hanno delle procedure di configurazione differenti da quei sistemi che eseguono gli stessi processi in uno spazio del kernel. Tali differenze verranno trattate nella sezione relativa a Load Balancer per IPv4 e IPv6.

Considerazioni speciali sulla piattaforma Linux

Sistemi Linux su zSeries

- **I sistemi Linux su zSeries richiedono libstdc++.so.5:** per una corretta installazione, i sistemi Linux su zSeries devono disporre del pacchetto rpm libstdc++.so.5, altrimenti l'installazione riporterà un errore.
- **Limitazione quando si utilizza l'interfaccia qeth/OSA:** per sistemi Linux su zSeries, esiste una limitazione relativa all'utilizzo dell'interfaccia qeth/OSA. L'inoltro di una interfaccia qeth/OSA non è supportato. Tuttavia, esiste una soluzione alternativa in quanto i sistemi Linux vengono eseguiti nello spazio utente e possono supportare il tunneling Linux.

Supporto del tunneling Linux

Su sistemi Linux, le installazioni Load Balancer per IPv4 e IPv6 possono essere inoltrate mediante tunnel quali IPIP e IPGRE. Quando si utilizza Linux su zSeries con un'interfaccia qeth/OSA, un tunnel Linux può essere definito per attraversare l'interfaccia qeth/OSA. I sistemi Linux possono essere inoltrati su macchine ubicate sulle stesse unità qeth/OSA o su unità diverse o su qualsiasi altra unità di rete.

Limitazioni dei server di backend

Sistemi Solaris: non esiste alcun supporto per il bilanciamento del carico del traffico IPv6 sui server Solaris 5.8 di backend. Su Solaris 5.8, esiste una incompatibilità con il pacchetto IPv6 MAC e lo stack IPv6 Solaris. Quando il cluster è configurato su un server di backend Solaris 5.8 mediante il comando `ifconfig lo0 (loopback)`, il pacchetto arriva sul nodo Solaris 5.8 ma non viene accettato. Tuttavia, è possibile utilizzare le installazioni Load Balancer per IPv4 e IPv6 per bilanciare il carico del traffico IPv4 sui server Solaris 5.8 di backend.

Sistemi z/OS: non esiste alcun supporto per il bilanciamento del carico del traffico IPv6 sui server z/OS di backend. Tuttavia, è possibile utilizzare le installazioni Load Balancer per IPv4 e IPv6 per bilanciare il carico del traffico IPv4 sui server z/OS di backend.

Installazione di Load Balancer per IPv4 e IPv6

In Load Balancer per IPv4 e IPv6, le fasi di installazione e i nomi dei pacchetti sono gli stessi di quelli utilizzati per il prodotto Load Balancer che supporta solo gli indirizzi server IPv4. Tuttavia, i pacchetti componente sono di numero inferiore, in quanto è disponibile solo il componente Dispatcher.

Quando si utilizzano gli strumenti di assemblaggio del sistema, l'ordine consigliato per l'installazione dei pacchetti è leggermente differente per le installazioni di Load Balancer per IPv4 e IPv6. È importante notare che il pacchetto del componente di gestione deve essere installato in seguito al pacchetto del componente dispatcher. L'ordine consigliato per l'installazione dei pacchetti per Load Balancer per IPv4 e IPv6 mediante gli strumenti di sistema è: base, licenza, componente dispatcher, gestione, documentazione e Metric Server.

Ad esempio, su sistemi AIX, l'ordine di installazione dei pacchetti Load Balancer per IPv4 e IPv6 è il seguente:

- `ibmlb.base.rte` (pacchetto Base)
- `ibmlb.lb.license` (pacchetto Licenza, se si esegue l'installazione da un CD)
- `ibmlb.lb.driver` (pacchetto dei driver di unità, che è un pacchetto univoco solo per sistemi AIX)
- `ibmlb.disp.rte` and `ibmlb.msg.lang.lb` (pacchetto del componente Dispatcher con un pacchetto di messaggi)
- `ibmlb.admin.rte` and `ibmlb.msg.lang.admin` (pacchetto Gestione con un pacchetto di messaggi)
- `ibmlb.doc.rte` and `ibmlb.msg.en_US.doc` (pacchetto Documentazione con un pacchetto di messaggi)
- `ibmlb.ms.rte` (pacchetto Metric Server)

È importante disinstallare la precedente versione di Load Balancer prima di installare Load Balancer per IPv4 e IPv6. Due versioni di Load Balancer non possono essere presenti sulla stessa macchina.

Per le istruzioni sull'installazione del prodotto, vedere Capitolo 4, "Installazione di Load Balancer", a pagina 29.

Considerazioni speciali e limitazioni per Load Balancer per IPv4 e IPv6

Il componente Dispatcher offre molte, anche se non tutte, delle funzioni offerte dallo stesso componente nelle installazioni di Load Balancer che supportano solo gli schemi di indirizzamento server IPv4. I seguenti argomenti descrivono le particolari differenze di configurazione e le limitazioni funzionali di Dispatcher in Load Balancer per IPv4 e IPv6.

Configurazione degli indirizzi locali del collegamento IPv6

Con l'indirizzamento IPv6, ogni macchina nella configurazione di Load Balancer deve avere un indirizzo locale di collegamento a IPv6.

Questo indirizzo è l'indirizzo utilizzato per il rilevamento del traffico per IPv6. Senza questo indirizzo sulla macchina Load Balancer e sui server di back-end, il rilevamento non viene eseguito e le macchine non sono visibili le une alle altre. Load Balancer per IPv6 non può inoltrare traffico senza un indirizzo IPv6 locale di collegamento configurato su un'interfaccia di ciascuna macchina nella configurazione di Load Balancer.

Coppie omogenee di cluster/server

Quando si configura Load Balancer per IPv4 e IPv6, tutti i server devono essere omogenei nel cluster. Ad esempio, se Cluster1 è stato definito con un indirizzo IPv4, tutti i server raggruppati nel Cluster1 devono essere IPv4. Se Cluster2 è stato definito con un indirizzo IPv6, tutti i server definiti in Cluster2 devono essere IPv6. Inoltre, il protocollo utilizzato dal client per inviare i pacchetti IP deve corrispondere al formato IP del cluster.

Il supporto di un ambiente client misto IPv4 e IPv6 richiede che, per ciascuna definizione cluster logica, vengano definite due definizioni cluster effettive – un cluster IPv4 e un cluster IPv6. I client che inviano pacchetti IPv4 sono instradati da Load Balancer al cluster logico che utilizza gli indirizzi IPv4 configurati per il cluster. I client che inviano pacchetti IPv6 sono instradati da Load Balancer al cluster logico che utilizza gli indirizzi IPv6 configurati per il cluster.

Funzioni di Dispatcher non supportate

Molte delle funzioni di Dispatcher descritte in Capitolo 6, "Pianificazione del Dispatcher", a pagina 49 e in Capitolo 22, "Funzioni avanzate di Dispatcher, CBR e Site Selector", a pagina 195 sono disponibili in Load Balancer per IPv4 e IPv6.

Di seguito viene riportato un elenco riepilogativo delle funzioni di Dispatcher che *non* sono supportate in Load Balancer per IPv4 e IPv6:

- metodo di inoltro cbr
- metodo di inoltro nat
- amministrazione remota
- bilanciamento del carico basato su regole
- agente secondario SNMP
- bilanciamento del carico per una rete geografica
- supporto protocollo UDP

Vedere "Funzioni del componente Dispatcher" a pagina 19 per una descrizione dettagliata delle funzioni di Dispatcher disponibili per la gestione della rete.

Configurazione degli advisor

Se si utilizza il protocollo IPv6 e si desidera utilizzare gli advisor, è necessario modificare il file del **protocollo**.

```
ipv6-icmp 58 IPv6-ICMP
```

Su sistemi Linux e UNIX, il file del protocollo si trova nella directory `/etc/protocols`. Su sistemi Windows, il file del protocollo si trova nella directory `C:\windows\system32\drivers\etc`.

Limitazione relativa all'utilizzo di advisor: se Load Balancer è in esecuzione su un computer con più schede adattatore di rete e se si desidera che il traffico degli advisor venga distribuito a un particolare adattatore, è possibile forzare l'indirizzo

IP di origine dei pacchetti a un indirizzo particolare. La proprietà -DLB_ADV_SRC_ADDR non è disponibile per le installazioni Load Balancer per IPv4 e IPv6.

Per ulteriori informazioni sugli advisor, vedere “Advisor” a pagina 240.

Configurazione della funzione di disponibilità elevata

Se si utilizza il protocollo IPv6 e si desidera utilizzare l’elevata disponibilità, è necessario verificare se protocollo 58 è definito come ICMPv6 nel file del **protocollo**. Per informazioni sulla modifica del file di protocollo, fare riferimento a “Configurazione degli advisor” a pagina 82.

Nelle installazioni di Load Balancer per IPv4 e IPv6, la configurazione di una macchina Dispatcher con disponibilità elevata è supportata con le seguenti limitazioni o considerazioni speciali:

- La funzione di disponibilità elevata reciproca non è supportata.
- Le coppie di heartbeat (meccanismo attivo tra il Dispatcher principale e il Dispatcher in standby per individuare gli errori del Dispatcher) devono essere entrambi in formato IPv4 o in formato IPv6.
- Per i sistemi che vengono eseguiti nello spazio utente, come i sistemi Linux: in un ambiente a elevata disponibilità o autonomi, è necessario non creare l’alias dell’indirizzo cluster rispetto alla scheda di rete.
- Per i sistemi che vengono eseguiti nello spazio utente, come i sistemi Linux: gli script go* e highavailChange possono essere spostati dalla directory .../ibm/edge/lb/servers/samples alla directory .../ibm/edge/lb/servers/bin in modo da registrare le modifiche allo stato di elevata disponibilità pre la macchina del Dispatcher, ma tali script non devono essere modificati.
- Per sistemi Linux su zSeries che utilizzano un’interfaccia qeth/OSA: solo per questo tipo di interfaccia di rete, la regola generale di non applicare gli alias dell’interfaccia per indirizzi cluster non è valida. È invece necessario utilizzare la seguente procedura per garantire che il traffico del cluster venga consegnato alla macchina guest Linux su un OSA:
 - Gli script go* sono richiesti e devono essere modificati come riportato di seguito utilizzando i comandi specificati in “Operazioni di configurazione del cluster per Linux su zSeries” a pagina 89:
 - goActive: aggiungere i comandi ip e iptables/ip6tables per configurare l’indirizzo del cluster e aggiungere la regola iptables.
 - goStandby: aggiungere i comandi ip e iptables/ip6tables per annullare la configurazione dell’indirizzo del cluster e rimuovere la regola iptables.
 - goInOp: aggiungere i comandi ip e iptables/ip6tables per annullare la configurazione dell’indirizzo del cluster e rimuovere la regola iptables.
 - goIdle: questo script non deve essere creato.

Per ulteriori informazioni sulla funzione di disponibilità elevata, vedere “Disponibilità elevata” a pagina 198.

Pozionamento dei server

Il posizionamento è una configurazione in cui Load Balancer può risiedere sulla stessa macchina di un server per il quale sta bilanciando il carico delle richieste.

Quando si utilizzano installazioni di Load Balancer per IPv4 e IPv6, la funzione di posizionamento è disponibile su tutti i sistemi operativi supportati eccetto i sistemi Windows e i sistemi che vengono eseguiti nello spazio utente, come i sistemi Linux.

Per ulteriori informazioni sul posizionamento dei server, vedere “Utilizzo dei server posizionati” a pagina 196.

Funzione di affinità per i sistemi che vengono eseguiti nello spazio utente (Linux)

La funzione di affinità di Load Balancer per i sistemi che vengono eseguiti nello spazio utente, come i sistemi Linux, opera in maniera differente dalla funzione di affinità per altri sistemi operativi che vengono eseguiti nello spazio del kernel.

Per i sistemi che vengono eseguiti nello spazio utente, Load Balancer associa l'indirizzo IP del client a un server di backend. L'affinità viene stabilita una volta che l'indirizzo IP di destinazione di un pacchetto viene associato al cluster, la porta di destinazione corrisponde alla porta di Load Balancer e l'indirizzo IP di origine corrisponde.

Quando viene stabilita l'affinità, i pacchetti successivi vengono inviati allo stesso server di backend. Se l'affinità viene interrotta, a causa dell'inattività del server o alla rimozione di un server, tutte le connessioni a tale server verranno interrotte.

Inoltre, non saranno presenti informazioni sulla "connessione" riportate sui client della riga comandi o della GUI. verrà utilizzato soltanto il numero di record di affinità attivi.

Questo approccio ha il vantaggio di fornire una elevata affinità ed è più efficiente per il Load Balancer.

Lo svantaggio dei sistemi che utilizzano il bilanciamento del carico nel kernel sta nel fatto che l'utilizzo dell'affinità IP aggiunge carico di CPU e memoria al meccanismo di inoltro della connessione. Su sistemi che eseguono il bilanciamento del carico nello spazio utente, il metodo di affinità utilizzato diminuisce l'utilizzo della CPU e della memoria rispetto all'inoltro della connessione.

Inoltre, a causa di questo modello a singolo record su sistemi in esecuzione in uno spazio utente, i valori di stickytime e staletimeout associati all'affinità sono stati uniti in un unico valore, staletimeout. Poiché la rimozione di un record di affinità interrompe le connessioni, quando si esegue la migrazione da un sistema che viene eseguito nello spazio kernel a un sistema che viene eseguito nello spazio utente, il valore massimo di staletimeout e stickytime deve essere utilizzato come nuovo valore di staletimeout per il Load Balancer in esecuzione sul sistema dello spazio utente.

Per informazioni generali sulla funzione di affinità per i sistemi in esecuzione nello spazio kernel rispetto allo spazio utente, fare riferimento a “Funzionamento della funzione di affinità di Load Balancer” a pagina 214.

Configurazione di Metric Server

Se si utilizza il protocollo IPv6 e si desidera utilizzare l'elevata disponibilità, è necessario verificare se protocollo 58 è definito come ICMPv6 nel file del **protocollo**. Per informazioni sulla modifica del file di protocollo, fare riferimento a “Configurazione degli advisor” a pagina 82.

In una configurazione di Load Balancer che supporta sia i cluster IPv4 che i cluster IPv6, i server che eseguono la funzione Metric Server possono essere configurati solo come server IPv4 o come server IPv6, ma non entrambi. Per far sì che il metric server utilizzi un determinato protocollo, IPv4 o IPv6, specificare la proprietà Java `java.rmi.server.hostname` nello script `metricsserver`.

IMPORTANTE: il nome host specificato nella proprietà Java deve essere l'indirizzo IP fisico di Metric Server.

Su sistemi UNIX o Linux: perché Metric Server comunichi sull'indirizzo IPv6 `2002:92a:8f7a:162:9:42:92:67`, specificare la proprietà Java dopo `$LB_CLASSPATH` nello script di avvio `metricsserver` (nella directory `/usr/bin`) come riportato di seguito:

```
/opt/ibm/edge/lb/java/jre/bin/java ..... $LB_CLASSPATH
-Djava.rmi.server.hostname=2002:92a:8f7a:162:9:42:92:67
com.ibm.internet.nd.sma.SMA_Agent
$LB_RMIPORT $LOG_LEVEL $LOG_SIZE $LOG_DIRECTORY $KEYS_DIRECTORY
$SCRIPT_DIRECTORY &
```

Su sistemi Windows: perché Metric Server comunichi sull'indirizzo IPv6 `2002:92a:8f7a:162:9:42:92:67`, è necessario modificare il file `metricsserver.cmd` (nella directory `C:\winnt\system32`) come riportato di seguito:

```
start
/min /wait %IBMLBPATH%\java\jre\bin\java
-Djava.rmi.server.hostname=2002:92a:8f7a:162:9:42:92:67
-Djava.net.preferIPv4Stack=false
-Djava.net.preferIPv6Stack=true
-Xrs -cp
%LB_CLASSPATH% com.ibm.internet.nd.sma.SMA_Agent
%RMI_PORT% %LOG_LEVEL% %LOG_SIZE% %LOG_DIRECTORY% %KEYS_DIRECTORY%
%SCRIPT_DIRECTORY%
goto done

:stop
%IBMLBPATH%\java\jre\bin\java
-Djava.rmi.server.hostname=2002:92a:8f7a:162:9:42:92:67
-Djava.net.preferIPv4Stack=false
-Djava.net.preferIPv6Stack=true
-cp %LB_CLASSPATH% com.ibm.internet.nd.sma.SMA_AgentStop %RMI_PORT%
:done
```

Per ulteriori informazioni, vedere "Metric Server" a pagina 191.

Abilitazione dell'elaborazione dei pacchetti IPv6 in Load Balancer per IPv4 e IPv6

Nei sistemi AIX, Linux e Windows: prima di avviare l'executor (`dscontrol executor start`), immettere quanto segue dalla riga comandi come root,

- Nei sistemi AIX: `autoconf6`
Per abilitare l'elaborazione interrotta dei pacchetti IPv6 (anche dopo un riavvio del sistema), modificare il file `/etc/rc.tcpip` e rimuovere il commento dalla seguente riga, aggiungendo l'indicatore `-A`: `start /usr/sbin/autoconf6 " " -A`
- Nei sistemi Linux: `modprobe ipv6`
- Nei sistemi Windows: `netsh interface ipv6 install`

Questi comandi abilitano l'elaborazione dei pacchetti IPv6 nei rispettivi sistemi operativi. Immettere questo comando una sola volta. Quindi, è possibile avviare e arrestare l'executor tutte le volte che lo si reputa necessario.

Senza il comando per abilitare l'elaborazione dei pacchetti IPv6 su questi sistemi, l'executor non viene avviato.

Nei sistemi HP-UX e Solaris: utilizzando il comando `ifconfig`, valutare gli indirizzi IPv6 e configurare un'interfaccia in modo che Dispatcher possa controllare i pacchetti IPv6. Prima di avviare l'executor (`dscontrol executor start`), immettere quanto segue dalla riga comandi come root,

- Nei sistemi HP-UX:
`ifconfig device inet6 up`
- Nei sistemi Solaris:
`ifconfig device inet6 plumb`
`ifconfig device inet6 address/prefix up`

Senza questi comandi, l'executor verrà avviato ma non sarà possibile visualizzare alcun pacchetto IPv6.

Creazione dell'alias del dispositivo interfaccia in Load Balancer per IPv4 e IPv6

Per configurare l'indirizzo cluster su una scheda di interfaccia di rete (NIC) della macchina Dispatcher, è possibile immettere il comando `dscontrol executor configure cluster_address`. Il comando `dscontrol executor configure` esegue i comandi di configurazione dell'adattatore del sistema operativo (ad esempio, i comandi `ifconfig`, `dsconfig` (solo IPv6) o `ip`). In alternativa, per creare l'alias della NIC della macchina Dispatcher, è possibile scegliere di immettere direttamente i comandi di configurazione dell'adattatore del sistema operativo anziché utilizzare il comando `executor configure`.

Nota: Per i sistemi che vengono eseguiti nello spazio utente, come i sistemi Linux: è necessario non configurare l'indirizzo cluster mediante il comando `dscontrol executor configure` o con il comando `ip` o `ifconfig`. Load Balancer utilizza di solito l'indirizzo cluster sulla rete. Inoltre, l'indirizzo cluster non viene visualizzato con un alias sull'interfaccia. Questo è normale.

Tuttavia, **ciò non si applica** a sistemi Linux su zSeries che utilizzano un'interfaccia qeth/OSA. Per questa piattaforma, è necessario configurare l'indirizzo del cluster. Fare riferimento a "Operazioni di configurazione del cluster per Linux su zSeries" a pagina 89 per maggiori dettagli.

Per creare l'alias del dispositivo loopback (lo0) sui server sottoposti al bilanciamento del carico, è necessario utilizzare i comandi di configurazione dell'adattatore del sistema operativo.

Nelle installazioni di Load Balancer per IPv4 e IPv6, è possibile utilizzare i seguenti comandi per creare l'alias dell'interfaccia di rete e del dispositivo loopback (*interface_name*).

Nei sistemi AIX (5.x),

- Per gli indirizzi IPv6:
`ifconfig interface_name inet6 cluster_address/prefix_length alias`

Ad esempio, per creare l'alias del dispositivo loopback sui server sottoposti al bilanciamento del carico:

```
ifconfig lo0 inet6 2002:4a::541:56/128 alias
```

- Per gli indirizzi IPv4: invariato. Vedere Tabella 5 a pagina 71 per creare l'alias del dispositivo loopback sui server sottoposti al bilanciamento del carico.

Nei sistemi HP-UX:

- Per gli indirizzi IPv6:
`ifconfig interface_name:alias inet6 cluster_address up prefix prefix_length`

Ad esempio, per creare l'alias del dispositivo loopback sui server sottoposti al bilanciamento del carico:

```
ifconfig lo0:1 inet6 3ffe:34::24:45 up prefix 128
```

- Per gli indirizzi IPv4: invariato. Vedere Tabella 5 a pagina 71 per creare l'alias del dispositivo loopback sui server sottoposti al bilanciamento del carico.

Nei sistemi Linux:

- Per gli indirizzi IPv6 o IPv4:
`ip -version addr add indirizzo_cluster/lunghezza_prefisso dev lo`

Ad esempio, per creare l'alias del dispositivo loopback sui server sottoposti al bilanciamento del carico:

```
ip -6 addr add 3ffe:34::24:45/128 dev lo
ip -4 addr add 12.42.38.125/32 dev lo
```

Nota: È possibile utilizzare anche il comando `ifconfig`. Fare riferimento a Tabella 5 a pagina 71 per creare l'alias del dispositivo loopback mediante il comando `ifconfig`.

Una volta emesso uno dei comandi di configurazione sulla macchina, utilizzare sempre lo stesso comando (**ip** or **ifconfig**) altrimenti si verificheranno degli errori.

Sui sistemi Solaris 8, 9 e 10:

- Per gli indirizzi IPv6:
`ifconfig interface_name inet6 addif cluster_address/prefix_length up`

Ad esempio, per creare l'alias del dispositivo loopback sui server sottoposti al bilanciamento del carico:

```
ifconfig lo0 inet6 addif 3ffe:34::24:45/128 up
```

- Per gli indirizzi IPv4: invariato. Vedere Tabella 5 a pagina 71 per creare l'alias del dispositivo loopback sui server sottoposti al bilanciamento del carico.

Nei sistemi Windows 2003 (Windows 2000 e Windows NT non supportano IPv6):

- Per gli indirizzi IPv4: invariato. Vedere Tabella 5 a pagina 71 per creare l'alias del dispositivo loopback sui server sottoposti al bilanciamento del carico.
- Per gli indirizzi IPv6:
 1. Utilizzare il comando `ipconfig /all` per determinare il nome dell'interfaccia per il dispositivo loopback. Questo comando individua la connessione con una descrizione di Microsoft Loopback Adapter. Il seguente esempio rappresenta l'output del comando `ipconfig /all`, dove Microsoft Loopback Adapter è Ethernet adapter Local Area Connection 2, pertanto la connessione è Local Area Connection 2:

Configurazione IP Windows

```
Host Name . . . . . : ndserv10
```

```

Primary Dns Suffix . . . . . : rtp.raleigh.ibm.com
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : rtp.raleigh.ibm.com

```

Ethernet adapter Local Area Connection 2:

```

Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Loopback Adapter
Physical Address. . . . . : 02-00-4C-4F-4F-50
DHCP Enabled. . . . . : No
IP Address. . . . . : 9.42.92.158
Subnet Mask . . . . . : 255.255.252.0
IP Address. . . . . : 9.42.92.159
Subnet Mask . . . . . : 255.255.252.0
IP Address. . . . . : 2002:92a:8f7a:162:9:42:92:160
IP Address. . . . . : 2002:92a:8f7a:162:9:42:92:159
IP Address. . . . . : fe80::4cff:fe4f:4f50%4
Default Gateway . . . . . :
DNS Servers . . . . . : 127.0.0.1
                        fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1

```

2. Aggiungere l'indirizzo cluster al loopback utilizzando il comando netsh. Ad esempio:

```

netsh interface ipv6 add address "Local Area Connection 2"
2002:92a:8f7a:162:9:42:92:161

```

3. Emettere di nuovo il comando ipconfig /all; verrà visualizzato l'indirizzo aggiunto all'adattatore loopback. Ad esempio:

Ethernet adapter Local Area Connection 2:

```

Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Loopback Adapter
Physical Address. . . . . : 02-00-4C-4F-4F-50
DHCP Enabled. . . . . : No
IP Address. . . . . : 9.42.92.158
Subnet Mask . . . . . : 255.255.252.0
IP Address. . . . . : 9.42.92.159
Subnet Mask . . . . . : 255.255.252.0
IP Address. . . . . : 2002:92a:8f7a:162:9:42:92:161
IP Address. . . . . : 2002:92a:8f7a:162:9:42:92:160
IP Address. . . . . : 2002:92a:8f7a:162:9:42:92:159
IP Address. . . . . : fe80::4cff:fe4f:4f50%4
Default Gateway . . . . . :
DNS Servers . . . . . : 127.0.0.1
                        fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1

```

4. Abilitare l'inoltro per tutte le interfacce sulla macchina utilizzando il comando netsh interface ipv6 show interface. Tutte le interfacce riportate con un nome Local Area Connection devono avere l'inoltro IP abilitato. Ad esempio:

```

netsh interface ipv6>show interface
Querying active state...

```

Idx	Met	MTU	State	Name
---	----	----	-----	-----
6	2	1280	Disconnected	Teredo Tunneling Pseudo-Interface
5	0	1500	Connected	Local Area Connection
4	0	1500	Connected	Local Area Connection 2
3	1	1280	Connected	6to4 Pseudo-Interface
2	1	1280	Connected	Automatic Tunneling Pseudo-Interface
1	0	1500	Connected	Loopback Pseudo-Interface

```
netsh interface ipv6>set interface "Local Area Connection"
forwarding=enabled
Ok.

netsh interface ipv6>set interface "Local Area Connection 2"
forwarding=enabled
Ok.
```

Nei sistemi OS/2:

- Per gli indirizzi IPv6 e IPv4: invariato. Vedere Tabella 5 a pagina 71 per creare l'alias del dispositivo loopback sui server sottoposti al bilanciamento del carico.

Operazioni di configurazione del cluster per Linux suzSeries

Per Linux su zSeries, per impostare il Load Balancer sono richieste le seguenti operazioni di configurazione aggiuntive:

1. Configurare l'indirizzo del cluster utilizzando il comando `ip` o `ifconfig`.

Per gli indirizzi IPv6 o IPv4:

```
ip -versione addr add indirizzo_cluster/lunghezza_prefisso dev dispositivo
```

Ad esempio:

```
ip -4 addr add 12.42.38.125/24 dev eth0
ip -6 addr add 3ffe:34::24:45/64 dev eth0
```

2. Aggiungere una regola `iptables` per eliminare i pacchetti in entrata destinati all'indirizzo del cluster:

Per gli indirizzi IPv4:

```
iptables -t filter -A INPUT -d indirizzo_cluster -j DROP
```

Per gli indirizzi IPv6:

```
ip6tables -t filter -A INPUT -d indirizzo_cluster -j DROP
```

Ad esempio:

```
iptables -t filter -A INPUT -d 12.42.38.125 -j DROP
ip6tables -t filter -A INPUT -d 3ffe:34::24:45 -j DROP
```

Per annullare la configurazione precedente, utilizzare i seguenti comandi:

```
ip -versione addr del indirizzo_cluster/lunghezza_prefisso dev dispositivo
iptables -t filter -D INPUT -d indirizzo_cluster -j DROP
ip6tables -t filter -D INPUT -d indirizzo_cluster -j DROP
```

Comandi Dispatcher (dscontrol) in Load Balancer per IPv4 e IPv6

Poiché Load Balancer per IPv4 e IPv6 non supporta tutte le funzioni del componente, i comandi `dscontrol` validi per questa installazione sono un gruppo secondario dei comandi `dscontrol` per le installazioni Load Balancer che supportano solo IPv4. Questa sezione descrive le differenze di sintassi dei comandi ed elenca tutti i comandi `dscontrol` supportati per il componente Dispatcher in Load Balancer per IPv4 e IPv6.

Differenze di sintassi dei comandi

Nell'installazione di Load Balancer per IPv4 e IPv6, la sintassi del comando Dispatcher (`dscontrol`) rimane la stessa, con un'unica importante eccezione. Il delimitatore dei comandi `dscontrol` è un simbolo chiocciola (`@`), anziché i due punti (`:`), quando si utilizza Load Balancer per IPv4 e IPv6.

È stato necessario definire un delimitatore diverso dai due punti (:) perché nel formato IPv6 tale simbolo si utilizza nello schema di indirizzamento.

Quanto riportato di seguito illustra il comando `dscontrol` utilizzando un delimitatore chiocciola (@)

- per aggiungere un server IPv6 (30::200) sulla porta 80, in un cluster IPv6 (30::100)
`dscontrol server add 30::100@80@30::200`
- per aggiungere un server IPv4 (192.4.40.35) sulla porta 80, in un cluster IPv4 (192.4.40.30)
`dscontrol server add 192.4.40.30@80@192.4.20.35`

IMPORTANTE: quando nel presente documento si fa riferimento ai comandi, ricordarsi di sostituire i due punti (:) con il simbolo @ come delimitatore nei comandi `dscontrol`.

Comandi `dscontrol` supportati

Per informazioni dettagliate ed esempi della sintassi di tutti i comandi `dscontrol`, vedere Capitolo 27, “Riferimenti sui comandi per Dispatcher e CBR”, a pagina 337.

Di seguito viene riportato un riepilogo di tutti i comandi supportati di Dispatcher nell’installazione di Load Balancer per IPv4 e IPv6:

- `dscontrol advisor`
 - Tutti gli argomenti e le relative chiavi sono valide.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol advisor` — controlla l’advisor” a pagina 339.
- `dscontrol binlog`
 - Tutti gli argomenti e le relative chiavi sono valide.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol binlog` — controlla il file di log binario” a pagina 344.
- `dscontrol cluster`
 - Tutti gli argomenti sono validi. I soli valori validi per le chiavi sono: `address` e `proportions`.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol cluster` — configura i cluster” a pagina 345.
- `dscontrol executor`
 - Tutti gli argomenti sono validi. Per l’argomento `set`, gli unici valori della chiave validi sono `nfa`, `hatimeout` e `hasynctimeout`.

Per i sistemi che vengono eseguiti nello spazio utente, come i sistemi Linux:

- Tutti gli argomenti sono validi, tranne `configure` e `unconfigure`. È importante tenere presente che gli indirizzi cluster non devono avere un `alias` sullo stack del sistema.
- Per l’argomento `set`, gli unici valori della chiave validi sono `nfa` e `hatimeout`.
- Per l’argomento `configure`, è necessario immettere *prefix_length* anziché *netmask*.

Per IPv6, la lunghezza del prefisso rappresenta il numero di bit nella porzione di rete degli indirizzi IPv6. La lunghezza del prefisso definisce l’indirizzo di rete dall’indirizzo host.

Per IPv4, determinare la lunghezza del prefisso come riportato di seguito: se la subnet mask è 255.255.252.0, l'equivalente esadecimale è FF.FF.FC.0. In valori binari, il valore è 11111111 11111111 11111100 00000000. Un numero pari a 1 nella subnet mask determina la lunghezza del prefisso. Se sono presenti 22 numeri uno nella subnet mask, allora il prefisso sarà 22.

La sintassi per `executor configure` è:

```
dscontrol executor configure indirizzo_inerfaccia nome_interfaccia lunghezza_prefisso
```

Esempio con indirizzo IPv6:

```
dscontrol executor configure 2002:092a:8f7a:4226:9:37:240:99 en0 112
```

Esempio con indirizzo IPv4, se la subnet mask è 255.255.252.0:

```
dscontrol e config 191.60.20.20 en1 22
```

È importante tenere presente che il comando `executor configure` non viene utilizzato per i sistemi che vengono eseguiti nello spazio utente, come ad esempio i sistemi Linux su installazioni Load Balancer per IPv4 e IPv6.

- Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol executor` — controlla l’executor” a pagina 349.
- `dscontrol file`
 - Tutti gli argomenti e le relative chiavi sono valide.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol file` — gestisce i file di configurazione” a pagina 354.
- `dscontrol help`
 - Tutti gli argomenti sono validi tranne `host` (configurazione di una macchina remota), `rule` (configurazione delle regole) e `subagent` (configurazione di un agente secondario SNMP). I comandi `host`, `rule` e `subagent` non sono supportati.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol help` — visualizza o stampa la guida per il comando in questione” a pagina 356.
- `dscontrol highavailability`
 - Tutti gli argomenti sono validi. Tutti i valori per le chiavi sono validi tranne `both` perché la funzione di disponibilità elevata reciproca non è supportata.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol highavailability` — controlla la disponibilità elevata” a pagina 357.
- `dscontrol logstatus`
 - Tutti gli argomenti e le relative chiavi sono valide.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol logstatus` — visualizza le impostazioni log del server” a pagina 362.
- `dscontrol manager`
 - Tutti gli argomenti sono validi tranne `version`. Tutti i valori per le chiavi sono validi.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol manager` — controlla il gestore” a pagina 363.
- `dscontrol metric`
 - Tutti gli argomenti e le relative chiavi sono valide.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol metric` — configura le metriche di sistema” a pagina 368.
- `dscontrol port`

- Tutti gli argomenti sono validi ad eccezione di `halfopenaddressreport`, che non è supportato.

I seguenti valori sono gli unici valori validi delle chiavi per gli argomenti `add` e `set` sul comando `dscontrol port`:

- `staletimeout`
- `weightbound`
- `stickymask`

Per sistemi che vengono eseguiti nello spazio utente, come i sistemi Linux: i seguenti valori delle chiavi sono validi per gli argomenti `add` e `set` sul comando `dscontrol port`:

- `staletimeout`
- `weightbound`
- `selectionalgorithm`

Le opzioni per `selectionalgorithm` (algoritmo di selezione server) sono:

- `connection` – la selezione del server si basa su una semplice selezione round-robin (impostazione predefinita)
- `affinity` – la selezione del server si basa sull'affinità del client.

Ad esempio:

```
dscontrol port add cluster@port selectionalgorithm affinity
```

- Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol port` — configura le porte” a pagina 369.

- `dscontrol server`

- Tutti gli argomenti sono validi.

I seguenti valori delle chiavi sono validi per l'argomento `add` sul comando `dscontrol server`:

- `address`
- `advisorrequest`
- `advisorresponse`
- `collocated`

La parola chiave `collocated` è disponibile su tutti i sistemi operativi supportati tranne che su Windows e su sistemi che vengono eseguiti nello spazio utente, come i sistemi Linux.

- `fixedweight`
- `weight`

I seguenti valori delle chiavi sono validi per l'argomento `set` sul comando `dscontrol server`:

- `advisorrequest`
- `advisorresponse`
- `collocated`

La parola chiave `collocated` è disponibile su tutti i sistemi operativi supportati tranne che su Windows e su sistemi che vengono eseguiti nello spazio utente, come i sistemi Linux.

- `fixedweight`
- `weight`

- Per la descrizione dettagliata della sintassi dei comandi, vedere: “`dscontrol server` — configura i server” a pagina 381.

- `dscontrol set`

- Tutti gli argomenti e le relative chiavi sono valide.
- Per la descrizione dettagliata della sintassi dei comandi, vedere: “dscontrol set — configura il log del server” a pagina 387.
- dscontrol status
 - Tutti gli argomenti e le relative chiavi sono valide.
 - Per la descrizione dettagliata della sintassi dei comandi, vedere: “dscontrol status — mostra se il gestore e gli advisor sono in esecuzione” a pagina 388.

Comandi dscontrol non supportati

I seguenti comandi *non* sono disponibili per Dispatcher nell’installazione di Load Balancer per IPv4 e IPv6:

- dscontrol host (configura una macchina remota)
- dscontrol rule (configura le regole)
- dscontrol subagent (configura l’agente secondario SNMP)

Parte 3. Componente Content Based Routing (CBR)

Questa sezione fornisce informazioni per una rapida configurazione, considerazioni sulla pianificazione e descrive i metodi di configurazione del componente CBR di Load Balancer. Contiene i seguenti capitoli:

- Capitolo 9, “Configurazione di avvio rapido”, a pagina 97
- Capitolo 10, “Pianificazione di Content Based Routing”, a pagina 103
- Capitolo 11, “Configurazione di Content Based Routing”, a pagina 107

Capitolo 9. Configurazione di avvio rapido

Questo esempio di avvio rapido mostra come configurare tre stazioni di lavoro collegate localmente utilizzando il componente CBR con Caching Proxy al fine di bilanciare il carico del traffico Web tra due server Web. (Per semplicità, questo esempio mostra i server sullo stesso segmento di LAN, tuttavia, CBR non pone limitazioni all'uso di server sulla stessa LAN.)

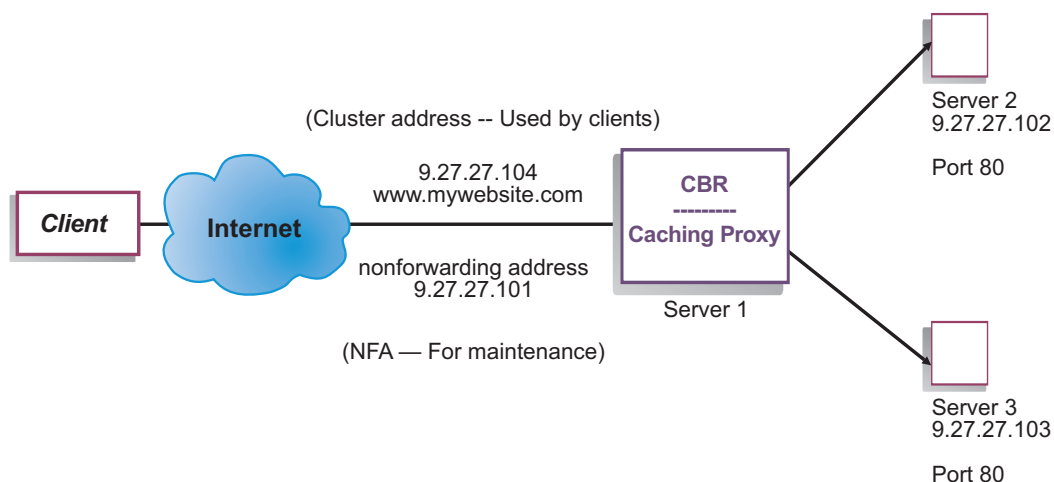


Figura 16. Una configurazione semplice di CBR locale

Elementi richiesti

Per l'esempio di avvio rapido, è necessario disporre di tre stazioni di lavoro e di quattro indirizzi IP. Una stazione di lavoro verrà utilizzata per il CBR, le altre due per i server Web. Ciascun server Web richiede un indirizzo IP. La stazione di lavoro CBR richiede un indirizzo effettivo e un indirizzo per il bilanciamento del carico.

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l'uso di Caching Proxy. Per ulteriori informazioni, vedere "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

Per utilizzare CBR, Caching Proxy deve essere installato sullo stesso server. Per configurare Caching Proxy per CBR, vedere "Fase 1. Configurazione di Caching Proxy per l'uso di CBR" a pagina 111.

Fasi di preparazione

1. Per questo esempio, impostare le stazioni di lavoro in modo da inserirle nello stesso segmento LAN. Verificare che il traffico di rete tra le tre macchine non debba attraversare router o bridge.
2. Configurare gli adattatori di rete delle tre stazioni di lavoro. Ad esempio, con la seguente configurazione di rete:

Stazione di lavoro	Nome	Indirizzo IP
1	server1.mywebsite.com	9.27.27.101
2	server2.mywebsite.com	9.27.27.102
3	server3.mywebsite.com	9.27.27.103
Netmask = 255.255.255.0		

Ciascuna stazione di lavoro contiene solo una scheda di interfaccia di rete Ethernet standard.

- Verificare che server1.mywebsite.com possa eseguire il ping su server2.mywebsite.com e server3.mywebsite.com.
- Verificare che server2.mywebsite.com e server3.mywebsite.com possano eseguire il ping su server1.mywebsite.com.
- Verificare che i server Web su server2.mywebsite.com e server3.mywebsite.com siano operativi. Utilizzare un browser Web per richiedere le pagine direttamente da **http://server2.mywebsite.com** (ad esempio, .../member/index.html) e **http://server3.mywebsite.com** (ad esempio .../guest/index.html).
- Acquisire un indirizzo IP valido per questo segmento LAN. Si tratta dell'indirizzo cluster fornito agli utenti che desiderano accedere al sito. Per questo esempio, vengono utilizzate le seguenti informazioni:

Name= www.mywebsite.com
IP=9.27.27.104

Configurazione del componente CBR

CBR consente di creare una configurazione dalla riga comandi, con la configurazione guidata o mediante l'interfaccia utente grafica (GUI). In questo esempio di avvio rapido, le fasi di configurazione sono illustrate utilizzando la riga comandi.

Nota: i valori dei parametri devono essere immessi utilizzando l'alfabeto inglese. Le uniche eccezioni sono rappresentate dai nomi host e dai nomi file.

Configurazione mediante la riga comandi

Da un prompt dei comandi, effettuare le seguenti operazioni:

- Avviare cbrserver. Eseguire il seguente comando come utente root o amministratore: **cbrserver**

Nota: Per la piattaforma Windows: avviare cbrserver (Content Based Routing) dal pannello Servizi: **Start > Impostazioni** (per Windows 2000) > **Pannello di controllo > Strumenti di amministrazione > Servizi**.

- Avviare la funzione executor di CBR:

cbrcontrol executor start

- Avviare Caching Proxy. (Caching Proxy può essere avviato in qualsiasi momento dopo l'avvio della funzione executor):

ibmproxy

Nota: sulle piattaforme Windows: è possibile avviare Caching Proxy anche dal pannello Servizi: **Start > Impostazioni** (in Windows 2000) > **Pannello di controllo > Strumenti di amministrazione > Servizi**.

- Aggiungere il cluster (il nome host, il sito Web, i client a cui collegarsi) alla configurazione CBR:

cbrcontrol cluster add www.mywebsite.com

5. Aggiungere l'indirizzo cluster (9.27.27.104) del sito Web alla scheda di interfaccia di rete sulla macchina CBR. Per ulteriori informazioni, consultare "Fase 5. Creazione dell'alias della scheda di interfaccia di rete (NIC) (facoltativa)" a pagina 113.
6. Aggiungere la porta del protocollo http alla configurazione CBR:
cbrcontrol port add www.mywebsite.com:80
7. Aggiungere ciascun server Web alla configurazione CBR:
cbrcontrol server add www.mywebsite.com:80:server2.mywebsite.com
cbrcontrol server add www.mywebsite.com:80:server3.mywebsite.com
8. Aggiungere le regole di contenuto alla configurazione CBR. (Una regola definisce come distinguere una richiesta URL per poterla inviare ai server o al gruppo di server appropriato):
cbrcontrol rule add www.mywebsite.com:80:memberRule type content
pattern uri=*/member/*
cbrcontrol rule add www.mywebsite.com:80:guestRule type content pattern
uri=*/guest/*

In questo esempio, se si utilizza la regola di contenuto, le richieste client indirizzate a un sito Web `www.mywebsite.com` sono inviate a un server diverso in base a una directory contenuta nel relativo percorso di richiesta URI. Per ulteriori informazioni, vedere Appendice B, "Sintassi della regola di contenuto (modello)", a pagina 463.

9. Aggiungere i server alle regole:
cbrcontrol rule useserver www.mywebsite.com:80:memberRule
server2.mywebsite.com
cbrcontrol rule useserver www.mywebsite.com:80:guestRule
server3.mywebsite.com

CBR eseguirà ora il bilanciamento del carico in base alla regola basata sul contenuto. Un client con una richiesta URL contenente `/member/` sarà indirizzato al `server2.mywebsite.com`. Un client con una richiesta URL contenente `/guest/` sarà indirizzato al `server3.mywebsite.com`.

10. Avviare la funzione gestore di CBR:
cbrcontrol manager start
11. Avviare la funzione advisor di CBR:
cbrcontrol advisor start http 80

A questo punto, CBR garantisce che le richieste client non verranno inviate a un server Web in errore.

La configurazione di base, con i server collegati localmente, è ora completa.

Verifica della configurazione

Verificare se la configurazione è in esecuzione:

1. Da un browser Web, andare all'indirizzo **`http://www.mywebsite.com/member/index.htm`**. Se viene visualizzata una pagina, allora la configurazione funziona correttamente.
2. Ricaricare la pagina nel browser Web.
3. Controllare i risultati del seguente comando:
cbrcontrol server report www.mywebsite.com:80:

La colonna delle connessioni totali dei due server dovrebbe visualizzare "2".

Configurazione mediante l'interfaccia utente grafica (GUI)

Per informazioni sull'uso della GUI in CBR, vedere "GUI" a pagina 109 and see Appendice A, "GUI: istruzioni generali", a pagina 455.

Configurazione mediante la procedura guidata

Per informazioni sull'uso della configurazione guidata di CBR, vedere "Configurazione guidata" a pagina 110.

Tipi di configurazioni di cluster, porte, server

Sono disponibili diversi metodi per configurare CBR in modo che supporti il sito. Se si dispone di un solo nome host per il sito, a cui si collegheranno tutti gli utenti, è possibile definire un unico cluster di server. Per ciascuno di questi server, configurare una porta dedicata alla comunicazione con CBR. Vedere Figura 9 a pagina 46.

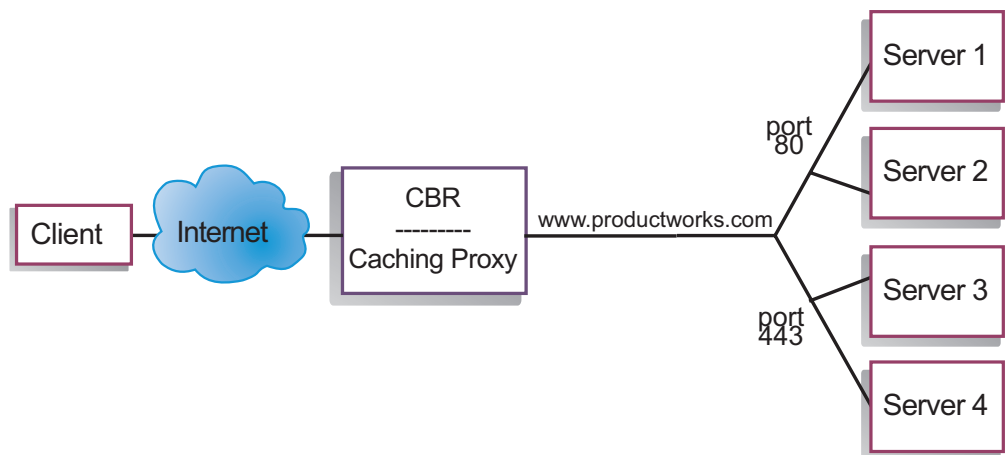


Figura 17. Esempio di CBR configurato con un unico cluster e 2 porte

In questo esempio per il componente CBR, un cluster è definito all'indirizzo `www.productworks.com`. Questo cluster dispone di due porte: la porta 80 per il traffico HTTP e la porta 443 per il traffico SSL. Un client che invia una richiesta a `http://www.productworks.com` (porta 80) sarà indirizzato a un server diverso da quello destinato a un client che invia la sua richiesta a `https://www.productworks.com` (porta 443).

Se il sito è molto grande e contiene molti server dedicati a ciascun protocollo supportato, sarebbe opportuno configurare altrimenti il componente CBR. In questo caso, è possibile definire un cluster per ciascun protocollo con un'unica porta ma con molti server, come mostrato nella Figura 10 a pagina 47.

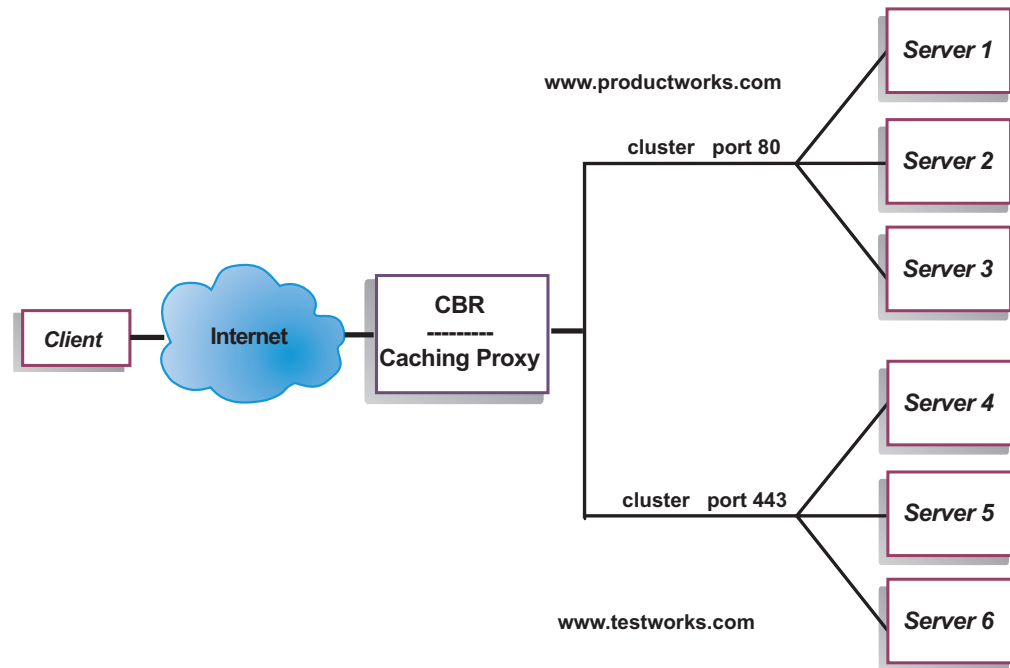


Figura 18. Esempio di CBR configurato con due cluster, una porta ciascuno

In questo esempio per il componente CBR, sono definiti due cluster: `www.productworks.com` per la porta 80 (HTTP) e `www.testworks.com` per la porta 443 (SSL).

Se il sito deve ospitare i contenuti di diverse aziende e reparti, ciascuno dei quali è indirizzato al sito con URL diversi, sarà opportuno adottare una terza configurazione. In questo caso, è possibile definire un cluster per ciascuna azienda o reparto, quindi definire le porte su cui si desidera ricevere le connessioni a quell'URL, come mostrato nella Figura 11 a pagina 48.

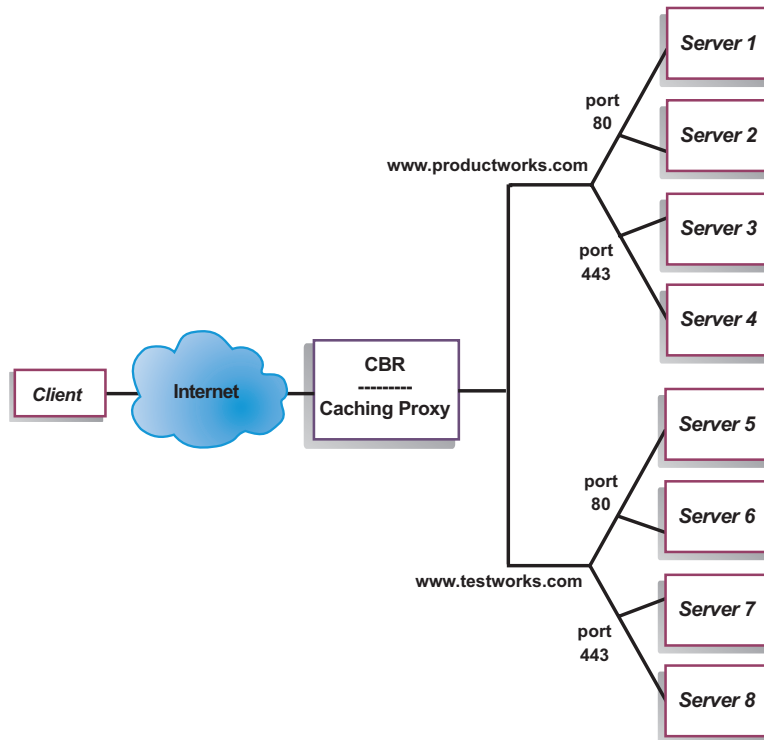


Figura 19. Esempio di CBR configurato con 2 cluster, 2 porte ciascuno

In questo esempio per il componente CBR, sono definiti due cluster con la porta 80 (HTTP) e la porta 443 (SSL) per ciascun sito con indirizzo `www.productworks.com` e `www.testworks.com`.

Capitolo 10. Pianificazione di Content Based Routing

Questo capitolo descrive i fattori che il responsabile della pianificazione di rete deve considerare prima di installare e configurare il componente CBR con Caching Proxy.

- Vedere Capitolo 3, “Gestione della rete: determinazione delle funzioni di Load Balancer da utilizzare”, a pagina 19 per una panoramica delle funzioni disponibili per la gestione della rete.
- Vedere Capitolo 11, “Configurazione di Content Based Routing”, a pagina 107, per informazioni sulla configurazione dei parametri di bilanciamento del carico di CBR.
- Vedere Capitolo 22, “Funzioni avanzate di Dispatcher, CBR e Site Selector”, a pagina 195 per informazioni sulla configurazione di Load Balancer per funzioni più avanzate.
- Vedere Capitolo 24, “Funzionamento e gestione di Load Balancer”, a pagina 253 per informazioni sull’amministrazione autenticata remota, sui log di Load Balancer e sull’uso dei componenti di Load Balancer.

Questo capitolo include le seguenti sezioni:

- “Considerazioni sulla pianificazione”
- “Uso del bilanciamento del carico basato sulle regole con CBR” a pagina 105
- “Bilanciamento del carico tra connessioni protette (SSL)” a pagina 105
- “Bilanciamento del carico client-proxy in SSL e proxy-server in HTTP” a pagina 106

Considerazioni sulla pianificazione

Il componente CBR consente di bilanciare il carico del traffico HTTP e SSL utilizzando Caching Proxy per inoltrare le richieste via proxy. Il componente CBR consente di bilanciare il carico dei server configurati con un apposito file di configurazione CBR tramite i comandi `cbrcontrol`.

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro `cbr` del componente Dispatcher di Load Balancer, per instradare i contenuti senza l’uso di Caching Proxy. Per ulteriori informazioni, vedere “Instradamento basato sul contenuto di Dispatcher (metodo di inoltro `cbr`)” a pagina 53.

CBR è molto simile a Dispatcher nella sua struttura. CBR è composto dalle seguenti funzioni:

- **cbrserver** gestisce le richieste provenienti dalla riga comandi e destinate all’**executor**, al gestore e agli advisor.
- L’**executor** supporta il bilanciamento del carico delle richieste client. Per poter utilizzare il componente CBR, è necessario che l’**executor** sia stato avviato.
- Il **gestore** imposta i pesi utilizzati dall’**executor** in base a:
 - Contatori interni all’**executor**
 - Informazioni restituite dai server fornite dagli advisor

- Informazioni restituite da un programma di monitoraggio del sistema, ad esempio Metric Server.

L'uso del gestore è facoltativo. Tuttavia, se il gestore non viene utilizzato, il bilanciamento del carico verrà eseguito utilizzando la pianificazione con il metodo round-robin basata sui pesi dei server correnti e gli advisor non saranno disponibili.

- Gli **advisor** interrogano i server e analizzano i risultati per protocollo prima di interpellare il gestore affinché imposti i pesi in modo appropriato. L'uso di questi advisor in una configurazione tipica potrebbe non essere necessario. È possibile anche scrivere advisor personalizzati. L'uso degli advisor è facoltativo ma consigliato. Load Balancer fornisce un advisor Caching Proxy (cachingproxy). Per ulteriori informazioni, vedere "Advisor" a pagina 181.
- Per configurare e gestire l'executor, gli advisor e il gestore, utilizzare la riga comandi (**cbrcontrol**) o l'interfaccia utente grafica (**lbadmin**).

Le tre funzioni chiave di CBR (executor, gestore e advisor) interagiscono per bilanciare e distribuire le richieste in entrata tra i server. Oltre a bilanciare il carico delle richieste, l'executor monitora il numero di nuove connessioni e il numero delle connessioni attive e fornisce tali informazioni al gestore.

Bilanciamento del carico di richieste per tipi diversi di contenuto

Il componente CBR consente di specificare un gruppo di server che gestirà una richiesta in base all'espressione regolare corrispondente al contenuto della richiesta client. CBR consente di suddividere il proprio sito in partizioni in modo che gruppi di server diversi possano provvedere a servizi di applicazioni o contenuti diversi. Questa partizione è trasparente per i client che accedono al proprio sito.

Suddivisione del contenuto del sito per ottimizzare i tempi di risposta

Una possibile soluzione di suddivisione del sito sarebbe assegnare a un gruppo di server la gestione delle richieste cgi e a un altro gruppo di server la gestione di tutte le altre richieste. Questo impedirebbe agli script cgi che svolgono calcoli complessi di rallentare i server in caso di normale traffico HTML con conseguente ottimizzazione complessiva dei tempi di risposta ai client. Questo schema consentirebbe anche di assegnare stazioni di lavoro più potenti alle richieste normali. Ciò migliorerebbe i tempi di risposta ai client senza dover affrontare le spese di un aggiornamento di tutti i server. Inoltre, questo consentirebbe di assegnare stazioni di lavoro più potenti alle richieste cgi.

Un'altra soluzione di suddivisione del sito potrebbe essere quella di indirizzare a un gruppo di server i client che accedono a pagine che prevedono la registrazione e a un altro gruppo di server tutte le altre richieste. Questo impedirebbe ai browser che accedono fortuitamente al sito di impegnare risorse che potrebbero essere altrimenti utilizzate dai client che intendono invece registrarsi. Inoltre, consentirebbe di dedicare stazioni di lavoro più potenti ai client che hanno completato la registrazione.

Naturalmente è possibile combinare i metodi sopra descritti per ottenere una flessibilità ancora maggiore e un servizio migliore.

Backup del contenuto del server Web

Poiché CBR consente di specificare più server per ciascun tipo di richiesta, il carico delle richieste può essere bilanciato per ottimizzare i tempi di risposta ai client. L'assegnazione di ciascun tipo di contenuto a più server protegge il sito in caso di malfunzionamento di una stazione di lavoro o di un server. CBR riconosce il malfunzionamento e continua a bilanciare il carico delle richieste client sugli altri server del gruppo.

Uso di più processi Caching Proxy per migliorare l'utilizzo della CPU

Caching Proxy comunica con un processo CBR tramite la relativa interfaccia del plug-in. Affinché ciò funzioni, CBR deve essere eseguito sulla macchina locale. Poiché questi due processi sono distinti, più istanze di Caching Proxy possono essere in esecuzione e funzionanti con un'unica istanza di CBR. Questa configurazione potrebbe consentire di isolare gli indirizzi o le funzionalità tra i Caching Proxy oppure di migliorare l'uso delle risorse della macchina grazie a più Caching Proxy che gestiscono il traffico dei client. Le istanze proxy possono restare in ascolto su porte diverse o essere associati a indirizzi IP univoci sulla stessa porta, a seconda di ciò che meglio soddisfa i requisiti di traffico.

Uso del bilanciamento del carico basato sulle regole con CBR

CBR con Caching Proxy esamina le richieste HTTP utilizzando tipi di regole specifici. Quando in esecuzione, Caching Proxy accetta le richieste client e interroga il componente CBR per individuare il server più adatto. Sulla base di questa interrogazione, CBR confronta la richiesta a fronte di un gruppo di regole in base a un ordine di priorità. Quando individua la regola corrispondente, sceglie un server adatto da un gruppo precedentemente configurato. Infine, CBR notifica a Caching Proxy il server proxy attraverso il quale dovrà essere inviata la richiesta.

Una volta definito un cluster da sottoporre al bilanciamento del carico, è necessario accertarsi che tutte le richieste indirizzate a quel cluster abbiano una regola che consenta di scegliere un server. Se non viene trovata una regola che corrisponda a una determinata richiesta, il client riceve una pagina di errore da Caching Proxy. Il modo più facile per garantire che tutte le richieste corrispondano a una regola è creare una regola del tipo "sempre true" e assegnarle una priorità molto elevata. Verificare che i server utilizzati da questa regola possano gestire tutte le richieste che non sono gestite esplicitamente dalle regole con priorità inferiore. (Nota: le regole con priorità inferiore vengono valutate per prime.)

Per ulteriori informazioni, vedere "Configurazione del bilanciamento del carico in base alle regole" a pagina 205.

Bilanciamento del carico tra connessioni protette (SSL)

CBR con Caching Proxy può ricevere sia la trasmissione SSL dal client al proxy (lato client-proxy) sia supportare la trasmissione dal proxy a un server SSL (lato proxy-server). In una configurazione CBR, la definizione su un server di una porta SSL dedicata a ricevere le richieste SSL provenienti dal client, offre la possibilità di gestire un sito totalmente protetto e di utilizzare CBR per bilanciare il carico tra i server (SSL) protetti.

Oltre ad altre modifiche al file `ibmproxy.conf` per CBR, è necessario aggiungere un'altra istruzione di configurazione al file `ibmproxy.conf` affinché Caching Proxy abiliti la codifica SSL sul lato proxy-server. Il formato deve essere:

```
proxy modello_uri modello_url indirizzo
```

dove *modello_uri* è un modello a cui corrispondere (ad esempio: /secure/*),
modello_url è un URL di sostituzione (ad esempio: https://clusterA/secure/*) e
indirizzo è l'indirizzo cluster (ad esempio: clusterA).

Bilanciamento del carico client-proxy in SSL e proxy-server in HTTP

CBR con Caching Proxy può anche ricevere trasmissioni SSL dai client e decodificare le richieste SSL prima di inviarle a un server HTTP attraverso un proxy. Affinché CBR supporti la trasmissione client-proxy in SSL e proxy-server in HTTP, è prevista una parola chiave facoltativa **mapport** per il comando `cbrcontrol server`. Utilizzare questa parola chiave quando si desidera indicare che la porta sul server è diversa dalla porta dove arrivano le richieste in entrata provenienti dal client. Di seguito viene riportato un esempio di aggiunta di una porta tramite la parola chiave `mapport`, dove la porta del client è 443 (SSL) e la porta del server è 80 (HTTP):

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

Il numero di porta di `mapport` può essere un qualsiasi numero intero positivo. Il valore predefinito è il numero della porta dove arrivano le richieste in entrata provenienti dal client.

Poiché CBR deve essere in grado di fornire informazioni su una richiesta HTTP per un server configurato sulla porta 443 (SSL), viene fornito un advisor speciale *ssl2http*. Questo advisor viene avviato sulla porta 443 (la porta delle richieste in entrata provenienti dal client) e fornisce informazioni sui server configurati su tale porta. Se vi sono due cluster configurati e per ciascun cluster la porta è 443 e i server sono configurati con un valore `mapport` diverso, un'unica istanza dell'advisor può aprire di conseguenza la porta appropriata. Di seguito viene riportato un esempio di questa configurazione:

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

Capitolo 11. Configurazione di Content Based Routing

Prima di eseguire le operazioni riportate in questo capitolo, vedere Capitolo 10, “Pianificazione di Content Based Routing”, a pagina 103. Questo capitolo illustra come creare una configurazione di base per il componente CBR di Load Balancer.

- Vedere Capitolo 21, “Funzioni gestore, advisor e Metric Server per Dispatcher, CBR e Site Selector”, a pagina 175 e Capitolo 22, “Funzioni avanzate di Dispatcher, CBR e Site Selector”, a pagina 195 per configurazioni più complesse di Load Balancer.
- Vedere Capitolo 24, “Funzionamento e gestione di Load Balancer”, a pagina 253 per informazioni sull’amministrazione autenticata remota, sui log di Load Balancer e sull’uso dei componenti di Load Balancer.

Panoramica delle attività di configurazione

Prima di iniziare le procedure di configurazione della tabella, verificare che la macchina CBR e tutte le macchine server siano collegate in rete, abbiano indirizzi IP validi e siano in grado di eseguire il ping reciprocamente.

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l’uso di Caching Proxy. Per ulteriori informazioni, vedere “Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)” a pagina 53.

Tabella 7. Attività di configurazione per il componente CBR

Attività	Descrizione	Informazioni correlate
Configurazione della macchina CBR.	Individuazione dei requisiti.	“Configurazione della macchina CBR” a pagina 111
Configurazione delle macchine da sottoporre a bilanciamento del carico.	Configurazione del bilanciamento del carico.	“Fase 7. Definizione delle macchine server con bilanciamento del carico” a pagina 115

Metodi di configurazione

Per creare una configurazione base del componente CBR di Load Balancer, sono disponibili quattro metodi di base:

- Riga comandi
- Script
- Interfaccia utente grafica (GUI)
- Configurazione guidata

Per poter utilizzare il componente CBR, è necessario che Caching Proxy sia installato.

Nota: Caching Proxy è un servizio che viene avviato automaticamente per impostazione predefinita dopo l’installazione. Prima di avviare la funzione

server CBR (cbrserver), è necessario arrestare Caching Proxy e modificare il servizio Caching Proxy in modo da essere avviato manualmente e non automaticamente.

- Per sistemi Linux o UNIX: arrestare Caching Proxy individuando l'identificativo del processo mediante il comando `ps -ef | grep ibmproxy` e modificare il processo utilizzando il comando `kill ID_processo`.
- Per sistemi Windows: arrestare Caching Proxy dal pannello Servizi.

Riga comandi

È il mezzo più diretto per la configurazione di CBR. I valori dei parametri dei comandi devono essere immessi utilizzando l'alfabeto inglese. Le uniche eccezioni riguardano i nomi host, utilizzati ad esempio nei comandi cluster e server, e i nomi di file.

Per avviare il componente CBR dalla riga comandi:

- Su sistemi Linux o UNIX: come utente root, emettere il comando **cbrserver** dal prompt dei comandi. Per arrestare il servizio, emettere **cbrserver stop**.
Su sistemi Windows: fare clic su **Start > Impostazioni** (per Windows 2000) > **Pannello di controllo > Strumenti di amministrazione > Servizi**. Fare clic con il tasto destro del mouse su **IBM Content Based Routing** e selezionare **Avvia**. Per arrestare il servizio, effettuare le stesse operazioni e selezionare **Arresta**.
- Quindi, immettere i comandi di controllo del CBR desiderati per impostare la propria configurazione. Le procedure descritte nel presente manuale presumono l'uso della riga comandi. Il comando è **cbrcontrol**. Per ulteriori informazioni sui comandi, vedere Capitolo 27, "Riferimenti sui comandi per Dispatcher e CBR", a pagina 337.
- Avviare Caching Proxy. Immettere il comando **ibmproxy** dal prompt dei comandi. (Prima di avviare Caching Proxy, è necessario avviare l'executor.)

Nota: Per piattaforme Windows: avviare Caching Proxy dal pannello Servizi facendo clic su **Start > Impostazioni** (per Windows 2000) > **Pannello di controllo > Strumenti di amministrazione > Servizi**.

È possibile immettere una versione abbreviata dei parametri del comando **cbrcontrol**. A tal fine, è sufficiente immettere le lettere che designano in modo univoco i parametri. Ad esempio, per richiamare la guida sul comando di salvataggio file, è possibile digitare **cbrcontrol he f** anziché **cbrcontrol help file**.

Per avviare l'interfaccia della riga comandi: immettere **cbrcontrol** per ricevere il prompt dei comandi per **cbrcontrol**.

Per chiudere l'interfaccia della riga comandi: immettere **exit** o **quit**.

Note:

1. Sulla piattaforma Windows, dsserver del componente Dispatcher viene avviato automaticamente. Se si utilizza solo il componente CBR e non il componente Dispatcher, è possibile arrestare l'avvio automatico di dsserver nel modo indicato di seguito:
 - a. Nella finestra Servizi, fare clic con il tasto destro del mouse su IBM Dispatcher.
 - b. Selezionare Proprietà.
 - c. Nel campo **Tipo di avvio**, selezionare Manuale.
 - d. Fare clic su OK e chiudere la finestra Servizi.

- Quando si configura il componente CBR (Content Based Routing) dal prompt dei comandi del sistema operativo anziché dal prompt `cbrcontrol>>`, prestare attenzione all'uso dei seguenti caratteri:

- () parentesi di apertura e chiusura
- & E commerciale
- | barra verticale
- ! punto esclamativo
- * asterisco

La shell del sistema operativo potrebbe interpretarli come caratteri speciali e trasformarli per alternare il testo prima che `cbrcontrol` li possa valutare.

I caratteri speciali dell'elenco sopra riportato sono caratteri opzionali del comando **`cbrcontrol rule add`** e vengono utilizzati per specificare un modello per una regola di contenuto. Ad esempio, il seguente comando potrebbe essere valido solo quando si utilizza il prompt `cbrcontrol>>`.

```
rule add 10.1.203.4:80:cbr_prod_rule_ek type content
  pattern uri=/nipoe/*
```

Affinché questo stesso comando funzioni sul prompt del sistema operativo, è necessario aggiungere le doppie virgolette (" ") prima e dopo il modello, come indicato di seguito:

```
cbrcontrol rule add 10.1.203.4:80:cbr_prod_rule_ek type content
  pattern "uri=/nipoe/*"
```

Se non si utilizzano le virgolette, è possibile che il modello venga troncato quando la regola viene salvata nel componente CBR. Notare che le virgolette non sono supportate quando si utilizza il prompt dei comandi `cbrcontrol>>`.

Script

È possibile immettere i comandi per la configurazione di CBR in un file script di configurazione per eseguirli tutti insieme.

Nota: Per eseguire rapidamente il contenuto di un file di script (ad esempio, `myscript`), utilizzare uno dei seguenti comandi:

- Per aggiornare la configurazione corrente, eseguire i comandi eseguibili dal proprio file di script:
`cbrcontrol file appendload myscript`
- Per sostituire completamente la configurazione corrente, eseguire i comandi eseguibili dal proprio file di script:
`cbrcontrol file newload myscript`

Per salvare la configurazione corrente nel file di script (ad esempio, `savescript`), eseguire il comando:

```
cbrcontrol file save savescript
```

Questo comando salva il file di script della configurazione nella directory **`...ibm/edge/lb/servers/configurations/cbr`**.

GUI

Per istruzioni generali e un esempio della GUI, vedere Figura 41 a pagina 456.

Per avviare la GUI, effettuare le seguenti operazioni.

- Verificare che `cbrserver` sia in esecuzione. Come utente `root` o amministratore, immettere quanto segue da un prompt dei comandi: **`cbrserver`**

2. A seconda del sistema operativo utilizzato, effettuare una delle seguenti operazioni:
 - Per sistemi AIX, HP-UX, Linux o Solaris: immettere **lbadmin**
 - Su sistemi Windows fare clic su **Start > Programmi > IBM WebSphere > Edge Components > IBM Load Balancer > Load Balancer**
3. Avviare Caching Proxy. (Dalla GUI, è necessario anzitutto collegarsi all'host ed avviare l'executor per il componente CBR prima di avviare Caching Proxy.) Effettuare una delle seguenti operazioni:
 - Su sistemi AIX, HP-UX, Linux o Solaris: per avviare Caching Proxy, immettere **ibmpoxy**
 - Su sistemi Windows: per avviare Caching Proxy, fare clic su **Start > Impostazioni** (per Windows 2000) > **Pannello di controllo > Strumenti di amministrazione > Servizi**

Per configurare il componente CBR dalla GUI, è necessario anzitutto selezionare **Content Based Routing** nella struttura ad albero. È possibile avviare il gestore dopo essersi collegati a un host. Inoltre, è possibile creare cluster contenenti porte e server e avviare gli advisor per il gestore.

La GUI può essere utilizzata per eseguire le operazioni che verrebbero effettuate con il comando **cbrcontrol**. Ad esempio, per definire un cluster utilizzando la riga comandi, si deve immettere il comando **cbrcontrol cluster add cluster**. Per definire un cluster dalla GUI, fare clic con il tasto destro del mouse su Executor, quindi nel menu a comparsa fare clic su **Add Cluster**. Immettere l'indirizzo del cluster nella finestra a comparsa, quindi fare clic su **OK**.

I file di configurazione CBR esistenti possono essere caricati utilizzando l'opzione **Load New Configuration** (per sostituire completamente la configurazione corrente) e l'opzione **Append to Current Configuration** (per aggiornare la configurazione corrente) contenuti nel menu a comparsa **Host**. Salvare periodicamente la configurazione di CBR su un file utilizzando l'opzione **Save Configuration File As** contenuta nel menu a comparsa **Host**. Il menu **File** situato sulla parte superiore della GUI consente di salvare le connessioni host correnti su un file o di ripristinare le connessioni nei file esistenti per tutti i componenti di Load Balancer.

È possibile accedere alla guida (**Help**) facendo clic sull'icona punto interrogativo nell'angolo in alto a destra della finestra di Load Balancer.

- **Help: Field level** — descrive i valori predefiniti di ciascun campo
- **Help: How do I** — elenca le attività possibili da questa schermata
- **InfoCenter** — consente l'accesso centralizzato alle informazioni sul prodotto

Per eseguire un comando dalla GUI: evidenziare il nodo Host dalla struttura ad albero della GUI e selezionare **Send command...** dal menu a comparsa Host. Nel campo di immissione dei comandi, digitare il comando che si desidera eseguire, ad esempio: **executor report**. I risultati e la cronologia dei comandi in esecuzione nella sessione corrente vengono visualizzati nella finestra fornita.

Per ulteriori informazioni sull'uso della GUI, vedere Appendice A, "GUI: istruzioni generali", a pagina 455.

Configurazione guidata

Se si utilizza la configurazione guidata, effettuare le seguenti operazioni:

1. Avviare cbrserver: immettere **cbrserver** sul prompt dei comandi come utente root o amministratore.
2. Avviare la funzione di configurazione guidata di CBR.
Avviare la configurazione guidata dal prompt dei comandi immettendo **cbrwizard**. In alternativa, selezionare Configuration Wizard dal menu del componente CBR presente nella GUI.
3. Avviare Caching Proxy per bilanciare il carico del traffico HTTP o HTTPS (SSL).
Su sistemi AIX, HP-UX, Linux o Solaris: per avviare Caching Proxy, immettere **ibmproxy**
Su sistemi Windows: per avviare Caching Proxy, fare clic su **Start > Impostazioni** (per Windows 2000) > **Pannello di controllo > Strumenti di amministrazione > Servizi**

La configurazione guidata di CBR illustra nei dettagli come creare una configurazione di base per il componente CBR. Pone delle domande relative alla rete e fornisce le istruzioni su come configurare un cluster in modo che il componente CBR possa eseguire il bilanciamento del carico sul traffico esistente tra i server di un gruppo.

Configurazione della macchina CBR

Per poter configurare la macchina CBR, è necessario disporre dei diritti di utente root (in AIX, HP-UX, Linux o Solaris) o di amministratore (in Windows).

Ciascun cluster di server configurato deve disporre di un indirizzo IP. Un indirizzo cluster è un indirizzo associato a un nome host (ad esempio, www.company.com). Questo indirizzo IP viene utilizzato da un client per collegarsi ai server di un cluster. In particolare, questo indirizzo si trova nella richiesta URL proveniente dal client. Tutte le richieste eseguite sullo stesso indirizzo cluster sono sottoposte a bilanciamento del carico da parte di CBR.

Solo per sistemi Solaris: prima di utilizzare il componente CBR, è necessario modificare i valori predefiniti del sistema per gli IPC (Inter-Process Communication). Le dimensioni massime di un segmento di memoria condivisa e il numero di identificatori di semaforo devono essere aumentati. Per ottimizzare il sistema in modo che supporti CBR, modificare il file **/etc/system** sul proprio sistema aggiungendo le seguenti istruzioni, quindi riavviare:

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

Se non si aumenta il segmento di memoria condiviso ai valori sopra riportati, il comando **cbrcontrol executor start** non verrà eseguito correttamente.

Fase 1. Configurazione di Caching Proxy per l'uso di CBR

Per poter utilizzare il componente CBR, è necessario che Caching Proxy sia installato.

Nota: Caching Proxy è un servizio che viene avviato automaticamente per impostazione predefinita dopo l'installazione. Prima di avviare la funzione

server CBR (cbrserver), è necessario arrestare Caching Proxy e modificare il servizio Caching Proxy in modo da essere avviato manualmente e non automaticamente.

- Su sistemi AIX, HP-UX, Linux e Solaris: per arrestare Caching Proxy, individuare l'identificatore di processo tramite il comando `ps -ef | grep ibmproxy`, quindi terminare il processo utilizzando il comando `kill process_id`.
- Per sistemi Windows: arrestare Caching Proxy dal pannello Servizi.

È necessario apportare le seguenti modifiche al file di configurazione di Caching Proxy (ibmproxy.conf):

Accertarsi che la direttiva URL in entrata **CacheByIncomingUrl** sia disattivata (impostazione predefinita).

Nella sezione relativa alla regola di mappatura del file di configurazione, per ciascun cluster, aggiungere una regola di mappatura analoga a:

```
Proxy    /* http://cluster.domain.com/*    cluster.domain.com
```

Nota: CBR imposta il protocollo, il server e la porta di destinazione in un secondo tempo.

Per il plug-in di CBR devono essere modificate quattro voci:

- ServerInit
- PostAuth
- PostExit
- ServerTerm

Ciascuna voce deve trovarsi su un'unica riga. Il file ibmproxy.conf contiene diverse istanze di "ServerInit", una per ciascun plug-in. Le voci di "CBR Plug-in" devono essere modificate e prive di commento.

Di seguito vengono riportate le aggiunte specifiche da inserire nel file di configurazione per ciascun sistema operativo.

Figura 20. File di configurazione di CBR su sistemi AIX, Linux e Solaris

```
ServerInit  /opt/ibm/edge/lb/servers/lib/liblbcbcr.so:ndServerInit
PostAuth    /opt/ibm/edge/lb/servers/lib/liblbcbcr.so:ndPostAuth
PostExit    /opt/ibm/edge/lb/servers/lib/liblbcbcr.so:ndPostExit
ServerTerm  /opt/ibm/edge/lb/servers/lib/liblbcbcr.so:ndServerTerm
```

Figura 21. File di configurazione di CBR per sistemi HP-UX

```
ServerInit  /opt/ibm/edge/lb/servers/lib/liblbcbcr.sl:ndServerInit
PostAuth    /opt/ibm/edge/lb/servers/lib/liblbcbcr.sl:ndPostAuth
PostExit    /opt/ibm/edge/lb/servers/lib/liblbcbcr.sl:ndPostExit
ServerTerm  /opt/ibm/edge/lb/servers/lib/liblbcbcr.sl:ndServerTerm
```

Figura 22. File di configurazione di CBR su sistemi Windows

```
ServerInit C:\Program Files\IBM\edge\lb\servers\lib\liblbcbr.dll:ndServerInit
PostAuth C:\Program Files\IBM\edge\lb\servers\lib\liblbcbr.dll:ndPostAuth
PostExit C:\Program Files\IBM\edge\lb\servers\lib\liblbcbr.dll:ndPostExit
ServerTerm C:\Program Files\IBM\edge\lb\servers\lib\liblbcbr.dll:ndServerTerm
```

Fase 2. Avvio della funzione server

Per avviare la funzione server CBR, digitare **cbrserver** sulla riga comandi.

Un file di configurazione predefinito (default.cfg) viene automaticamente caricato all'avvio di cbrserver. Se si decide di salvare la configurazione CBR in default.cfg, tutto quello che è stato salvato in questo file verrà automaticamente caricato al successivo avvio di cbrserver.

Fase 3. Avvio della funzione executor

Per avviare la funzione executor, immettere il comando **cbrcontrol executor start**. È inoltre possibile modificare le varie impostazioni dell'executor in questa fase. Vedere "dscontrol executor — controlla l'executor" a pagina 349.

Fase 4. Definizione di un cluster e impostazione delle relative opzioni

CBR esegue il bilanciamento delle richieste inviate per il cluster sui rispettivi server configurati sulle porte di quel determinato cluster.

Cluster è il nome simbolico situato nella porzione host dell'URL e deve corrispondere al nome utilizzato nell'istruzione Proxy del file ibmproxy.conf.

I cluster definiti in CBR devono essere definiti in modo da corrispondere alla richiesta in entrata. Per definire un cluster, utilizzare lo stesso nome host o lo stesso indirizzo IP che sarà presente nella richiesta in entrata. Ad esempio, se la richiesta arriverà come indirizzo IP, il cluster deve essere definito come indirizzo IP. Se esistono più nomi host che puntano a un unico indirizzo IP (e le richieste possono arrivare con uno qualsiasi di questi nomi host), sarà necessario definire come cluster tutti i nomi host.

Per definire un cluster, immettere il seguente comando:

```
cbrcontrol cluster add cluster
```

Per impostare le opzioni del cluster, immettere il seguente comando:

```
cbrcontrol cluster set cluster option value
```

Per ulteriori informazioni, vedere Capitolo 27, "Riferimenti sui comandi per Dispatcher e CBR", a pagina 337.

Fase 5. Creazione dell'alias della scheda di interfaccia di rete (NIC) (facoltativa)

Se il Caching Proxy in esecuzione è configurato come proxy inverso, quando si esegue il bilanciamento del carico su più siti Web, è necessario aggiungere

l'indirizzo cluster di ciascun sito Web su almeno una delle schede di interfaccia di rete della macchina Load Balancer. In caso contrario, è possibile ignorare questa fase.

Su sistemi **AIX, HP-UX, Linux o Solaris**: per aggiungere l'indirizzo cluster all'interfaccia di rete, utilizzare il comando `ifconfig`. Utilizzare il comando appropriato per il sistema operativo in uso come indicato nella Tabella 8.

Tabella 8. Comandi per creare l'alias della NIC

AIX	<code>ifconfig interface_name alias cluster_address netmask netmask</code>
HP-UX	<code>ifconfig interface_name cluster_address netmask netmask up</code>
Linux	<code>ifconfig interface_name cluster_address netmask netmask up</code>
Solaris 8, Solaris 9 e Solaris 10	<code>ifconfig nome_interfaccia addif indirizzo_cluster netmask netmask up</code>

Nota: Per sistemi Linux e HP-UX, *nome_interfaccia* deve avere un numero univoco per ciascun indirizzo cluster aggiunto, ad esempio: `eth0:1`, `eth0:2` e così via.

In **Windows 2000**: per aggiungere l'indirizzo cluster all'interfaccia di rete, effettuare le seguenti operazioni:

1. Fare clic su **Start > Impostazioni > Pannello di controllo**
2. Fare doppio clic su **Rete e connessioni remote**.
3. Fare clic con il tasto destro del mouse su **Connessione alla rete locale**.
4. Selezionare **Proprietà**.
5. Selezionare **Protocollo Internet (TCP/IP)** e fare clic su **Proprietà**.
6. Selezionare **Utilizza il seguente indirizzo IP**, quindi fare clic su **Avanzate**.
7. Fare clic su **Aggiungi**, quindi digitare l'indirizzo IP e la subnet mask per il cluster.

In **Windows 2003**: per aggiungere l'indirizzo cluster all'interfaccia di rete, effettuare le seguenti operazioni:

1. Fare clic su **Start > Pannello di controllo > Connessioni di rete > LAN (Local Area Connection)**
2. Fare clic su **Proprietà**.
3. Selezionare **Protocollo Internet (TCP/IP)** e fare clic su **Proprietà**.
4. Selezionare **Utilizza il seguente indirizzo IP**, quindi fare clic su **Avanzate**.
5. Fare clic su **Aggiungi**, quindi digitare l'indirizzo IP e la subnet mask per il cluster.

Fase 6. Definizione delle porte e impostazioni delle relative opzioni

Il numero di porta indica la porta su cui le applicazioni del server rimangono in ascolto. Per CBR con Caching Proxy in esecuzione per il traffico HTTP, la porta è in genere 80.

Per definire una porta sul cluster definito nella fase precedente, immettere quanto segue:

```
cbrcontrol port add cluster:porta
```


Per impostare le opzioni della porta, immettere quanto segue:

```
cbrcontrol port set cluster:porta option value
```

Per ulteriori informazioni, vedere Capitolo 27, “Riferimenti sui comandi per Dispatcher e CBR”, a pagina 337.

Fase 7. Definizione delle macchine server con bilanciamento del carico

Le macchine server sono le macchine su cui vengono eseguite le applicazioni che si desidera sottoporre a bilanciamento del carico. *Server* è il nome simbolico o l'indirizzo decimale separato da punti della macchina server. Per definire un server sul cluster e sulla porta, immettere il seguente comando:

```
cbrcontrol server add cluster:port:server
```

Per poter effettuare un bilanciamento del carico, è necessario definire più di un server per porta su un cluster.

Fase 8. Aggiunta di regole alla configurazione

Questa è l'operazione chiave nella configurazione di CBR con Caching Proxy. Una regola definisce come distinguere una richiesta URL per poterla inviare al gruppo di server appropriato. Il tipo di regola particolare utilizzata da CBR viene denominata una regola di contenuto. Per definire una regola di contenuto, immettere il seguente comando:

```
cbrcontrol rule add cluster:port:rule type content pattern modello
```

Il valore *modello* è l'espressione regolare che verrà confrontata con l'URL in ciascuna richiesta client. Per ulteriori informazioni su come configurare il modello, vedere Appendice B, “Sintassi della regola di contenuto (modello)”, a pagina 463.

Alcuni altri tipi di regola definiti in Dispatcher possono essere utilizzati anche in CBR. Per ulteriori informazioni, vedere “Configurazione del bilanciamento del carico in base alle regole” a pagina 205.

Fase 9. Aggiunta di server alle regole

Quando una richiesta client corrisponde a una regola, viene eseguita una query sul gruppo di server della regola per individuare il server migliore. Il gruppo di server della regola è un gruppo secondario di server definito sulla porta. Per aggiungere dei server al gruppo di server della regola, immettere il seguente comando:

```
cbrcontrol rule useserver cluster:port:rule server
```

Fase 10. Avvio della funzione gestore (facoltativo)

La funzione gestore migliora il bilanciamento del carico. Per avviare il gestore, immettere il seguente comando:

```
cbrcontrol manager start
```

Fase 11. Avvio della funzione advisor (facoltativo)

Gli advisor forniscono al gestore ulteriori informazioni sulla capacità delle macchine server con bilanciamento del carico di rispondere alle richieste. Un advisor è specifico di un protocollo. Ad esempio, per avviare l'advisor HTTP, immettere il seguente comando:

```
cbrcontrol advisor start http port
```

Fase 12. Impostazione delle proporzioni dei cluster secondo necessità

Se si avviano gli advisor, è possibile modificare le proporzioni di importanza attribuite alle informazioni raccolte dall'advisor che devono essere incluse nelle decisioni relative al bilanciamento del carico. Per impostare le proporzioni del cluster, immettere il comando **cbrcontrol cluster set cluster proportions**. Per ulteriori informazioni, vedere "Proporzione di importanza attribuita alle informazioni sullo stato" a pagina 176.

Fase 13. Avvio di Caching Proxy

- Su sistemi AIX: aggiungere la variabile d'ambiente LIBPATH:
`/opt/ibm/edge/lb/servers/lib`
- Su sistemi Linux, HP-UX o Solaris: aggiungere alla variabile d'ambiente LD_LIBRARY_PATH quanto riportato di seguito:
`/opt/ibm/edge/lb/servers/lib`
- Su sistemi Windows: aggiungere alla variabile d'ambiente PATH quanto riportato di seguito:
`C:\Program Files\IBM\edge\lb\servers\lib`

Nel nuovo ambiente, avviare Caching Proxy: dal prompt dei comandi, immettere **ibmpoxy**

Nota: Su sistemi Windows: avviare Caching Proxy dal pannello Servizi: **Start-> Impostazioni**-(in Windows 2000) > **Pannello di controllo -> Strumenti di amministrazione -> Servizi**.

Esempio di configurazione di CBR

Per configurare CBR, effettuare le seguenti operazioni:

1. Avviare CBR: immettere il comando **cbrserver**.
2. Avviare l'interfaccia della riga comandi: immettere il comando **cbrcontrol**.
3. Viene visualizzato il prompt **cbrcontrol**. Immettere i seguenti comandi.
(cluster(c),port(p),rule(r),server(s))
 - `executor start`
 - `cluster add c`
 - `port add c:p`
 - `server add c:p:s`
 - `rule add c:p:r type content pattern uri=*`
 - `rule useserver c:p:r s`
4. Avviare Caching Proxy: immettere il comando **ibmpoxy**. (Sulla piattaforma Windows, avviare Caching Proxy dal pannello Servizi).
5. Eliminare tutte le configurazioni proxy dal browser.
6. Caricare `http://c/` nel browser dove "`c`" è il cluster configurato precedentemente.
 - Viene richiamato il server "`s`"
 - Viene visualizzata la seguente pagina Web `http://s/`

Parte 4. Componente Site Selector

Questa sezione fornisce informazioni per una rapida configurazione, considerazioni sulla pianificazione e descrive i metodi di configurazione del componente Site Selector di Load Balancer. Contiene i seguenti capitoli:

- Capitolo 12, "Configurazione di avvio rapido", a pagina 119
- Capitolo 13, "Pianificazione di Site Selector", a pagina 123
- Capitolo 14, "Configurazione di Site Selector", a pagina 127

Capitolo 12. Configurazione di avvio rapido

Questo esempio di avvio rapido illustra come creare una configurazione dei nomi del sito utilizzando Site Selector per bilanciare il traffico tra un gruppo di server basato sul nome dominio utilizzato su una richiesta del client.

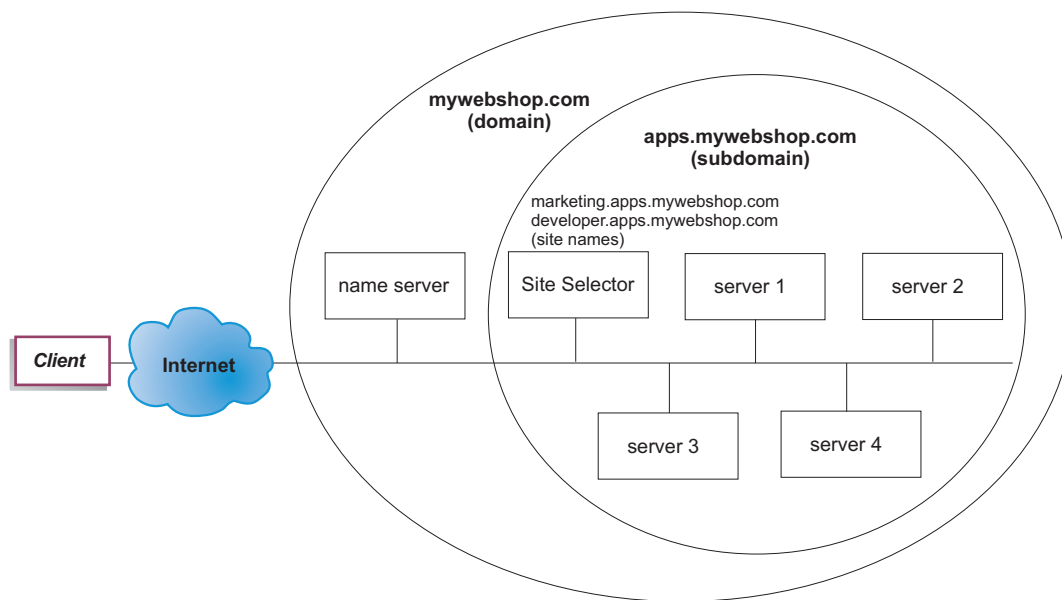


Figura 23. Una configurazione Site Selector semplice

Elementi richiesti

Per questo esempio di configurazione di avvio rapido, sono necessari i seguenti elementi:

- Accesso amministrativo al server dei nomi del sito
- Quattro server (server1, server2, server3, server4) configurati sulla rete e un ulteriore server con il componente Site Selector installato

Nota: se si posiziona Site Selector su uno dei server sottoposto a bilanciamento del carico, saranno necessari quattro server anziché cinque. Tuttavia, il posizionamento influisce sulle prestazioni dei server sottoposti a bilanciamento del carico.

Fasi di preparazione

In questo esempio di avvio rapido, il dominio del sito dell'azienda è mywebshop.com. Site Selector è responsabile di un dominio secondario all'interno di mywebshop.com. Quindi, è necessario definire un dominio secondario nell'ambito di mywebshop.com. Ad esempio: apps.mywebshop.com. Site Selector non è un DNS completamente implementato, come BIND, e svolge le funzioni di un nodo secondario in una gerarchia DNS. Site Selector è obbligatorio per il dominio secondario apps.mywebshop.com. Il dominio secondario

apps.mywebshop.com include i nomi di sito seguenti:
marketing.apps.mywebshop.com and developer.apps.mywebshop.com.

1. Aggiungere il DNS del sito dell'azienda (vedere Figura 23 a pagina 119). Creare un record del server dei nomi nel file named.data per il dominio secondario (apps.mywebshop.com) dove Site Selector è il server dei nomi obbligatorio:
apps.mywebshop.com. IN NS siteselector.mywebshop.com
2. Verificare che il nome host completo o il sito non vengono risolti nel sistema DNS corrente.
3. Installare Metric Server sui server (server1, server2, server3, server4) per cui si desidera eseguire il bilanciamento del carico con Site Selector. Per ulteriori informazioni, vedere "Metric Server" a pagina 191.

Configurazione del componente Site Selector

Site selector consente di creare una configurazione dalla riga comandi, con la configurazione guidata o mediante l'interfaccia utente grafica (GUI). In questo esempio di avvio rapido, le fasi di configurazione sono illustrate utilizzando la riga comandi.

Nota: i valori dei parametri devono essere immessi utilizzando l'alfabeto inglese. Le uniche eccezioni sono rappresentate dai nomi host e dai nomi file.

Configurazione mediante la riga comandi

Da un prompt dei comandi, effettuare le seguenti operazioni:

1. Avviare ssserver sulla macchina che ospita Site Selector. Come utente root o amministratore, immettere quanto segue da un prompt dei comandi: **ssserver**

Nota: sulle piattaforme Windows: avviare ssserver (IBM Site Selector) dal pannello Servizi: **Start > Impostazioni** (in Windows 2000) > **Pannello di controllo > Strumenti di amministrazione > Servizi**.

2. Avviare il server dei nomi sulla configurazione Site Selector:
sscontrol nameserver start
3. Configurare i nomi del sito (marketing.apps.mywebshop.com e developer.apps.mywebshop.com) su Site Selector:
sscontrol sitename add marketing.apps.mywebshop.com
sscontrol sitename add developer.apps.mywebshop.com
4. Aggiungere i server alla configurazione Site Selector. (Configurare server1 e server2 sul nome sito marketing.apps.mywebshop.com. Configurare server3 e server4 sul nome sito developer.apps.mywebshop.com):
sscontrol server add marketing.apps.mywebshop.com:server1+server2
sscontrol server add developer.apps.mywebshop.com:server3+server4
5. Avviare la funzione gestore di Site Selector:
sscontrol manager start
6. Avviare la funzione advisor di Site Selector (advisor HTTP per marketing.apps.mywebshop.com e advisor FTP per developer.apps.mywebshop.com):
sscontrol advisor start http marketing.apps.mywebshop.com:80
sscontrol advisor start ftp developer.apps.mywebshop.com:21

Il Site Selector garantisce, a questo punto, che le richieste client non verranno inviate a un server in errore.

7. Verificare che Metric Server sia stato avviato su ciascuno dei server sottoposti al bilanciamento del carico.

La configurazione Site Selector base è ora completa.

Verifica della configurazione

Verificare se la configurazione è in esecuzione:

1. Da un client, che ha un DNS principale configurato come il responsabile del server dei nomi per mywebshop.com, cercare di eseguire il ping su uno dei nomi del sito configurati.
2. Collegarsi all'applicazione. Ad esempio:
 - Aprire un browser, richiedere marketing.apps.mywebshop.com, verrà visualizzata una pagina valida
 - Aprire un client FTP su developer.apps.mywebshop.com e immettere un utente valido e una password
3. Controllare i risultati del seguente comando:
sscontrol server status marketing.apps.mywebshop.com:
sscontrol server status developer.apps.mywebshop.com:
Il totale delle voci corrispondenti di ciascun server dovrebbe aggiungersi alla richiesta di ping e dell'applicazione

Configurazione mediante l'interfaccia utente grafica (GUI)

Per informazioni sull'uso della GUI in Site Selector, vedere "GUI" a pagina 129 e Appendice A, "GUI: istruzioni generali", a pagina 455.

Configurazione mediante la procedura guidata

Per informazioni sull'uso della configurazione guidata di Site Selector, vedere "Configurazione guidata" a pagina 129.

Capitolo 13. Pianificazione di Site Selector

Questo capitolo descrive i fattori che un responsabile della pianificazione di rete deve considerare prima di installare e configurare il componente Site Selector.

- Vedere, Capitolo 3, “Gestione della rete: determinazione delle funzioni di Load Balancer da utilizzare”, a pagina 19 per una panoramica delle opzioni disponibili per la gestione della rete.
- Vedere Capitolo 14, “Configurazione di Site Selector”, a pagina 127, per informazioni sulla configurazione dei parametri di bilanciamento del carico di Site Selector.
- Vedere Capitolo 22, “Funzioni avanzate di Dispatcher, CBR e Site Selector”, a pagina 195, per informazioni su come configurare Load Balancer per funzioni più avanzate.
- Vedere Capitolo 24, “Funzionamento e gestione di Load Balancer”, a pagina 253 per informazioni sull’amministrazione autenticata remota, sui log di Load Balancer e sull’uso dei componenti di Load Balancer.

Questo capitolo include le seguenti sezioni:

- “Considerazioni sulla pianificazione”
- “Considerazioni su TTL” a pagina 125
- “Uso della funzione di prossimità della rete” a pagina 126

Considerazioni sulla pianificazione

Site Selector interagisce con un DNS (Domain Name Server) per eseguire il bilanciamento del carico tra un gruppo di server utilizzando le misure e i pesi raccolti. È possibile creare una configurazione del sito per consentire il bilanciamento del carico del traffico tra un gruppo di server basato sul nome dominio utilizzato per una richiesta del client.

Limitazioni: le interrogazioni DNS supportate da Site Selector sono solo le interrogazioni di Tipo A. Tutti gli altri tipi di interrogazione restituiranno un codice di errore NOTIMPL (non implementato). Se un intero dominio è delegato su Site Selector, verificare che il dominio riceva solo interrogazioni di Tipo A.

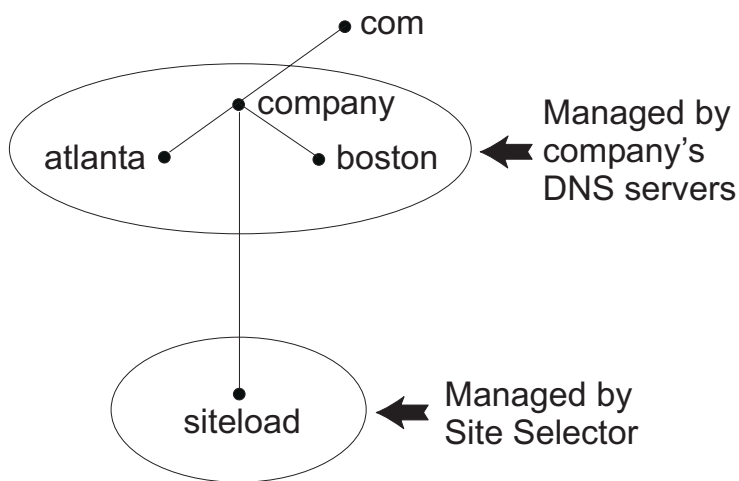


Figura 24. Esempio di un ambiente DNS

Durante la configurazione di un sottodominio di Site Selector nell'ambiente DNS, Site Selector deve disporre dell'autorità sul sottodominio. Ad esempio, (vedere Figura 24), all'azienda viene assegnata l'autorità sul dominio **company.com**. Nell'azienda, sono disponibili alcuni sottodomini. In questo caso, Site Selector avrebbe l'autorità per **siteload.company.com**, mentre i server DNS manterrebbero quella per **atlanta.company.com** e **boston.company.com**.

Affinché il server dei nomi dell'azienda riconosca l'autorità di Site Selector sul sottodominio siteload, è necessario aggiungere una voce server dei nomi al relativo file di dati denominato. Ad esempio, su AIX, una voce server dei nomi potrebbe essere:

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

Dove **siteselector.company.com** è il nome host della macchina Site Selector. Voci equivalenti dovrebbero essere inserite in altri file database denominati per l'uso da parte dei server DNS.

Un client invia una richiesta di risoluzione di un nome dominio a un server dei nomi presente nella rete. Il server dei nomi inoltra la richiesta alla macchina Site Selector. Quindi, Site Selector risolve il nome dominio nell'indirizzo IP di uno dei server configurati per quel nome del sito. Site Selector restituisce l'indirizzo IP del server selezionato al server dei nomi. Il server dei nomi restituisce l'indirizzo IP al client. (Site Selector funziona come un server dei nomi non ricorsivo (nodo secondario) e restituisce un errore nel caso in cui non risolva la richiesta del nome dominio.)

Fare riferimento alla Figura 5 a pagina 14 che illustra un sito in cui Site Selector viene utilizzato insieme a un sistema DNS per eseguire il bilanciamento del carico attraverso i server locali e remoti.

Site Selector è composto dalle seguenti funzioni:

- **ssserver** gestisce le richieste provenienti dalla riga comandi al server dei nomi, al gestore e agli advisor.
- La funzione **server dei nomi** supporta il bilanciamento del carico delle richieste in entrata sul server dei nomi. Affinché Site Selector inizi a fornire la risoluzione DNS, è necessario avviare la funzione server dei nomi. Site Selector è in ascolto delle richieste DNS in entrata sulla porta 53. Se il nome del sito richiedente è

configurato, Site Selector restituisce un solo indirizzo server (da un gruppo di indirizzi server) associato al nome del sito.

- Il **gestore** imposta i pesi utilizzati dal server dei nomi in base a:
 - Informazioni restituite dai server fornite dagli advisor
 - Informazioni restituite da un programma di monitoraggio del sistema, ad esempio Metric Server.

L'uso del gestore è facoltativo. Tuttavia, se il gestore non viene utilizzato, il bilanciamento del carico verrà eseguito utilizzando la pianificazione con il metodo round-robin basata sui pesi dei server correnti e gli advisor non saranno disponibili.

- **Metric Server** è un componente di monitoraggio del sistema di Load Balancer che viene installato sulla macchina server di backend. (Se Load Balancer viene posizionato sulla macchina server sottoposta a bilanciamento del carico, Metric Server deve essere installato sulla macchina Load Balancer.)

Insieme a Metric Server, Site Selector può monitorare il livello di attività su un server, rilevare un server che sta elaborando un carico inferiore rispetto agli altri e individuare un server in errore. Il carico misura il traffico sul server.

L'amministratore Site Selector del sistema controlla il tipo di misurazione utilizzato per calcolare il carico. È possibile configurare Site Selector in base all'ambiente, prendendo in considerazione fattori quali la frequenza degli accessi, il numero totale degli utenti e i tipi di accesso (ad esempio, query brevi e lunghe oppure carichi che richiedono molto spazio sulla CPU).

Il bilanciamento del carico si basa sui pesi dei server. Per Site Selector, il gestore utilizza quattro proporzioni per stabilire i pesi:

- CPU
- memoria
- porta
- sistema

I valori della CPU e della memoria sono tutti forniti da Metric Server. Di conseguenza, l'uso di Metric Server è *consigliato* con il componente Site Selector.

Per ulteriori informazioni, consultare "Metric Server" a pagina 191.

- Gli **advisor** interrogano i server e analizzano i risultati per protocollo prima di interpellare il gestore affinché imposti i pesi in modo appropriato. L'uso di questi advisor in una configurazione tipica potrebbe non essere necessario. È possibile anche scrivere advisor personalizzati. L'uso degli advisor è facoltativo ma consigliato. Per ulteriori informazioni, consultare "Advisor" a pagina 181.
- Per configurare e gestire il server dei nomi, gli advisor, Metric Server e il gestore, utilizzare la riga comandi (**sscontrol**) o l'interfaccia utente grafica (**ladmin**).

Le quattro funzioni chiave di Site Selector(server dei nomi, gestore, Metric Server e advisor) interagiscono per bilanciare e distribuire le richieste in entrata tra i server.

Considerazioni su TTL

L'uso del bilanciamento del carico basato su DNS richiede che la memorizzazione nella cache delle risoluzioni dei nomi venga disabilitata. Il valore TTL (time to live) determina la funzionalità del bilanciamento del carico basato su DNS. TTL determina il tempo durante il quale un altro server dei nomi memorizzerà nella cache la risposta risolta. I valori TTL ridotti consentono la realizzazione più rapida di piccole modifiche al carico del server o della rete. Tuttavia, disabilitando la memorizzazione nella cache i client devono contattare il server dei nomi autorevole

per tutte le richieste di risoluzione dei nomi, aumentando potenzialmente la latenza del client. Quando si sceglie un valore TTL, prestare particolare attenzione all'impatto che la disabilitazione della memorizzazione nella cache ha su un ambiente. Inoltre, tenere presente che il bilanciamento del carico basato su DNS è potenzialmente limitato dalla memorizzazione nella cache lato client delle risoluzioni dei nomi.

È possibile configurare TTL utilizzando il comando **sscontrol sitename [add | set]**. Per ulteriori informazioni, consultare "sscontrol sitename — configura un sitename" a pagina 414.

Uso della funzione di prossimità della rete

La prossimità della rete è il calcolo della vicinanza di ciascun server al client richiedente. Per stabilire tale prossimità, l'agente Metric Server (che deve risiedere su ciascun server con bilanciamento del carico) invia un ping all'indirizzo IP client e restituisce il tempo di risposta a Site Selector. Site Selector utilizza la risposta di prossimità nella decisione di bilanciamento del carico. Site Selector combina il valore di risposta della prossimità della rete con il peso proveniente dal gestore per creare un peso finale combinato per il server.

L'uso della funzione di prossimità della rete con Site Selector è facoltativo.

Site Selector fornisce le seguenti opzioni di prossimità della rete che possono essere impostate per nome del sito:

- **Durata della cache:** la quantità di tempo durante la quale una risposta di prossimità sarà valida e verrà salvata nella cache.
- **Percentuale di prossimità:** l'importanza della risposta di prossimità rispetto allo stato del server (come input dal peso del gestore).
- **Attesa di tutte le risposte:** determina se attendere tutte le risposte (ping) di prossimità dai server prima di rispondere alla richiesta del client.

Se impostata su **sì (yes)**, Metric Server invia il ping al client per ottenere il tempo di risposta della prossimità. Il server dei nomi attende tutte le risposte di Metric Servers oppure attende che si verifichi un time-out. Quindi, per ciascun server, il server dei nomi combina il tempo di risposta della prossimità con il peso del gestore calcolato per creare un valore del "peso combinato" per ciascun server. Site Selector fornirà al client l'indirizzo IP del server con il miglior peso combinato. (Si prevede che la maggior parte dei server dei nomi client abbia un time-out di 5 secondi. Site Selector tenta di rispondere prima che venga superato questo time-out.)

Se impostato su **no**, verrà fornita al client una risoluzione dei nomi basata sui pesi correnti del gestore. Quindi, Metric Server invia un ping al client per ottenere il tempo di risposta della prossimità. Il server dei nomi memorizza nella cache il tempo di risposta ricevuto da Metric Server. Quando il client effettua una seconda richiesta, il server dei nomi combina il peso del gestore corrente con il valore della risposta ping memorizzato nella cache per ciascun server per ottenere il server con il miglior "peso combinato". Site Selector restituisce questo indirizzo IP del server al client per la seconda richiesta.

Le opzioni di prossimità della rete possono essere impostate sul comando **sscontrol sitename [add | set]**. Per ulteriori informazioni, consultare Capitolo 28, "Riferimenti sui comandi per Site Selector", a pagina 391.

Capitolo 14. Configurazione di Site Selector

Prima di eseguire le operazioni riportate in questo capitolo, vedere Capitolo 13, “Pianificazione di Site Selector”, a pagina 123. Questo capitolo illustra come creare una configurazione di base per il componente Site Selector di Load Balancer.

- Vedere Capitolo 21, “Funzioni gestore, advisor e Metric Server per Dispatcher, CBR e Site Selector”, a pagina 175 e Capitolo 22, “Funzioni avanzate di Dispatcher, CBR e Site Selector”, a pagina 195 per configurazioni più complesse di Load Balancer.
- Vedere Capitolo 24, “Funzionamento e gestione di Load Balancer”, a pagina 253 per informazioni sull’amministrazione autenticata remota, sui log di Load Balancer e sull’uso dei componenti di Load Balancer.

Panoramica delle attività di configurazione

Nota: prima di iniziare le procedure di configurazione della tabella, verificare che la macchina Site Selector e tutte le macchine server siano collegate in rete, abbiano indirizzi IP validi e siano in grado di eseguire il ping reciprocamente.

Tabella 9. Configurazione delle attività per il componente Site Selector

Attività	Descrizione	Informazioni correlate
Configurazione della macchina Site Selector.	Individuazione dei requisiti.	“Configurazione della macchina Site Selector” a pagina 130
Configurazione delle macchine da sottoporre a bilanciamento del carico.	Configurazione del bilanciamento del carico.	“Fase 4. Definizione delle macchine server con bilanciamento del carico” a pagina 131

Metodi di configurazione

Per creare una configurazione di base del componente Site Selector di Load Balancer, sono disponibili quattro metodi di base di configurazione del componente Site Selector:

- Riga comandi
- Script
- Interfaccia utente grafica (GUI)
- Configurazione guidata

Riga comandi

È il mezzo più diretto per la configurazione di Site Selector. I valori dei parametri dei comandi devono essere immessi utilizzando l’alfabeto inglese. Le uniche eccezioni riguardano i nomi host, (utilizzati ad esempio nei comandi site name e server) e i nomi di file.

Per avviare Site Selector dalla riga comandi:

1. Immettere il comando **ssserver** nel prompt dei comandi. Per arrestare il servizio, digitare: **ssserver stop**

Nota: Su sistemi Windows, fare clic su **Start > Impostazioni** (per Windows 2000)> **Pannello di controllo > Strumenti di amministrazione > Servizi**. Fare clic con il tasto destro del mouse su **IBM Site Selector** e selezionare **Avvia**. Per arrestare il servizio, effettuare le stesse operazioni e selezionare **Arresta**.

2. Quindi, immettere i comandi di controllo di Site Selector per impostare la propria configurazione. Le procedure descritte nel presente manuale presumono l'uso della riga comandi. Il comando è **sscontrol**. Per ulteriori informazioni sui comandi, vedere Capitolo 28, "Riferimenti sui comandi per Site Selector", a pagina 391.

È possibile immettere una versione ridotta dei parametri del comando **sscontrol**. A tal fine, è sufficiente immettere le lettere che designano in modo univoco i parametri. Ad esempio, per richiamare la guida sul comando di salvataggio file, è possibile digitare **sscontrol he f** invece di **sscontrol help file**.

Per avviare l'interfaccia della riga comandi: immettere **sscontrol** per ricevere un prompt dei comandi per **sscontrol**.

Per chiudere l'interfaccia della riga comandi: immettere **exit** o **quit**.

Nota: sulla piattaforma Windows, **dsserver** del componente Dispatcher viene avviato automaticamente. Se si utilizza solo Site Selector e non il componente Dispatcher, è possibile arrestare l'avvio automatico di **dsserver** nel modo indicato di seguito:

1. In Servizi di Windows, fare clic con il tasto destro del mouse su **IBM Dispatcher**.
2. Selezionare **Proprietà**.
3. Nel campo **Tipo di avvio**, selezionare **Manuale**.
4. Fare clic su **OK** e chiudere la finestra **Servizi**.

Script

I comandi per la configurazione di Site Selector possono essere inseriti in un file di script della configurazione ed essere eseguiti insieme.

Nota: Per eseguire rapidamente il contenuto di un file di script (ad esempio, **myscript**), utilizzare uno dei seguenti comandi:

- Per aggiornare la configurazione corrente, eseguire i comandi eseguibili dal proprio file di script utilizzando —
sscontrol file appendload myscript
- Per sostituire completamente la configurazione corrente, eseguire i comandi eseguibili dal proprio file di script utilizzando —
sscontrol file newload myscript

Per salvare la configurazione corrente nel file di script (ad esempio, **savescript**), eseguire il comando:

sscontrol file save savescript

Questo comando salva il file di script della configurazione nella directory **...ibm/edge/lb/servers/configurations/ss**.

GUI

Per istruzioni generali e un esempio della GUI, vedere Figura 41 a pagina 456.

Per avviare la GUI, effettuare le seguenti operazioni.

1. Verificare che ssserver sia in esecuzione. Come utente root o amministratore, immettere quanto segue da un prompt dei comandi: **ssserver**
2. Quindi, effettuare una delle seguenti operazioni:
 - Per sistemi AIX, HP-UX, Linux o Solaris: immettere **lbadm**
 - Su sistemi Windows fare clic su **Start > Programmi > IBM WebSphere > Edge Components > IBM Load Balancer > Load Balancer**

Per configurare il componente Site Selector dalla GUI, è necessario anzitutto selezionare **Site Selector** nella struttura ad albero. Se connessi a un host su cui è in esecuzione ssserver, è possibile creare i nomi dei siti contenenti i server, avviare il gestore e avviare gli advisor.

La GUI può essere utilizzata per eseguire le operazioni che verrebbero effettuate con il comando **sscontrol**. Ad esempio, per definire un nome del sito utilizzando la riga comandi, si deve immettere il comando **sscontrol sitename add sitename**. Per definire un nome del sito dalla GUI, fare clic con il pulsante destro del mouse su Name Server, quindi nel menu a comparsa fare clic su **Add Site Name**. Immettere il nome del sito nella finestra a comparsa, quindi fare clic su **OK**.

I file di configurazione Site Selector esistenti possono essere caricati utilizzando l'opzione **Load New Configuration** (per sostituire completamente la configurazione corrente) e l'opzione **Append to Current Configuration** (per aggiornare la configurazione corrente) contenute nel menu a comparsa **Host**. Salvare periodicamente la configurazione di Site Selector su un file utilizzando l'opzione **Save Configuration File As** contenuta nel menu a comparsa **Host**. Il menu **File** situato sulla parte superiore della GUI consente di salvare le connessioni host correnti su un file o di ripristinare le connessioni nei file esistenti per tutti i componenti di Load Balancer.

Per eseguire un comando dalla GUI: evidenziare il nodo Host dalla struttura ad albero della GUI e selezionare **Send command....** dal menu a comparsa. Nel campo di immissione dei comandi, digitare il comando che si desidera eseguire, ad esempio: **nameserver status**. I risultati e la cronologia dei comandi in esecuzione nella sessione corrente vengono visualizzati nella finestra fornita.

È possibile accedere alla guida (**Help**) facendo clic sull'icona punto interrogativo nell'angolo in alto a destra della finestra di Load Balancer.

- **Help: Field level** — descrive i valori predefiniti di ciascun campo
- **Help: How do I** — elenca le attività possibili da questa schermata
- **InfoCenter** — consente l'accesso centralizzato alle informazioni sul prodotto

Per ulteriori informazioni sull'uso della GUI, vedere Appendice A, "GUI: istruzioni generali", a pagina 455.

Configurazione guidata

Se si utilizza la configurazione guidata, effettuare quanto segue:

1. Avviare ssserver su Site Selector:
 - Eseguire quanto riportato di seguito come root o come amministratore:

ssserver

2. Avviare la funzione della procedura guidata di Site Selector, **sswizard**..

È possibile avviare questa configurazione guidata dal prompt dei comandi immettendo **sswizard**. In alternativa, selezionare Configuration Wizard dal menu del componente Site Selector presente nella GUI.

La procedura guidata di Site Selector illustra nei dettagli come creare una configurazione di base del componente Site Selector. Pone delle domande relative alla rete e fornisce le istruzioni su come configurare un nome del sito in modo che il componente Site Selector possa eseguire il bilanciamento del carico sul traffico esistente tra un gruppo di server.

Configurazione della macchina Site Selector

Per poter configurare la macchina Site Selector, è necessario disporre dei diritti di utente root (su AIX, HP-UX, Linux o Solaris) o di amministratore (in Windows).

È necessario un nome host completo non risolvibile da utilizzare come nome del sito per un gruppo di server configurati. Il nome del sito è il nome che i client utilizzano per accedere al sito (ad esempio, www.yourcompany.com). Site Selector eseguirà il bilanciamento del carico del traffico per questo nome del sito tra il gruppo di server che utilizza DNS.

Fase 1. Avvio della funzione server

Per avviare la funzione server Site Selector, digitare **ssserver** sulla riga comandi.

Nota: un file di configurazione predefinito (default.cfg) viene caricato automaticamente all'avvio di ssserver. Se si decide di salvare la configurazione in default.cfg, tutto quello che è stato salvato in questo file verrà automaticamente caricato al successivo avvio di ssserver.

Fase 2. Avvio del Server dei nomi

Per avviare il Server dei nomi, immettere il comando **sscontrol nameserver start**.

Facoltativamente, avviare il Server dei nomi utilizzando la parola chiave **bindaddress** per collegarsi solo all'indirizzo specificato.

Fase 3. Definizione di un nome del sito e impostazione delle relative opzioni

Site Selector esegue il bilanciamento delle richieste inviate per il nome del sito sui rispettivi server configurati su di esso.

Il nome del sito è un nome host non risolvibile che il client richiederà. Il nome del sito deve essere un nome dominio completo (ad esempio, www.dnsdownload.com). Quando un client richiede questo nome del sito, verrà restituito uno degli indirizzi IP del server associati al nome del sito.

Per definire un nome del sito, immettere il seguente comando:

```
sscontrol sitename add sitename
```

Per impostare le opzioni del nome del sito, immettere il seguente comando:

```
sscontrol sitename set sitename option value
```


Per ulteriori informazioni, vedere Capitolo 28, “Riferimenti sui comandi per Site Selector”, a pagina 391.

Fase 4. Definizione delle macchine server con bilanciamento del carico

Le macchine server sono le macchine su cui vengono eseguite le applicazioni che si desidera sottoporre a bilanciamento del carico. *Server* è il nome simbolico o l'indirizzo decimale separato da punti della macchina server. Per definire un server sul nome del sito dalla fase 3, immettere il seguente comando:

```
sscontrol server add sitename:server
```

Per poter effettuare un bilanciamento del carico, è necessario definire più di un server per il nome del sito.

Fase 5. Avvio della funzione gestore (facoltativo)

La funzione gestore migliora il bilanciamento del carico. Prima di avviare la funzione gestore, verificare che il server delle metriche sia installato in tutte le macchine con bilanciamento del carico.

Per avviare il gestore, immettere il seguente comando:

```
sscontrol manager start
```

Fase 6. Avvio della funzione advisor (facoltativo)

Gli advisor forniscono al gestore ulteriori informazioni sulla capacità delle macchine server con bilanciamento del carico di rispondere alle richieste. Un advisor è specifico di un protocollo. Load Balancer fornisce molti advisor. Ad esempio, per avviare l'advisor HTTP per un nome del sito specifico, immettere il seguente comando:

```
sscontrol advisor start http sitename:port
```

Fase 7. Definizione della metrica del sistema (facoltativo)

Vedere “Metric Server” a pagina 191 per informazioni sull'uso delle metriche del sistema e di Metric Server.

Fase 8. Impostazione delle proporzioni del nome del sito secondo necessità

Se si avviano gli advisor, è possibile modificare le proporzioni di importanza attribuite alle informazioni dall'advisor (porta) che devono essere incluse nelle decisioni relative al bilanciamento del carico. Per impostare le proporzioni del nome del sito, immettere il comando **sscontrol sitename set sitename proportions**. Per ulteriori informazioni, vedere “Proporzione di importanza attribuita alle informazioni sullo stato” a pagina 176.

Configurazione della macchine server per il bilanciamento del carico

Utilizzare Metric Server con il componente Site Selector. Fare riferimento a “Metric Server” a pagina 191 per informazioni sulla configurazione di Metric Server su tutte le macchine server per cui Site Selector sta eseguendo il bilanciamento del carico.

Parte 5. Componente Controller Cisco CSS

Questa sezione fornisce informazioni per una rapida configurazione, considerazioni sulla pianificazione e descrive i metodi di configurazione del componente Controller Cisco CSS di Load Balancer. Contiene i seguenti capitoli:

- Capitolo 15, "Configurazione di avvio rapido", a pagina 135
- Capitolo 16, "Pianificazione di Controller Cisco CSS", a pagina 139
- Capitolo 17, "Configurazione di Controller Cisco CSS", a pagina 145

Capitolo 15. Configurazione di avvio rapido

Questo esempio di avvio rapido illustra come creare una configurazione utilizzando il componente Cisco CSS Controller. Cisco CSS Controller fornisce informazioni sui pesi dei server che supportano Switch Cisco CSS nella determinazione e selezione del server più adatto per le decisioni sul bilanciamento del carico.

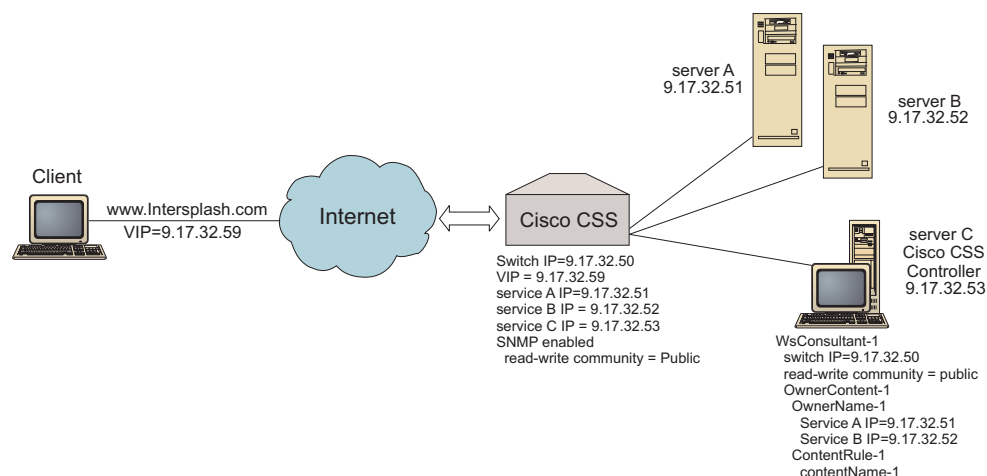


Figura 25. Una configurazione Cisco CSS Controller semplice

Elementi richiesti

Per questo esempio di configurazione di avvio rapido, sono necessari i seguenti elementi:

- Un Switch Cisco CSS
- Una macchina server con il componente Cisco CSS Controller
- Due macchine server Web
- Questo esempio di configurazione richiede cinque indirizzi IP:
 - Un indirizzo IP da fornire ai client per accedere al sito Web, www.Intersplashx.com (9.17.32.59)
 - Un indirizzo IP per un'interfaccia (gateway) con Switch Cisco CSS (9.17.32.50)
 - Un indirizzo IP per il server A (9.17.32.51)
 - Un indirizzo IP per il server B (9.17.32.52)
 - Un indirizzo IP per il server C con Cisco CSS Controller (9.17.32.53)

Fasi di preparazione

Prima di iniziare la configurazione per questo esempio, verificare che i passi seguenti siano stati completati:

- Verificare che lo Switch Cisco CSS sia configurato correttamente. Per informazioni sulla configurazione, fare riferimento a *Cisco Content Services Switch Getting Started Guide*.

- Verificare che la macchina Cisco CSS Controller possa eseguire il ping su Switch Cisco CSS (9.17.32.50), sul server A (9.17.32.51) e sul server B (9.17.32.52).
- Verificare che la macchina client possa eseguire il ping sul VIP (9.17.32.59)

Configurazione del componente Cisco CSS Controller

Cisco CSS Controller consente di creare una configurazione dalla riga comandi o mediante l'interfaccia utente grafica (GUI). In questo esempio di avvio rapido, le fasi di configurazione sono illustrate utilizzando la riga comandi.

Nota: i valori dei parametri devono essere immessi utilizzando l'alfabeto inglese. Le uniche eccezioni sono rappresentate dai nomi host e dai nomi file.

Configurazione mediante la riga comandi

Da un prompt dei comandi, effettuare le seguenti operazioni:

1. Avviare ccoserver su Load Balancer. Come utente root o amministratore, immettere quanto segue da un prompt dei comandi: **ccoserver**
2. Aggiungere un consultant dello switch alla configurazione Cisco CSS Controller, specificando l'indirizzo di interfaccia IP di Switch Cisco CSS e il nome comunità in lettura/scrittura. Questi valori devono corrispondere agli attributi su Switch Cisco CSS:

```
cococontrol consultant add SwConsultant-1 address 9.17.32.50 community public
```

Questo consente di controllare la connettività a Switch Cisco CSS e verificare che il nome comunità di SNMP in lettura/scrittura funzioni correttamente.

3. Aggiungere ownercontent (OwnerContent-1) al consultant dello switch, specificando ownername (OwnerName-1) e contentrule (ContentRule-1):

```
cococontrol ownercontent add SwConsultant-1:OwnerContent-1 ownername OwnerName-1 contentrule ContentRule-1
```

Questi valori devono corrispondere agli attributi su Switch Cisco CSS.

Cisco CSS Controller può ora comunicare con lo switch sul protocollo SNMP e ottenere così le necessarie informazioni sulla configurazione provenienti dallo switch. Dopo questa fase, in Cisco CSS Controller è possibile esaminare le informazioni sui servizi che sono stati configurati su Switch Cisco CSS per ownercontent specificato.

4. Configurare il tipo di metriche da raccogliere (connessioni attive, frequenza di connessione, HTTP) e la proporzione per ciascuna metrica su ownercontent:

```
cococontrol ownercontent metrics SwConsultant-1:OwnerContent-1 activeconn 45 connrate 45 http 10
```

Questo comando configura le informazioni metriche e le proporzioni che si desidera ottenere dai servizi in modo da poterli utilizzare per il calcolo dei pesi. Il totale delle proporzioni di tutte le metriche deve essere 100.

5. Avviare la funzione consultant dello switch di Cisco CSS Controller:

```
cococontrol consultant start SwConsultant-1
```

Questo comando consente di avviare tutti gli strumenti di raccolta delle metriche e iniziare i calcoli sui pesi dei servizi. Cisco CSS Controller comunica i risultati dei calcoli eseguiti sui pesi dei servizi a Switch Cisco CSS tramite SNMP.

La configurazione Cisco CSS Controller base è ora completa.

Verifica della configurazione

Verificare se la configurazione è in esecuzione:

1. Dal browser Web del client, andare all'indirizzo **http://www.Intersplashx.com**.
Se viene visualizzata una pagina, allora la configurazione funziona correttamente.
2. Ricaricare la pagina nel browser Web.
3. Controllare i risultati del seguente comando: **ccocontrol service report SwConsultant-1:OwnerContent-1:Service-1**. La somma totale della colonna connessioni dei due server Web deve essere "2."

Configurazione mediante l'interfaccia utente grafica (GUI)

Per informazioni sull'uso della GUI in Cisco CSS Controller, vedere "GUI" a pagina 147 e Appendice A, "GUI: istruzioni generali", a pagina 455.

Capitolo 16. Pianificazione di Controller Cisco CSS

Questo capitolo descrive i fattori che il responsabile della pianificazione di rete deve considerare prima di installare e configurare il componente Controller Cisco CSS.

- Vedere Capitolo 17, “Configurazione di Controller Cisco CSS”, a pagina 145, per informazioni sulla configurazione dei parametri di bilanciamento del carico del componente Cisco CSS Controller.
- Vedere Capitolo 23, “Funzioni avanzate di Controller Cisco CSS e Controller Nortel Alteon”, a pagina 235, per informazioni su come configurare Load Balancer per funzioni più avanzate.
- Vedere Capitolo 24, “Funzionamento e gestione di Load Balancer”, a pagina 253 per informazioni sull’amministrazione autenticata remota, sui log di Load Balancer e sull’uso dei componenti di Load Balancer.

Questo capitolo include:

- “Requisiti di sistema”
- “Considerazioni sulla pianificazione”
 - “Posizione del consultant nella rete” a pagina 140
 - “Disponibilità elevata” a pagina 142
 - “Calcolo dei pesi” a pagina 142
 - “Individuazione dei problemi” a pagina 143

Requisiti di sistema

Per i requisiti di sistema hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Inoltre, sarà necessario

- Un sistema su cui eseguire Cisco CSS Controller.
- Uno switch dei servizi di contenuto Cisco CSS serie 11000 installato e configurato

Considerazioni sulla pianificazione

Cisco CSS Controller gestisce una serie di consultant dello switch. Ciascun consultant stabilisce i pesi per i servizi il cui bilanciamento dei carichi viene eseguito da uno switch singolo. Lo switch per cui il consultant fornisce i pesi viene configurato per il bilanciamento del carico dei contenuti. Il consultant utilizza il protocollo SNMP per inviare i pesi calcolati allo switch. Lo switch utilizza i pesi per selezionare un servizio per la regola di contenuto per cui sta eseguendo il bilanciamento del carico quando l’algoritmo del bilanciamento del carico è caricato con il metodo round-robin. Per determinare i pesi, il consultant utilizza una o più delle seguenti parti di informazioni:

- Disponibilità e tempi di risposta, determinati attraverso l’uso degli **advisor** delle applicazioni che comunicano con le applicazioni in esecuzione sul servizio.
- Informazioni sul carico del sistema, determinate richiamando un valore delle metriche dagli **agenti Metric Server** in esecuzione sul servizio.
- Informazioni di connessione relative al servizio, ottenute dallo switch.

- Informazioni sull'accessibilità, ottenute eseguendo il ping del servizio.

Vedere *Cisco Content Services Switch Getting Started Guide* per una descrizione del bilanciamento del carico dei contenuti e per informazioni dettagliate sulla configurazione dello switch.

Affinché un consultant ottenga le informazioni per determinare i pesi dei servizi, deve disporre di:

- Connettività IP tra il consultant e i servizi per cui vengono calcolati i pesi.
- Connettività IP tra il consultant e lo switch che sta eseguendo il bilanciamento del carico dei server per cui vengono calcolati i pesi.
- SNMP abilitato sullo switch. Accesso in lettura e scrittura abilitato.

Posizione del consultant nella rete

Come indicato in Figura 26 a pagina 141, il consultant deve essere connesso alla rete dietro lo switch o gli switch per cui fornisce i pesi. Alcuni parametri devono essere configurati sullo switch e alcuni sul controller per abilitare la connettività tra il controller, lo switch e i servizi.

Nella Figura 26 a pagina 141:

- Un consultant è connesso alla rete dietro gli switch per cui sta fornendo i pesi.
- La rete è costituita da due VLAN.
- Affinché il consultant comunichi con i servizi in entrambe VLAN, è necessario abilitare l'inoltro IP sulle interfacce a cui sono connessi i servizi e sull'interfaccia a cui è connesso il consultant.
- L'indirizzo IP dello switch deve essere configurato come gateway predefinito sul consultant e sui sistemi di servizi.

Fare riferimento a *Cisco Content Services Switch Getting Started Guide* per informazioni dettagliate sulla configurazione delle VLAN e dell'indirizzamento IP sullo switch.

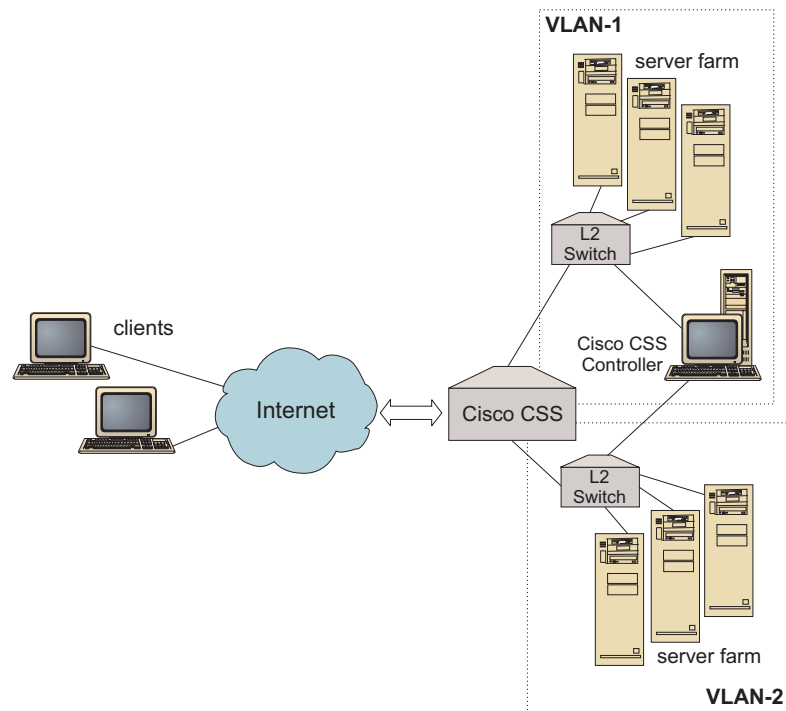


Figura 26. Esempio di un consultant connesso dietro gli switch

È possibile gestire Cisco CSS Controller utilizzando le seguenti interfacce:

- Un browser
- Una GUI (remota o locale)
- Una riga comandi (remota o locale)

Per la gestione remota, nella Figura 27 a pagina 142:

- Il consultant è connesso dietro gli switch per cui sta fornendo i pesi.
- L'interfaccia utente è in esecuzione su un sistema remoto davanti allo switch.
- Lo switch deve essere configurato per consentire la comunicazione del sistema remoto con il sistema del controller.

Fare riferimento a *Cisco Content Services Switch Getting Started Guide* per le informazioni dettagliate.

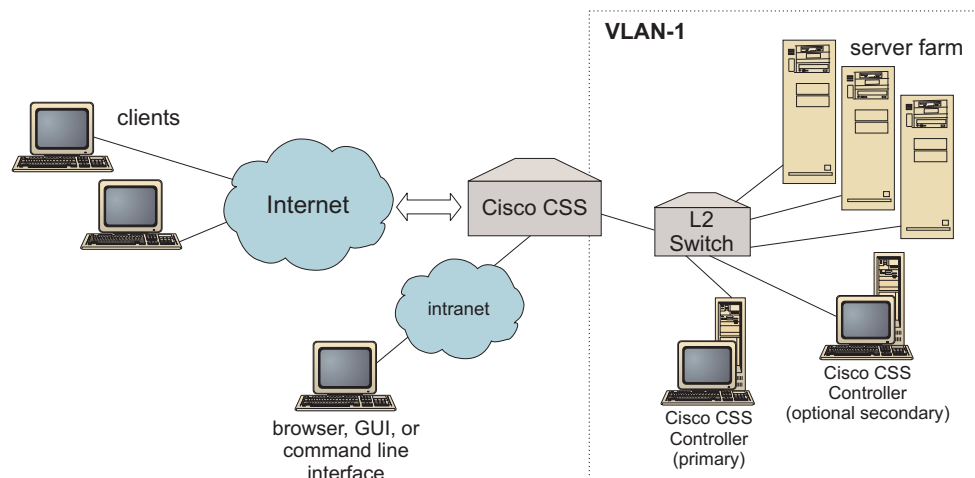


Figura 27. Esempio di consultant (con partner di disponibilità elevata facoltativo), configurato dietro lo switch con l'interfaccia utente davanti allo switch

Disponibilità elevata

La disponibilità elevata del controller migliora le funzioni di tolleranza degli errori di Load Balancer. Progettata sulla base della disponibilità elevata dell'inoltro del pacchetto, la disponibilità elevata del controller riguarda i due controller in esecuzione contemporaneamente, uno nel ruolo principale e l'altro in quello secondario.

Ciascun controller è configurato con le stesse informazioni sullo switch ed è attivo solo un controller alla volta. Ciò significa che, come stabilito dalla logica della disponibilità elevata, solo il controller attivo calcola e aggiorna lo switch con nuovi pesi.

La disponibilità elevata del controller comunica con i partner tramite i pacchetti UDP (user datagram protocol) semplici su un indirizzo e una porta configurati dall'utente. Questi pacchetti vengono utilizzati per consentire lo scambio di informazioni tra i controller relative alla disponibilità elevata (informazioni sull'accessibilità) e per determinare la disponibilità dei controller partner (heartbeat). Se il controller in standby stabilisce che il controller attivo non funziona per qualche motivo, il controller in standby diventa quello attivo. Il controller di standby, quindi, diventa il controller attivo e inizia a calcolare e aggiornare lo switch con i nuovi pesi.

Oltre alla disponibilità dei partner, le destinazioni accessibili possono essere configurate per la disponibilità elevata. La disponibilità elevata del controller utilizza le informazioni sull'accessibilità per stabilire quale controller è attivo e quale in standby. Il controller attivo è quello che può eseguire il ping di più destinazioni e che è accessibile dai relativi partner.

Per ulteriori informazioni, consultare "Disponibilità elevata" a pagina 235.

Calcolo dei pesi

Se il consultant stabilisce che un servizio non è disponibile, sospende quel servizio sullo switch per impedire che quest'ultimo consideri il server nelle richieste di

bilanciamento del carico. Quando il servizio è nuovamente disponibile, il consultant attiva il servizio sullo switch in modo che venga considerato per le richieste di bilanciamento del carico.

Individuazione dei problemi

Cisco CSS Controller invia le voci ai seguenti log:

- server.log
- consultant.log
- highavailability.log
- metriccollector.log
- binary.log

Questi log sono disponibili nelle seguenti directory:

- Su sistemi AIX, HP-UX, Linux e Solaris: `...ibm/edge/lb/servers/logs/cco/nomeconsultant`
- Su sistemi Windows: `...ibm\edge\lb\servers\logs\cco\nomeconsultant`

In ciascun log, è possibile impostare le dimensioni e il livello del log. Per ulteriori informazioni, consultare “Uso dei log di Load Balancer” a pagina 257.

Capitolo 17. Configurazione di Controller Cisco CSS

Prima di eseguire le operazioni riportate in questo capitolo, vedere Capitolo 16, “Pianificazione di Controller Cisco CSS”, a pagina 139. Questo capitolo illustra come creare una configurazione di base per il componente Controller Cisco CSS di Load Balancer.

- Vedere Capitolo 23, “Funzioni avanzate di Controller Cisco CSS e Controller Nortel Alteon”, a pagina 235 per configurazioni più complesse.
- Vedere Capitolo 24, “Funzionamento e gestione di Load Balancer”, a pagina 253 per informazioni sull’amministrazione autenticata remota, sui log e sull’uso del componente Controller Cisco CSS.

Panoramica delle attività di configurazione

Prima di iniziare qualsiasi metodo di configurazione riportato in questo capitolo:

1. Verificare che lo switch Cisco CSS e tutte le macchine server siano configurate correttamente.
2. Configurare Cisco CSS Controller, verificando che l’indirizzo di Switch Cisco CSS e il nome della comunità SNMP corrispondano agli attributi sullo switch Cisco CSS. Per ulteriori informazioni sulla configurazione del consultant, vedere “ccocontrol consultant — configura e controlla un consultant” a pagina 420.

Tabella 10. Configurazione delle attività per il componente Controller Cisco CSS

Attività	Descrizione	Informazioni correlate
Configurazione della macchina Controller Cisco CSS	Individuazione dei requisiti	“Configurazione della macchina Controller per switch Cisco CSS” a pagina 148
Verifica della configurazione	Conferma che configurazione funziona correttamente	“Verifica della configurazione” a pagina 150

Metodi di configurazione

Per creare una configurazione di base per il componente Controller Cisco CSS di Load Balancer, sono disponibili tre metodi:

- Riga comandi
- File XML
- Interfaccia utente grafica (GUI)

Riga comandi

Questo metodo è il mezzo più diretto di configurazione di Controller Cisco CSS. Le procedure descritte nel presente manuale presumono l’uso della riga comandi. I valori dei parametri dei comandi devono essere immessi utilizzando l’alfabeto inglese. Le uniche eccezioni riguardano i nomi host (utilizzati ad esempio nei comandi **consultant add**) e i nomi di file.

Per avviare Controller Cisco CSS dalla riga comandi:

1. Immettere il comando **ccoserver** nel prompt dei comandi. Per arrestare il server, digitare: **ccoserver stop**

Note:

- a. Su sistemi Windows, fare clic su **Start > Impostazioni** (per Windows 2000)> **Pannello di controllo > Strumenti di amministrazione > Servizi**. Fare clic con il tasto destro del mouse su **IBM Cisco CSS Controller** e selezionare **Avvia**. Per arrestare il servizio, effettuare le stesse operazioni e selezionare **Arresta**.
 - b. Su Windows, è possibile avviare automaticamente **ccoserver** all'avvio del sistema:
 - 1) Fare clic su **Start > Impostazioni > Pannello di controllo > Strumenti di amministrazione > Servizi**.
 - 2) Fare clic con il tasto destro del mouse su **IBM Cisco CSS Controller**, quindi selezionare **Proprietà**.
 - 3) Fare clic sulla freccia del campo **Tipo di avvio**, quindi selezionare **Automatico**.
 - 4) Fare clic su **OK**.
2. Successivamente, immettere i comandi di controllo Cisco CSS Controller con i quali si desidera impostare la configurazione. Le procedure descritte nel presente manuale presumono l'uso della riga comandi. Il comando è **ccocontrol**. Per ulteriori informazioni sui comandi, vedere Capitolo 29, "Riferimenti sui comandi per Cisco CSS Controller", a pagina 419.

È possibile immettere una versione abbreviata dei parametri del comando **ccocontrol**. A tal fine, è sufficiente immettere le lettere che designano in modo univoco i parametri. Ad esempio, per visualizzare le informazioni sul comando di salvataggio del file, è possibile digitare **ccocontrol he f** invece di **ccocontrol help file**.

Per avviare l'interfaccia della riga comandi: immettere **ccocontrol** per ricevere un prompt dei comandi per **ccocontrol**.

Per chiudere l'interfaccia della riga comandi: immettere **exit** o **quit**.

Nota: Sulle piattaforme Windows, il **dserver** del componente Dispatcher viene avviato automaticamente. Se si utilizza solo Controller Cisco CSS e non il componente Dispatcher, è possibile arrestare l'avvio automatico di **dserver** nel modo indicato di seguito:

1. In Servizi di Windows, fare clic con il tasto destro del mouse su **IBM Dispatcher**.
2. Selezionare **Proprietà**.
3. Nel campo **Tipo di avvio**, selezionare **Manuale**.
4. Fare clic su **OK** e chiudere la finestra Servizi.

XML

La configurazione attualmente definita può essere salvata su un file XML. In questo modo, la configurazione può essere caricata in un momento successivo quando si desidera creare rapidamente la configurazione.

Per eseguire il contenuto di un file XML (ad esempio, **myscript.xml**), utilizzare uno dei seguenti comandi:

- Per salvare la configurazione corrente in un file XML, immettere il seguente comando:
ccocontrol file save XMLFilename
- Per caricare una configurazione salvata, immettere il seguente comando:
ccocontrol file load XMLFileName
Utilizzare il comando load solo se precedentemente è stato eseguito un comando **file save**.

I file XML vengono salvati nella directory **...ibm/edge/lb/servers/configurations/cco/**.

GUI

Per istruzioni generali e un esempio della GUI, vedere Figura 41 a pagina 456.

Per avviare la GUI, effettuare le seguenti operazioni.

1. Se ccoserver non è già in esecuzione, avviarlo eseguendo quanto segue come root:
ccoserver.
2. Quindi, effettuare una delle seguenti operazioni:
 - Per sistemi AIX, HP-UX, Linux o Solaris: immettere **lbadm**
 - Su sistemi Windows fare clic su **Start > Programmi > IBM WebSphere > Edge Components > IBM Load Balancer > Load Balancer**

Per configurare il componente di Controller Cisco CSS dalla GUI:

1. Fare clic con il tasto destro del mouse su Controller Cisco CSS nella struttura ad albero.
2. Collegarsi a un Host.
3. Creare uno o più consultant dello switch con gli ownercontent desiderati e le metriche associate.
4. Avviare il consultant.

La GUI può essere utilizzata per eseguire le operazioni che verrebbero effettuate con il comando **ccocontrol**. Ad esempio:

- Per definire un consultant dalla riga comandi, digitare **ccocontrol consultant add consultantID address IPAddress community name**.
- Per definire un consultant dalla GUI, fare clic con il tasto destro del mouse sul nodo Host, quindi su **Add a switch consultant**. Digitare l'indirizzo dello switch e il nome della comunità nella finestra a comparsa, quindi fare clic su OK.
- Utilizzare **Load Configuration** presente nel menu a comparsa Host per caricare i file di configurazione Controller Cisco CSS pre-esistenti e per aggiungere la configurazione corrente.
- Selezionare **Save Configuration File As** per salvare periodicamente la configurazione di Controller Cisco CSS su un file.
- Selezionare **File** dalla barra dei menu per salvare le connessioni host correnti su un file oppure per ripristinare le connessioni in file esistenti attraverso tutti i componenti di Load Balancer.

Per eseguire un comando dalla GUI:

1. Fare clic con il tasto destro del mouse sul nodo **Host** e selezionare **Send command...**

2. Nel campo di immissione Command, digitare il comando da eseguire; ad esempio, **consultant report**.
3. Fare clic su Send.

I risultati e la cronologia dei comandi eseguiti nella sessione corrente vengono visualizzati nella casella Result.

Per accedere all'**Help**, fare clic sull'icona punto interrogativo nell'angolo superiore destro della finestra di Load Balancer.

- **Help: Field level** — descrive i valori predefiniti di ciascun campo
- **Help: How do I** — elenca le attività possibili da questa schermata
- **InfoCenter** — consente l'accesso centralizzato alle informazioni sul prodotto

Per ulteriori informazioni sull'uso della GUI, vedere Appendice A, "GUI: istruzioni generali", a pagina 455.

Configurazione della macchina Controller per switch Cisco CSS

Per poter configurare la macchina Controller Cisco CSS, è necessario disporre dei diritti di utente root (in AIX, HP-UX, Linux o Solaris) o di amministratore (in Windows).

Il Consultant deve essere in grado di collegarsi a Switch Cisco CSS come amministratore di Switch Cisco CSS.

Durante la configurazione del consultant, è necessario configurare l'indirizzo e il nome comunità SNMP in modo che corrispondano agli attributi su Switch Cisco CSS.

Per maggiori informazioni sui comandi utilizzati in questa procedura, vedere Capitolo 29, "Riferimenti sui comandi per Cisco CSS Controller", a pagina 419.

Fase 1. Avvio della funzione del server

Se ccoserver non è già in esecuzione, digitare **ccoserver** come root per avviarlo.

Nota: Su sistemi Windows, fare clic su **Start > Impostazioni** (per Windows 2000)> **Pannello di controllo > Strumenti di amministrazione > Servizi**. Fare clic con il tasto destro del mouse su IBM Cisco Controller e selezionare Avvia.

Fase 2. Avvio dell'interfaccia della riga comandi

Digitare **cococontrol** per avviare l'interfaccia della riga comandi.

Fase 3. Configurazione del consultant

Configurare l'indirizzo switch e il nome comunità SNMP. Questi valori devono corrispondere agli attributi su Switch Cisco CSS.

Per aggiungere un consultant, digitare:

```
consultant add switchConsultantID address switchIPAddress  
community communityName
```

Fase 3. Configurazione di un ownercontent

Un ownercontent è la rappresentazione di una regola di contenuto di un proprietario definita su Switch Cisco CSS. Il nome proprietario e il nome della regola di contenuto devono corrispondere con quelli definiti sullo switch.

Per definire un ownercontent, digitare:

```
ownercontent add switchConsultantID:ownercontentID ownername ownerName  
contentrule contentRuleName
```

Fase 4. Verifica della corretta definizione dei servizi

Quando viene definito ownercontent, il consultant completa la configurazione richiamando i servizi configurati sullo switch. Confrontare la configurazione sullo switch con quella per il consultant per verificare che i servizi corrispondano.

Fase 5. Configurazione delle metriche

Le metriche sono le misurazioni utilizzate per stabilire i pesi dei servizi e le proporzioni associate (l'importanza di una metrica rispetto ad un'altra) e possono essere costituite da qualsiasi combinazione di metriche dei dati di connessione, degli advisor delle applicazioni e dei server delle metriche. La somma delle proporzioni deve essere sempre pari a 100.

Quando viene configurato l'ownercontent, le metriche predefinite vengono indicate come **activeconn** e **connrate**. Se si desiderano metriche aggiuntive o metriche completamente diverse da quelle predefinite, digitare:

```
ownercontent metrics switchConsultantID:ownercontentID metric1 proportion1  
metric2 proportion2...metricN proportionN
```

Fase 6. Avvio del consultant

Per avviare il consultant, digitare:

```
consultant start switchConsultantID
```

In questo modo, vengono avviati gli strumenti di raccolta delle metriche e viene avviato il calcolo dei pesi.

Fase 7. Avvio di Metric Server (facoltativo)

Se le metriche del sistema vengono definite nella fase 5, il server delle metriche deve essere avviato sulle metriche del servizio. Per informazioni sull'uso del server delle metriche, vedere "Metric Server" a pagina 191.

Fase 8. Configurazione della disponibilità elevata (facoltativa)

Per configurare la disponibilità elevata, digitare:

```
highavailability add address  
IPaddress partneraddress  
IPaddress port 80  
role primary
```

In un ambiente a disponibilità elevata, è possibile configurare più switch. Per garantire che le informazioni sui pesi siano sempre disponibili quando uno switch di backup diventa attivo prendendo il posto di un altro switch, Controller Cisco CSS deve essere configurato per fornire i pesi per tutti gli switch e i relativi backup.

Per informazioni dettagliate su come utilizzare e configurare la disponibilità elevata del controller, vedere Capitolo 23, “Funzioni avanzate di Controller Cisco CSS e Controller Nortel Alteon”, a pagina 235.

Verifica della configurazione

Verificare se la configurazione è in esecuzione:

1. Impostare il livello di log del consultant su 4.
2. Disconnettere un server da Switch Cisco CSS per un minuto, oppure arrestare il server delle applicazioni per un minuto.
3. Riconnettere il server oppure riavviare il server delle applicazioni.
4. Riportare il livello di log del consultant sul livello desiderato (1).
5. Visualizzare il file consultant.log situato nelle seguenti directory e ricercare **setServerWeights setting service**:
 - Su sistemi AIX, HP-UX, Linux e Solaris: `...ibm/edge/lb/servers/logs/cco/nomeconsultant`
 - Su sistemi Windows: `...ibm\edge\lb\servers\logs\cco\nomeconsultant`

Parte 6. Componente Controller Nortel Alteon

Questa sezione fornisce informazioni per una rapida configurazione, considerazioni sulla pianificazione e descrive i metodi di configurazione del componente Controller Nortel Alteon di Load Balancer. Contiene i seguenti capitoli:

- Capitolo 18, "Configurazione di avvio rapido", a pagina 153
- Capitolo 19, "Pianificazione di Controller Nortel Alteon", a pagina 157
- Capitolo 20, "Configurazione di Controller Nortel Alteon", a pagina 167

Capitolo 18. Configurazione di avvio rapido

Questo esempio di avvio rapido illustra come creare una configurazione utilizzando il componente Controller Nortel Alteon. Controller Nortel Alteon fornisce le informazioni sui pesi dei server a Switch Nortel Alteon Web. Questi pesi vengono utilizzati per selezionare i server per i servizi su cui lo switch sta eseguendo il bilanciamento del carico.

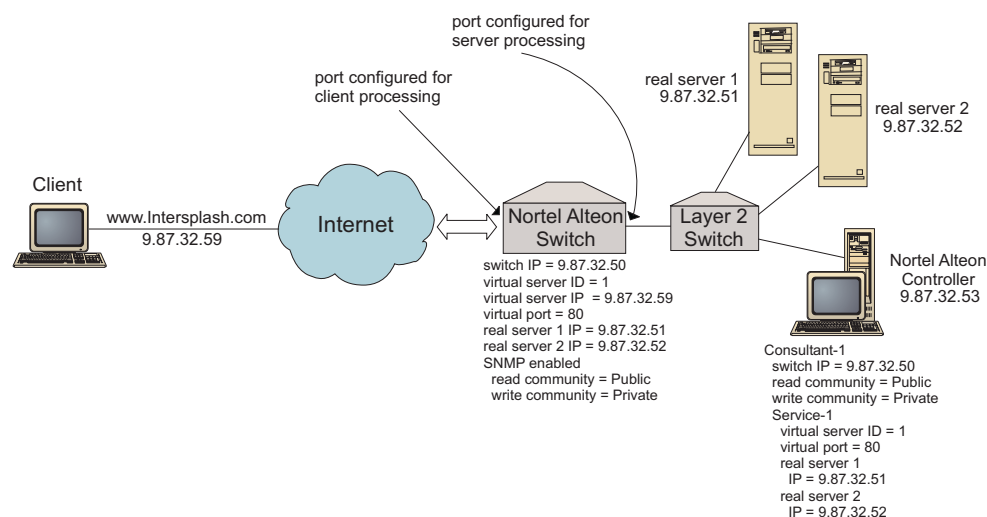


Figura 28. Una configurazione Controller Nortel Alteon semplice

Elementi richiesti

Per questo esempio di configurazione di avvio rapido, sono necessari i seguenti elementi:

- Uno Switch Nortel Alteon Web, in esecuzione sulla versione del sistema operativo Web 9.0 o 10.0
- Una macchina server con il componente Controller Nortel Alteon
- Due macchine server Web
- Uno switch a 2 livelli collegato a una porta su Switch Nortel Alteon Web

Nota: se non si utilizza uno switch a 2 livelli, la macchina Controller Nortel Alteon e le macchine server Web possono essere collegate direttamente alle porte su Switch Nortel Alteon Web.

- Questo esempio di configurazione richiede cinque indirizzi IP:
 - Un indirizzo IP da fornire ai client per accedere al sito Web, www.Intersplashx.com (9.87.32.59)
 - Un indirizzo IP per un'interfaccia configurata su Switch Nortel Alteon Web (9.87.32.50)
 - Un indirizzo IP per il server reale 1 (9.87.32.51)
 - Un indirizzo IP per il server reale 2 (9.87.32.52)
 - Un indirizzo IP per Controller Nortel Alteon (9.87.32.53)

Fasi di preparazione

Prima di iniziare la configurazione per questo esempio, verificare che i passi seguenti siano stati completati:

- Verificare che Switch Nortel Alteon Web sia configurato correttamente. (Per informazioni più dettagliate sulla configurazione, fare riferimento a Nortel Alteon Web OS Application Guide):
 - Abilitare il bilanciamento del carico server livello 4 sullo switch.
 - Configurare un'interfaccia IP (9.87.32.50) su Switch Nortel Alteon Web
 - Abilitare SNMP su Switch Nortel Alteon Web
 - Abilitare il client di bilanciamento del carico dei server in elaborazione sulla porta Switch Nortel Alteon Web che riceve le richieste client.
 - Abilitare il server di bilanciamento del carico dei server in elaborazione sulla porta Switch Nortel Alteon Web attraverso cui sono connessi i server.
 - Configurare il gateway predefinito per svolgere il ruolo di interfaccia IP dello switch (9.87.32.50) sul server effettivo 1, sul server effettivo 2 e su Controller Nortel Alteon.
 - Configurare Switch Nortel Alteon Web con il server effettivo 1 e con il server effettivo 2.
 - Configurare Switch Nortel Alteon Web con un gruppo di server, in cui sono contenuti il server effettivo 1 e il server effettivo 2. Assegnare al gruppo un ID pari a 1.
 - Configurare Switch Nortel Alteon Web con un server virtuale. L'indirizzo IP del server virtuale è 9.87.32.59. Assegnare un ID pari a 1 al server virtuale.
 - Configurare Switch Nortel Alteon Web con un servizio che utilizzi la porta virtuale 80 e sia servito dal gruppo 1.
- Verificare che la macchina client possa eseguire il ping sull'indirizzo IP del server virtuale 9.87.32.59.
- Verificare che la macchina Controller Nortel Alteon possa eseguire il ping sull'interfaccia IP di Switch Nortel Alteon Web (9.87.32.50), sul server effettivo 1 (9.87.32.51) e sul server effettivo 2 (9.87.32.52).

Configurazione del componente Controller Nortel Alteon

Controller Nortel Alteon consente di creare una configurazione dalla riga comandi o mediante l'interfaccia utente grafica (GUI). In questo esempio di avvio rapido, le fasi di configurazione sono illustrate utilizzando la riga comandi.

Nota: i valori dei parametri devono essere immessi utilizzando l'alfabeto inglese. Le uniche eccezioni sono rappresentate dai nomi host e dai nomi file.

Configurazione mediante la riga comandi

Da un prompt dei comandi, effettuare le seguenti operazioni:

1. Avviare nalserver su Controller Nortel Alteon. Come utente root o amministratore, immettere quanto segue da un prompt dei comandi: **nalserver**
2. Aggiungere un consultant alla configurazione Controller Nortel Alteon, specificando l'indirizzo di interfaccia IP di Switch Nortel Alteon Web. (Specificare la comunità in lettura e la comunità in scrittura solo se differiscono dai valori predefiniti (public, private)):
nalcontrol consultant add Consultant-1 address 9.87.32.50

Questo consente di controllare la connettività a Switch Nortel Alteon Web e verificare che i nomi comunità SNMP funzionino correttamente.

3. Aggiungere un servizio (Service-1) al consultant (Consultant-1), specificando l'identificatore del server virtuale (1) e il numero di porta virtuale (80) per il servizio:

nalcontrol service add Consultant-1:Service-1 vsid 1 vport 80

Controller Nortel Alteon comunicherà ora con lo switch sul protocollo SNMP e otterrà così le necessarie informazioni sulla configurazione provenienti dallo switch. Dopo questa fase, in Controller Nortel Alteon è possibile esaminare le informazioni sui server che sono stati configurati su Switch Nortel Alteon Web per il servizio.

4. Configurare le metriche che devono essere raccolte per il gruppo di server associati al servizio:

nalcontrol service metrics Consultant-1:Service-1 http 40 activeconn 30 connrate 30

Questo comando configura le informazioni metriche che si desidera raccogliere dai server e l'importanza relativa di tali metriche durante il calcolo dei pesi.

5. Avviare la funzione consultant di Controller Nortel Alteon:

nalcontrol consultant start Consultant-1

Questo comando consente di avviare tutti gli strumenti di raccolta delle metriche e iniziare i calcoli sui pesi dei server. Controller Nortel Alteon comunica i risultati dei calcoli eseguiti sui pesi dei servizi a Switch Nortel Alteon Web tramite SNMP.

La configurazione Controller Nortel Alteon base è ora completa.

Verifica della configurazione

Verificare se la configurazione è in esecuzione:

1. Dal browser Web del client, andare all'indirizzo **http://www.Intersplashx.com** . Se viene visualizzata una pagina, allora la configurazione funziona correttamente.
2. Ricaricare la pagina nel browser Web.
3. Controllare i risultati del seguente comando: **nalcontrol service report Consultant-1:Service-1**. La somma totale della colonna connessioni dei due server Web deve essere "2."

Configurazione mediante l'interfaccia utente grafica (GUI)

Per informazioni sull'uso della GUI in Controller Nortel Alteon, vedere "GUI" a pagina 169 and Appendice A, "GUI: istruzioni generali", a pagina 455.

Capitolo 19. Pianificazione di Controller Nortel Alteon

Questo capitolo descrive i fattori che il responsabile della pianificazione di rete deve considerare prima di installare e configurare il componente Controller Nortel Alteon.

- Vedere Capitolo 20, "Configurazione di Controller Nortel Alteon", a pagina 167, per informazioni sulla configurazione dei parametri di bilanciamento del carico del componente Controller Nortel Alteon.
- Vedere Capitolo 23, "Funzioni avanzate di Controller Cisco CSS e Controller Nortel Alteon", a pagina 235, per informazioni su come configurare gli advisor e i server delle metriche.
- Vedere Capitolo 24, "Funzionamento e gestione di Load Balancer", a pagina 253 per informazioni sull'amministrazione autenticata remota, sui log di Load Balancer e sull'uso dei componenti di Load Balancer.

Questo capitolo include:

- "Requisiti di sistema"
- "Considerazioni sulla pianificazione"
 - "Posizione del consultant nella rete" a pagina 158
 - "Attributi server sullo switch (impostati dal controller)" a pagina 160
 - "Configurazione dei server di backup" a pagina 161
 - "Configurazione dei gruppi" a pagina 162
 - "Disponibilità elevata" a pagina 162
 - "Ottimizzazione" a pagina 164
 - "Individuazione dei problemi" a pagina 164

Requisiti di sistema

Per i requisiti di sistema hardware e software, compresi i browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Inoltre, sarà necessario

- Un sistema su cui eseguire Controller Nortel Alteon.
- Un Switch Nortel Alteon Web installato e configurato. Le piattaforme hardware dello switch Web sono AD3, AD4, 180e 184 e il livello 4/7 per Passport 8600.

Considerazioni sulla pianificazione

Controller Nortel Alteon gestisce una serie di consultant dello switch. Ciascun consultant stabilisce i pesi per i server il cui bilanciamento dei carichi viene eseguito da uno switch singolo. Lo switch per cui il consultant fornisce i pesi viene configurato per il bilanciamento del carico dei server. Il consultant utilizza il protocollo SNMP per inviare i pesi calcolati allo switch. Lo switch utilizza i pesi per selezionare un server per il servizio per cui sta eseguendo il bilanciamento del carico. Per determinare i pesi, il consultant utilizza una o più delle seguenti parti di informazioni:

- Disponibilità e tempi di risposta, determinati attraverso l'uso degli **advisor** che comunicano con le applicazioni in esecuzione sui server.

- Informazioni sul carico del sistema, determinate richiamando un valore delle metriche dagli **agenti Metric Server** in esecuzione sui server.
- Informazioni di connessione relative ai server, ottenute dallo switch.
- Informazioni sull'accessibilità, ottenute eseguendo il ping dei server.

Vedere Nortel Alteon Web OS Application Guide per una descrizione del bilanciamento del carico dei server e per informazioni dettagliate sulla configurazione dello switch.

Affinché un consultant ottenga le informazioni per determinare i pesi dei server, deve disporre di:

- Connettività IP tra il consultant e i server per cui vengono calcolati i pesi.
- Connettività IP tra il consultant e lo switch che sta eseguendo il bilanciamento del carico dei server per cui vengono calcolati i pesi.
- SNMP abilitato sullo switch. Accesso in lettura e scrittura abilitato.

Posizione del consultant nella rete

Il consultant può essere connesso alla rete davanti o dietro lo switch o gli switch per cui fornisce i pesi. Alcuni parametri devono essere configurati sullo switch e alcuni sul controller per abilitare la connettività tra il controller, lo switch e i server.

Nella Figura 29 a pagina 159:

- Un consultant è connesso alla rete dietro gli switch per cui sta fornendo i pesi.
- La rete è costituita da due VLAN.
- Affinché il consultant comunichi con i server in entrambe VLAN, è necessario abilitare l'inoltro IP sulle interfacce a cui sono connessi i server e sull'interfaccia a cui è connesso il consultant.
- L'indirizzo IP dello switch deve essere configurato come gateway predefinito sul consultant e sui sistemi di server.

Fare riferimento a Nortel Alteon Web OS Application Guide o Command Reference per informazioni dettagliate sulla configurazione delle VLAN e dell'indirizzamento IP sullo switch.

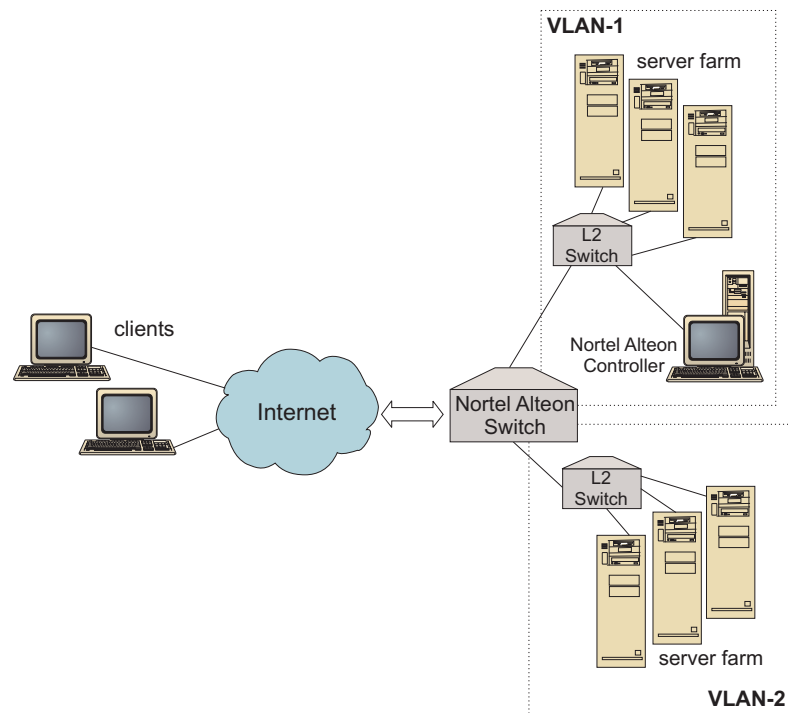


Figura 29. Esempio di consultant connesso dietro lo switch

Nella Figura 30 a pagina 160:

- Il consultant è connesso allo switch attraverso una rete intranet davanti allo switch.
- La modalità di accesso diretto al bilanciamento del carico dei server deve essere abilitata sullo switch per consentire al consultant di comunicare con lo switch e con i server.
- Con la modalità di accesso diretto al bilanciamento del carico dei server, qualsiasi client può indirizzare direttamente il traffico su qualsiasi server. Per limitare l'accesso diretto al server esclusivamente al consultant, specificare il bilanciamento del carico *mnet* e *mmask* sullo switch. Fare riferimento a Nortel Alteon Web OS Application Guide o Command Reference per informazioni dettagliate sulla configurazione del bilanciamento del carico dei server e sull'interazione diretta dei server.

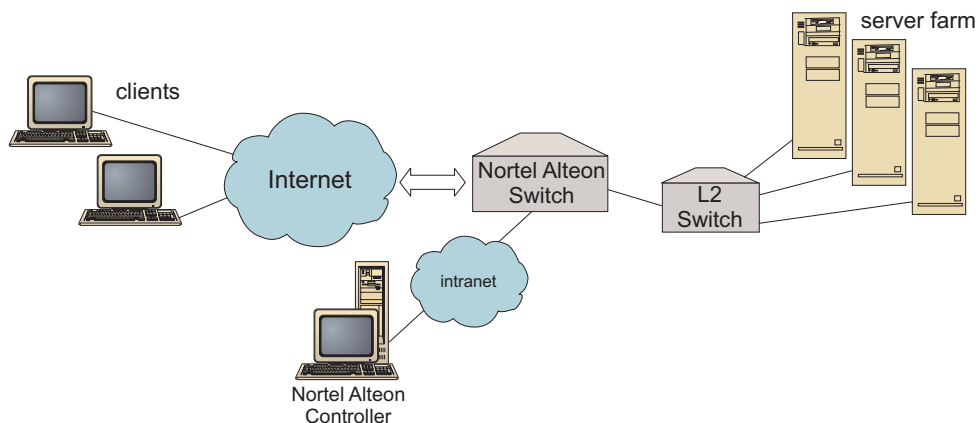


Figura 30. Esempio di consultant connesso attraverso una rete intranet davanti allo switch

È possibile gestire Controller Nortel Alteon utilizzando le seguenti interfacce:

- Un browser
- Una GUI
- Una riga comandi remota

Nella Figura 31:

- Il consultant è connesso dietro gli switch per cui sta fornendo i pesi.
- L'interfaccia utente è in esecuzione su un sistema remoto davanti allo switch.
- La rete deve essere configurata in modo che l'interfaccia utente possa comunicare con il controller.

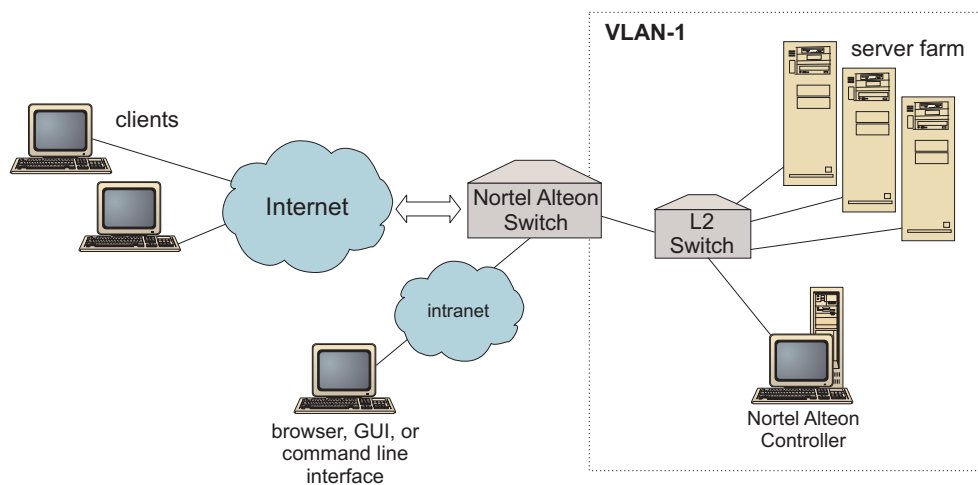


Figura 31. Esempio di consultant dietro lo switch e dell'interfaccia utente davanti allo switch

Attributi server sullo switch (impostati dal controller)

Quando un consultant calcola i pesi per i server che forniscono un servizio sottoposto a bilanciamento del carico da uno switch, il consultant disabilita il controllo dello stato normale del server sullo switch per ridurre il traffico inutile sui server. Il consultant riabilita il controllo dello stato quando interrompe l'invio dei pesi per il servizio. L'intervallo dei controlli dello stato del server corrisponde alla variabile MIB `slbNewCgRealServerPingInterval`.

Se il consultant stabilisce che un server non è disponibile, il consultant imposta il numero massimo di connessioni del server su zero per impedire che lo switch consideri il server nelle richieste di bilanciamento del carico. Quando il server è nuovamente disponibile, il numero massimo di connessioni viene riportato al valore originale. Il valore delle connessioni massime al server corrisponde alla variabile MIB `slbNewCfgRealServerMaxCons`.

Quando viene calcolato il peso di un server effettivo, il peso viene impostato per il server. Il valore del peso del server corrisponde alla variabile MIB `slbNewCfgRealServerWeight`.

Configurazione dei server di backup

Lo switch consente la configurazione di alcuni server come backup di altri. Se lo switch stabilisce che un server con un backup non è disponibile, tale switch può iniziare ad inviare le richieste al backup. Quando il consultant calcola i pesi per un servizio con un backup, li calcola per entrambi i server di backup e principale e, successivamente, utilizza i pesi per la scelta del server di backup necessario.

Il peso per un server di backup potrebbe essere superiore a quello per un server principale. Questo perché nessuna richiesta viene inoltrata a quest'ultimo che, quindi, ha pesi ridotti fino a quando lo switch non decide di utilizzarli.

Per evitare risorse inutilizzate dei server, solitamente i server assegnati a un servizio vengono utilizzati come backup per i server assegnati a un servizio differente. Durante l'implementazione di una configurazione simile a questa, evitare di assegnare gli stessi server effettivi a più server attivi contemporaneamente. Se ciò si verifica, il peso per il server viene sovrascritto dal consultant per ciascun servizio di cui fa parte il server.

Ciascun server effettivo viene identificato da un numero intero e ha un peso e un attributo indirizzo IP. Due server effettivi potrebbero avere lo stesso indirizzo IP. In questo caso, i due server effettivi vengono associati alla stessa macchina server fisica. I server effettivi identificati come backup devono essere configurati esclusivamente come backup di un singolo servizio. Se le stesse macchine server fisiche rappresentano i server di backup assegnati a più servizi, devono essere configurate una volta per ciascun servizio e devono ricevere un'identificazione server univoca per ciascun servizio. Questo consente ai server di backup di avere un peso univoco per ciascun servizio di cui rappresentano il backup.

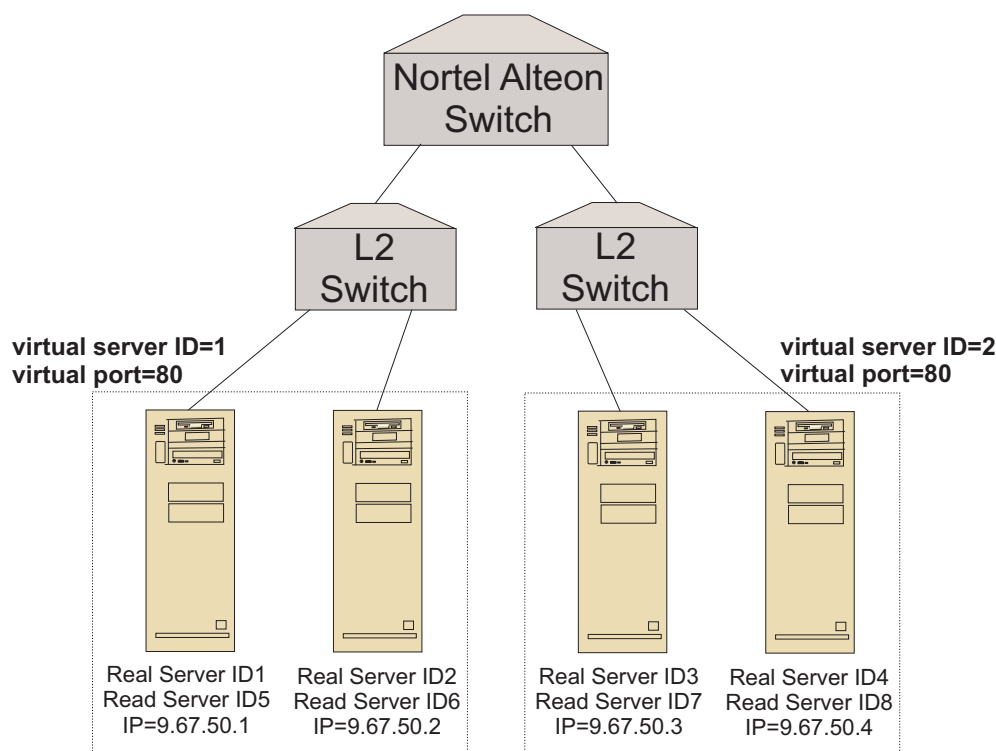


Figura 32. Esempio di consultant configurato con server di backup

Configurazione dei gruppi

I server su uno switch possono essere configurati come parte di più gruppi e i gruppi sullo switch possono essere configurati per più servizi.

Poiché è possibile configurare lo stesso server per più servizi, il peso verrà calcolato per ciascun servizio di cui fa parte il server. È possibile, quindi, che il peso non sia corretto poiché il servizio per cui è previsto quel peso non si conosce.

Inoltre, se il consultant stabilisce i pesi per un servizio e non per un altro, è possibile che il servizio per cui il consultant non ha calcolato i pesi abbia il controllo dello stato dei server disabilitato. In questo caso, lo switch potrebbe non eseguire correttamente il bilanciamento del carico di quel servizio.

Per questi motivi, verificare che un server effettivo non sia assegnato a più servizi per cui viene eseguito il bilanciamento del carico. Ciò non significa che la stessa macchina server non può eseguire le richieste di più servizi ma che è necessario configurare un server effettivo sullo switch con un identificatore univoco per ciascun servizio per cui la macchina server gestisce le richieste.

Disponibilità elevata

Sia Controller Nortel Alteon che Switch Nortel Alteon Web hanno disponibilità elevata.

È possibile configurare due controller da eseguire su sistemi differenti in una configurazione hot-standby.

Due o più switch possono agire l'uno come backup dell'altro se configurati per funzionare come VIR (virtual IP interface router) o come VSR (virtual IP server router).

Un consultant (gestito dal controller) fornisce i pesi per un solo switch. Poiché uno switch di backup può diventare attivo in qualsiasi momento e quindi diventare lo switch principale, è necessario configurare il controller con un consultant per ciascuno switch che ha la possibilità di diventare principale. In questo modo, quando uno switch diventa principale, disporrà sicuramente dei pesi necessari.

Inoltre, quando i controller sono connessi a un VIR, la comunicazione con i server, con gli switch e con il controller di backup è garantita, anche se dovesse perdere la connettività con uno degli switch.

Fare riferimento a Nortel Alteon Web OS Application Guide per informazioni sulla disponibilità elevata sullo switch.

La disponibilità elevata del controller migliora le funzioni di tolleranza degli errori di Load Balancer. Progettata sulla base della disponibilità elevata dell'inoltro del pacchetto classica, la disponibilità elevata del controller riguarda i due controller in esecuzione contemporaneamente, uno nel ruolo principale e l'altro in quello secondario.

Ciascun controller è configurato con le stesse informazioni sullo switch. Analogamente alla disponibilità elevata classica, è attivo solo un controller alla volta. Ciò significa che, come stabilito dalla logica della disponibilità elevata, solo il controller attivo calcola e aggiorna lo switch con nuovi pesi.

La disponibilità elevata del controller comunica con i partner tramite i pacchetti UDP (user datagram protocol) semplici su un indirizzo e una porta configurati dall'utente. Questi pacchetti vengono utilizzati per consentire lo scambio di informazioni tra i controller relative alla disponibilità elevata (informazioni sull'accessibilità) e per determinare la disponibilità dei controller partner (heartbeat). Se il controller in standby stabilisce che il controller attivo non funziona per qualche motivo, il controller in standby diventa quello attivo. Il controller di standby, quindi, diventa il controller attivo e inizia a calcolare e aggiornare lo switch con i nuovi pesi.

Oltre alla disponibilità dei partner, le destinazioni accessibili possono essere configurate per la disponibilità elevata. Come con la disponibilità elevata classica, la disponibilità elevata del controller utilizza le informazioni sull'accessibilità per stabilire quale controller è attivo e quale in standby. Il controller attivo è quello che può eseguire il ping di più destinazioni e che è accessibile dai relativi partner.

Per ulteriori informazioni, consultare "Disponibilità elevata" a pagina 235.

Nella Figura 33 a pagina 164:

- Due Controller Nortel Alteon sono connessi dietro agli switch.
- Un controller è il principale e fornisce attivamente i pesi dei server agli switch; l'altro è quello di backup.
- Per sapere quando diventare controller principali, i controller devono disporre della comunicazione TCP/IP con il backup.
- Vengono configurati due Switch Nortel Alteon Web, un VIR e un VSR.
- VIR fornisce la disponibilità elevata per le connessioni ai server.

- VSR fornisce la disponibilità elevata per l'accesso ai server virtuali configurati sugli switch.
- Uno degli switch è il principale e l'altro è quello di backup.
- Il controller principale fornisce i pesi per entrambi gli switch.
- Il controller di backup invia gli heartbeat al controller principale per stabilire quando diventare attivo.

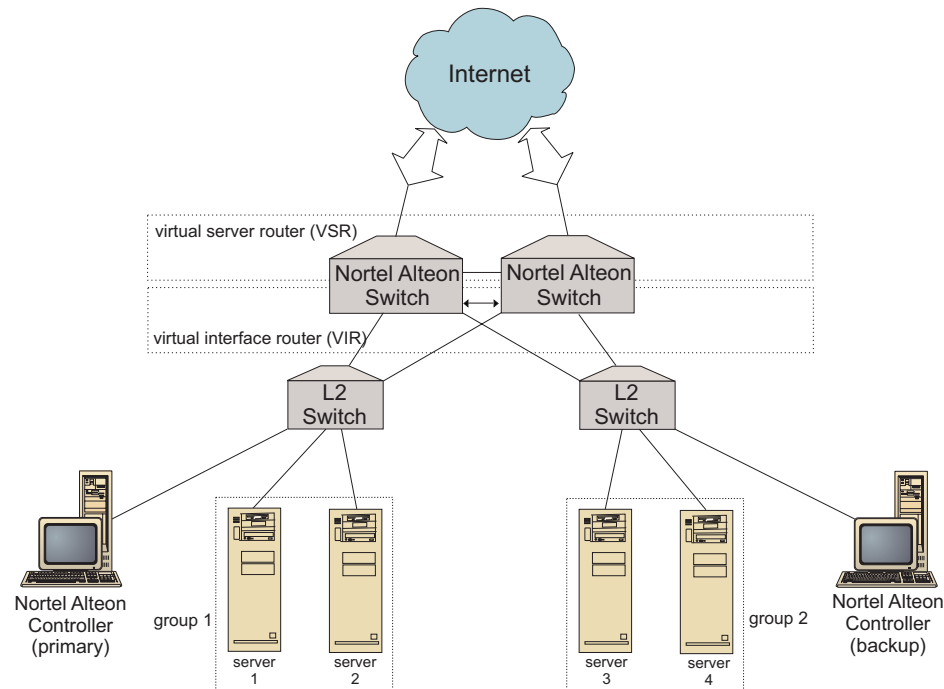


Figura 33. Esempio della disponibilità elevata di Controller Nortel Alteon e Switch Nortel Alteon Web

Ottimizzazione

Per evitare continue variazioni di pesi, è possibile configurare il consultant con una soglia di sensibilità. Tale soglia specifica l'entità della variazione tra i vecchi e i nuovi pesi necessaria affinché un peso possa essere modificato. Per ulteriori informazioni, consultare "Soglia di sensibilità" a pagina 239.

Se lo switch diventa troppo occupato durante l'aggiornamento dei pesi, è possibile aumentare i tempi di inattività del consultant per ridurre il traffico tra il controller e i server e lo switch. Tali tempi impostano l'intervallo di inattività in secondi tra i cicli di impostazione dei pesi.

Se i server gestiscono troppe richieste di controllo provenienti dal consultant, è possibile modificare i tempi di inattività degli strumenti di raccolta delle metriche. Per una descrizione dettagliata, vedere "Tempi di inattività nel calcolo dei pesi" a pagina 239.

Individuazione dei problemi

Cisco CSS Controller invia le voci ai seguenti log:

- server.log
- consultant.log
- highavailability.log

- metriccollector.log
- binary.log

Questi log sono disponibili nelle seguenti directory:

- Su sistemi AIX, HP-UX, Linux e Solaris: ...ibm/edge/lb/servers/logs/nal/*nomeconsultant*
- Su sistemi Windows: ...ibm\edge\lb\servers\logs\nal\i*nomeconsultant*

In ciascun log, è possibile impostare le dimensioni e il livello del log. Per ulteriori informazioni, consultare “Uso dei log di Load Balancer” a pagina 257.

Capitolo 20. Configurazione di Controller Nortel Alteon

Prima di eseguire le operazioni riportate in questo capitolo, vedere Capitolo 19, “Pianificazione di Controller Nortel Alteon”, a pagina 157. Questo capitolo illustra come creare una configurazione di base per il componente Controller Nortel Alteon di Load Balancer.

- Vedere Capitolo 23, “Funzioni avanzate di Controller Cisco CSS e Controller Nortel Alteon”, a pagina 235 per configurazioni più complesse.
- Vedere Capitolo 24, “Funzionamento e gestione di Load Balancer”, a pagina 253 per informazioni sull’amministrazione autenticata remota, sui log e sull’uso del componente Controller Nortel Alteon.

Panoramica delle attività di configurazione

Prima di iniziare qualsiasi metodo di configurazione riportato in questo capitolo, verificare che Switch Nortel Alteon Web e tutte le macchine server siano configurate correttamente.

Tabella 11. Configurazione delle attività per il componente Controller Nortel Alteon

Attività	Descrizione	Informazioni correlate
Configurazione di Switch Nortel Alteon Web e dei server	Configurazione dello switch.	Come configurare lo switch, a pagina 170
Configurazione della macchina Controller Nortel Alteon	Configurazione del controller.	“Fase 1. Avvio della funzione del server” a pagina 170
Verifica della configurazione	Conferma della procedura di configurazione in corso	“Verifica della configurazione” a pagina 172

Metodi di configurazione

Per creare una configurazione di base per il componente Controller Nortel Alteon di Load Balancer, sono disponibili tre metodi:

- Riga comandi
- File XML
- Interfaccia utente grafica (GUI)

Riga comandi

È il mezzo più diretto per la configurazione di Controller Nortel Alteon. Le procedure riportate in questo manuale presuppongono l’uso della riga comandi.

Per avviare Controller Nortel Alteon dalla riga comandi:

1. Immettere il comando **nalserver** nel prompt dei comandi. Per arrestare il servizio, digitare: **nalserver stop**

Note:

- a. Su sistemi Windows, fare clic su **Start > Impostazioni** (per Windows 2000)> **Pannello di controllo > Strumenti di amministrazione > Servizi**. Fare clic con il tasto destro del mouse su IBM Controller Nortel Alteon e selezionare **Avvia**. Per arrestare il servizio, effettuare le stesse operazioni e selezionare **Arresta**.

- b. Su sistemi Windows, è possibile avviare automaticamente nalserver all'avvio del sistema:
 - 1) Fare clic su **Start > Impostazioni** (in Windows 2000) > **Pannello di controllo > Strumenti di amministrazione > Servizi**.
 - 2) Fare clic con il tasto destro del mouse su IBM Controller Nortel Alteon, quindi selezionare Proprietà.
 - 3) Fare clic sulla freccia del campo Tipo di avvio, quindi selezionare Automatico.
 - 4) Fare clic su OK.
2. Successivamente, immettere i comandi di controllo Controller Nortel Alteon con i quali si desidera impostare la configurazione. Le procedure riportate in questo manuale presuppongono l'uso della riga comandi. Il comando è **nalcontrol**. Per ulteriori informazioni sui comandi, vedere Capitolo 30, "Riferimenti sui comandi per Controller Nortel Alteon", a pagina 437.

È possibile utilizzare una versione abbreviata dei parametri del comando **nalcontrol** digitando le lettere che designano in modo univoco i parametri. Ad esempio, per visualizzare le informazioni sul comando di salvataggio dei file, è possibile digitare **nalcontrol he f** invece di **nalcontrol help file**.

Per terminare l'interfaccia della riga comandi: digitare **exit** o **quit**.

Note:

1. Utilizzare i caratteri inglesi per tutti i valori dei parametri dei comandi. Le sole eccezioni sono rappresentate dai nomi host (utilizzati nei comandi server) e dai nomi file (utilizzati nei comandi file).
2. Su sistemi Windows, il dsserver del componente Dispatcher viene avviato automaticamente. Se si sta utilizzando solo Controller Nortel Alteon e non il componente Dispatcher, è possibile impedire l'avvio automatico di ndserver nel seguente modo:
 - a. In Servizi di Windows, fare clic con il tasto destro del mouse su IBM Dispatcher.
 - b. Selezionare Proprietà.
 - c. Nel campo **Tipo di avvio**, selezionare Manuale.
 - d. Fare clic su OK e chiudere la finestra Servizi.

XML

La configurazione attualmente definita può essere salvata su un file XML. In questo modo, la configurazione può essere caricata in un momento successivo quando si desidera creare rapidamente la configurazione.

Per eseguire il contenuto di un file XML (ad esempio, **myscript.xml**), utilizzare i seguenti comandi:

- Per salvare la configurazione corrente in un file XML, immettere il seguente comando:
nalcontrol file save XMLFilename
 Utilizzare il comando load solo se precedentemente è stato eseguito un comando **file save**.
- Per caricare una configurazione salvata, immettere il seguente comando:
nalcontrol file load XMLFileName
 Utilizzare il comando load solo se precedentemente è stato eseguito un comando **file save**.

I file XML vengono salvati nella directory `...ibm/edge/lb/servers/configurations/nal/`.

GUI

Per un esempio dell'interfaccia utente grafica (GUI), vedere Figura 41 a pagina 456.

Per avviare la GUI:

1. Se `nalserver` non è già in esecuzione, avviarlo ora digitando **nalserver** come root.
2. Quindi, effettuare una delle seguenti operazioni:
 - Per sistemi AIX, HP-UX, Linux o Solaris: immettere **lbadmin**
 - Su sistemi Windows: fare clic su Start > **Programmi** > **IBM WebSphere** > **Edge Components** > **IBM Load Balancer** > **Load Balancer**

Per configurare il componente Controller Nortel Alteon dalla GUI:

1. Fare clic con il tasto destro del mouse su Controller Nortel Alteon nella struttura ad albero.
2. Collegarsi a un Host.
3. Creare uno o più consultant dello switch contenente i servizi desiderati e le metriche associate.
4. Avviare il consultant.

La GUI può essere utilizzata per eseguire le operazioni che verrebbero effettuate con il comando **nalcontrol**. Ad esempio:

- Per definire una destinazione accessibile utilizzare la riga comandi, digitare **nalcontrol highavailability usereach address**. Per definire una destinazione accessibile dalla GUI, fare clic con il tasto destro del mouse su High Availability > Add Reach Target.... Digitare l'indirizzo della destinazione accessibile nella finestra a comparsa, quindi fare clic su OK.
- Utilizzare **Load Configuration** presente nel menu a comparsa Host per aggiungere la configurazione memorizzata in un file alla configurazione in esecuzione. Per caricare una *nuova* configurazione, arrestare e riavviare il server prima di caricare il file.
- Fare clic con il tasto destro del mouse sul nodo Host, quindi selezionare **Save Configuration File As** per salvare periodicamente la configurazione di Controller Nortel Alteon su un file.
- Selezionare **File** dalla barra dei menu per salvare le connessioni host correnti su un file oppure per ripristinare le connessioni in file esistenti attraverso tutti i componenti di Load Balancer.

Per eseguire un comando dalla GUI:

1. Fare clic con il tasto destro del mouse sul nodo **Host** e selezionare **Send command....**
2. Nel campo di immissione Command, digitare il comando da eseguire; ad esempio, **consultant report**.
3. Fare clic su Send.

I risultati e la cronologia dei comandi eseguiti nella sessione corrente vengono visualizzati nella casella Result.

Per accedere all'Help, fare clic sull'icona punto interrogativo nell'angolo superiore destro della finestra di Load Balancer.

- **Help: Field level** — descrive i valori predefiniti di ciascun campo
- **Help: How do I** — elenca le attività possibili da questa schermata
- **InfoCenter** — consente l'accesso centralizzato alle informazioni sul prodotto

Per ulteriori informazioni sull'uso della GUI, vedere Appendice A, "GUI: istruzioni generali", a pagina 455.

Impostazione di Controller Nortel Alteon

Per maggiori informazioni sui comandi utilizzati in questa procedura, vedere Capitolo 30, "Riferimenti sui comandi per Controller Nortel Alteon", a pagina 437.

Prima di configurare la macchina Controller Nortel Alteon:

- È necessario disporre dei diritti di utente root (su AIX, HP-UX, Linux e Solaris) o di amministratore (su Windows).
- Controller Nortel Alteon deve disporre della connettività IP a Switch Nortel Alteon Web e a tutti i server per cui verranno calcolati i pesi.
- Configurare Switch Nortel Alteon Web come segue:
 1. Abilitare il bilanciamento del carico server livello 4 sullo switch.
 2. Configurare un'interfaccia IP.
 3. Abilitare SNMP.
 4. Abilitare il client di bilanciamento del carico del server in elaborazione sulla porta che riceve le richieste client.
 5. Abilitare il server di bilanciamento del carico del server in elaborazione sulla porta attraverso cui sono connessi i server effettivi.
 6. Configurare i server effettivi per le macchine server Web.
 7. Configurare un gruppo di server effettivo composto da server effettivi su cui è in esecuzione il server delle applicazioni.
 8. Configurare un server virtuale.
 9. Configurare un servizio su una porta virtuale e assegnare il gruppo di server effettivo su cui eseguire il servizio.

Fase 1. Avvio della funzione del server

Se `nalserver` non è già in esecuzione, digitare `nalserver` come root per avviarlo.

Nota: Su Windows, fare clic su **Start > Impostazioni** (in Windows 2000) > **Pannello di controllo > Strumenti di amministrazione > Servizi**. Fare clic con il tasto destro del mouse su IBM Controller Nortel Alteon e selezionare **Avvia**.

Fase 2. Avvio dell'interfaccia della riga comandi

Digitare `nalcontrol` per avviare l'interfaccia della riga comandi.

Fase 3. Definizione di un consultant Switch Nortel Alteon Web

Per aggiungere un consultant dello switch, digitare:

```
consultant add switchconsultantID address switchIPAddress
```

Fase 4. Aggiunta di un servizio a un consultant dello switch

Per aggiungere un servizio, digitare:


```
service add switchConsultantID:serviceID vsid virtualServerID vport  
virtualPortNumber
```

Un servizio viene identificato da un VSID (identificatore server virtualer) e da un numero VPORT (porta virtuale), entrambi associati a un server virtuale precedentemente configurato sullo switch.

Fase 5. Configurazione delle metriche

Le metriche sono le informazioni utilizzate per determinare i pesi del server. Ciascuna metrica viene assegnata a una proporzione per indicare l'importanza relativa ad altre metriche. È possibile configurare tutte le combinazioni di metriche: metriche dei dati di connessione, degli advisor delle applicazioni e dei server delle metriche. La somma delle proporzioni deve essere sempre pari a 100.

Quando viene configurato un servizio, le metriche predefinite vengono indicate come **activeconn** e **connrate**. Se si desiderano metriche aggiuntive o metriche completamente diverse da quelle predefinite, digitare:

```
service metrics switchConsultantID:serviceID metricName 50  
metricName2 50
```

Fase 6. Avvio del consultant

Per avviare il consultant, digitare:

```
consultant start switchConsultantID
```

In questo modo, vengono avviati gli strumenti di raccolta delle metriche e viene avviato il calcolo dei pesi.

Fase 7. Configurazione della disponibilità elevata (facoltativa)

Per configurare la disponibilità elevata, digitare:

```
highavailability add address IPaddress partneraddress IPaddress port 80  
role primary
```

Per informazioni dettagliate su come utilizzare e configurare la disponibilità elevata del controller, vedere Capitolo 23, "Funzioni avanzate di Controller Cisco CSS e Controller Nortel Alteon", a pagina 235.

Fase 8. Avvio di Metric Server (facoltativo)

Se le metriche del sistema vengono definite nella fase 5, il server delle metriche deve essere avviato sulle metriche del servizio. Per informazioni sull'uso del server delle metriche, vedere "Metric Server" a pagina 245.

Fase 9. Aggiornamento della configurazione di Controller Nortel Alteon

Se viene modificata la configurazione su Switch Nortel Alteon Web, è possibile aggiornare la configurazione del controller. Digitare:

```
service refresh
```

Si consiglia di arrestare il consultant prima di eseguire un aggiornamento della configurazione. Dopo aver aggiornato la configurazione tramite il comando refresh, riavviare il consultant.

Verifica della configurazione

Verificare se la configurazione è in esecuzione:

1. Impostare il livello di log del consultant su 4.
2. Disconnettere un server da Switch Nortel Alteon Web per un minuto, oppure arrestare il server delle applicazioni per un minuto.
3. Riconnettere il server oppure riavviare il server delle applicazioni.
4. Riportare il livello di log del consultant sul livello desiderato (1).
5. Visualizzare il file consultant.log situato nelle seguenti directory e ricercare **setServerWeights setting service**. Ciò significa che è stato effettuato un tentativo di inviare pesi allo switch.
 - Su sistemi AIX, HP-UX, Linux e Solaris: `...ibm/edge/lb/servers/logs/cco/nomeconsultant`
 - Su sistemi Windows: `...ibm\edge\lb\servers\logs\cco\nomeconsultant`
6. Visualizzare i pesi dei server sullo switch e verificare che corrispondano ai pesi mostrati sul report del controller.

Parte 7. Funzioni e caratteristiche avanzate di Load Balancer

Questa sezione fornisce informazioni sulle funzioni e sulle caratteristiche avanzate di configurazione disponibili per Load Balancer. Contiene i seguenti capitoli:

- Capitolo 21, "Funzioni gestore, advisor e Metric Server per Dispatcher, CBR e Site Selector", a pagina 175
- Capitolo 22, "Funzioni avanzate di Dispatcher, CBR e Site Selector", a pagina 195
- Capitolo 23, "Funzioni avanzate di Controller Cisco CSS e Controller Nortel Alteon", a pagina 235

Capitolo 21. Funzioni gestore, advisor e Metric Server per Dispatcher, CBR e Site Selector

Questo capitolo illustra come configurare i parametri per il bilanciamento del carico e come impostare le funzioni gestore, advisor e Metric Server di Load Balancer.

Nota: se, durante la lettura di questo capitolo, *non* si sta utilizzando il componente Dispatcher, sostituire "dscontrol" con quanto segue:

- Per CBR, utilizzare **cbrcontrol**
- Per Site Selector, utilizzare **sscontrol** (vedere Capitolo 28, "Riferimenti sui comandi per Site Selector", a pagina 391)

IMPORTANTE: se si sta utilizzando l'installazione di Load Balancer per IPv4 e IPv6, vedere Capitolo 8, "Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6", a pagina 79 per evidenziare le limitazioni e le differenze di configurazione prima di esaminare i contenuti di questa sezione.

Tabella 12. Attività di configurazione avanzate di Load Balancer

Attività	Descrizione	Informazioni correlate
Facoltativamente, modificare le impostazioni di bilanciamento del carico	È possibile modificare le seguenti impostazioni di bilanciamento del carico: <ul style="list-style-type: none">• Proporzione di importanza attribuita alle informazioni sullo stato Il rapporto predefinito è 50-50-0-0. Se si utilizza tale valore, le informazioni provenienti dagli advisor, da Metric Server e da WLM non vengono utilizzate.• Pesi• Pesi fissi del gestore• Intervalli del gestore• Soglia di sensibilità• Indice di arrotondamento	"Ottimizzazione del bilanciamento del carico in Load Balancer" a pagina 176
Utilizzo degli script per generare un avviso o registrare un malfunzionamento dei server quando il gestore contrassegna i server come attivi/inattivi	Load Balancer fornisce uscite utente che attivano script personalizzabili quando il gestore contrassegna i server come attivi/inattivi.	"Uso degli script per generare un avviso o registrare un malfunzionamento dei server" a pagina 180
Utilizzo degli advisor	Descrive ed elenca gli advisor che notificano stati specifici dei server	"Advisor" a pagina 181
Utilizzo dell'opzione di richiesta/risposta (URL) degli advisor HTTP o HTTPS	Definisce una stringa URL HTTP client univoca, specifica per un servizio che si desidera interrogare sulla macchina	"Configurazione dell'advisor HTTP o HTTPS utilizzando l'opzione richiesta/risposta (URL)" a pagina 186
Utilizzo di advisor autonomo	Fornisce lo stato di carico sul server di backend in una configurazione WAN a due livelli di Load Balancer	"Utilizzo dell'advisor autonomo in una configurazione WAN a due livelli" a pagina 187
Creazione di advisor personalizzati	Descrive come scrivere gli advisor personalizzati	"Creazione di advisor personalizzati" a pagina 188

Tabella 12. Attività di configurazione avanzate di Load Balancer (Continua)

Attività	Descrizione	Informazioni correlate
Utilizzo dell'agente Metric Server	Metric Server fornisce le informazioni sul carico del sistema a Load Balancer	"Metric Server" a pagina 191
Utilizzo dell'advisor WLM (Workload Manager)	L'advisor WLM fornisce le informazioni sul carico del sistema a Load Balancer	"Advisor Workload Manager" a pagina 193

Ottimizzazione del bilanciamento del carico in Load Balancer

La funzione gestore di Load Balancer esegue il bilanciamento del carico in base alle seguenti impostazioni:

- "Proporzione di importanza attribuita alle informazioni sullo stato"
- "Pesi" a pagina 177
- "Intervalli del gestore" a pagina 179
- "Intervalli dell'advisor" a pagina 183
- "Timeout report dell'advisor" a pagina 183
- "Soglia di sensibilità" a pagina 179
- "Indice di arrotondamento" a pagina 179

Queste impostazioni possono essere modificate per ottimizzare il bilanciamento del carico nella rete in uso.

Proporzione di importanza attribuita alle informazioni sullo stato

Nelle decisioni relative al calcolo dei pesi, il gestore può utilizzare completamente o in parte i seguenti fattori esterni

- *Connessioni attive*: il numero di connessioni attive su ciascuna macchina server con bilanciamento del carico (registrato dall'executor). Questa proporzione non si applica a Site Selector.

Oppure —

CPU: la percentuale di CPU in uso su ciascuna macchina server con bilanciamento del carico (input dell'agente Metric Server). Esclusivamente per Site Selector, questa proporzione viene visualizzata al posto della colonna delle proporzioni delle connessioni attive.

- *Nuove connessioni*: il numero di connessioni nuove su ciascuna macchina server con bilanciamento del carico (registrato dall'executor). Questa proporzione non si applica a Site Selector.

Oppure —

Memoria: la percentuale di memoria in uso (input dell'agente Metric Server) su ciascun server con bilanciamento del carico. Esclusivamente per Site Selector, questa proporzione viene visualizzata al posto della colonna delle proporzioni delle connessioni nuove.

- *Specifici della porta*: l'input degli advisor in ascolto sulla porta.
- *Metriche del sistema*: l'input degli strumenti di monitoraggio del sistema, ad esempio Metric Server o WLM.

Insieme al peso corrente di ciascun server e ad altre informazioni necessarie per i relativi calcoli, il gestore ottiene i primi due valori (connessioni nuove e attive) dall'executor. Questi valori si basano sulle informazioni generate e memorizzate internamente nell'executor.

Nota: Per Site Selector, il gestore ottiene i primi due valori (CPU e memoria) da Metric Server.

È possibile modificare la proporzione di importanza da attribuire ai quattro valori metrici per ciascun cluster (o nome del sito). È opportuno considerare la proporzione come percentuale; la somma delle proporzioni deve essere uguale al 100%. Il rapporto predefinito è 50/50/0/0, che ignora le informazioni dell'advisor e del sistema. Nell'ambiente in uso, può essere necessario tentare combinazioni diverse delle proporzioni per individuare la combinazione che offra le prestazioni migliori.

Nota: quando si aggiunge un advisor (diverso da WLM), se la **proporzione della porta** è uguale a zero, il gestore aumenta questo valore a 1. Poiché la somma delle proporzioni deve essere uguale a 100, il valore più alto viene ridotto di 1.

Quando si aggiunge un advisor WLM, se la **proporzione delle metriche del sistema** è uguale a zero, il gestore aumenta questo valore a 1. Poiché la somma delle proporzioni deve essere uguale a 100, il valore più alto viene ridotto di 1.

Il numero delle connessioni attive dipende dal numero di client e dal tempo necessario per l'utilizzo dei servizi forniti dalle macchine server con bilanciamento del carico. Se le connessioni client sono rapide (ad esempio, piccole pagine Web richiamate tramite HTTP GET), il numero delle connessioni attive sarà abbastanza basso. Se le connessioni client sono più lente (ad esempio, query del database), il numero delle connessioni attive sarà più alto.

È necessario evitare di impostare valori di proporzioni delle connessioni attive e nuove troppo bassi. Il bilanciamento del carico e l'arrotondamento verranno disabilitati a meno che ciascuno dei primi due valori non sia impostato almeno su 20.

Per impostare la proporzione dei valori di importanza, utilizzare il comando **dscontrol cluster set *cluster* proportions**. Per ulteriori informazioni, consultare "dscontrol cluster — configura i cluster" a pagina 345.

Pesi

I pesi vengono impostati dalla funzione gestore in base ai contatori interni all'executor, alle informazioni restituite dagli advisor e alle informazioni restituite dal programma di monitoraggio del sistema, ad esempio Metric Server. Per impostare i pesi manualmente durante l'esecuzione del gestore, specificare l'opzione **fixedweight** sul comando **dscontrol server**. Per una descrizione dell'opzione **fixedweight**, vedere "Pesi fissi del gestore" a pagina 178.

I pesi vengono applicati a tutti i server su una porta. Per ogni particolare porta, le richieste vengono distribuite tra i servizi in base ai loro pesi rispettivi. Ad esempio, se un server è impostato su un peso pari a 10 e l'altro su un peso pari a 5, il server impostato su 10 riceverà il doppio delle richieste del server impostato su 5.

Per specificare il limite massimo del peso che un server può avere, utilizzare il comando **dscontrol port set *port* weightbound *weight***. Questo comando influisce sulla differenza che può sussistere tra il numero delle richieste a ciascun server. Se il valore **weightbound** (limite di peso) massimo è impostato su 1, tutti i server possono avere un peso di 1, 0 se inattivo o -1 se contrassegnato come guasto.

Aumentando questo numero, la differenza del calcolo dei pesi attribuibili ai server aumenta. A un valore `weightbound` (limite di peso) massimo di 2, un server può ricevere il doppio delle richieste di un altro server. A un valore `weightbound` (limite di peso) massimo di 10, un server può ricevere 10 volte le richieste di un altro server. Il valore `weightbound` predefinito massimo è 20.

Se un advisor rileva che un server è inattivo, notifica questa condizione al gestore che imposta il peso per tale server su zero. Di conseguenza, l'executor non invierà connessioni aggiuntive a tale server fin tanto che il valore del peso rimarrà zero. In caso di connessioni attive su quel server prima che venisse modificato il peso, queste verranno completate normalmente.

Se tutti i server sono inattivi, il gestore imposta i pesi sul metà del valore `weightbound`.

Pesi fissi del gestore

Senza il gestore, gli advisor non possono essere eseguiti e non possono rilevare se un server è inattivo. Se si sceglie di eseguire gli advisor, ma *non* si desidera che il gestore aggiorni il peso impostato per un determinato server, utilizzare l'opzione **fixedweight** sul comando `dscontrol server`. Ad esempio:

```
dscontrol server set cluster:port:server fixedweight yes
```

Dopo aver impostato `fixedweight` su sì (yes), utilizzare il comando **dscontrol server set weight** per impostare il peso sul valore desiderato. Il valore del peso del server rimane fisso mentre il gestore è in esecuzione finché non si immette un altro comando `dscontrol server` con `fixedweight` impostato su no. Per ulteriori informazioni, vedere “`dscontrol server` — configura i server” a pagina 381.

Invio di un comando TCP reset a un server guasto (solo componente Dispatcher)

Se viene attivato il **ripristino** TCP, Dispatcher invierà un comando TCP reset al client connesso a un server con peso impostato su 0. Il peso del server può essere 0 se configurato su tale valore o se l'advisor lo contrassegna come inattivo. Un comando TCP reset chiude immediatamente la connessione. Questa opzione è utile per connessioni lunghe in cui viene accelerata la capacità del client di negoziare nuovamente una connessione non riuscita. Per attivare il ripristino TCP, utilizzare il comando **dscontrol port add | set port reset yes**. Il valore predefinito per il comando reset è no.

Nota: il comando TCP reset si applica a tutti i metodi di inoltro del Dispatcher. Tuttavia, per poter utilizzare l'opzione di ripristino TCP, il **clientgateway** sul comando **dscontrol executor** deve essere impostato su un indirizzo router.

Un'opzione utile da configurare, insieme al ripristino TCP, è **nuovi tentativi degli advisor**. Con questa funzione, un advisor può tentare nuovamente una connessione prima di contrassegnare come inattivo un server. In questo modo si evita che un server venga contrassegnato come inattivo prematuramente e, di conseguenza, si evitano problemi di ripristino della connessione. Ossia, solo perché il primo tentativo dell'advisor non è riuscito non significa che anche le connessioni esistenti non riescano. Per ulteriori informazioni, consultare “Nuovi tentativi dell'advisor” a pagina 184.

Intervalli del gestore

Per ottimizzare le prestazioni generali, il gestore viene limitato nella frequenza di interazione con l'executor. È possibile modificare questo intervallo immettendo i comandi **dscontrol manager interval** e **dscontrol manager refresh**.

L'intervallo del gestore imposta la frequenza con cui il gestore aggiornerà i pesi dei server che l'executor utilizza per instradare le connessioni. Se l'intervallo è impostato su un valore troppo basso, le prestazioni possono ridursi notevolmente come conseguenza delle continue interruzioni dell'executor da parte del gestore. Se l'intervallo del gestore è impostato su un valore troppo alto, l'instradamento delle richieste da parte dell'executor non si baserà su informazioni precise e aggiornate.

Ad esempio, per impostare l'intervallo del gestore su 1 secondo, immettere il seguente comando:

```
dscontrol manager interval 1
```

Il ciclo di aggiornamento del gestore specifica la frequenza con cui il gestore richiede all'executor le informazioni sullo stato. Il ciclo di aggiornamento si basa sul tempo dell'intervallo.

Ad esempio, per impostare il ciclo di aggiornamento del gestore su 3, immettere il seguente comando:

```
dscontrol manager refresh 3
```

In questo modo il gestore attende per 3 secondi prima di richiedere all'executor le informazioni sullo stato.

Soglia di sensibilità

Per ottimizzare il bilanciamento del carico sui server, sono disponibili altri metodi. Per garantire la massima velocità, gli aggiornamenti dei pesi dei server vengono eseguiti solo se i pesi sono stati modificati significativamente. Un aggiornamento continuo dei pesi quando lo stato dei server non viene sottoposto a modifiche di entità considerevole creerebbe solo un sovraccarico superfluo. Quando la variazione percentuale del peso complessivo di tutti i server su una porta supera la soglia di sensibilità, i pesi utilizzati dall'executor per distribuire le connessioni vengono aggiornati dal gestore. Supporre, ad esempio, che il peso totale passi da 100 a 105. La variazione è del 5%. Se la soglia di sensibilità predefinita è 5, i pesi utilizzati dall'executor non vengono aggiornati dal gestore, in quanto la variazione in percentuale non **supera** la soglia. Tuttavia, se la variazione del peso totale passa da 100 a 106, il gestore aggiorna i pesi. Per impostare la soglia di sensibilità del gestore su un valore diverso da quello predefinito (ad esempio 6), immettere il seguente comando:

```
dscontrol manager sensitivity 6
```

Nella maggior parte dei casi, non è necessario modificare questo valore.

Indice di arrotondamento

Il gestore calcola i pesi sul server in modo dinamico. Di conseguenza, un peso aggiornato può essere differente da quello precedente. Nella maggior parte dei casi, questo non rappresenta un problema. Tuttavia, in alcuni casi, potrebbe causare un'oscillazione nel modo in cui viene eseguito il bilanciamento del carico delle richieste. Ad esempio, un server può interrompere la ricezione della maggior parte delle richieste a causa di un peso elevato. Il gestore rileva che il server ha un

numero di connessioni attive elevato e che risponde lentamente. Quindi, passerà il peso sui server liberi, sui quali si verificherà la stessa situazione, creando un uso inefficiente delle risorse.

Per risolvere questo problema, il gestore utilizza un indice di arrotondamento. Tale indice limita la quantità di peso che è possibile modificare su un server, arrotondando in modo effettivo la variazione nella distribuzione delle richieste. Un indice di arrotondamento più alto fa in modo che i pesi del server subiscano delle variazioni meno drastiche. Con un indice più basso, i pesi del server subiranno delle variazioni più drastiche. Il valore predefinito per l'indice di arrotondamento è 1.5. Con tale impostazione, i pesi del server possono essere piuttosto dinamici, mentre un indice di 4 o 5 renderà i pesi più stabili. Ad esempio, per impostare l'indice di arrotondamento su 4, immettere il seguente comando:

```
dscontrol manager smoothing 4
```

Nella maggior parte dei casi, non è necessario modificare questo valore.

Uso degli script per generare un avviso o registrare un malfunzionamento dei server

Load Balancer fornisce uscite utente che attivano script personalizzabili. È possibile creare gli script per eseguire azioni automatizzate, quali avvisare un amministratore quando i server sono contrassegnati come inattivi dal gestore o semplicemente registrare l'evento del malfunzionamento. Gli script di esempio, personalizzabili, si trovano nella directory di installazione **...ibm/edge/lb/servers/samples**. Per eseguire questi file, spostarli nella directory **...ibm/edge/lb/servers/bin** ed eliminare l'estensione file "sample". Vengono forniti i seguenti script di esempio:

- **serverDown** — un server è contrassegnato come inattivo dal gestore.
- **serverUp** — un server è contrassegnato come server di backup dal gestore.
- **managerAlert** — tutti i server sono contrassegnati come inattivi per una determinata porta.
- **managerClear** — almeno un server è attivo, dopo che tutti sono stati contrassegnati come inattivi per una determinata porta.

Se tutti i server in un cluster sono contrassegnati come inattivi (dall'utente o dagli advisor), viene eseguito **managerAlert** (se configurato) e Load Balancer tenta di instradare il traffico ai server con una tecnica round-robin. Lo script **serverDown** non viene eseguito quando l'ultimo server del cluster viene rilevato come non in linea.

Da schema, Load Balancer tenta di continuare a instradare il traffico nel caso in cui un server ritorni in linea e risponda alla richiesta. Se, al contrario, Load Balancer, elimina il traffico, il client non riceverebbe alcuna risposta.

Quando Load Balancer rileva che il primo server di un client è nuovamente in linea, viene eseguito lo script **managerClear** (se configurato) ma lo script **serverUp** (se configurato) non viene eseguito fino a quando un altro server non viene riportato in linea.

Considerazioni sull'uso degli script **serverUp** e **serverDown**:

- Se il ciclo del gestore viene definito su un valore inferiore al 25% del tempo dell'advisor, possono risultare falsi report di server attivi o inattivi. Per impostazione predefinita, il gestore viene eseguito ogni 2 secondi mentre l'advisor ogni 7. Quindi, il gestore prevede nuove informazioni dall'advisor entro 4 cicli. Eliminando questa limitazione (ossia, definendo il ciclo del gestore

su un valore superiore al 25% del tempo dell'advisor) si riducono significativamente le prestazioni poiché più advisor possono fornire le informazioni a un solo server.

- Quando un server diventa inattivo, viene eseguito lo script serverDown. Tuttavia, se viene emesso un comando serverUp, si presume che il server sia attivo fino a quando il gestore non ottiene le nuove informazioni dal ciclo dell'advisor. Se il server rimane inattivo, lo script serverDown viene eseguito nuovamente.

Advisor

Gli advisor sono agenti di Load Balancer il cui scopo è quello di valutare lo stato e il carico delle macchine server. Questa operazione viene eseguita con uno scambio proattivo del tipo client con i server. Gli advisor possono essere considerati come client leggeri dei server delle applicazioni.

Il prodotto fornisce alcuni advisor specifici per i protocolli più diffusi. Tuttavia, è inutile utilizzare tutti gli advisor forniti con ciascun componente di Load Balancer. (Ad esempio, con il componente CBR non si utilizzerebbe l'advisor Telnet.) Load Balancer supporta, inoltre, il concetto di "advisor personalizzato" che consente agli utenti di scrivere i propri advisor.

Limitazione sull'utilizzo delle applicazioni server specifiche del

collegamento: Per poter utilizzare gli advisor sui server specifici di collegamento, avviare due istanze del server: una da collegare su cluster:porta e l'altra da collegare su server:porta. Per determinare se il server è bind specifico, emettere il comando netstat -an e ricercare server:porta. Se il server non è bind specifico, il risultato di questo comando sarà 0.0.0.0:80. Se invece il server è bind specifico, verrà visualizzato un indirizzo del tipo 192.168.15.103:80.

Su sistemi HP-UX e Solaris, limitazione all'uso delle applicazioni server

specifiche del collegamento: Se si utilizza il comando arp publish invece di ifconfig alias, Load Balancer *supporterà* l'uso degli advisor durante il bilanciamento del carico dei server con applicazioni server specifiche del collegamento (inclusi altri componenti Load Balancer quali CBR o Site Selector) quando si collegano all'indirizzo IP cluster. Tuttavia, l'uso degli advisor sull'applicazione server specifica del collegamento non consente di posizionare Load Balancer sulla stessa macchina con l'applicazione server.

Nota: quando Load Balancer è in esecuzione su un computer con più schede adattatore di rete e se si desidera che il traffico degli advisor venga distribuito a un particolare adattatore, è possibile forzare l'indirizzo IP di origine dei pacchetti a un indirizzo particolare. Per forzare l'indirizzo di origine del pacchetto advisor su un indirizzo particolare, aggiungere quanto segue alla riga java...SRV_XXXConfigServer... del file di script di avvio di Load Balancer appropriato (dsserver, cbrserver o ssserver):

```
-DLB_ADV_SRC_ADDR=indirizzo_IP
```

Funzionamento degli advisor

Gli advisor aprono periodicamente una connessione TCP con ciascun server e inviano un messaggio di richiesta al server. Il contenuto del messaggio è specifico del protocollo in esecuzione sul server. Ad esempio, l'advisor HTTP invia una richiesta HTTP "HEAD" al server.

Quindi, gli advisor restano in ascolto di una risposta dal server. Dopo aver ricevuto la risposta, l'advisor esegue una valutazione del server. Per calcolare questo valore di "carico", la maggior parte degli advisor misura il tempo impiegato dal server per rispondere, quindi utilizza questo valore, espresso in millisecondi, come valore del carico.

Gli advisor notificano il valore del carico alla funzione gestore, dove viene visualizzato nella colonna "Port" del report del gestore. Il gestore calcola i valori dei pesi aggregati provenienti da tutte le fonti, in base alle relative proporzioni, e invia tali valori dei pesi alla funzione executor. L'Executor utilizza questi pesi per bilanciare il carico delle nuove connessioni client in entrata.

Se l'advisor stabilisce che un server è attivo e funzionante, notifica al gestore un numero di carico positivo, diverso da zero. Se l'advisor stabilisce che un server non è attivo, restituisce un valore di carico particolare pari a meno uno (-1). Il gestore e l'executor non inoltrano ulteriori connessioni a quel server finché il server non è di nuovo attivo.

Nota: prima di inviare il messaggio di richiesta iniziale, l'advisor invierà un ping al server. In questo modo, viene fornito rapidamente lo stato per determinare se la macchina è in linea. Quando il server risponde al ping, non verranno inviati altri ping. Per disabilitare i ping, aggiungere -DLB_ADV_NB_PING al file di script di avvio di Load Balancer.

Avvio e arresto di un advisor

È possibile avviare un advisor per una porta particolare attraverso tutti i cluster (advisor di gruppo). Oppure, scegliere di eseguire diversi advisor sulla stessa porta ma su cluster differenti (advisor specifici per cluster/sito). Ad esempio, se Load Balancer è definito con tre cluster (*clusterA*, *clusterB*, *clusterC*), ciascuno con la porta 80 è possibile effettuare quanto segue:

- Advisor specifico per cluster/sito: per avviare un advisor sulla porta 80 per *clusterA*, specificare sia il cluster che la porta:
`dscontrol advisor start http clusterA:80`

Questo comando consente di avviare l'advisor HTTP sulla porta 80 per *clusterA*. L'advisor HTTP esaminerà tutti i server collegati alla porta 80 per il clusterA.

- Advisor del gruppo: per avviare un advisor personalizzato sulla porta 80 per tutti gli altri cluster, è sufficiente specificare la porta:
`dscontrol advisor start ADV_custom 80`

Questo comando consente di avviare l'advisor *ADV_custom* sulla porta 80 per *clusterB* e *clusterC*. L'advisor personalizzato esaminerà tutti i server collegati alla porta 80 per *clusterB* e *clusterC*. (Per ulteriori informazioni sugli advisor personalizzati, vedere "Creazione di advisor personalizzati" a pagina 188).

Nota: l'advisor del gruppo esaminerà tutti i cluster/siti che attualmente non dispongono di un advisor specifico.

Utilizzando l'esempio di configurazione per l'advisor del gruppo riportato sopra, è possibile scegliere di arrestare l'advisor personalizzato *ADV_custom* per la porta 80 su un solo cluster o su entrambi i cluster (*clusterB* e *clusterC*).

- Per arrestare l'advisor personalizzato per la porta 80 solo sul *clusterB*, specificare cluster e porta:

```
dscontrol advisor  
stop ADV_custom clusterB:80
```

- Per arrestare l'advisor personalizzato per la porta 80 sul *clusterB* e sul *clusterC*, specificare solo la porta:

```
dscontrol advisor stop ADV_custom 80
```

Intervallo dell'advisor

Nota: le impostazioni predefinite dell'advisor dovrebbero funzionare efficacemente nella maggior parte degli scenari possibili. Prestare attenzione quando si specificano dei valori diversi da quelli predefiniti.

L'intervallo dell'advisor consente di impostare la frequenza con cui un advisor chiede lo stato dei server sulla porta su cui esegue il monitoraggio e notifica i risultati al gestore. Se l'intervallo dell'advisor è impostato su un valore troppo basso, le prestazioni possono ridursi notevolmente come conseguenza delle continue interruzioni dei server da parte dell'advisor. Se l'intervallo dell'advisor è impostato su un valore troppo alto, le decisioni del gestore sul calcolo dei pesi non si baseranno su informazioni precise e aggiornate.

Ad esempio, per impostare l'intervallo dell'advisor HTTP per la porta 80 su 3 secondi, immettere il seguente comando:

```
dscontrol advisor interval http 80 3
```

Non specificare un intervallo dell'advisor inferiore a quello del gestore. L'intervallo predefinito dell'advisor è di sette secondi.

Timeout report dell'advisor

Per garantire che il gestore non utilizzi informazioni non aggiornate nelle decisioni per il bilanciamento del carico, il gestore non utilizzerà le informazioni provenienti dall'advisor la cui data/ora è precedente all'ora impostata nel timeout report dell'advisor. Il timeout report dell'advisor deve essere maggiore dell'intervallo di polling dell'advisor. Se minore, il gestore ignora i report che dovrebbero essere utilizzati localmente. Per impostazione predefinita, i report dell'advisor non sono sottoposti a timeout — il valore predefinito è illimitato.

Ad esempio, per impostare il timeout report dell'advisor HTTP per la porta 80 su 3 secondi, immettere il seguente comando:

```
dscontrol advisor timeout http 80 30
```

Per ulteriori informazioni sull'impostazione del timeout report advisor, vedere "dscontrol advisor — controlla l'advisor" a pagina 339.

Timeout di connessione e timeout di ricezione dell'advisor per i server

In Load Balancer, è possibile impostare i valori di timeout dell'advisor ai quali rileva che una porta particolare sul server (un servizio) non funziona. I valori di timeout per i server che non hanno funzionato correttamente (connecttimeout e receivetimeout) stabiliscono per quanto tempo l'advisor deve rimanere in attesa prima di notificare che l'operazione di connessione o l'operazione di ricezione non ha avuto esito positivo.

Per ottenere il rilevamento più rapido dei server che non hanno funzionato correttamente, impostare i timeout di connessione e di ricezione dell'advisor sul valore più piccolo (un secondo) e impostare l'intervallo del gestore e dell'advisor sul valore più piccolo (un secondo).

Nota: se l'ambiente presenta un traffico medio-alto che aumenta il tempo di risposta dei server, non impostare dei valori connecttimeout e receivetimeout troppo piccoli oppure l'advisor potrebbe contrassegnare prematuramente un server occupato come guasto.

Ad esempio, per impostare connecttimeout e receivetimeout su 9 secondi per l'advisor HTTP sulla porta 80, immettere il seguente comando:

```
dscontrol advisor connecttimeout http 80 9
dscontrol advisor receivetimeout http 80 9
```

Il valore predefinito del timeout di connessione e di ricezione è 3 volte il valore specificato per l'intervallo dell'advisor.

Nuovi tentativi dell'advisor

Gli advisor possono tentare nuovamente una connessione prima di contrassegnare come inattivo un server. L'advisor non contrassegna un server come inattivo finché la query eseguita sul server non ha avuto esito negativo per il numero di tentativi più 1. Si consiglia di non impostare un valore di **tentativi** superiore a 3. Il seguente comando imposta un valore dei tentativi di 2 per l'advisor LDAP sulla porta 389:

```
dscontrol advisor retry ldap 389 2
```

Elenco di advisor

- L'advisor **HTTP** apre una connessione, invia una richiesta HEAD per impostazione predefinita, attende una connessione di risposta quindi restituisce il tempo trascorso come carico. Vedere "Configurazione dell'advisor HTTP o HTTPS utilizzando l'opzione richiesta/risposta (URL)" a pagina 186 per ulteriori informazioni su come modificare il tipo di richiesta inviato dall'advisor HTTP.
- L'advisor **HTTPS** è un advisor "heavyweight" per le connessioni SSL. Esegue una connessione socket SSL completa al server. L'advisor HTTP apre una connessione SSL, invia una richiesta HTTPS, attende una risposta, chiude la connessione quindi restituisce il tempo trascorso come carico. (Vedere anche l'advisor SSL, che è l'advisor "lightweight" per le connessioni SSL.)

Nota: l'advisor HTTPS non ha alcuna dipendenza dalla chiave server o dal contenuto del certificato ma questi non devono scadere.

- L'advisor **SIP** apre una connessione, invia una richiesta OPTIONS, attende una risposta, chiude la connessione, quindi restituisce il tempo trascorso come carico. L'advisor SIP supportato viene eseguito solo sul protocollo TCP e richiede l'installazione di un'applicazione su un server che risponde a una richiesta OPTIONS.
- L'advisor **FTP** apre una connessione, invia una richiesta SYST, attende una risposta, chiude la connessione, quindi restituisce il tempo trascorso come carico.
- L'advisor **LDAP** apre una connessione, invia una richiesta BIND anonima, attende una risposta, chiude la connessione, quindi restituisce il tempo trascorso come carico.
- L'advisor **Telnet** apre una connessione, attende un messaggio iniziale dal server, chiude la connessione, quindi restituisce il tempo trascorso come carico.

- L'advisor **NNTP** apre una connessione, attende un messaggio iniziale dal server, invia un comando quit, chiude la connessione, quindi restituisce il tempo trascorso come carico.
- L'advisor **IMAP** apre una connessione, attende un messaggio iniziale dal server, invia un comando quit, chiude la connessione, quindi restituisce il tempo trascorso come carico.
- L'advisor **POP3** apre una connessione, attende un messaggio iniziale dal server, invia un comando quit, chiude la connessione, quindi restituisce il tempo trascorso come carico.
- L'advisor **SMTP** apre una connessione, attende un messaggio iniziale dal server, invia un comando quit, chiude la connessione, quindi restituisce il tempo trascorso come carico.
- L'advisor **SSL** è un advisor "lightweight" per le connessioni SSL. Non stabilisce una connessione socket SSL completa al server. L'advisor SSL apre una connessione, invia una richiesta SSL CLIENT_HELLO, attende una risposta, chiude la connessione, quindi restituisce il tempo trascorso come carico. (Vedere anche l'advisor HTTPS, che è l'advisor "heavyweight" per le connessioni SSL.)

Nota: l'advisor SSL non ha alcuna dipendenza dalla gestione delle chiavi o dai certificati.

- L'advisor **ssl2http** avvia ed esamina i server elencati per la porta 443 ma aprirà una connessione socket a "mapport" per le richieste HTTP. Utilizzare solo l'advisor ssl2http per CBR se il protocollo client-proxy è SSL e il protocollo proxy-server è HTTP. Per ulteriori informazioni, vedere "Bilanciamento del carico client-proxy in SSL e proxy-server in HTTP" a pagina 106.
- L'advisor Caching Proxy (cachingproxy) apre una connessione, invia una richiesta HTTP GET specifica di Caching Proxy e interpreta la risposta come carico Caching Proxy.

Nota: quando si utilizza Caching Proxy, Caching Proxy deve essere in esecuzione su tutti i server con bilanciamento del carico. La macchina su cui Load Balancer risiede non deve avere Caching Proxy installato a meno che non si trovi sulla stessa macchina su cui sta eseguendo il bilanciamento del carico.

- L'advisor **DNS** apre una connessione, invia una query del puntatore per DNS, attende una risposta, chiude la connessione, quindi restituisce il tempo trascorso come carico.
- L'advisor di **connessione** non scambia i dati specifici del protocollo con il server ma calcola semplicemente il tempo impiegato per aprire e chiudere una connessione TCP con il server. Questo advisor è utile per le applicazioni server che utilizzano TCP ma con un protocollo di livello superiore per cui non è disponibile un advisor personalizzato o fornito da IBM.
- L'advisor **ping** non apre una connessione TCP con i server ma notifica se il server risponde a un ping. Mentre un advisor ping potrebbe essere utilizzato su qualsiasi porta, è ideato anche per le configurazioni che utilizzano una porta jolly su cui può essere distribuito il traffico di più protocolli. È utile anche per configurazioni che utilizzano protocolli non TCP con i relativi server, come ad esempio UDP.
- L'advisor **reach** invia un ping alle relative macchine di destinazione. Questo advisor è progettato per i componenti a disponibilità elevata di Dispatcher per determinare l'accessibilità di ciascuna destinazione. I risultati vengono distribuiti al componente a disponibilità elevata e *non* vengono visualizzati nel report del

gestore. A differenza degli altri advisor, l'advisor reach viene avviato automaticamente dalla funzione gestore del componente Dispatcher.

- L'advisor **DB2** interagisce con i server DB2. Dispatcher dispone della capacità incorporata di controllare lo stato dei server DB2 senza che i clienti debbano scrivere i loro advisor personalizzati. L'advisor DB2 comunica solo con la porta di connessione DB2 e non con la porta Java.
- L'advisor **autonomo** raccoglie le informazioni sullo stato del carico sui server di backend. È possibile utilizzare l'advisor autonomo durante l'uso di Dispatcher in una configurazione a due-livelli, in cui Dispatcher fornisce le informazioni provenienti dall'advisor autonomo al Load Balancer di livello superiore. L'advisor autonomo calcola specificatamente le connessioni al secondo sui server di backend del Dispatcher a livello dell'executor. Per ulteriori informazioni, consultare "Utilizzo dell'advisor autonomo in una configurazione WAN a due livelli" a pagina 187.
- L'advisor **WLM** (Workload Manager) è progettato per interagire con i server sui mainframe OS/390 su cui è in esecuzione il componente MVS Workload Manager (WLM). Per ulteriori informazioni, vedere "Advisor Workload Manager" a pagina 193.
- Dispatcher consente a un cliente di scrivere un advisor *personalizzato* (personalizzabile), garantendo così il supporto dei protocolli proprietari (sul livello superiore di TCP) per cui IBM non ha sviluppato un advisor specifico. Per ulteriori informazioni, vedere "Creazione di advisor personalizzati" a pagina 188.
- L'advisor **WAS** (WebSphere Application Server) interagisce con i server WebSphere Application. I file di esempio personalizzabili per questo advisor sono forniti nella directory di installazione. Per ulteriori informazioni, vedere "Advisor WAS" a pagina 189.

Configurazione dell'advisor HTTP o HTTPS utilizzando l'opzione richiesta/risposta (URL)

L'opzione URL per l'advisor HTTP o HTTPS è disponibile per i componenti Dispatcher e CBR.

Dopo aver avviato un advisor HTTP o HTTPS, è possibile definire una stringa URL HTTP client univoca, specifica del servizio che si desidera interrogare sul server. In questo modo si consente all'advisor di valutare lo stato dei singoli servizi all'interno di un server. Ciò è possibile definendo i server logici con nomi server univoci con lo stesso indirizzo IP fisico. Per ulteriori informazioni, consultare "Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)" a pagina 55.

Per ciascun server logico definito nella porta HTTP, è possibile specificare una stringa URL HTTP client univoca, specifica per il servizio che si desidera interrogare sul server. L'advisor HTTP o HTTPS utilizza la stringa **advisorrequest** per verificare lo stato dei server. Il valore predefinito è HEAD / HTTP/1.0. La stringa **advisorresponse** è la risposta alla scansione da parte dell'advisor della risposta HTTP. L'advisor utilizza la stringa **advisorresponse** per confrontare la risposta effettiva ricevuta dal server. Il valore predefinito è null.

Importante: se la stringa URL HTTP contiene uno spazio:

- Quando si emette il comando dal prompt della shell **dscontrol>>**, è necessario racchiudere la stringa tra virgolette se questa contiene uno spazio. Ad esempio:

```
server set cluster:port:server advisorrequest "head / http/1.0"  
server set cluster:port:server advisorresponse "HTTP 200 OK"
```


- Quando si emette il comando **dscontrol** dal prompt del sistema operativo, il testo deve essere preceduto da "\" e seguito da \". Ad esempio:

```
dscontrol server set cluster:port:server
advisorrequest "\"head / http/1.0\""
```

```
dscontrol server set cluster:port:server advisorresponse "\"HTTP 200 OK\""
```

Durante la creazione della richiesta HTTP o HTTPS che l'advisor invia ai server di backend per vedere se funzionano, viene digitato l'inizio della richiesta HTTP e Load Balancer completa la fine della richiesta come segue:

```
\r\nAccept:
*/*\r\nUser-Agent:IBM_Network_Dispatcher_HTTP_Advisor\r\n\r\n
```

Per aggiungere un altro campo di intestazione HTTP prima che Load Balancer aggiunga questa stringa alla fine della richiesta, includere la propria stringa \r\n nella richiesta. Di seguito è riportato un esempio di cosa è possibile digitare per aggiungere un campo di intestazione host HTTP alla richiesta:

```
GET /pub/WWW/TheProject.html HTTP/1.0 \r\nHost: www.w3.org
```

Nota: Dopo aver avviato un advisor HTTP o HTTPS per un numero di porta HTTP specificato, il valore della richiesta/risposta dell'advisor è abilitato per i server presenti su quella porta HTTP.

Per ulteriori informazioni, consultare "dscontrol server — configura i server" a pagina 381.

Utilizzo dell'advisor autonomo in una configurazione WAN a due livelli

L'advisor autonomo è disponibile sul componente Dispatcher.

Per Load Balancer in una configurazione WAN (wide area network) a due livelli, Dispatcher fornisce un advisor *autonomo* che collega le informazioni sullo stato del carico sui server di backend.

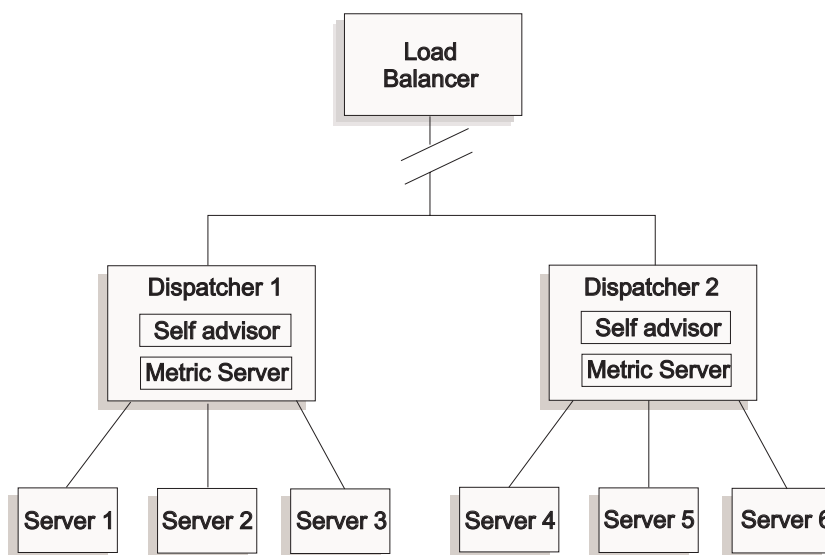


Figura 34. Esempio di una configurazione WAN a due livelli utilizzando l'advisor autonomo

In questo esempio, l'advisor autonomo risiede, insieme a Metric Server, sulle due macchine Dispatcher sottoposte a bilanciamento del carico da Load Balancer di livello superiore. L'advisor autonomo calcola specificatamente le connessioni al secondo sui server di backend del Dispatcher a livello dell'executor.

L'advisor autonomo scrive i risultati sul file `dsloadstat`. Load Balancer, inoltre, fornisce la metrica esterna denominata `dsload`. L'agente Metric Server su ciascuna macchina Dispatcher esegue la relativa configurazione che richiama la metrica esterna `dsload`. Lo script `dsload` consente l'estrazione di una stringa dal file `dsloadstat` e la restituisce all'agente Metric Server. Di conseguenza, ciascun agente Metric Server (da ciascun Dispatcher) restituisce il valore sullo stato del carico di Load Balancer di livello superiore per determinare il Dispatcher da utilizzare per inoltrare le richieste client.

L'eseguibile `dsload` risiede nella directory `...ibm/edge/lb/ms/script` di Load Balancer.

Per ulteriori informazioni sull'uso di Dispatcher nelle configurazioni WAN, vedere "Configurazione del supporto di Dispatcher per una rete geografica" a pagina 221. Per ulteriori informazioni su Metric Server, vedere "Metric Server" a pagina 191.

Creazione di advisor personalizzati

L'advisor personalizzato (personalizzabile) è una piccola parte di codice Java che l'utente deve fornire come file di classe, richiamato dal codice di base. Il codice di base fornisce tutti i servizi amministrativi, come l'avvio e l'arresto di un'istanza dell'advisor personalizzato, l'indicazione di stato e report e la registrazione di informazioni cronologiche in un file di log. Inoltre, notifica i risultati al componente gestore. Periodicamente, il codice di base esegue un ciclo di advisor, durante il quale valuta singolarmente lo stato di tutti i server della configurazione. Per prima cosa, apre una connessione a una macchina server. Se il socket viene aperto, il codice di base richiama il metodo (funzione) `getLoad` nell'advisor personalizzato. L'advisor personalizzato quindi esegue le operazioni necessarie per valutare lo stato del server. In genere, invia al server un messaggio definito dall'utente e attende quindi una risposta. (L'accesso al socket aperto viene fornito all'advisor personalizzato.) Il codice di base, quindi, chiude il socket con il server e invia le informazioni sul carico al gestore.

Il codice di base e l'advisor personalizzato possono funzionare in modalità normale o in modalità di sostituzione. La scelta della modalità di funzionamento viene specificata nel file dell'advisor personalizzato come un parametro nel metodo del costruttore.

In modalità normale, l'advisor personalizzato scambia i dati con il server, il codice dell'advisor di base programma lo scambio e calcola il valore del carico. Il codice di base invia questo valore del carico al gestore. L'advisor personalizzato deve solo restituire uno zero (esito positivo) o meno uno (-1) (errore). Per specificare la modalità normale, l'indicatore di sostituzione nel costruttore è impostato su `false`.

In modalità di sostituzione, il codice di base non esegue nessuna misurazione temporizzata. Il codice dell'advisor personalizzato esegue qualsiasi operazione desiderata per i relativi requisiti univoci e restituisce un numero di carico effettivo. Il codice di base accetta il numero e lo notifica al gestore. Per ottenere risultati migliori, normalizzare i numeri del carico tra 10 e 1000; 10 indica un server veloce e 1000 indica un server lento. Per specificare la modalità di sostituzione, l'indicatore di sostituzione nel costruttore è impostato su `true`.

Questa funzione consente di scrivere i propri advisor in modo da fornire le informazioni precise sui server che sono necessarie. Un advisor personalizzato di esempio, **ADV_sample.java**, viene fornito con il prodotto Load Balancer. Dopo aver installato Load Balancer, è possibile trovare il codice di esempio nella directory di installazione

...<directory install>/servers/samples/CustomAdvisors.

La *directory install* predefinita è:

- Per sistemi AIX, HP-UX, Linux e Solaris: /opt/ibm/edge/lb
- Per sistemi Windows: C:\Program Files\IBM\edge\lb

Nota: Se si aggiunge un advisor personalizzato a Dispatcher o a qualsiasi altro componente Load Balancer applicabile, è necessario arrestare e riavviare **dsserver** (oppure il servizio per Windows) per consentire al processo Java di leggere i file di classe del nuovo advisor personalizzato. I file di classe dell'advisor personalizzato vengono caricati solo all'avvio. Non è necessario arrestare l'executor. Questo, infatti, continua ad essere eseguito anche quando dsserver, o il servizio, è stato arrestato.

Se l'advisor personalizzato fa riferimento a ulteriori classi Java, il percorso di classe nel file di script di avvio di Load Balancer (dsserver, cbrserver, sssserver) deve essere aggiornato per includere la posizione.

Advisor WAS

I file advisor personalizzati di esempio specifici per l'advisor WAS (WebSphere Application Server) sono forniti nella directory di installazione di Load Balancer.

- ADV_was.java è il file da compilare e da eseguire sulla macchina Load Balancer
- LBAdvisor.java.servlet (da rinominare LBAdvisor.java) è il file da compilare ed eseguire sulla macchina WebSphere Application Server.

I file di esempio dell'advisor WebSphere Application Server risiedono nella stessa directory degli esempi del file ADV_sample.java.

Convenzione di denominazione

Il nome file dell'advisor personalizzato deve avere il formato "ADV_myadvisor.java." Il prefisso "ADV_" all'inizio deve essere scritto in maiuscolo. I restanti caratteri devono essere tutti in minuscolo.

In base alle convenzioni Java, il nome della classe definita nel file deve corrispondere al nome del file. Se si copia il codice di esempio, accertarsi di modificare tutte le istanze di "ADV_sample" all'interno del file in base al nuovo nome di classe.

Compilazione

Gli advisor personalizzati vengono scritti in linguaggio Java. Utilizzare il compilatore Java installato con Load Balancer. Durante la compilazione si fa riferimento a questi file:

- il file advisor personalizzato
- i file di classe di base, ibmlb.jar, presenti nella directory di installazione
...ibm/edge/lb/servers/lib.

Durante la compilazione, il percorso classe deve indicare il file dell'advisor personalizzato e il file delle classi di base.

Per i sistemi Windows, un semplice comando di compilazione è:

```
dir_install/java/bin/javac -classpath  
dir_install\lb\servers\lib\ibmlb.jar ADV_fred.java
```

dove:

- Il file dell'advisor è denominato ADV_fred.java
- Il file dell'advisor è memorizzato nella directory corrente

L'output della compilazione è un file di classe, ad esempio

ADV_fred.class

Prima di avviare l'advisor, copiare il file di classe sulla directory di installazione
...ibm/edge/lb/servers/lib/CustomAdvisors.

Nota: gli advisor personalizzati possono essere compilati su un sistema operativo ed eseguiti su un altro sistema. Ad esempio, è possibile compilare l'advisor su un sistema Windows, copiare il file di classe (in formato binario) su una macchina AIX ed eseguirvi quindi l'advisor personalizzato.

Per sistemi AIX, HP-UX, Linux e Solaris, la sintassi è simile.

Esecuzione

Per eseguire l'advisor personalizzato, è necessario anzitutto copiare il file di classe sulla directory di installazione appropriata:

```
...ibm/edge/lb/servers/lib/CustomAdvisors/ADV_fred.class
```

Configurare il componente, avviare la funzione gestore ed immettere il comando per avviare l'advisor personalizzato:

```
dscontrol advisor start fred 123
```

dove:

- fred è il nome dell'advisor, come in ADV_fred.java
- 123 è la porta su cui l'advisor funzionerà

Se l'advisor personalizzato fa riferimento a ulteriori classi Java, il percorso di classe nel file di script di avvio di Load Balancer (dsserver, cbrserver, ssserver) deve essere aggiornato per includere la posizione.

Routine richieste

Come tutti gli advisor, un advisor personalizzato estende la funzione dell'advisor di base, definito ADV_Base. L'advisor di base esegue effettivamente la maggior parte delle funzioni dell'advisor, come ad esempio la notifica dei carichi al gestore affinché li utilizzi nell'algoritmo di valutazione. Inoltre, tale advisor effettua le operazioni di connessione e chiusura del socket e fornisce i metodi di invio e di ricezione per l'uso da parte dell'advisor. L'advisor in sé viene utilizzato unicamente per l'invio e la ricezione dei dati sulla porta specifica del server esaminato. I metodi TCP interni all'advisor di base sono programmati per calcolare il carico. Se desiderato, un'indicatore all'interno del costruttore dell'advisor di base sostituisce il carico esistente con il nuovo carico restituito dall'advisor.

Nota: in base al valore impostato nel costruttore, l'advisor di base fornisce il carico all'algoritmo di valutazione a intervalli specifici. Se l'advisor effettivo non ha completato l'elaborazione e non può restituire un carico valido, l'advisor di base utilizza il carico inviato precedentemente.

I metodi di classe di base sono:

- Una routine **constructor**. Il costruttore richiama il costruttore della classe di base (vedere il file dell'advisor di esempio)
- Un metodo **ADV_AdvisorInitialize**. Questo metodo fornisce una possibile soluzione in caso siano necessarie ulteriori operazioni dopo che la classe di base ha completato la propria inizializzazione.
- Una routine **getload**. La classe dell'advisor di base esegue il socket aperto; quindi per completare il ciclo dell'advisor, getload deve generare soltanto le richieste di invio e di ricezione appropriate.

Ordine di ricerca

Load Balancer esamina innanzitutto l'elenco degli advisor nativi forniti, quindi nel caso in cui non trovi un determinato advisor, esamina l'elenco degli advisor personalizzati del cliente.

Denominazione e percorso

- La classe dell'advisor personalizzato deve trovarsi all'interno della directory secondaria **...ibm/edge/lb/servers/lib/CustomAdvisors/** nella directory base di Load Balancer. I valori predefiniti di questa directory variano a seconda del sistema operativo:
 - Sistemi AIX, HP-UX, Linux e Solaris
/opt/ibm/edge/lb/servers/lib/CustomAdvisors/
 - Sistemi Windows
C:\Program Files\IBM\edge\lb\servers\lib\CustomAdvisors
- È consentito utilizzare solo caratteri alfabetici in minuscolo. Ciò semplifica l'immissione dei comandi sulla riga comandi. Il nome del file dell'advisor deve essere preceduto dal prefisso **ADV_**.

Advisor di esempio

Il listato del programma di un advisor di esempio è riportato in "Advisor di esempio" a pagina 473. Dopo l'installazione, è possibile trovare questo advisor di esempio nella directory **...ibm/edge/lb/servers/samples/CustomAdvisors**.

Metric Server

Questa funzione è disponibile per tutti i componenti Load Balancer.

Metric Server fornisce informazioni sul carico dei server a Load Balancer sotto forma di metriche specifiche del sistema notificando lo stato dei server. Il gestore di Load Balancer interroga l'agente Metric Server che risiede su ciascun server, assegnando pesi al processo di bilanciamento del carico utilizzando le metriche raccolte dagli agenti. I risultati vengono inseriti nel report del gestore.

Nota: quando vengono raccolte due o più metriche e normalizzate per ciascun server in un unico valore di carico del sistema, potrebbero verificarsi errori di arrotondamento.

Per informazioni sul Metric Server operativo (avvio e arresto) e sull'utilizzo dei log di Metric Server, fare riferimento a "Uso del componente Metric Server" a pagina 270.

Per un esempio di configurazione, vedere Figura 5 a pagina 14.

Restrizione WLM

Analogamente all'advisor WLM, Metric Server effettua la notifica ai sistemi server come insieme piuttosto che ai singoli daemon server specifici dei protocolli. Sia WLM che Metric Server inseriscono i relativi risultati nella colonna del sistema del report del gestore. Di conseguenza, l'esecuzione contemporanea dell'advisor WLM e di Metric Server non è supportata.

Prerequisiti

L'agente Metric Server deve essere installato e in esecuzione su tutti i server che sono sottoposti al bilanciamento del carico.

Modalità d'uso di Metric Server

Di seguito vengono riportate le operazioni necessarie per configurare Metric Server per Dispatcher. Operazioni simili possono essere utilizzate per configurare Metric Server per altri componenti di Load Balancer.

- Gestore Load Balancer (lato Load Balancer)
 1. Avviare **dsserver**.
 2. Immettere il comando: **dscontrol manager start** *manager.log port*
port è la porta RMI scelta per eseguire tutti gli agenti Metric Server. La porta RMI predefinita impostata nel file `metricserver.cmd` è 10004.
 3. Immettere il comando: **dscontrol metric add** *cluster:systemMetric*
systemMetric è il nome dello script (che risiede sul server di backend) che deve essere eseguito su ciascun server nella configurazione del cluster specificato (o nome sito). Vengono forniti due script per il cliente - **cpuload** e **memload**. Altrimenti, è possibile creare script delle metriche del sistema personalizzati. Lo script contiene un comando che deve restituire un valore numerico compreso tra 0 e 100 oppure un valore di -1 se il server non è attivo. Questo valore numerico deve rappresentare una misura di carico non un valore della disponibilità.

Nota: in Site Selector, `cpuload` e `memload` vengono eseguiti automaticamente.

Limitazione: sulle piattaforme Windows, se il nome dello script System Metric ha un'estensione diversa da ".exe", è necessario specificare il nome completo del file (ad esempio, "mysystemscript.bat"). Questo è dovuto a una limitazione Java.

4. Aggiungere alla configurazione solo server con un agente Metric Server in esecuzione sulla porta specificata nel file `metricserver.cmd`. La porta deve corrispondere al valore porta specificato nel comando **manager start**.

Nota: garantire la sicurezza —

- Sulla macchina Load Balancer, creare un file di chiavi (utilizzando il comando **lbkeys create**). Per ulteriori informazioni su `lbkeys`, vedere "RMI (Remote Method Invocation)" a pagina 254.
 - Sulla macchina server di backend, copiare il file di chiavi risultante, per il componente che si sta utilizzando nella directory **...ibm/edge/lb/admin/keys**. Verificare che le autorizzazioni del file di chiavi consentano la lettura del file da parte della root.
- Agente Metric Server (lato macchina server)
 1. Installare il pacchetto Metric Server dall'installazione di Load Balancer.

2. Controllare lo script **metricserver** nella directory **/usr/bin** per verificare che venga utilizzata la porta RMI desiderata. (Per Windows 2003, la directory è C:\WINDOWS\system32.) La porta RMI predefinita è 10004.

Nota: il valore della porta RMI specificata deve corrispondere al valore della porta RMI specificata per Metric Server sulla macchina Load Balancer.

3. I seguenti due script sono già forniti per il cliente: **cpuload** (restituisce la percentuale di CPU in uso con un valore compreso tra 0 e 100) e **memload** (restituisce la percentuale di memoria in uso con un valore compreso tra 0 e 100). Questi script risiedono nella directory **...ibm/edge/lb/ms/script**.

Facoltativamente, i clienti possono scrivere i file script delle metriche personalizzati che definiscono il comando che Metric Server invierà alle macchine server. Accertarsi che gli script personalizzati siano eseguibili e posizionati nella directory **...ibm/edge/lb/ms/script**. Gli script personalizzati **devono** restituire un valore di carico numerico compreso tra 0 e 100.

Nota: uno script delle metriche personalizzato deve essere un programma o uno script valido con estensione ".bat" o ".cmd". In particolare, su Sistemi Linux e UNIX, gli script devono iniziare con la dichiarazione shell; altrimenti potrebbero non essere eseguiti correttamente.

4. Avviare l'agente immettendo il comando **metricserver**.
5. Per arrestare l'agente Metric Server, immettere il comando **metricserver stop**.

Per eseguire Metric Server su un indirizzo diverso dall'host locale, modificare il file **metricserver** sulla macchina server con bilanciamento del carico. Nel file **metricserver**, dopo "java", inserire quanto segue:

```
-Djava.rmi.server.hostname=OTHER_ADDRESS
```

Inoltre, prima delle istruzioni "if" nel file **metricserver**, aggiungere la seguente riga:
hostname OTHER_ADDRESS .

Per la piattaforma Windows: è necessario creare l'alias di **OTHER_ADDRESS** sullo stack Microsoft della macchina di Metric Server. Ad esempio:

```
call netsh interface ip add address  
"Local Area Connection"  
addr=9.37.51.28 mask=255.255.240.0
```

Quando si raccolgono le metriche tra i diversi domini, è necessario impostare esplicitamente **java.rmi.server.hostname** nello script server (**dsserver**, **cbrserver** e così via) sul nome dominio completo FQDN (fully domain name) della macchina che sta richiedendo le metriche. Questa operazione è necessaria poiché, a seconda della configurazione e del sistema operativo, **InetAddress.getLocalHost.getHostName()** potrebbe non restituire l'FQDN.

Advisor Workload Manager

WLM è il codice che viene eseguito sui mainframe MVS. È possibile eseguire delle query sul carico sulla macchina MVS.

Quando Workload Management MVS è stato configurato sul sistema OS/390, Dispatcher può accettare le informazioni sulla capacità provenienti da WLM e utilizzarle nel processo di bilanciamento del carico. Utilizzando l'advisor WLM, Dispatcher apre periodicamente le connessioni tramite la porta WLM su ciascun server nella tabella host del Dispatcher e accetta i numeri interi sulla capacità che

vengono restituiti. Poiché tali numeri interi rappresentano la capacità ancora disponibile e i consultant si aspettano al contrario i valori dei carichi di ciascuna macchina, i numeri interi della capacità vengono invertiti dall'advisor e normalizzati in valori del carico (ad esempio, un numero intero grande che rappresenta la capacità e un numero piccolo che rappresenta il carico indicano entrambi un server in buono stato di funzionamento). I carichi risultanti vengono inseriti nella colonna del sistema del report del gestore.

Numerose importanti differenze distinguono l'advisor WLM dagli altri advisor del Dispatcher:

1. Gli altri advisor aprono delle connessioni ai server sulla stessa porta utilizzata per l'abituale traffico del client. L'advisor WLM apre le connessioni ai server su una porta diversa da quella utilizzata per il traffico abituale. L'agente WLM di ciascuna macchina server deve essere configurato per restare in ascolto sulla stessa porta su cui è stato avviato l'advisor WLM di Dispatcher. La porta WLM predefinita è 10007.
2. Gli altri advisor valutano esclusivamente quei server definiti nella configurazione cluster:port:server di Dispatcher per cui la porta del server corrisponde con quella dell'advisor. L'advisor WLM esegue l'esame di *tutti* i server nella configurazione Dispatcher (indipendentemente da cluster:port). Quindi, non definire i server diversi da WLM quando si utilizza un advisor WLM.
3. Gli altri advisor inseriscono le informazioni sul carico nel report del gestore nella colonna "Port". L'advisor WLM inserisce le informazioni sul carico nel report del gestore nella colonna del sistema.
4. È possibile utilizzare entrambi gli advisor specifici del protocollo con l'advisor WLM. Gli advisor specifici del protocollo eseguiranno la scansione ciclica dei server sulle porte su cui si svolge il traffico abituale, l'advisor WLM eseguirà la scansione ciclica del carico del sistema utilizzando la porta WLM.

Restrizione Metric Server

Analogamente all'agente Metric Server, l'agente WLM effettua la notifica ai sistemi server come insieme piuttosto che ai singoli daemon server specifici dei protocolli. Metric Server e WLM inseriscono i relativi risultati nella colonna del sistema del report del gestore. Di conseguenza, l'esecuzione contemporanea dell'advisor WLM e di Metric Server non è supportata.

Capitolo 22. Funzioni avanzate di Dispatcher, CBR e Site Selector

Questo capitolo descrive come configurare i parametri per il bilanciamento del carico e come impostare le funzioni avanzate di Load Balancer.

Nota: se durante la lettura di questo capitolo, *non* si sta utilizzando il componente Dispatcher, sostituire "dscontrol" con quanto segue:

- Per CBR, utilizzare **cbrcontrol**
- Per Site Selector, utilizzare **sscontrol** (vedere Capitolo 28, "Riferimenti sui comandi per Site Selector", a pagina 391)

IMPORTANTE: se si sta utilizzando l'installazione di Load Balancer per IPv4 e IPv6, consultare Capitolo 8, "Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6", a pagina 79 per evidenziare le limitazioni e le differenze di configurazione prima di esaminare i contenuti di questo capitolo.

Tabella 13. Attività di configurazione avanzate di Load Balancer

Attività	Descrizione	Informazioni correlate
Posizionare Load Balancer su una macchina che esegue il bilanciamento del carico	Impostare una macchina Load Balancer posizionata.	"Utilizzo dei server posizionati" a pagina 196
Configurare la disponibilità elevata semplice e reciproca	Impostare una seconda macchina Dispatcher che funzioni da backup.	"Disponibilità elevata" a pagina 198
Configurare il bilanciamento del carico in base alle regole	Definire le condizioni in base alle quali utilizzare un sottoinsieme di server.	"Configurazione del bilanciamento del carico in base alle regole" a pagina 205
Utilizzare la funzione "ignora affinità di porta" per permettere a un server di ignorare la funzione di aderenza alla porta	Permette a un server di ignorare l'impostazione del tempo di aderenza sulla sua porta.	"ignora affinità di porta" a pagina 213
Utilizzare la funzione di aderenza (affinità) per configurare la porta di un cluster e renderla aderente	Consente di indirizzare le richieste dei client a uno stesso server.	"Funzionamento della funzione di affinità di Load Balancer" a pagina 214
Utilizzare l'affinità multiporta per espandere la funzione di aderenza (affinità) tra le porte	Fa in modo che le richieste dei client, ricevute da diverse porte, vengano indirizzate allo stesso server.	"Affinità multiporta" a pagina 215
Utilizzare la funzione maschera indirizzo affinità per indicare un indirizzo di sottorete IP comune	Permette che le richieste dei client, ricevute dalla stessa sottorete, vengano indirizzate sullo stesso server.	"Maschera indirizzo affinità (stickymask)" a pagina 216
Utilizzare l'affinità cookie attiva per bilanciare il carico dei server di CBR	L'opzione di una regola che consente a una sessione di mantenere l'affinità per un server particolare.	"Affinità cookie attivo" a pagina 218
Utilizzare l'affinità cookie passivo per bilanciare il carico dei server per l'instradamento in base al contenuto di Dispatcher e per il componente CBR	L'opzione di una regola che consente a una sessione di mantenere l'affinità per un server particolare in base al valore e al nome cookie.	"Affinità cookie passivo" a pagina 219

Tabella 13. Attività di configurazione avanzate di Load Balancer (Continua)

Attività	Descrizione	Informazioni correlate
Utilizzare l'affinità URI per bilanciare il carico tra i server Caching Proxy con contenuto univoco da memorizzare su ogni singolo server	L'opzione di una regola che consente a una sessione di mantenere l'affinità per un server particolare in base all'URI.	"Affinità URI" a pagina 220
Configurare il supporto di Dispatcher per una rete geografica	Impostare un Dispatcher remoto per bilanciare il carico su una rete geografica (WAN, wide area network). Oppure, bilanciare il carico attraverso una rete geografica (WAN, Wide Area Network), senza un Dispatcher remoto, utilizzando una piattaforma server che supporta GRE.	"Configurazione del supporto di Dispatcher per una rete geografica" a pagina 221
Utilizzare un collegamento esplicito	Impedisce di ignorare Dispatcher nei collegamenti.	"Utilizzo di un collegamento esplicito" a pagina 228
Utilizzare una rete privata	Configurare Dispatcher in modo da bilanciare il carico dei server su una rete privata.	"Utilizzo di una configurazione di rete privata" a pagina 228
Utilizzare cluster jolly per combinare le configurazioni di server comuni	Gli indirizzi che non sono esplicitamente configurati utilizzeranno i cluster jolly per bilanciare il traffico.	"Utilizzo del cluster jolly per combinare le configurazioni di server" a pagina 229
Utilizzare il cluster jolly per bilanciare il carico dei firewall	Tutto il traffico verrà bilanciato sui firewall.	"Utilizzo di cluster jolly per bilanciare il carico dei firewall" a pagina 230
Utilizzare il cluster jolly con Caching Proxy come proxy trasparente	Consente di utilizzare Dispatcher per attivare un proxy trasparente.	"Utilizzo del cluster jolly con Caching Proxy per proxy trasparente" a pagina 230
Utilizzare la porta jolly per indirizzare il traffico non configurato sulle porte	Gestisce il traffico che non è configurato per nessuna porta in particolare.	"Utilizzo della porta jolly per indirizzare il traffico per una porta non configurata" a pagina 231
Utilizzare il rilevamento attacchi di tipo "Denial of Service" per notificare agli amministratori (con un avviso) eventuali attacchi	Dispatcher analizza le richieste in entrata per una grande quantità di connessioni TCP aperte a metà sui server.	"Rilevamento attacco di tipo Denial of service" a pagina 231
Utilizzare i file binari di log per analizzare le statistiche dei server	Permette la memorizzazione e il richiamo delle informazioni relative ai server dai file binari.	"Uso della registrazione binaria per analizzare le statistiche dei server" a pagina 232
Utilizzare una configurazione client posizionato	Consente al Load Balancer di trovarsi sulla stessa macchina del client	"Utilizzo di un client posizionato" a pagina 234

Utilizzo dei server posizionati

Load Balancer può risiedere sulla stessa macchina di un server per il quale sta bilanciando il carico delle richieste. Questa condizione viene definita *posizionamento* di un server. È applicabile esclusivamente ai componenti Dispatcher e Site Selector. Il posizionamento è supportato anche per CBR, ma solo se si utilizzano dei server web Caching Proxy specifici del collegamento.

Nota: un server posizionato si contende le risorse con Load Balancer nei momenti di traffico elevato. Tuttavia, anche quando non ci sono macchine sovraccariche, l'uso di un server posizionato riduce il numero totale delle macchine necessarie per configurare un sito con bilanciamento del carico.

Per il componente Dispatcher

Su sistemi **Linux**: per configurare contemporaneamente il posizionamento e l'alta disponibilità (HA, high availability), mentre il componente Dispatcher è in esecuzione con il metodo di inoltro mac, consultare "Alternative per l'aggiunta dell'alias loopback Linux quando si utilizza il metodo di inoltro mac di Load Balancer" a pagina 76.

Su sistemi Windows: per configurare contemporaneamente il posizionamento e l'alta disponibilità (HA, high availability), mentre il componente Dispatcher è in esecuzione con il metodo di inoltro mac, consultare "Configurazione di posizionamento e elevata disponibilità (sistemi Windows)" a pagina 205.

Sistemi **Solaris**: esiste un limite secondo il quale non è possibile configurare gli advisor WAN se Dispatcher entry-point è posizionato. Vedere "Utilizzo di advisor remoti con il supporto rete geografica di Dispatcher" a pagina 223.

Nelle release precedenti, era necessario specificare che l'indirizzo del server posizionato doveva essere uguale all'indirizzo NFA (nonforwarding address, indirizzo di non inoltro) nella configurazione. Tale restrizione è stata eliminata.

Per configurare un server da posizionare, il comando **dscontrol server** fornisce un'opzione chiamata **collocated** che può essere impostata su *sì* o *no*. Il valore predefinito è *no*. L'indirizzo del server deve essere un indirizzo IP valido di una scheda di interfaccia di rete della macchina. Il parametro **collocated** non dovrebbe essere impostato per i server posizionati mediante metodo di inoltro nat o cbr di Dispatcher.

È possibile configurare un server posizionato in uno dei seguenti modi:

- Se si sta utilizzando NFA come indirizzo del server posizionato: impostare NFA mediante il comando **dscontrol executor set nfa IP_address**. Quindi, aggiungere il server mediante l'indirizzo NFA con il comando **dscontrol server add cluster:port:server**.
- Se si sta utilizzando un indirizzo diverso da NFA: aggiungere il server con l'indirizzo IP desiderato con il parametro **collocated** impostato su *sì* nel seguente modo: **dscontrol server add cluster:port:server collocated yes**.

Per il protocollo nat o per l'inoltro cbr di Dispatcher, è necessario configurare (alias) un indirizzo di adattatore non utilizzato su NFA. Il server dovrebbe essere configurato per essere in ascolto su questo indirizzo. Configurare il server utilizzando la seguente sintassi:

```
dscontrol server add cluster:port:new_alias address  
new_alias router router_ip returnaddress  
return_address
```

Una configurazione errata può causare errori di sistema, una mancata risposta del server, o entrambe le condizioni.

Configurazione del posizionamento del server mediante il metodo di inoltro nat di Dispatcher

Quando si configura un server posizionato mediante il metodo di inoltro nat del Dispatcher, il router specificato nel comando **dscontrol server add** deve essere un indirizzo reale del router e non un indirizzo IP del server.

Il supporto per il posizionamento, durante la configurazione del metodo di inoltramento di Dispatcher, può essere applicato su tutti i sistemi operativi nel caso in cui le seguenti operazioni siano eseguite sulla macchina di Dispatcher:

- Su sistemi **AIX**, il server posizionato viene configurato come qualsiasi altro server. Non sono necessarie modifiche alla configurazione.
- Su sistemi **Linux**, il server posizionato viene configurato come qualsiasi altro server. Non sono necessarie modifiche alla configurazione.
- Su sistemi **Solaris e HP-UX**, viene creato un alias per il cluster mediante il comando `ifconfig`; tuttavia, l'indirizzo mittente deve essere definito mediante il comando `arp publish` e non tramite alias. Per fare ciò, eseguire questo comando:
`arp -s hostname ether_addr pub`

usando l'indirizzo MAC locale per `ether_addr`. In questo modo, l'applicazione locale è in grado di inviare il traffico all'indirizzo mittente nel kernel.

- Su **piattaforme Windows**, il cluster e l'indirizzo mittente devono essere configurati mediante il comando **`dscontrol executor configure`** e non inseriti in Windows Networking. Per l'applicazione locale, è necessario aggiungere un nuovo alias IP all'adattatore locale in Windows Networking. Nelle impostazioni TCP/IP, trovare l'opzione Avanzate che consente di aggiungere altri IP a un adattatore. Il secondo IP viene utilizzato come definizione del server nella configurazione di Dispatcher.

Per il componente CBR

CBR supporta il posizionamento su tutte le piattaforme senza ulteriori configurazioni. Tuttavia, i server Web e il Caching Proxy utilizzati devono essere specifici del collegamento.

Per il componente Site Selector

Site Selector supporta il posizionamento su tutte le piattaforme senza ulteriori configurazioni.

Disponibilità elevata

La funzione Disponibilità elevata (configurabile tramite il comando **`dscontrol highavailability`**) è disponibile per il componente Dispatcher (ma non per i componenti CBR o Site Selector).

Per aumentare la disponibilità di Dispatcher, la funzione di Disponibilità elevata utilizza i seguenti meccanismi:

- Due Dispatcher con connettività agli stessi client e con lo stesso cluster di server e la connettività tra i Dispatcher. Entrambi i Dispatcher devono essere in esecuzione sullo stesso tipo di sistema operativo e piattaforma.
- Un meccanismo "heartbeat" tra i due Dispatcher per rilevare eventuali errori. Almeno una coppia di heartbeat deve avere gli NFA della coppia come indirizzo di origine e destinazione.

Se possibile, è consigliabile che almeno una coppia di heartbeat venga inviata attraverso una sottorete separata rispetto al traffico regolare del cluster. Separando il traffico di heartbeat, è possibile evitare falsi takeover durante carichi di rete pesanti e migliorare i tempi di recupero dopo un failover.

- Un elenco di destinazioni finali, indirizzi che entrambe le macchine Dispatcher devono essere in grado di contattare per poter bilanciare il traffico. Per ulteriori informazioni, vedere "Capacità di rilevamento di errori mediante heartbeat e la destinazione accessibile" a pagina 201.

- La sincronizzazione delle informazioni Dispatcher (ovvero, le tabelle di connessione, di accessibilità e altre informazioni).
- La logica per scegliere il Dispatcher attivo, che controlla un determinato cluster di server e il Dispatcher standby che viene continuamente sincronizzato con quel cluster di server.
- Un meccanismo per eseguire il takeover IP quando la logica o l'operatore decidono di cambiare lo stato da attivo a standby.

Nota: per una descrizione di una configurazione di *disponibilità elevata reciproca*, dove due macchine Dispatcher che condividono due serie di cluster forniscono un backup reciproco, consultare "Disponibilità elevata reciproca" a pagina 58. La disponibilità elevata reciproca è simile alla disponibilità elevata ma si basa soprattutto su un indirizzo cluster anziché su una macchina Dispatcher completa. Entrambe le macchine devono configurare i cluster condivisi allo stesso modo.

Configurazione della disponibilità elevata

La sintassi completa per **dscontrol highavailability** è in "dscontrol highavailability — controlla la disponibilità elevata" a pagina 357.

Per un quadro più completo delle attività riportate di seguito, vedere "Configurazione della macchina Dispatcher" a pagina 64.

1. Creare dei file di script alias sulle due macchine Dispatcher. Vedere "Utilizzo di script" a pagina 202.
2. Avviare il server su entrambe le macchine server Dispatcher.
3. Avviare l'executor su entrambe le macchine.
4. Verificare che l'NFA (nonforwarding address) di ciascuna macchina Dispatcher sia configurato e che sia un indirizzo IP valido per la sottorete di macchine Dispatcher.
5. Aggiungere le informazioni heartbeat su entrambe le macchine:

```
dscontrol highavailability heartbeat
add sourceaddress destinationaddress
```

Nota: *sourceaddress* e *destinationaddress* sono gli indirizzi IP (nomi DNS o indirizzi IP) delle macchine Dispatcher. I valori verranno riversati in ciascuna macchina. Ad esempio:

```
Primary - highavailability heartbeat add 9.67.111.3 9.67.186.8
Backup - highavailability heartbeat add 9.67.186.8 9.67.111.3
```

Almeno una coppia di heartbeat deve avere gli NFA della coppia come indirizzo di origine e destinazione.

Se possibile, è consigliabile che almeno una coppia di heartbeat venga inviata attraverso una sottorete separata rispetto al traffico regolare del cluster. Separando il traffico di heartbeat, è possibile evitare falsi takeover durante carichi di rete pesanti e migliorare i tempi di recupero dopo un failover.

Impostare il numero di secondi che l'executor deve utilizzare come timeout per gli heartbeat di disponibilità elevata. Ad esempio:

```
dscontrol executor set hatimeout 3
```

Il valore predefinito è 2 secondi.

6. Su entrambe le macchine, configurare un elenco di indirizzi IP che il Dispatcher deve poter raggiungere per offrire un servizio completo, utilizzando il comando **reach add**. Ad esempio:
`dscontrol highavailability reach add 9.67.125.18`

Le destinazioni finali sono consigliate ma non obbligatorie. Per ulteriori informazioni, consultare “Capacità di rilevamento di errori mediante heartbeat e la destinazione accessibile” a pagina 201.

7. Aggiungere le informazioni di backup su ciascuna macchina:
 - Per la macchina **principale**:
`dscontrol highavailability backup add primary [auto | manual] port`
 - Per la macchina di **backup**:
`dscontrol highavailability backup add backup [auto | manual] port`
 - Per la disponibilità elevata reciproca, ciascuna macchina Dispatcher ha **entrambi** i ruoli, principale e di backup:
`dscontrol highavailability backup add both [auto | manual] port`

Nota: selezionare una porta non utilizzata sulle macchine che abbia il valore di *port*. Il numero di porta immesso verrà utilizzato come chiave per garantire che l’host corretto riceva il pacchetto.

8. Controllare lo stato di disponibilità elevata di ciascuna macchina:
`dscontrol highavailability status`

Ciascuna macchina deve avere il ruolo corretto (backup, principale o entrambi), gli stati e gli stati secondari. La macchina principale deve essere attiva e sincronizzata; quella di backup dovrebbe essere in modalità standby e sincronizzata in breve tempo. Le strategie devono essere le stesse.

9. Impostare le informazioni del cluster, della porta e del server su entrambe le macchine.

Nota: per la configurazione di disponibilità elevata reciproca (Figura 14 a pagina 58), ad esempio, configurare il gruppo di cluster condivisi tra i due Dispatcher nel seguente modo:

- Per Dispatcher 1, emettere:
`dscontrol cluster set clusterA primaryhost NFADispatcher1`
`dscontrol cluster set clusterB primaryhost NFADispatcher2`
- Per Dispatcher 2, emettere:
`dscontrol cluster set clusterB primaryhost NFADispatcher2`
`dscontrol cluster set clusterA primaryhost NFADispatcher1`

10. Avviare il gestore e gli advisor su entrambe le macchine.

Note:

1. Per configurare solo una macchina Dispatcher per instradare i pacchetti senza un backup, non emettere all’avvio nessuno dei comandi di disponibilità elevata.
2. Per convertire due macchine Dispatcher configurate per la disponibilità elevata in un’unica macchina, arrestare l’executor su una delle due macchine, quindi eliminare le funzioni di disponibilità elevata (heartbeat, accessibilità e backup) sull’altra.
3. In entrambi i casi, è necessario creare un alias per la scheda interfaccia di rete con indirizzi cluster, come richiesto.

4. Quando due macchine Dispatcher sono in esecuzione in una configurazione di disponibilità elevata e sono sincronizzate, si consiglia di inserire tutti i comandi dscontrol (per aggiornare la configurazione) prima sulla macchina in standby, poi su quella attiva.
5. Se due macchine Dispatcher sono in esecuzione in una configurazione di disponibilità elevata, potrebbero verificarsi dei risultati imprevisti nel caso in cui si imposta uno dei parametri dell'executor, del cluster, della porta o del server (ad esempio, port stickytime) su valori diversi per le due macchine.
6. Per la disponibilità elevata reciproca, considerare il caso in cui uno dei Dispatcher deve instradare attivamente i pacchetti per il cluster principale e controllare l'instradamento dei pacchetti per il cluster di backup. Verificare che questo non superi la velocità di trasmissione di questa macchina.
7. Su sistemi Linux, quando si configura contemporaneamente la disponibilità elevata e il posizionamento utilizzando il metodo di inoltro della porta MAC del componente Dispatcher, consultare "Alternative per l'aggiunta dell'alias loopback Linux quando si utilizza il metodo di inoltro mac di Load Balancer" a pagina 76.
8. Su sistemi Windows, quando si configura contemporaneamente la disponibilità elevata e il posizionamento, fare riferimento a "Configurazione di posizionamento e elevata disponibilità (sistemi Windows)" a pagina 205.
9. Per suggerimenti su come risolvere i problemi legati alla configurazione HA (high availability) come:
 - Connessioni interrotte in seguito al takeover
 - Macchine partner che non vengono sincronizzate
 - Richieste dirette erroneamente alla macchina del partner di backup
 Vedere "Problema: suggerimenti sulla configurazione dell'HA (high availability)" a pagina 310.

Capacità di rilevamento di errori mediante heartbeat e la destinazione accessibile

Oltre ai criteri fondamentali del rilevamento di errori (la perdita di connettività tra Dispatcher attivi e in standby rilevata tramite i messaggi heartbeat), esiste un altro meccanismo di rilevamento degli errori denominato *criteri di accessibilità*. Quando si configura il Dispatcher, è possibile fornire un elenco degli host che ciascun Dispatcher deve raggiungere per poter funzionare correttamente. I due partner della configurazione a disponibilità elevata sono continuamente in contatto tramite gli heartbeat e aggiornano reciprocamente il numero di destinazioni finali che sono comunicate grado di sottoporre a ping. Se la macchina in standby sottopone a ping un numero di destinazioni finali superiore a quelli attivi, si verifica un failover.

Gli heartbeat vengono inviati dal Dispatcher attivo ed è previsto che vengano ricevuti dal Dispatcher in standby ogni mezzo secondo. Se il Dispatcher in standby non riceve alcun heartbeat entro 2 secondi, inizia un failover. Per consentire il takeover da un Dispatcher in standby, tutti gli heartbeat devono essere interrotti. In altre parole, se sono configurate due coppie di heartbeat, entrambi gli heartbeat devono essere interrotti. Per stabilizzare un ambiente a disponibilità elevata e per evitare il failover, è consigliabile aggiungere più di una coppia di heartbeat.

Per le destinazioni finali, scegliere almeno un host per ogni sottorete utilizzata dalla macchina Dispatcher. Gli host possono essere router, server IP e altri tipi di host. L'accessibilità degli host si ottiene tramite l'advisor reach, che esegue il ping sull'host. Il failover si verifica se si interrompe la trasmissione degli heartbeat

oppure se i criteri di accessibilità vengono soddisfatti in misura maggiore dal Dispatcher in standby rispetto al Dispatcher principale. Per prendere una decisione in base alle informazioni disponibili, il Dispatcher attivo invia regolarmente al Dispatcher in standby informazioni sulle sue capacità di accessibilità. Il Dispatcher in standby, quindi, confronta tali capacità con le proprie e decide se deve avvenire la commutazione.

Nota: quando si configura la destinazione accessibile, è necessario avviare anche l'*advisor reach*. L'*advisor reach* si avvia automaticamente all'avvio della funzione gestore. Per ulteriori informazioni sull'*advisor reach*, vedere pagina 185.

Strategia di ripristino

Sono configurate due macchine Dispatcher: la macchina principale e una seconda macchina, chiamata di *backup*. All'avvio, la macchina principale invia tutti i dati di connessione alla macchina di backup fino a quando quella macchina non è sincronizzata. La macchina principale diventa *attiva*, ovvero, inizia il bilanciamento del carico. La macchina di backup, nel frattempo, controlla lo stato della macchina principale e si trova in stato di *standby*.

Se la macchina di backup rileva qualche errore nella macchina principale, esegue un *takeover* delle funzioni di bilanciamento del carico della macchina principale e diventa la macchina attiva. Dopo che la macchina principale è diventata di nuovo operativa, le macchine rispondono in base al modo in cui la strategia di ripristino è stata configurata dall'utente. Esistono due tipi di strategie:

Automatica

La macchina principale riprende a instradare i pacchetti nel momento in cui diventa di nuovo operativa.

Manuale

La macchina di backup continua a instradare i pacchetti anche dopo che la macchina principale è diventata operativa. È necessario un intervento manuale per riportare la macchina principale allo stato attivo e ripristinare la macchina di backup sullo stato di *standby*.

Il parametro della strategia deve essere impostato allo stesso modo su entrambe le macchine.

La strategia di ripristino manuale consente di forzare l'instradamento dei pacchetti su una macchina particolare usando il comando *takeover*. Il ripristino manuale è utile per eseguire la manutenzione sull'altra macchina. La strategia di ripristino automatico è utile in una configurazione senza operatore.

Per una configurazione di disponibilità elevata reciproca, non esiste errore di cluster. Se si verifica un problema con una macchina, che riguarda anche un solo cluster, l'altra macchina prenderà il controllo di entrambi i cluster.

Nota: durante le situazioni di *takeover*, alcuni aggiornamenti delle connessioni potrebbero andare persi. Ciò potrebbe determinare l'interruzione di connessioni di lunga durata esistenti (come ad esempio, *telnet*) in caso di accesso alla fine del *takeover*.

Utilizzo di script

Affinché il Dispatcher indirizzi i pacchetti, è necessario creare un alias per ciascun indirizzo cluster sull'unità di interfaccia di rete.

- In una configurazione di Dispatcher autonomo, è necessario creare un alias per ogni indirizzo cluster su una scheda di interfaccia di rete (ad esempio, en0, tr0).
- In una configurazione di disponibilità elevata:
 - Sulla macchina attiva, è necessario creare un alias per ogni indirizzo cluster su una scheda di interfaccia di rete (ad esempio, en0, tr0).
 - Su una macchina standby, è necessario creare un alias per ogni indirizzo cluster su un'unità loopback (ad esempio, lo0) se si utilizza il metodo di inoltro nat con i server posizionati.
- In ogni macchina in cui l'executor è stato arrestato, tutti gli alias devono essere rimossi per evitare conflitti con un'altra macchina che è stata avviata.

Per informazioni sull'alias della scheda di rete, fare riferimento a "Fase 5. Creazione dell'alias della scheda di interfaccia di rete (NIC)" a pagina 67.

Poiché le macchine Dispatcher cambiano di stato quando viene rilevato un errore, i comandi indicati in precedenza devono essere emessi automaticamente. Per far ciò, Dispatcher eseguirà gli script creati dall'utente. Gli script di esempio si trovano nella directory `...ibm/edge/lb/servers/samples` e *devono* essere spostati sulla directory `...ibm/edge/lb/servers/bin` per poter essere eseguiti. Gli script vengono eseguiti automaticamente solo se dsserver è in esecuzione.

Note:

1. Per una configurazione di disponibilità elevata reciproca, ogni script "go" verrà richiamato dal Dispatcher con un parametro che identifica l'indirizzo del Dispatcher principale. Lo script deve interrogare questo parametro ed eseguire i comandi **executor configure** per quegli indirizzi cluster associati al Dispatcher principale.
2. per poter configurare la disponibilità elevata per il metodo di inoltro nat del Dispatcher, è necessario aggiungere gli indirizzi di ritorno ai file di script.

È possibile utilizzare i seguenti script di esempio:

goActive

Lo script goActive viene eseguito quando un Dispatcher è in stato attivo e inizia l'instradamento dei pacchetti.

- Se Dispatcher è in esecuzione con una configurazione di disponibilità elevata, è necessario creare questo script. Questo script elimina gli alias loopback e aggiunge gli alias di unità.
- Se Dispatcher è in esecuzione con una configurazione autonoma, questo script non è necessario.

goStandby

Lo script goStandby viene eseguito quando un Dispatcher va in stato di standby durante il controllo della condizione della macchina attiva, ma non durante l'instradamento di pacchetti.

- Se Dispatcher è in esecuzione con una configurazione di disponibilità elevata, è necessario creare questo script. Questo script elimina gli alias delle unità e aggiunge gli alias loopback.
- Se Dispatcher è in esecuzione con una configurazione autonoma, questo script non è necessario.

goInOp

Lo script goInOp viene eseguito quando un executor di Dispatcher viene arrestato.

- Se, normalmente, Dispatcher è in esecuzione con una configurazione di disponibilità elevata, è necessario creare questo script. Questo script elimina tutte gli alias delle unità e di loopback.
- Se, normalmente, Dispatcher è in esecuzione con una configurazione autonoma, questo script è facoltativo. È possibile crearlo per eliminare automaticamente gli alias delle unità oppure eliminarli manualmente.

goIdle Lo script goIdle viene eseguito quando un Dispatcher è in stato inattivo e inizia l'instradamento dei pacchetti. Ciò avviene quando le funzioni di disponibilità elevata non sono state aggiunte, come ad esempio in una configurazione autonoma. Avviene anche in una configurazione di disponibilità elevata prima che le funzioni di disponibilità elevata vengano aggiunte o dopo che sono state rimosse.

- Se di solito Dispatcher è in esecuzione con una configurazione di disponibilità elevata, è necessario creare questo script.
- Se, normalmente, Dispatcher è in esecuzione con una configurazione autonoma, questo script è facoltativo. È possibile crearlo per aggiungere automaticamente gli alias delle unità oppure aggiungerli manualmente. Se non si crea lo script per la configurazione autonoma, sarà necessario utilizzare il comando **dscontrol executor configure** o configurare manualmente gli alias ogni volta che viene avviato l'executor.

highavailChange

Lo script highavailChange viene eseguito ogni volta che lo stato di disponibilità elevata viene modificato nel Dispatcher, come quando viene richiamato uno degli script "go". L'unico parametro inviato a questo script è il nome dello script "go" eseguito da Dispatcher. È possibile creare questo script per utilizzare le informazioni sui cambiamenti di stato, ad esempio, per avvisare un amministratore o semplicemente per registrare un evento.

Sui sistemi Windows: durante la configurazione, se Site Selector bilancia il carico di due macchine Dispatcher, operative in un ambiente a disponibilità elevata, sarà necessario aggiungere un alias sullo stack Microsoft per i Metric Server. Questo alias va aggiunto allo script goActive. Ad esempio:

```
call netsh interface ip add address
"Local Area Connection"
addr=9.37.51.28 mask=255.255.240.0
```

Negli script goStandby e goInOp, l'alias dovrà essere rimosso. Ad esempio:

```
call netsh interface ip delete address
"Local Area Connection"
addr=9.37.51.28
```

Se la macchina dispone di più NIC, controllare prima quale interfaccia utilizzare emettendo il seguente comando sul prompt dei comandi: `netsh interface ip show address`. Questo comando restituirà un elenco delle interfacce attualmente configurate numerando ciascuna "Connessione alla rete locale (LAN)" (ad esempio, "Connessione alla rete locale (LAN) 2"); in questo modo, è possibile stabilire quale utilizzare.

Su sistemi Linux per S/390: Dispatcher emette un ARP gratuito per spostare gli indirizzi IP da un Dispatcher all'altro. Questo meccanismo è, quindi, legato al tipo di rete sottostante. Quando si esegue Linux per S/390, Dispatcher può eseguire, in modalità nativa, takeover in disponibilità elevata (compresi gli spostamenti dell'indirizzo IP) solo su quelle interfacce che possono emettere un ARP gratuito e configurare l'indirizzo sull'interfaccia locale. Questo meccanismo non funzionerà

correttamente sulle interfacce point-to-point, come ad esempio IUCV e CTC, e non funzionerà correttamente in alcune configurazioni di qeth/QDIO.

Per quelle interfacce e configurazioni in cui la funzione di takeover IP nativa del Dispatcher non funziona correttamente, il cliente può inserire dei comandi adatti negli script go per spostare manualmente gli indirizzi. In questo modo, quelle topologie di rete possono trarre beneficio dalla disponibilità elevata.

Configurazione di posizionamento e elevata disponibilità (sistemi Windows)

Sui server Windows, è possibile configurare sia l'elevata disponibilità che il posizionamento. Tuttavia, sono richieste delle operazioni aggiuntive per configurare queste funzioni di Load Balancer insieme sui sistemi Windows.

Su sistemi Windows, quando si utilizza il posizionamento con l'elevata disponibilità, sarà necessario un ulteriore indirizzo IP, una specie di indirizzo IP fittizio, che possa essere aggiunto all'adattatore loopback sul sistema Windows. L'adattatore loopback deve essere installato sia sulla macchina primaria che su quella di backup. Per l'installazione del dispositivo loopback su sistemi Windows, effettuare le operazioni riportate in "Configurazione delle macchine server per il bilanciamento del carico" a pagina 70.

Quando le operazioni indicano di aggiungere l'indirizzo IP del cluster al loopback, è necessario aggiungere un indirizzo IP fittizio e non l'indirizzo del cluster. Il motivo è che gli script go* di elevata disponibilità per i sistemi Windows devono eliminare e aggiungere l'indirizzo del cluster al dispositivo loopback, a seconda se la macchina di Load Balancer è attiva o in standby.

I sistemi Windows non consentono la rimozione dell'ultimo indirizzo IP configurato dal dispositivo loopback in quanto questo dispositivo non funziona in modalità DHCP. L'indirizzo fittizio consente a Load Balancer di rimuovere l'indirizzo del cluster in qualsiasi momento. L'indirizzo IP fittizio non verrà utilizzato per alcun tipo di traffico e potrà essere utilizzato sia sulla macchina attiva che sulla macchina standby.

Aggiornare e spostare gli script go* di Load Balancer sia sulla macchina attiva che su quella standby, quindi avviare il Dispatcher. L'indirizzo del cluster verrà aggiunto e rimosso dall'interfaccia di rete e dal dispositivo loopback tutte le volte necessarie.

Configurazione del bilanciamento del carico in base alle regole

È possibile utilizzare il bilanciamento del carico in base alle regole per ottimizzare i tempi e le condizioni in cui i pacchetti devono essere inviati a determinati server. Load Balancer rivede le regole aggiunte dall'utente a partire dalla prima priorità fino all'ultima, fermandosi sulla prima regola che ritiene valida; quindi bilancia il carico dei contenuti tra i vari server associati a quella regola. Bilancia inoltre il carico in base alla destinazione e alla porta, ma tramite le regole aumenta la capacità di distribuire le connessioni.

Nella maggior parte dei casi, quando si configurano le regole è consigliabile configurare una regola predefinita come **sempre true**, per poter rilevare qualsiasi richiesta che viene inclusa tra altre regole di priorità più elevata. Se tutti gli altri server non soddisfano la richiesta del client, la risposta potrebbe essere "Il sito non è attivo, riprovare in seguito".

Si consiglia di utilizzare il bilanciamento del carico in base alle regole con Dispatcher e Site Selector quando, per qualche motivo, si desidera utilizzare un sottoinsieme di server. È *necessario* utilizzare sempre le regole del componente CBR.

La scelta è tra i seguenti tipi di regole:

- Per Dispatcher:
 - Indirizzo IP client
 - Porta client
 - Ora del giorno
 - Tipo di servizio (TOS, Type of service)
 - Connessioni al secondo
 - Numero totale di connessioni attive
 - Larghezza di banda riservata
 - Larghezza di banda condivisa
 - Sempre true
 - Contenuto di una richiesta
- Per CBR:
 - Indirizzo IP client
 - Ora del giorno
 - Connessioni al secondo
 - Numero totale di connessioni attive
 - Sempre true
 - Contenuto di una richiesta
- Per Site Selector:
 - Indirizzo IP client
 - Ora del giorno
 - Metric all
 - Media metrica
 - Sempre true

È consigliabile pianificare la logica che le regole devono seguire prima di iniziare ad aggiungere regole alla configurazione.

Modalità di valutazione delle regole

Tutte le regole hanno un nome, un tipo e una priorità e possono disporre di un intervallo di inizio e di fine, insieme a un gruppo di server. Inoltre, la regola del tipo di contenuto del componente CBR ha un modello di espressione regolare corrispondente associato ad essa. (Per gli esempi e gli scenari relativi alle modalità di utilizzo delle regole di contenuto e della sintassi dei modelli valida per tali regole, consultare Appendice B, “Sintassi della regola di contenuto (modello)”, a pagina 463).

Le regole vengono valutate in ordine di priorità. In altre parole, una regola con priorità 1 (numero più basso) verrà valutata prima di una regola con priorità 2 (numero più alto). Verrà utilizzata la prima regola soddisfatta. Una volta soddisfatta una regola, non verranno valutate altre regole.

Per soddisfare una regola, sono necessarie due condizioni:

1. Il predicato della regola deve essere true. Vale a dire che, il valore che si sta valutando deve essere compreso tra l'intervallo iniziale e finale oppure il contenuto deve corrispondere all'espressione regolare specificata nel modello della regola di contenuto. Per le regole di tipo "true," il predicato viene sempre soddisfatto, a prescindere dagli intervalli di inizio e fine.
2. Se vi sono server associati alla regola, almeno uno di loro deve avere un peso maggiore di 0 a cui inoltrare i pacchetti.

Se una regola non ha server associati, è necessaria solo la condizione uno affinché la regola venga soddisfatta. In questo caso Dispatcher interrompe la richiesta di collegamento, Site Selector restituisce il nome della richiesta del server con un errore e CBR fa in modo che Caching Proxy restituisca una pagina di errore.

Se non viene soddisfatta alcuna regola, Dispatcher seleziona un server dalla serie completa di server disponibili sulla porta, Site Selector seleziona un server dalla serie completa di server disponibili sul nome sito e CBR fa in modo che Caching Proxy restituisca una pagina di errore.

Utilizzo delle regole basate sull'indirizzo IP del client

Questo tipo di regola è disponibile nel componente Dispatcher, CBR o Site Selector.

È possibile utilizzare le regole basate sull'indirizzo IP client se si desidera visualizzare i clienti e allocare le risorse in base alla provenienza.

Ad esempio, è stato notificato che la rete sta ricevendo molto traffico non pagato, e per questo indesiderato, dai client appartenenti a un gruppo specifico di indirizzi IP. Si crea una regola mediante il comando **dscontrol rule**, ad esempio:

```
dscontrol rule add 9.67.131.153:80:ni type ip  
beginrange 9.0.0.0 endrange 9.255.255.255
```

Questa regola "ni" visualizza le connessioni dai client non desiderati. A questo punto è possibile aggiungere alla regola i server che si desidera rendere accessibili ai dipendenti IBM oppure, se non si aggiunge alcun server, le richieste provenienti dagli indirizzi 9.x.x.x non verranno soddisfatte da nessun server.

Utilizzo delle regole basate sulla porta client

Questo tipo di regola è disponibile solo nel componente Dispatcher.

È possibile utilizzare regole basate sulla porta client se i client utilizzano alcuni tipi di software che richiedono una porta specifica da TCP/IP per generare le richieste.

Ad esempio, si può creare una regola che attesta che qualsiasi richiesta con una porta client 10002 utilizzerà una serie di server speciali veloci, in quanto la richiesta client con tale porta proviene da un gruppo di clienti di elite.

Utilizzo delle regole basate sull'ora del giorno

Questo tipo di regola è disponibile nel componente Dispatcher, CBR o Site Selector.

È possibile utilizzare le regole basate sull'ora del giorno per poter pianificare le capacità. Ad esempio, se il traffico sul sito Web è più elevato sempre nelle stesse ore del giorno, è possibile dedicare cinque server durante il periodo di maggior traffico.

Un altro motivo per cui si può utilizzare una regola basata sull'ora del giorno è quando si decide di disattivare, per la manutenzione, alcuni server ogni notte a mezzanotte; per questo è possibile impostare una regola che escluda quei server durante il periodo di manutenzione necessario.

Utilizzo delle regole basate sul tipo di servizio (TOS, type of service)

Questo tipo di regola è disponibile solo nel componente Dispatcher.

È possibile utilizzare le regole basate sul contenuto del campo "tipo di servizio" (TOS) nell'intestazione IP. Ad esempio, se una richiesta del client arriva con un valore TOS che indica un servizio normale, è possibile instradarla verso un gruppo di server. Se una richiesta client diversa arriva con un valore TOS diverso che indica una priorità di servizio più elevata, è possibile instradarla verso un gruppo diverso di server.

La regola TOS consente di configurare completamente ogni bit del byte TOS usando il comando **dscontrol rule**. Se si desidera che alcuni bit importanti corrispondano all'interno del byte TOS, utilizzare 0 o 1. Altrimenti, il valore usato è x. Di seguito viene riportato un esempio di aggiunta di una regola TOS:

```
dscontrol rule add  
9.67.131.153:80:tsr type service tos 0xx1010x
```

Utilizzo delle regole basate sulle connessioni al secondo

Questo tipo di regola è disponibile nei componenti Dispatcher e CBR.

Nota: è necessario che il gestore sia in esecuzione affinché le seguenti azioni funzionino correttamente.

È possibile utilizzare regole basate sulle connessioni al secondo per poter condividere i server con altre applicazioni. Ad esempio, si possono impostare due regole:

1. Se il numero di connessioni al secondo sulla porta 80 è compreso tra 0 e 2000, utilizzare questi 2 server
2. Se il numero di connessioni al secondo sulla porta 80 è superiore a 2000, utilizzare questi 10 server

Oppure, è possibile utilizzare Telnet e riservare due dei cinque server per Telnet, tranne quando il numero di connessioni al secondo supera un certo livello. In questo modo, Dispatcher bilancia il carico tra tutti e cinque i server nei momenti di traffico elevato.

Impostazione dell'opzione di valutazione delle regole "upserversonrule" insieme alla regola di tipo "connessione": quando si utilizza il tipo di regola delle connessioni e si imposta l'opzione **upserversonrule**, se alcuni server del gruppo sono disattivati, sicuramente i server rimanenti non verranno sovraccaricati. Per ulteriori informazioni, consultare "Opzione di valutazione dei server per le regole" a pagina 213.

Utilizzo delle regole basate sul numero totale di connessioni attive

Questo tipo di regola è disponibile nei componenti Dispatcher o CBR.

Nota: è necessario che il gestore sia in esecuzione affinché le seguenti azioni funzionino correttamente.

È possibile utilizzare le regole basate sul numero totale di connessioni attive su una porta se i server sono sovraccarichi e cominciano, quindi, ad eliminare i pacchetti. Alcuni server Web continuano ad accettare le connessioni anche se non dispongono di thread sufficienti per rispondere alle richieste. Ne consegue che le richieste dei client scadono e il cliente che visita il sito Web non viene assistito. Le regole basate sulle connessioni attive servono a bilanciare la capacità all'interno di un lotto di server.

Ad esempio, si sa, per esperienza, che i server smetteranno di soddisfare le richieste dopo aver accettato 250 connessioni. Si crea una regola mediante il comando **dscontrol rule** o il comando **cbrcontrol rule**, ad esempio:

```
dscontrol rule add 130.40.52.153:80:pool2 type active
beginrange 250 endrange 500
```

o

```
cbrcontrol rule add 130.40.52.153:80:pool2 type active
beginrange 250 endrange 500
```

Si aggiunge quindi la regola ai server correnti e ad altri server aggiunti che verrebbero, altrimenti, utilizzati per altri processi.

Utilizzo delle regole basate sulla larghezza di banda riservata e condivisa

Le regole della larghezza di banda riservata e della larghezza di banda condivisa sono disponibili solo nel componente Dispatcher.

Per le regole della larghezza di banda, Dispatcher calcola la larghezza di banda come la velocità con cui i dati vengono distribuiti ai client attraverso un gruppo specifico di server. Dispatcher traccia la capacità ai livelli server, regola, porta, cluster ed executor. Per ciascuno di questi livelli è disponibile un campo per il numero di byte: kilobyte trasferiti al secondo. Dispatcher calcola queste velocità in un intervallo di 60 secondi. I valori della velocità sono visibili dalla GUI o dal risultato visualizzato dalla riga comandi.

Regola della larghezza di banda riservata

La regola della larghezza di banda riservata permette di controllare il numero di kilobyte al secondo distribuiti da un gruppo di server. Impostando una soglia (assegnando cioè un'intervallo specifico per la larghezza di banda) per ogni gruppo di server della configurazione, è possibile controllare e garantire una parte determinata della larghezza di banda utilizzata da ciascuna combinazione porta-cluster.

Di seguito viene riportato un esempio di aggiunta di una regola `reservedbandwidth`:

```
dscontrol rule add 9.67.131.153:80:rbw type reservedbandwidth
beginrange 0 endrange 300
```

Gli intervalli di inizio e di fine vengono specificati in kilobyte al secondo.

Regola della larghezza di banda condivisa

Prima di configurare la regola della larghezza di banda condivisa, è necessario specificare la quantità massima di larghezza di banda (kilobyte al secondo) che

può essere condivisa a livello executor o cluster tramite il comando **dscontrol executor** o **dscontrol cluster** con l'opzione **sharedbandwidth**. Il valore **sharebandwidth** non deve superare la larghezza di banda totale (capacità di rete totale) disponibile. Utilizzando il comando **dscontrol** per impostare la larghezza di banda condivisa, si fornisce solo un limite superiore per la regola.

Di seguito sono riportati esempi di sintassi del comando:

```
dscontrol executor set sharedbandwidth size
dscontrol cluster [add | set] 9.12.32.9 sharedbandwidth size
```

Il valore *size* di **sharedbandwidth** è un numero intero (kilobyte al secondo). Il valore predefinito è zero. Se il valore è zero, la larghezza di banda non può essere condivisa.

La condivisione della larghezza di banda al livello di cluster permette a quest'ultimo di utilizzare una larghezza di banda massima specificata. Fino a quando la larghezza di banda utilizzata dal cluster è inferiore alla quantità specificata, questa regola verrà considerata valida, *true*. Se la larghezza di banda totale è superiore alla quantità specificata, questa regola sarà considerata non valida, *false*.

La condivisione della larghezza di banda al livello di executor permette all'intera configurazione di Dispatcher di condividere una quantità massima di larghezza di banda. Fino a quando la larghezza di banda utilizzata al livello di executor è inferiore alla quantità specificata, questa regola verrà considerata valida, *true*. Se la larghezza di banda totale è superiore a quella definita, questa regola sarà considerata non valida, *false*.

Di seguito vengono riportati esempi di aggiunta o impostazione di una regola **sharedbandwidth**:

```
dscontrol rule add 9.20.30.4:80:shbw type sharedbandwidth sharelevel value
dscontrol rule set 9.20.34.11:80:shrul sharelevel value
```

Il valore *value* di **sharelevel** è **executor** o **cluster**. **Sharelevel** è un parametro obbligatorio sulla regola **sharebandwidth**.

Utilizzo delle regole di larghezza di banda riservata e condivisa

Dispatcher consente di assegnare una larghezza di banda specifica a gruppi di server all'interno della configurazione mediante la regola *larghezza di banda riservata*. Indicando un intervallo di inizio e uno di fine, è possibile controllare il numero di kilobyte distribuiti da un gruppo di server ai client. Se la regola non è più valida (l'intervallo di fine è stato superato), verrà valutata la regola successiva con priorità inferiore. Se quest'ultima è una regola "sempre true", viene selezionato un server che risponda al client con una risposta "sito occupato".

Ad esempio: si supponga che sulla porta 2222 vi sia un gruppo di tre server. Se la larghezza di banda riservata è impostata su 300, il numero massimo di kbyte al secondo sarà 300 in un intervallo di tempo di 60 secondi. Quando questa velocità viene superata, la regola non viene più considerata valida. Se questa fosse la sola regola, Dispatcher selezionerebbe uno dei tre server per gestire la richiesta. Se ci fosse una regola "sempre true" con priorità minore, la richiesta potrebbe essere indirizzata a un altro server e ricevere una risposta "sito occupato".

La regola di larghezza di banda condivisa fornisce ai client maggiore accessibilità ai server. Nello specifico, se utilizzato come regola di priorità inferiore seguito da

una regola di larghezza di banda riservata, un client può ancora accedere a un server anche se la larghezza di banda riservata è stata superata.

Ad esempio: utilizzando una regola di larghezza di banda condivisa seguita da una regola di larghezza di banda riservata, è possibile permettere ai client di accedere ai tre server in modo controllato. Fino a quando sarà possibile utilizzare una larghezza di banda, la regola verrà valutata come true e l'accesso verrà garantito. Se non è disponibile alcuna larghezza di banda condivisa, la regola non sarà true e verrà valutata la regola successiva. Se segue una regola "sempre true", la richiesta può essere indirizzata secondo necessità.

Utilizzando una larghezza di banda riservata e condivisa, come descritto nell'esempio precedente, è possibile esercitare maggiore controllo e flessibilità nel permettere (o nel negare) l'accesso ai server. I server di una porta specifica possono essere limitati nell'uso della larghezza di banda, mentre altri possono utilizzare una larghezza di banda aggiuntiva per tutto il tempo in cui questa è disponibile.

Nota: Dispatcher traccia la larghezza di banda misurando il traffico dei client, come ad esempio gli "acks" dei dati, che affluiscono su un server. Se, per alcune ragioni, questo traffico non viene "visto" da Dispatcher, i risultati che derivano dall'uso delle regole della larghezza di banda sono imprevedibili.

Regola Metric all

Questo tipo di regola è disponibile solo nel componente Site Selector.

Per quanto riguarda la regola metric all, scegliendo una metrica di sistema (cpuload, memload, oppure lo script della metrica di sistema personalizzato), Site Selector confronta il valore della metrica di sistema (restituito dall'agente Metric Server presente su ogni server con bilanciamento del carico) con l'intervallo di inizio e di fine specificato nella regola. Il valore attuale della metrica di sistema, per tutti i server all'interno del gruppo, deve essere incluso nell'intervallo della regola da eseguire.

Nota: Lo script della regola di sistema scelto deve risiedere su ogni server su cui viene eseguito il bilanciamento del carico.

Di seguito viene riportato un esempio di aggiunta di una regola metric all alla configurazione:

```
sscontrol rule add dnsload.com:allrule1 type metricall  
metricname cpuload beginrange 0 endrange 100
```

Regola media metrica

Questo tipo di regola è disponibile solo nel componente Site Selector.

Per quanto riguarda la regola Media metrica, si sceglie una metrica di sistema (cpuload, memload, oppure lo script della metrica di sistema personalizzato) e Site Selector confronta il valore della metrica di sistema (restituito dall'agente Metric Server presente su ogni server con bilanciamento del carico) con l'intervallo di inizio e di fine specificato nella regola. La *media* dei valori della metrica di sistema attuale, per tutti i server all'interno del gruppo, deve essere inclusa nell'intervallo della regola da generare.

Nota: lo script della regola di sistema scelto deve risiedere su ogni server su cui viene eseguito il bilanciamento del carico.

Di seguito viene riportato un esempio di aggiunta di una regola media metrica alla configurazione:

```
sscontrol rule add dnsload.com:avgrule1 type metricavg  
metricname cpuload beginrange 0 endrange 100
```

Utilizzo di regole il cui valore è sempre true

Questo tipo di regola è disponibile nel componente Dispatcher, CBR o Site Selector.

È possibile creare una regola che sia “sempre true.” Tale regola verrà sempre selezionata, a meno che tutti i server ad essa associati non siano disattivati. Per questo motivo, questa regola dovrebbe avere sempre una priorità inferiore rispetto alle altre.

È possibile disporre di più regole che siano “sempre true”, ognuna con un gruppo di server associati. Viene scelta la prima regola true disponibile. Ad esempio, si supponga di avere sei server. Due di loro devono gestire il traffico in ogni circostanza, a meno che non siano disattivati. Se i primi due server sono disattivati, si sceglie un secondo gruppo di server per gestire il traffico. Se tutti e quattro i server scelti sono disattivati, si utilizzano gli ultimi due disponibili. Si possono impostare tre regole sulla condizione “sempre true”. Verrà scelto sempre il primo gruppo di server fino a quando almeno uno dei server è attivo. Se entrambi sono disattivati, si sceglie un server del secondo gruppo, e così via.

Un altro esempio prevede una regola “sempre true” in grado di assicurare che se i client in entrata non corrispondono a nessuna delle regole impostate, le loro richieste non verranno soddisfatte. Si crea una regola mediante il comando **dscontrol rule**, come ad esempio:

```
dscontrol rule add 130.40.52.153:80:jamais type true priority 100
```

A questo punto, nessun altro server viene aggiunto alla regola poiché i pacchetti client verrebbero eliminati senza risposta.

Nota: Non è necessario impostare un intervallo di fine o di inizio quando si crea una regola sempre true.

Si possono definire più regole “sempre true” e, quindi, impostare la regola da eseguire modificandone i livelli di priorità.

Utilizzo delle regole basate sul contenuto delle richieste

Questo tipo di regola è disponibile nei componenti CBR o Dispatcher (quando si usa il metodo di inoltro cbr di Dispatcher).

Le regole del tipo di contenuto vengono utilizzate per inviare le richieste a gruppi di server impostati per gestire alcuni sottogruppi di traffico del sito. Ad esempio, un gruppo di server può gestire le richieste *cgi-bin*, un altro gruppo gestisce le richieste dei flussi audio e un terzo gruppo gestisce tutte le altre richieste. È possibile aggiungere una regola con un modello che corrisponde al percorso della directory *cgi-bin*, un'altra che corrisponde al tipo di file dei file di flussi audio e una terza regola sempre true per gestire il resto del traffico. Si aggiungono, poi, i server appropriati per ciascuna regola.

Importante: per gli esempi e gli scenari relativi alle modalità di utilizzo delle regole di contenuto e della sintassi dei modelli valida per tali regole, consultare Appendice B, “Sintassi della regola di contenuto (modello)”, a pagina 463.

ignora affinità di porta

Con la funzione ignora affinità di porta, si ignora l'aderenza di una porta per un server specifico. Ad esempio, si sta utilizzando una regola per limitare la quantità di connessioni a ciascun server delle applicazioni e su uno dei server si è verificato un overflow, mentre la regola sempre true informa l'utente di "riprovare in seguito" per poter utilizzare l'applicazione richiesta. La porta ha un valore di tempo di aderenza di 25 minuti e non è consigliabile che il client rimanga aderente a quel server. La funzione ignora affinità di porta permette di cambiare il server in overflow per ignorare l'affinità che normalmente è associata a quella porta. Quando il client effettuerà una nuova richiesta al cluster, il carico viene bilanciato verso il miglior server delle applicazioni disponibile e non sul server in overflow.

Consultare "dscontrol server — configura i server" a pagina 381, per informazioni dettagliate sulla sintassi di comando relativa alla funzione ignora affinità di porta mediante il server **aderente**.

Aggiunta di regole alla configurazione

È possibile aggiungere delle regole utilizzando il comando **dscontrol rule add**, modificando il file di configurazione di esempio oppure usando una GUI (graphical user interface). Si possono aggiungere più regole su ciascuna porta definita.

Si tratta di un processo a due fasi: si aggiunge la regola e si definiscono i server da supportare se la regola è true. Ad esempio, l'amministratore di sistema desidera quantificare l'uso dei server proxy da parte di ciascuna divisione del sito. Gli indirizzi IP sono assegnati a ogni divisione. Creare il primo gruppo di regole in base all'indirizzo IP del client per separare il carico di ogni divisione:

```
dscontrol rule add 130.40.52.153:80:div1 type ip b 9.1.0.0 e 9.1.255.255
dscontrol rule add 130.40.52.153:80:div2 type ip b 9.2.0.0 e 9.2.255.255
dscontrol rule add 130.40.52.153:80:div3 type ip b 9.3.0.0 e 9.3.255.255
```

Quindi, aggiungere un server diverso ad ogni regola e misura il carico su ogni server per fatturare correttamente la divisione in base ai servizi utilizzati. Ad esempio:

```
dscontrol rule useserver 130.40.52.153:80:div1 207.72.33.45
dscontrol rule useserver 130.40.52.153:80:div2 207.72.33.63
dscontrol rule useserver 130.40.52.153:80:div3 207.72.33.47
```

Opzione di valutazione dei server per le regole

L'opzione di valutazione dei server è disponibile solo nel componente Dispatcher.

Sul comando **dscontrol rule** è presente un'opzione di valutazione dei server per le regole. Utilizzare l'opzione *evaluate* per valutare la condizione delle regole su tutti i server sulla porta oppure per valutare la condizione delle regole solo sui server inclusi nella regola. (Nelle versioni precedenti di Load Balancer, è possibile misurare ogni condizione di regola su tutti i server sulla porta).

Note:

1. L'opzione di valutazione del server è valida solo per le regole che si basano sulle caratteristiche dei server: la regola Numero totale di connessioni (al secondo), la regola Connessioni attive e la regola Larghezza di banda riservata.
2. La regola di tipo "connessione" ha un'opzione di valutazione in più da scegliere — **upserversonrule**. Per ulteriori informazioni, consultare "Utilizzo delle regole basate sulle connessioni al secondo" a pagina 208.

Di seguito vengono riportati esempi di aggiunta o impostazione dell'opzione di valutazione su una regola di larghezza di banda riservata:

```
dscontrol rule add 9.22.21.3:80:rbweval type reservedbandwidth evaluate level  
dscontrol rule set 9.22.21.3:80:rbweval evaluate level
```

Il valore *evaluate level* può essere impostato su porta, regola o upserversonrule. Il valore predefinito è porta.

Valutazione dei server in una regola

L'opzione per la misurazione della condizione della regola sui server inclusi in una regola, permette di configurare due regole con le seguenti caratteristiche:

- La prima regola valutata contiene tutti i server che gestiscono il contenuto del sito Web e l'opzione di valutazione è impostata su *rule* (valutare la condizione della regola sui server inclusi nella regola).
- La seconda è una regola sempre true che contiene un unico server la cui risposta è di tipo "sito occupato".

Il risultato è che quando il traffico supera la soglia dei server inclusi nella prima regola, il traffico verrà inviato al server del "sito occupato" incluso nella seconda regola. Quando il traffico scende sotto la soglia dei server della prima regola, il nuovo traffico continua ad affluire su tali server.

Valutazione dei server sulla porta

Utilizzando le due regole descritte nell'esempio precedente, se si imposta l'opzione di valutazione su *port* per la prima regola (valutare la condizione della regola su tutti i server della porta), nel momento in cui il traffico supera la soglia di quella regola, viene indirizzato al server "sito occupato" associato alla seconda regola.

La prima regola misura il traffico di tutti il server (compreso il server "sito occupato") sulla porta per determinare se il traffico supera la soglia. Con il diminuire della congestione dei server associati alla prima regola, potrebbe verificarsi un risultato imprevisto nel punto in cui il traffico continua sul server "sito occupato", poiché il traffico sulla porta supera ancora la soglia della prima regola.

Funzionamento della funzione di affinità di Load Balancer

Per i componenti Dispatcher e CBR: si abilita la funzione di affinità quando la porta del cluster viene configurata come aderente. La configurazione di una porta del cluster sulla condizione di aderenza permette alle successive richieste client di essere indirizzate allo stesso server. Ciò è possibile impostando su un certo numero di secondi il valore di **stickytime** a livello di executor, del cluster o della porta. La funzione viene disabilitata impostando stickytime su zero.

se si abilita l'affinità multiporta, i valori di stickytime delle porte condivise devono essere uguali (numero diverso da zero). Per ulteriori informazioni, consultare "Affinità multiporta" a pagina 215.

Per il componente Site Selector: si abilita la funzione di affinità quando si configura un nome sito come aderente. In questo modo, il client può utilizzare lo stesso server per più richieste di servizio nome. Ciò è possibile impostando il valore **stickytime** del nome sito su un certo numero di secondi. La funzione si disabilita impostando stickytime su zero.

L'intervallo compreso tra la chiusura di una connessione e l'apertura di una nuova connessione durante il quale un client verrà rinviato allo stesso server utilizzato

durante la prima connessione. Dopo questo intervallo, il client potrebbe essere inviato a un server diverso dal primo. Il valore dell'intervallo per un server viene configurato utilizzando i comandi `dscontrol executor, port o cluster`. Quando il comando del server inattivo (`dscontrol server down`) viene utilizzato per porre un server offline, se il valore dell'intervallo è diverso da zero per tale server, i client esistenti continuano a funzionare sul server fino a che viene raggiunto l'intervallo. Il server non sarà reso inattivo fino a che non viene raggiunto il valore dell'intervallo.

Funzionamento con affinità disabilitata

Con la funzione di affinità disabilitata, ogni volta che si riceve una nuova connessione TCP da un client, Load Balancer seleziona il server adatto in quel momento e gli inoltra i pacchetti. Se un'altra connessione viene dallo stesso client, Load Balancer la considera come una nuova connessione non correlata e seleziona di nuovo il server più adatto in quel momento.

Funzionamento con affinità abilitata

Con la funzione di affinità abilitata, se una richiesta viene dallo stesso client, sarà poi indirizzata allo stesso server.

Nel corso del tempo, il client termina di inviare le transazioni e il record di affinità non sarà più necessario. Da qui, il significato di "tempo di aderenza". Ogni record di affinità ha una durata che equivale al valore "stickytime" espresso in secondi. Quando si ricevono altre connessioni durante il tempo di aderenza, il record di affinità è ancora valido e la richiesta viene indirizzata allo stesso server. Se si riceve un'altra connessione al di fuori del tempo di aderenza, il record viene eliminato; una connessione ricevuta oltre quell'intervallo di tempo, verrà supportata da un altro server.

Il comando del server inattivo (`dscontrol server down`) viene utilizzato per porre un server offline. Il server sarà attivo fino a che viene raggiunto il valore dell'intervallo di aderenza.

Affinità multiporta

L'affinità multiporta si applica esclusivamente ai metodi di inoltro MAC e NAT/NATP del componente Dispatcher.

L'affinità multiporta è una funzione di aderenza che è stata estesa per coprire più porte. Ad esempio, se una richiesta client viene ricevuta su una porta e la richiesta successiva su un'altra porta, l'affinità multiporta permette a Dispatcher di inviare la richiesta di quel client allo stesso server. Per poter utilizzare questa funzione, le porte devono:

- condividere lo stesso indirizzo cluster
- condividere gli stessi server
- avere lo stesso valore **stickytime** (diverso da zero) valore
- avere lo stesso valore **stickymask** valore

È possibile collegare più porte alla stessa affinità **multiporta**. Quando le connessioni provengono dallo stesso client sulla stessa porta o su una porta condivisa, accedono allo stesso server. Di seguito viene riportato un esempio di configurazione di più porte con affinità multiporta sulla porta 10:

```
dscontrol port set cluster:20 crossport 10
dscontrol port set cluster:30 crossport 10
dscontrol port set cluster:40 crossport 10
```

Una volta stabilita l'affinità multiporta, è possibile modificare il valore stickytime della porta. Tuttavia, è consigliabile impostare i valori stickytime di tutte le porte condivise sullo stesso valore per evitare che si verifichino risultati imprevisti.

Per rimuovere l'affinità multiporta, impostare nuovamente il valore crossport sul numero di porta originale. Consultare “dscontrol port — configura le porte” a pagina 369, per informazioni dettagliate sulla sintassi di comando relativa all'opzione **crossport**.

Maschera indirizzo affinità (stickymask)

La funzione maschera indirizzo affinità si applica esclusivamente al componente Dispatcher.

La funzione maschera indirizzo affinità è un potenziamento della funzione di aderenza che serve a raggruppare i client in base agli indirizzi di sottorete comuni. Specificando **stickymask** nel comando **dscontrol port**, è possibile applicare una maschera ai bit più significativi dell'indirizzo IP a 32 bit. Se questa funzione è configurata, quando una richiesta client stabilisce la prima connessione alla porta, tutte le successive richieste dai client con lo stesso indirizzo di sottorete (rappresentato da quella parte dell'indirizzo IP con maschera) verranno indirizzate allo stesso server.

Nota: per abilitare stickymask, il valore di porta **stickytime** deve essere diverso da zero.

Ad esempio, se si desidera che tutte le richieste client in entrata, con lo stesso indirizzo Classe A di rete, vengano indirizzate allo stesso server, è sufficiente impostare il valore stickymask su 8 (bit) per la porta. Per raggruppare le richieste client con lo stesso indirizzo Classe B di rete, impostare il valore stickymask su 16 (bit). Per raggruppare le richieste client con lo stesso indirizzo Classe C di rete, impostare il valore stickymask su 24 (bit).

Per ottenere dei risultati più soddisfacenti, impostare il valore stickymask al primo avvio di Load Balancer. Modificando in modo dinamico il valore stickymask, i risultati potrebbero essere imprevedibili.

Interazione con l'affinità multiporta: se si abilita l'affinità multiporta, i valori stickymask delle porte condivise, devono essere gli stessi. Per ulteriori informazioni, consultare “Affinità multiporta” a pagina 215.

Per abilitare la maschera indirizzo affinità, emettere un comando **dscontrol port** simile al seguente:

```
dscontrol port set cluster:port stickytime 10 stickymask 8
```

I valori possibili di stickymask sono 8, 16, 24 e 32. Un valore 8 indica che verrà applicata una maschera ai primi 8 bit più significativi dell'indirizzo IP (indirizzo Classe A di rete). Un valore 16 indica che verrà applicata una maschera ai primi 16 bit più significativi dell'indirizzo IP (indirizzo Classe B di rete). Un valore 24 indica che verrà applicata una maschera ai primi 24 bit più significativi dell'indirizzo IP (indirizzo Classe C di rete). Il valore 32 indica che si sta applicando una maschera all'intero indirizzo IP che, in effetti, disabilita la funzione di maschera indirizzo affinità. Il valore predefinito di stickymask è 32.

Consultare “dscontrol port — configura le porte” a pagina 369, per informazioni dettagliate sulla sintassi di stickymask (funzione maschera indirizzo affinità).

Gestione della disattivazione delle connessioni server

La gestione della disattivazione si applica ai componenti Dispatcher e CBR.

Per rimuovere un server dalla configurazione di Load Balancer per qualsiasi motivo (aggiornamenti, manutenzione, e così via), utilizzare il comando **dscontrol manager quiesce**. Il comando secondario di disattivazione fa in modo che le connessioni esistenti vengano completate (senza essere interrotte) e inoltra solo le successive nuove connessioni dal client al server disattivato, se la connessione è designata come aderente e il tempo di aderenza non è scaduto. Tale comando impedisce qualsiasi altra connessione al server.

Gestione della disattivazione per le connessioni aderenti

Utilizzare l'opzione di disattivazione "now" se è stato impostato un tempo di aderenza e si intende inviare le nuove connessioni a un altro server (diverso dal server disattivato) prima della scadenza di tale tempo. Di seguito viene riportato un esempio sull'uso dell'opzione now che permette di disattivare il server 9.40.25.67:

```
dscontrol manager quiesce 9.40.25.67 now
```

L'opzione now determina il modo in cui verranno gestite le connessioni aderenti:

- Se *non* si specifica "now," dopo il completamento delle connessioni esistenti, le successive nuove connessioni, provenienti dai client le cui connessioni sono designate come aderenti, verranno inoltrate al server disattivato fino a quando quest'ultimo non riceve la nuova richiesta prima della scadenza del tempo di aderenza. (Tuttavia, se la funzione aderenza (affinità) non è abilitata, il server disattivato non può ricevere nessuna nuova connessione).

Questo è il modo meno brusco di disattivare i server. Ad esempio, si può disattivare un server con molta delicatezza e aspettare il momento in cui il traffico è minore (probabilmente la mattina molto presto) per rimuoverlo del tutto dalla configurazione.

- Specificando "now," si disattiva il server; in questo modo le connessioni esistenti possono essere completate ma tutte le nuove connessioni, incluse quelle successive provenienti dai client che hanno connessioni esistenti e indicate come aderenti, non sono consentite. Questo metodo di disattivazione dei server è più brusco ed era l'unico utilizzato nelle versioni precedenti di Load Balancer.

Opzione di affinità della regola basata sul contenuto della richiesta client

È possibile specificare i seguenti tipi di affinità sul comando **dscontrol rule**:

- Cookie attivo — permette di bilanciare il carico del traffico Web con caratteristiche di affinità con lo stesso server tramite cookie generati da Load Balancer.

L'affinità cookie attivo si applica solamente al componente CBR.

- Cookie passivo — permette di bilanciare il carico del traffico Web con caratteristiche di affinità con lo stesso server tramite la creazione di cookie auto-identificativi da parte dei server. Insieme all'affinità del cookie passivo, è necessario specificare anche il parametro cookiename (nome cookie) sul comando della regola.

Il cookie passivo si applica al componente CBR e al metodo di inoltro cbr del componente Dispatcher.

- URI — permette il bilanciamento del carico del traffico Web sui server caching-proxy in modo tale da aumentare la capacità della cache.

L'affinità URI si applica al componente CBR e al metodo di inoltro cbr del componente Dispatcher.

Il valore predefinito per l'opzione di affinità è "none." L'opzione **stickytime** del comando della porta deve essere impostata su zero (non abilitata) per poter configurare l'opzione **affinità** sul comando della regola del cookie attivo, cookie passivo e URI. Se l'affinità è impostata sulla regola, non è possibile abilitare stickytime sulla porta.

Affinità cookie attivo

L'affinità cookie attivo si applica solamente al componente CBR.

Permette di rendere i client "aderenti" a un particolare server. Questa funzione viene abilitata regolando il valore **stickytime** di una regola su un numero positivo e configurando l'affinità su "activecookie". Ciò è possibile quando si aggiunge una regola o si utilizza il comando di impostazione di una regola. Consultare "dscontrol rule — configura le regole" a pagina 375, per informazioni dettagliate sulla sintassi del comando.

Una volta abilitata la regola affinità cookie attivo, le nuove richieste client verranno bilanciate grazie a degli algoritmi CBR standard, mentre le richieste successive provenienti dallo stesso client verranno inviate al server scelto inizialmente. Quest'ultimo viene memorizzato come cookie nella risposta per il client. Fino a quando le future richieste del client conterranno il cookie, e ogni richiesta arriva nell'intervallo stickytime stabilito, il client conserverà l'affinità con il server iniziale.

L'affinità cookie attivo viene utilizzata per garantire che un client continui ad essere bilanciato con lo stesso server per un determinato periodo di tempo. Ciò è possibile inviando un cookie che verrà memorizzato dal browser dei client. Il cookie contiene la regola cluster:port:rule utilizzata per prendere la decisione, il server in base al quale è stato bilanciato il carico e la data e l'ora di scadenza che indicano la fine della validità dell'affinità. Il cookie è nel seguente formato: **IBMCBR=cluster:port:rule+server-time!** Le informazioni *cluster:port:rule* e *server* sono codificate per impedire che la configurazione CBR venga rivelata.

Funzionamento dell'affinità cookie attivo

Ogni volta che viene generata una regola con affinità cookie attivo abilitata, il cookie inviato dal client viene esaminato.

- Se si rileva un cookie contenente l'identificativo della regola cluster:port:rule generata, il server con il carico bilanciato e la data e l'ora di scadenza vengono estratti dal cookie.
- Se il server fa ancora parte del gruppo utilizzato dalla regola il suo peso è positivo o si tratta di un server disattivato, e la data e ora di scadenza sono successive alla data e all'ora attuali, viene scelto il server che si trova nel cookie per bilanciare il carico.
- Se una delle precedenti condizioni non viene soddisfatta, si sceglie un server utilizzando un algoritmo normale.
- Dopo aver scelto un server (tramite uno dei due metodi) viene creato un nuovo cookie contenente informazioni IBMCBR, cluster:port:rule, server_chosen e un valore di data e ora. Quest'ultimo valore rappresenta la scadenza dell'affinità. Le informazioni "cluster:port:rule e server_chosen" sono codificate per impedire che la configurazione CBR venga rivelata.

- Nel cookie viene inserito anche un parametro “expires”. Questo parametro è in un formato noto al browser e fa in modo che il cookie non sia più valido sette giorni dopo la data di scadenza. In questo modo il database dei cookie dei client è sempre in ordine.

Questo nuovo cookie viene inserito nelle intestazioni che verranno restituite al client e se il browser di quest’ultimo è configurato per accettare i cookie, restituirà le richieste successive.

Ogni istanza di affinità del cookie sarà di 65 byte di lunghezza e terminerà con un punto esclamativo. Ne deriva che un cookie di 4096 byte può contenere circa 60 regole di cookie attivi per dominio. Una volta saturo, tutte le istanze di affinità scadute verranno eliminate. Se tutte le istanze sono ancora valide, si elimina la più obsoleta per fare spazio e aggiungere le nuove istanze della regola corrente.

Nota: CBR sostituisce le occorrenze dei cookie IBM CBR di formato vecchio non appena compaiono nel proxy.

L’opzione affinità cookie attivo, del comando della regola, può essere impostata solo su activecookie se il valore stickytime della porta è zero (non abilitato). Una volta abilitata l’affinità cookie attivo su una regola, non è possibile abilitare stickytime sulla porta.

Come abilitare l’affinità cookie attivo

Per abilitare l’affinità cookie attivo di una regola particolare, utilizzare il comando del gruppo di regole:

```
rule set cluster:port:rule stickytime 60
rule set cluster:port:rule affinity activecookie
```

Perché utilizzare l’affinità cookie attivo

Una regola di aderenza viene utilizzata normalmente per CGI o i servlet che memorizzano lo stato dei client sul server. Lo stato viene identificato da un ID cookie (questi sono i cookie dei server). Lo stato del client è presente solo sul server selezionato, quindi il client ha bisogno del cookie di quel server per conservare lo stato tra le richieste.

Scadenza dell’affinità cookie attivo ignorata

L’affinità cookie attivo ha una scadenza predefinita relativa alla data del server corrente, più l’intervallo stickytime, più ventiquattro ore. Se i sistemi dei client (quelli che inviano le richieste alla macchina CBR) hanno una data errata (ad esempio, sono avanti di un giorno rispetto alla data del server), ignorano i cookie che provengono da CBR in quanto il sistema presuppone che tali cookie siano già scaduti. Per impostare una data di scadenza più lunga, modificare lo script cbrserver. Nel file di script, modificare la riga javaw aggiungendo il seguente parametro dopo LB_SERVER_KEYS: -DCOOKIEEXPIREINTERVAL=X dove X è il numero di giorni da aggiungere alla data di scadenza.

Su sistemi AIX, Solaris e Linux, il file cbrserver si trova nella directory /usr/bin.

Su sistemi Windows, il file cbrserver si trova nella directory \winnt\system32.

Affinità cookie passivo

L’affinità cookie passivo si applica al metodo di inoltro cbr (content-based routing) del componente Dispatcher e al componente CBR. Consultare “Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)” a pagina 53 per informazioni su come configurare il metodo di inoltro cbr di Dispatcher.

L'affinità cookie passivo permette di rendere aderenti i client di un particolare server. Abilitando l'affinità di una regola su "passivecookie", l'affinità cookie passivo consente di bilanciare il carico del traffico Web con caratteristiche di affinità con lo stesso server tramite la creazione di cookie auto-identificativi da parte dei server. È possibile configurare l'affinità cookie passivo al livello della regola.

Quando viene generata la regola, se l'affinità cookie passivo è abilitata, Load Balancer sceglierà il server in base al nome cookie nell'intestazione HTTP della richiesta client. Load Balancer confronta il nome del cookie dell'intestazione HTTP del client con il valore del cookie configurato per ciascun server.

La prima volta in cui Load Balancer rileva un server il cui valore cookie *contiene* il nome cookie del client, Load Balancer sceglie quel server per la richiesta.

Nota: Load Balancer permette tale flessibilità per gestire i casi in cui il server può generare un valore cookie che abbia una parte statica aggiunta e una parte variabile. Ad esempio, il valore del cookie del server potrebbe essere il nome del server (un valore statico) aggiunto e un valore data/ora (un valore variabile).

Se il nome del cookie nella richiesta client non si trova o non corrisponde al contenuto dei valori del cookie del server, quest'ultimo verrà scelto tra una selezione di server esistente o tramite la tecnica dei pesi del metodo round-robin.

Per configurare l'**affinità cookie passivo**:

- Per Dispatcher, configurare prima il metodo di inoltro cbr di Dispatcher. (Consultare "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.) Questo passaggio viene omesso per il componente CBR.
- Impostare il parametro **affinity** su "passivecookie" sul comando **dscontrol rule [add|set]**. Inoltre, il parametro **cookieName** deve essere impostato sul nome del cookie che Load Balancer deve ricercare nella richiesta intestazione HTTP del client.
- Impostare il parametro **cookievalue**, per ogni server del gruppo di server della regola, sul comando **dscontrol server [add|set]**.

L'opzione affinità cookie passivo, del comando della regola, può essere impostata solo su passivecookie se il valore stickytime della porta è zero (non abilitato). Una volta abilitata l'affinità cookie passivo su una regola, non è possibile abilitare stickytime sulla porta.

Affinità URI

L'affinità URI si applica al metodo di inoltro cbr del Dispatcher e al componente CBR. Consultare "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53 per informazioni su come configurare il metodo di inoltro cbr.

L'affinità URI permette di bilanciare il carico del traffico Web sui server Caching Proxy che consentono di memorizzare nella cache il contenuto unico di ciascun server. In questo modo, si aumenta effettivamente la capacità della cache del sito evitando che i contenuti vengano memorizzati su più macchine. Configurare l'affinità URI al livello della regola. Una volta creata la regola, se l'affinità URI è abilitata e lo stesso gruppo di server è attivo e risponde, Load Balancer inoltra le richieste in arrivo dei client con lo stesso URI sullo stesso server.

Normalmente, Load Balancer può distribuire le richieste su più server che supportano lo stesso contenuto. Se si utilizza Load Balancer con un gruppo di caching server, i contenuti più esaminati vengono memorizzati nella cache di tutti i server. Questo consente di supportare un carico di client molto elevato riproducendo i contenuti identici memorizzati nella cache su più macchine. Questo espediente risulta molto utile quando si gestiscono siti Web con un volume elevato di traffico.

Tuttavia, se il sito Web supporta un volume ridotto di traffico client di diverso contenuto, e si preferisce avere maggiore disponibilità di cache sui vari server, il sito funzionerebbe meglio se ogni caching server avesse un contenuto unico e Load Balancer distribuisse la richiesta esclusivamente al caching server con quel contenuto.

Con l'affinità URI, Load Balancer permette di distribuire il contenuto memorizzato nella cache sui singoli server, evitando una memorizzazione ridondante su più macchine. Con questo potenziamento, si migliorano anche le prestazioni dei siti server di diverso contenuto che utilizzano i server Caching Proxy. Le stesse richieste vengono inviate allo stesso server, per cui il contenuto viene memorizzato nella cache dei singoli server. Quindi, la dimensione effettiva della cache aumenta ogni volta che si aggiunge una nuova macchina server al lotto.

Per configurare l'**Affinità URI**:

- Per Dispatcher, configurare prima il metodo di inoltro cbr di Dispatcher. (Consultare "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.) Questo passaggio viene omesso per il componente CBR.
- Impostare il parametro **affinity** su "uri" sul comando **dscontrol rule [add|set]** o **cbrcontrol rule [add|set]**.

L'opzione affinità URI, del comando della regola, può essere impostata su URI se il valore stickytime della porta è zero (non abilitato). Una volta abilitata l'affinità URI su una regola, non è possibile abilitare il valore stickytime sulla porta.

Configurazione del supporto di Dispatcher per una rete geografica

Questa funzione è disponibile esclusivamente per il componente Dispatcher.

Se non si sta utilizzando il supporto rete geografica di Dispatcher, né il metodo di inoltro nat di Dispatcher, una configurazione Dispatcher richiede che la macchina Dispatcher e i server relativi siano collegati allo stesso segmento LAN (vedere Figura 35 a pagina 222). Una richiesta client arriva nella macchina Dispatcher e viene inviata al server. Dal server, la risposta viene restituita direttamente al client.

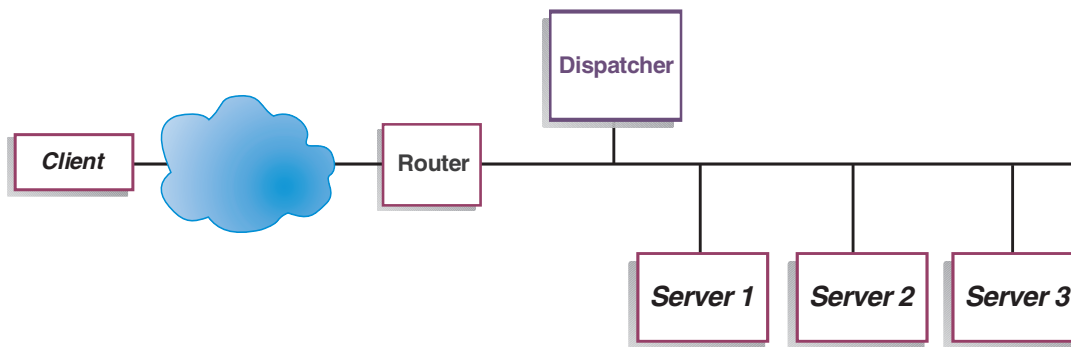


Figura 35. Esempio di una configurazione costituita da un unico segmento LAN

La funzione di rete geografica di Dispatcher fornisce un supporto ai server esterni, noti come *server remoti* (consultare Figura 36). Se GRE non è supportato sul sito remoto e se il metodo di inoltro nat di Dispatcher non viene utilizzato, il sito remoto deve essere costituito da una macchina Dispatcher remota (Dispatcher 2) e dai relativi server collegati localmente (ServerG, ServerH e ServerI). Un pacchetto client andrà da Internet alla macchina Dispatcher iniziale. Dal Dispatcher iniziale, il pacchetto raggiunge la macchina Dispatcher che si trova in una posizione geograficamente remota e uno dei server collegati localmente.

Tutte le macchine Dispatcher (locale e remota) devono eseguire lo stesso tipo di sistema operativo e piattaforma per poter creare delle configurazioni WAN.

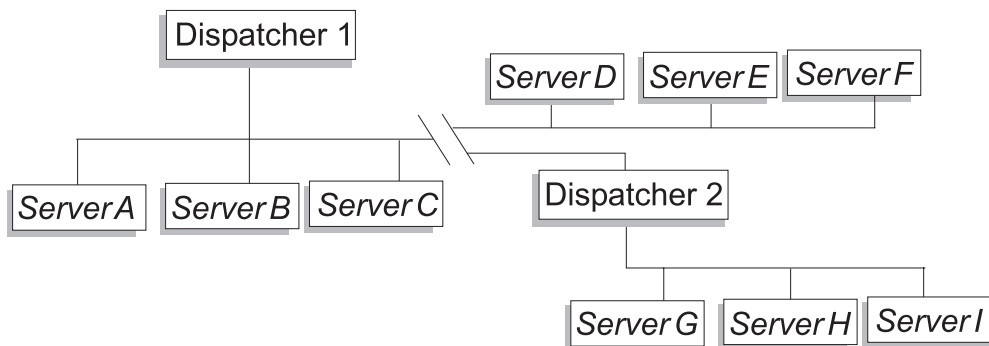


Figura 36. Esempio di configurazione che utilizza server locali e remoti

Questa configurazione a un indirizzo cluster di supportare tutte le richieste di client in tutto il mondo e di distribuire il carico su server altrettanto remoti.

La macchina Dispatcher che riceve inizialmente il pacchetto può avere dei server locali collegati e può distribuire il carico tra i server locali e quelli remoti.

Sintassi dei comandi

Per configurare il supporto rete geografica:

1. Aggiungere i server. Quando si aggiunge un server a un Dispatcher, definire se il server è locale o remoto (vedere paragrafo precedente). Per aggiungere un server e definirlo come locale, emettere il comando **dscontrol server add** senza specificare un router. Questo è il valore di default. Per definire il server come remoto, specificare il router attraverso il quale Dispatcher deve inviare il pacchetto per poter raggiungere il server remoto. Il server deve essere un altro Dispatcher e l'indirizzo server deve essere l'indirizzo di non inoltro del

Dispatcher. Ad esempio, in Figura 37 a pagina 225, se si aggiunge *LB 2* come server remoto sotto *LB 1*, indicare *router 1* come l'indirizzo router. Sintassi generale:

```
dscontrol server add cluster:port:server router address
```

Per maggiori informazioni sulla parola chiave *router*, consultare “dscontrol server — configura i server” a pagina 381.

2. Configurare gli alias. Sulla prima macchina Dispatcher (dove le richieste client arrivano da Internet), è necessario creare un alias per l'indirizzo cluster utilizzando il comando **executor configure**. (Per i sistemi Linux o UNIX, è possibile utilizzare il comando **executor configure** o **ifconfig**). Sulle macchine Dispatcher remote, tuttavia, *non* viene creato un alias per l'indirizzo cluster su una scheda di interfaccia di rete.

Utilizzo di advisor remoti con il supporto rete geografica di Dispatcher

Sui Dispatcher entry-point:

I Dispatcher entry-point in esecuzione sulle piattaforme AIX, Linux (che utilizza GRE) o Solaris, visualizzeranno correttamente i carichi degli advisor. Le altre piattaforme devono basarsi sul bilanciamento del carico round-robin oppure utilizzare i metodi di inoltro nat/cbr di Dispatcher anziché la rete geografica (WAN, wide area networking).

Sistemi AIX

- Non sono necessarie procedure di configurazione speciali.

Sistemi HP-UX

- Quando si utilizza un Dispatcher entry-point in esecuzione su una piattaforma HP-UX in una configurazione WAN, esiste un limite dell'uso degli advisor remoti. Con il metodo di inoltro mac di Dispatcher, gli advisor HP-UX vengono destinati direttamente all'indirizzo del server anziché del cluster. Poiché non vengono indirizzati al cluster, il Dispatcher remoto non bilancia il carico delle richieste degli advisor sui server remoti. Tuttavia, gli advisor remoti funzionano correttamente se si utilizzano i metodi di inoltro cbr o nat di Dispatcher.

Sistemi Linux

- Quando si utilizza un Dispatcher entry-point in esecuzione su una piattaforma Linux in una configurazione WAN, esiste un limite dell'uso degli advisor remoti. Con il metodo di inoltro mac di Dispatcher, gli advisor Linux vengono destinati direttamente all'indirizzo del server anziché del cluster. Poiché non vengono indirizzati al cluster, il Dispatcher remoto non bilancia il carico delle richieste degli advisor sui server remoti. Tuttavia, gli advisor remoti funzionano correttamente se si utilizzano i metodi di inoltro cbr o nat di Dispatcher.
- Se si utilizza GRE (generic routing encapsulation) per indirizzare il traffico su un server remoto senza la presenza di un Dispatcher remoto nella configurazione, non esiste una limitazione sull'uso degli advisor quando si eseguono i metodi di inoltro mac, nat o cbr di Dispatcher su una piattaforma Linux. Per ulteriori informazioni su GRE, consultare “Supporto GRE (Generic Routing Encapsulation)” a pagina 227.

Sistemi Solaris

- Quando si utilizza un Dispatcher entry-point in esecuzione su una piattaforma Solaris in una configurazione WAN, è necessario utilizzare il metodo di configurazione arp anziché i metodi di configurazione executor ifconfig o dscontrol. Ad esempio:

```
arp -s my_cluster_address my_mac_address pub
```

- Le seguenti limitazioni riguardano la piattaforma Solaris:
 - Gli advisor WAN funzionano solo con il metodo arp della configurazione cluster.
 - Gli advisor dei server specifici del collegamento funzionano solo con il metodo arp della configurazione cluster.
 - Gli advisor dei server specifici del collegamento funzionano solo con il metodo arp della configurazione cluster. Quando si utilizzano advisor per i server specifici del collegamento, non posizionare Load Balancer sullo stesso server con l'applicazione specifica del collegamento.

Sistemi Windows

- Quando si utilizza un Dispatcher entry-point in esecuzione su una piattaforma Windows in una configurazione WAN, esiste un limite dell'uso degli advisor remoti. Con il metodo di inoltro mac di Dispatcher, gli advisor Windows vengono destinati direttamente all'indirizzo del server anziché del cluster. Poiché non vengono indirizzati al cluster, il Dispatcher remoto non bilancia il carico delle richieste degli advisor sui server remoti. Tuttavia, gli advisor remoti funzionano correttamente se si utilizzano i metodi di inoltro cbr o nat di Dispatcher.

Sui Dispatcher remoti: effettuare le seguenti procedure di configurazione per ogni indirizzo cluster remoto. Per una configurazione di disponibilità elevata sul Dispatcher remoto, eseguire queste operazioni su entrambe le macchine.

Sistemi AIX

- Dispatcher deve avere ciascun cluster configurato sull'interfaccia con una netmask 255.255.255.255, affinché gli advisor funzionino correttamente. Utilizzare uno dei seguenti formati di sintassi per configurare un cluster:
 - `ifconfig interface_name alias cluster_address netmask 255.255.255.255.`
Ad esempio,
`ifconfig en0 alias
10.10.10.99 netmask 255.255.255.255`
 - `dscontrol executor configure interface_address interface_name netmask.`
Ad esempio,
`dscontrol executor configure 204.67.172.72 en0 255.255.255.255`

Nota: sono obbligatori gli advisor in esecuzione su entrambi i Dispatcher, remoto e locale.

Sistemi HP-UX, Sistemi Linux, Solaris e Windows

- Non sono necessarie ulteriori procedure di configurazione.

Esempio di configurazione

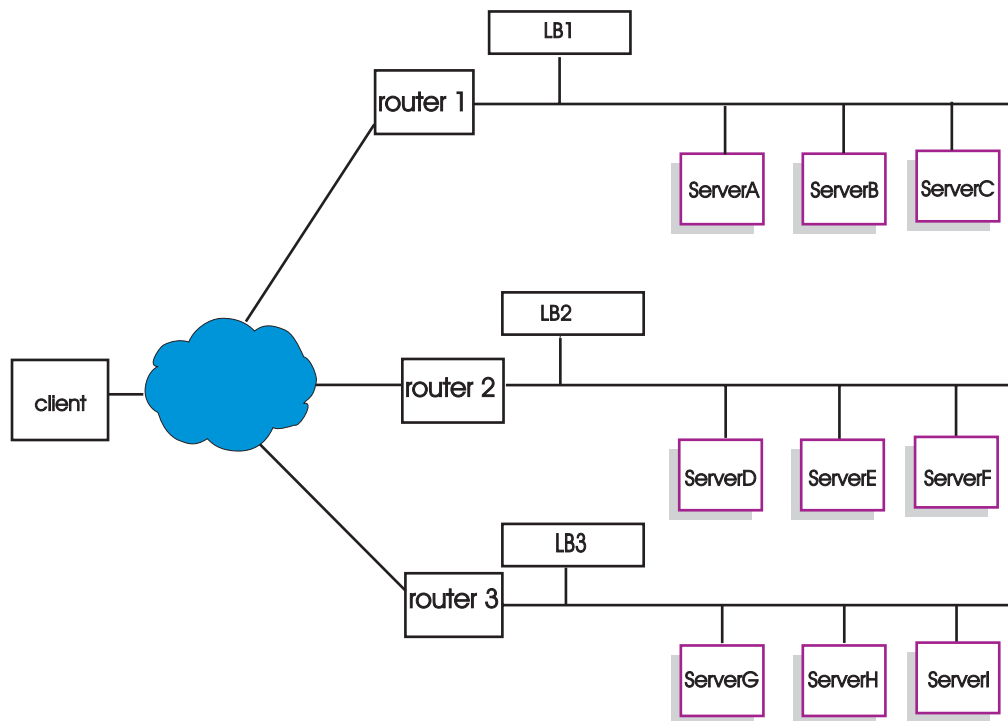


Figura 37. Configurazione di esempio di rete geografica con Load Balancer remoti

Questo esempio si applica alla configurazione illustrata nella Figura 37.

Di seguito viene spiegato come configurare le macchine Dispatcher per supportare l'indirizzo cluster xebec sulla porta 80. LB1 è il Load Balancer "entry-point". Viene utilizzata una connessione Ethernet. Notare che LB1 ha cinque server definiti: tre locali (ServerA, ServerB, ServerC) e due remoti (LB2 e LB3). I server remoti LB2 e LB3 hanno, ognuno, altri tre server locali definiti.

Sulla console del primo Dispatcher (LB1), eseguire queste operazioni:

1. Avviare l'executor.
dscontrol executor start
2. Impostare l'indirizzo di non inoltro della macchina Dispatcher.
dscontrol executor set nfa LB1
3. Definire il cluster.
dscontrol cluster add xebec
4. Definire la porta.
dscontrol port add xebec:80
5. Definire i server.
 - a. **dscontrol server add xebec:80:ServerA**
 - b. **dscontrol server add xebec:80:ServerB**
 - c. **dscontrol server add xebec:80:ServerC**
 - d. **dscontrol server add xebec:80:LB2 router Router1**
 - e. **dscontrol server add xebec:80:LB3 router Router1**
6. Configurare l'indirizzo cluster.

dscontrol executor configure xebec

Sulla console del secondo Dispatcher (LB2):

1. Avviare l'executor.
dscontrol executor start
2. Impostare l'indirizzo di non inoltro della macchina Dispatcher.
dscontrol executor set nfa LB2
3. Definire il cluster.
dscontrol cluster add xebec
4. Definire la porta.
dscontrol port add xebec:80
5. Definire i server.
 - a. **dscontrol server add xebec:80:ServerD**
 - b. **dscontrol server add xebec:80:ServerE**
 - c. **dscontrol server add xebec:80:ServerF**

Sulla console del terzo Dispatcher (LB3):

1. Avviare l'executor.
dscontrol executor start
2. Impostare l'indirizzo di non inoltro della macchina Dispatcher.
dscontrol executor set nfa LB3
3. Definire il cluster.
dscontrol cluster add xebec
4. Definire la porta.
dscontrol port add xebec:80
5. Definire i server.
 - a. **dscontrol server add xebec:80:ServerG**
 - b. **dscontrol server add xebec:80:ServerH**
 - c. **dscontrol server add xebec:80:ServerI**

Note

1. Su tutti i server (A-I), creare l'alias dell'indirizzo cluster sul loopback.
2. I cluster e le porte vengono aggiunti con **dscontrol** su tutte le macchine Dispatcher collegate: il Dispatcher entry-point e le macchine remote.
3. Vedere "Utilizzo di advisor remoti con il supporto rete geografica di Dispatcher" a pagina 223 per informazioni su come utilizzare gli advisor remoti con un supporto di rete geografica.
4. Il supporto di rete geografica impedisce i loop di instradamento infiniti. (Se una macchina Dispatcher riceve un pacchetto da un altro Dispatcher, non lo inoltra a un terzo Dispatcher.) La rete geografica supporta solo un livello di macchine remote.
5. La rete geografica supporta UDP e TCP.
6. La disponibilità elevata è disponibile anche sulle reti geografiche: ogni Dispatcher può disporre di una macchina di backup adiacente in standby (all'interno della stessa LAN).
7. Il gestore e gli advisor possono funzionare su una rete geografica e, se utilizzati, devono essere avviati su tutte le macchine Dispatcher collegate.

8. Load Balancer supporta le reti geografiche (WAN) esclusivamente con sistemi operativi simili.

Supporto GRE (Generic Routing Encapsulation)

GRE (Generic Routing Encapsulation) è un protocollo Internet specificato in RFC 1701 e RFC 1702. Con GRE, Load Balancer è in grado di racchiudere i pacchetti IP client all'interno dei pacchetti IP/GRE e inviarli alle piattaforme server, come ad esempio OS/390 che supportano GRE. Il supporto GRE permette al componente Dispatcher di bilanciare il carico dei pacchetti su più indirizzi server associati a un indirizzo MAC.

Load Balancer implementa GRE come parte della funzione WAN. Ciò permette a Load Balancer di bilanciare il carico della rete geografica direttamente su ciascun sistema server in grado di aprire i pacchetti GRE. Non è necessario che Load Balancer sia installato sul sito remoto se i server remoti supportano i pacchetti GRE racchiusi. Load Balancer racchiude i pacchetti WAN con il campo chiave GRE impostato sul valore decimale 3735928559.

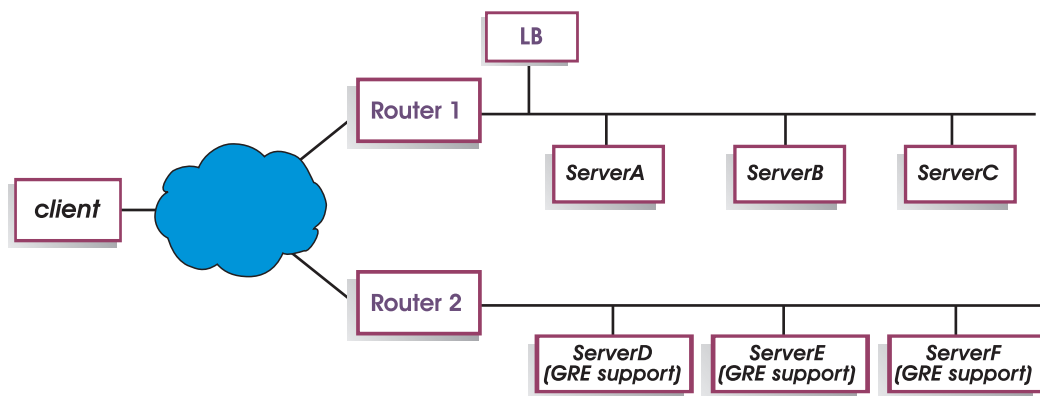


Figura 38. Configurazione di esempio di rete geografica con piattaforma server che supporta GRE

In questo esempio (Figura 38), per aggiungere il server ServerD remoto, che supporta GRE, definirlo nella configurazione di Load Balancer come se si stesse definendo un server WAN nella gerarchia cluster:port:server:

```
dscontrol server add cluster:port:ServerD router Router1
```

Su sistemi Linux, configurazione dell'incapsulamento GRE perWAN

Linux ha la capacità nativa di racchiudere GRE che consente a Load Balancer di bilanciare il carico delle immagini del server Linux/390, dove molte immagini server condividono un indirizzo MAC. Questo permette al Load Balancer entry-point di bilanciare il carico direttamente sui server WAN di Linux, senza passare per un Load Balancer in una posizione remota. Ciò consente agli advisor di Load Balancer entry-point di funzionare direttamente con ogni server remoto.

Su Load Balancer entry point, eseguire una configurazione come quella descritta per WAN.

Per configurare ogni server di back-end di Linux, emettere i seguenti comandi come root. (Questi comandi possono essere aggiunti alla funzionalità di avvio del sistema in modo che le modifiche vengano conservate anche con i successivi riavvii).

```
# modprobe ip_gre
# ip tunnel add gre-nd mode gre ikey 3735928559
# ip link set gre-nd up
# ip addr add cluster address dev gre-nd
```

Nota: il server Linux, configurato con queste istruzioni, *non deve* essere sullo stesso segmento fisico di Load Balancer entry-point. Questo perché il server Linux risponde alle richieste "ARP who-has" dell'indirizzo cluster determinando una condizione di competizione che potrebbe causare un "corto circuito" in cui tutto il traffico diretto all'indirizzo cluster viene indirizzato solo al vincitore della competizione ARP.

Utilizzo di un collegamento esplicito

Normalmente, le funzioni di bilanciamento del carico del Dispatcher funzionano indipendentemente dal contenuto dei siti su cui viene utilizzato il prodotto. Tuttavia, esiste un'area in cui i contenuti del sito assumono una grande importanza e dove le decisioni relative ai contenuti possono avere un impatto significativo sull'efficienza del Dispatcher. Ciò avviene nell'area di indirizzamento del collegamento.

Se le pagine specificano dei collegamenti che portano ai singoli server del sito, in effetti si sta forzando un client ad andare su una macchina in particolare ignorando, così, la funzione di bilanciamento del carico che potrebbe, altrimenti, essere attiva. Per questo motivo, si consiglia di utilizzare sempre l'indirizzo del Dispatcher in tutti i collegamenti presenti nelle pagine. Notare che il tipo di indirizzamento utilizzato potrebbe non sempre essere evidente se il sito utilizza la programmazione automatizzata che crea le HTML in modo dinamico. Per ottimizzare il bilanciamento del carico, bisognerebbe conoscere qualsiasi indirizzamento esplicito ed evitarlo laddove è possibile.

Utilizzo di una configurazione di rete privata

È possibile impostare le macchine del Dispatcher e del server TCP utilizzando una rete privata. Questa configurazione può ridurre il conflitto sulla rete pubblica o esterna e può avere conseguenze sulle prestazioni.

Per AIX, questa configurazione può trarre vantaggio dalle velocità elevate di High Performance Switch SP se le macchine del Dispatcher e del server TCP sono in esecuzione sui nodi in un Frame SP.

Per creare una rete privata, ogni macchina deve avere almeno due schede LAN, una delle quali collegata alla rete privata. È necessario, inoltre, configurare la seconda scheda LAN su una rete secondaria diversa. La macchina del Dispatcher invierà le richieste client alle macchine del server TCP attraverso la rete privata.

Su sistemi **Windows**: configurare l'indirizzo di non inoltrare mediante il comando `executor configure`.

I server aggiunti con il comando **dscontrol server add** devono essere aggiunti mediante gli indirizzi di rete privati; ad esempio, facendo riferimento all'esempio del server Apple nella Figura 39 a pagina 229, il comando dovrebbe essere codificato come:

```
dscontrol server add cluster_address:80:10.0.0.1
```

non

```
dscontrol server add cluster_address:80:9.67.131.18
```

Se si sta utilizzando Site Selector per fornire al Dispatcher informazioni sul carico, configurare Site Selector per notificare i carichi sugli indirizzi privati.

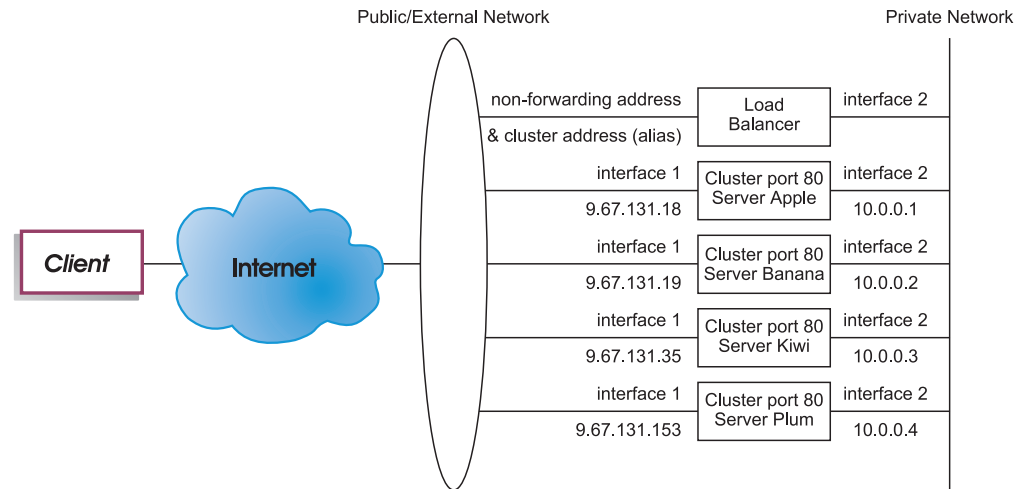


Figura 39. Esempio di una rete privata che utilizza Dispatcher

L'uso di una configurazione di rete privata si applica esclusivamente al componente Dispatcher.

Utilizzo del cluster jolly per combinare le configurazioni di server

L'uso di un cluster jolly per combinare le configurazioni dei server si applica esclusivamente al componente Dispatcher.

Il "carattere jolly" fa riferimento alla capacità del cluster di corrispondere a diversi indirizzi IP (vale a dire, agisce da jolly). L'indirizzo cluster 0.0.0.0 viene utilizzato per specificare un cluster jolly.

Se si dispone di molti indirizzi cluster da bilanciare e le configurazioni porta/server sono identiche per tutti i cluster, si possono combinare tutti i cluster in un'unica configurazione di cluster jolly.

È necessario configurare esplicitamente ogni indirizzo cluster su uno degli adattatori di rete della stazione di lavoro del Dispatcher. Non aggiungere nessun indirizzo cluster alla configurazione Dispatcher mediante il comando di aggiunta cluster dscontrol.

Aggiungere solo il cluster jolly (indirizzo 0.0.0.0) e configurare le porte e i server per il bilanciamento del carico. Il traffico indirizzato a qualsiasi indirizzo configurato degli adattatori verrà bilanciato mediante la configurazione del cluster jolly.

Un vantaggio di questo approccio è dato dal fatto che il traffico, diretto a tutti gli indirizzi cluster, viene preso in considerazione quando si sceglie il miglior server da raggiungere. Se un cluster sta ricevendo molto traffico e ha creato molte connessioni attive su uno dei server, il traffico diretto ad altri indirizzi cluster verrà bilanciato mediante queste informazioni.

Si possono combinare i cluster jolly con i cluster effettivi se vi sono alcuni indirizzi cluster con configurazioni porta/server univoche e altri con configurazioni comuni. Le configurazioni univoche devono essere assegnate ognuna a un indirizzo cluster effettivo. Tutte le configurazioni comuni possono essere assegnate a un cluster jolly.

Utilizzo di cluster jolly per bilanciare il carico dei firewall

L'uso di un cluster jolly per bilanciare il carico dei firewall si applica esclusivamente al componente Dispatcher. L'indirizzo cluster 0.0.0.0 viene utilizzato per specificare un cluster jolly.

Il cluster jolly si può utilizzare per bilanciare il traffico verso gli indirizzi che non sono configurati esplicitamente su nessun adattatore di rete della stazione di lavoro del Dispatcher. Affinché funzioni, il Dispatcher deve essere in grado di vedere tutto il traffico di cui deve bilanciare il carico. La stazione di lavoro del dispatcher non vedrà il traffico diretto agli indirizzi che non sono stati configurati esplicitamente su uno degli adattatori di rete, a meno che non sia impostato come instradamento predefinito per una parte del traffico.

Dopo aver configurato il Dispatcher come instradamento predefinito, il traffico TCP o UDP, in transito sulla macchina Dispatcher, verrà bilanciato mediante la configurazione del cluster jolly.

Un'applicazione ha lo scopo di bilanciare il carico dei firewall. Poiché i firewall possono elaborare pacchetti provenienti da diversi indirizzi e porte di destinazione, è necessario poter bilanciare il carico del traffico indipendentemente dalla porta e dall'indirizzo di destinazione.

I firewall vengono utilizzati per gestire il traffico proveniente da client non protetti e diretto a server protetti e le risposte provenienti da tali server, così come il traffico di client del lato protetto verso i server del lato non protetto e le relative risposte.

È necessario impostare due macchine Dispatcher, una per bilanciare il carico del traffico non protetto su indirizzi firewall non protetti ed un'altra per bilanciare il carico del traffico protetto su indirizzi firewall protetti. Poiché entrambi i Dispatcher devono utilizzare il cluster e la porta jolly con diversi gruppi di indirizzi server, i due Dispatcher devono trovarsi su due stazioni di lavoro separate.

Utilizzo del cluster jolly con Caching Proxy per proxy trasparente

L'uso del cluster jolly con Caching Proxy per proxy trasparente si applica esclusivamente al componente Dispatcher. L'indirizzo cluster 0.0.0.0 viene utilizzato per specificare un cluster jolly.

La funzione cluster jolly consente di utilizzare Dispatcher per abilitare la funzione proxy trasparente per un server Caching Proxy che si trova sulla stessa macchina del Dispatcher. Questa è una funzione esclusiva di AIX, in quanto ci deve essere comunicazione dal componente dispatcher al componente TCP del sistema operativo.

Per abilitare questa funzione, è necessario avviare l'ascolto di Caching Proxy delle richieste client sulla porta 80. Configurare, quindi, un cluster jolly (0.0.0.0). Nel cluster jolly, configurare la porta 80. Sulla porta 80, configurare NFA della macchina Dispatcher come server unico. A questo punto, il traffico client verso

qualsiasi indirizzo della porta 80 verrà distribuito sul server Caching Proxy in esecuzione sulla stazione di lavoro Dispatcher. La richiesta client verrà inviata tramite proxy, come di norma, e la risposta verrà restituita al client da Caching Proxy. In questo modo, il componente Dispatcher non esegue nessun bilanciamento del carico.

Utilizzo della porta jolly per indirizzare il traffico per una porta non configurata

La porta jolly può essere utilizzata per gestire il traffico che non è destinato ad una porta configurata esplicitamente. Uno di questi usi è per il bilanciamento del carico dei firewall. Un secondo uso è quello di garantire che il traffico, diretto su una porta non configurata, venga gestito in modo appropriato. Definendo una porta jolly senza server, si garantisce che qualsiasi richiesta a una porta, che non è stata configurata, verrà scartata anziché rimandata indietro al sistema operativo. Il numero di porta 0 (zero) indica una porta jolly, ad esempio:

```
dscontrol port add cluster:0
```

Porta jolly per la gestione del traffico FTP

Quando si configura un cluster per gestire l'FTP passivo e la porta jolly, l'FTP passivo utilizza per impostazione predefinita l'intero intervallo di porte TCP non privilegiato per la connessione dei dati. Ciò vuol dire che un client, con una connessione esistente che passa per un cluster di bilanciamento del carico e arriva a una porta di controllo FTP, avrà connessioni di controllo e le connessioni con numero di porta elevato (porta >1023), destinate allo stesso cluster, automaticamente indirizzate da Load Balancer verso lo stesso server della connessione di controllo FTP.

Se la porta jolly e la porta FTP sullo stesso cluster non hanno lo stesso gruppo di server, le applicazioni con numero di porta elevato (porta >1023) potrebbero non funzionare correttamente se un client utilizza una connessione di controllo FTP esistente. Quindi, non è consigliabile configurare diversi gruppi di server per le porte jolly e FTP sullo stesso cluster. Se si vuole questo tipo di scenario, impostare l'intervallo di porte passive del daemon FTP nella configurazione Load Balancer.

Rilevamento attacco di tipo Denial of service

Questa funzione è disponibile esclusivamente per il componente Dispatcher.

Dispatcher consente di rilevare potenziali attacchi di tipo "denial of service" e di avvisare gli amministratori tramite un avviso. Dispatcher fa questo analizzando le richieste in entrata per una grande quantità di connessioni TCP solo parzialmente aperte sui server, caratteristica comune agli attacchi di tipo denial of service. In un attacco di tipo denial of service, un sito riceve una grande quantità di pacchetti SYN provenienti da un gran numero di indirizzi IP di origine e numeri di porta di origine, ma il sito non riceve altri pacchetti per le connessioni TCP. Ciò determina un gran numero di connessioni TCP aperte a metà sui server e, nel tempo, i server possono diventare molto lenti e rifiutare nuove connessioni in arrivo.

Nota: deve esserci traffico in entrata attraverso la porta e il cluster, che sono sotto attacco, affinché Dispatcher stabilisca la fine di un attacco di tipo denial of service. Questo perché Dispatcher non stabilisce la fine di un attacco fino a quando il traffico non inizia a fluire di nuovo.

Load Balancer fornisce uscite utente che attivano script personalizzabili in grado di avvisare l'amministratore di un possibile attacco di tipo denial of service.

Dispatcher fornisce i seguenti file di script di esempio nella directory

...ibm/edge/lb/servers/samples:

- halfOpenAlert — è stato rilevato un possibile attacco DoS (denial of service)
- halfOpenAlertDone — l'attacco DoS è terminato

Per poter eseguire i file, è necessario spostarli sulla directory **...ibm/edge/lb/servers/bin** e rimuovere l'estensione ".sample".

Per implementare il rilevamento di attacchi DoS, impostare il parametro **maxhalfopen** sul comando **dscontrol port**, come riportato di seguito:

```
dscontrol port set 127.40.56.1:80 maxhalfopen 1000
```

Nell'esempio precedente, Dispatcher confronta il numero totale corrente di connessioni aperte a metà (per tutti i server che si trovano sul cluster 127.40.56.1 sulla porta 80) con il valore soglia uguale a 1000 (specificato dal parametro maxhalfopen). Se le connessioni correnti aperte a metà superano la soglia, viene effettuata una chiamata a uno script di avviso (halfOpenAlert). Quando il numero di connessioni aperte a metà scende sotto la soglia, si effettua una chiamata a un altro script di avviso (halfOpenAlertDone) per indicare che l'attacco è finito.

Per stabilire come impostare il valore maxhalfopen: eseguire periodicamente (forse ogni 10 minuti) un report di connessioni aperte a metà (**dscontrol port halfopenaddressreport cluster:port**) se il sito sta sostenendo un traffico che da normale tende ad essere intenso. Il report di connessioni aperte a metà restituisce il numero "totale di connessioni ricevute aperte a metà". È consigliabile impostare maxhalfopen su un valore che sia tra il 50 e il 200% superiore al numero massimo di connessioni aperte a metà sostenute dal sito.

Oltre ai dati statistici riportati, halfopenaddressreport genera anche delle voci nel log (**..ibm/edge/lb/servers/logs/dispatcher/halfOpen.log**) per tutti gli indirizzi client (fino a 8000 coppie indirizzi circa) che hanno accesso a server con connessioni aperte a metà.

Nota: è presente una trap di SNMP corrispondente agli script halfOpenAlert e halfOpenAlertDone. Se l'agente SNMP è configurato e in esecuzione, le trap corrispondenti verranno inviate nelle stesse condizioni che attivano gli script. Per maggiori informazioni sull'agente secondario SNMP, vedere "Uso del protocollo SNMP (Simple Network Management Protocol) con il componente Dispatcher" a pagina 261.

Per una maggiore protezione dagli attacchi di tipo denial of service per i server di backend, è possibile configurare porte e cluster jolly. In particolare, in ogni cluster configurato, aggiungere una porta jolly senza server. Aggiungere anche un cluster jolly con una porta jolly senza server. In questo modo, verranno scartati tutti i pacchetti che non sono indirizzati a una porta e a un cluster non jolly. Per informazioni sulle porte e sui cluster jolly, vedere "Utilizzo del cluster jolly per combinare le configurazioni di server" a pagina 229 e "Utilizzo della porta jolly per indirizzare il traffico per una porta non configurata" a pagina 231.

Uso della registrazione binaria per analizzare le statistiche dei server

Nota: la funzione registrazione binaria si applica esclusivamente ai componenti Dispatcher e CBR.

La funzione di registrazione binaria consente di memorizzare le informazioni sui server in file binari. È quindi possibile elaborare tali file per analizzare le informazioni sui server che sono state raccolte nel corso del tempo.

Nel log binario di ciascun server definito nella configurazione vengono memorizzate le seguenti informazioni.

- Indirizzo del cluster
- Numero di porta
- ID server
- Indirizzo del server
- Peso del server
- Numero totale di connessioni del server
- Connessioni attive del server
- Carico della porta del server
- Carico del sistema del server

Parte di queste informazioni viene richiamata dall'executor come parte del ciclo del gestore. Per questo, il gestore deve essere in esecuzione affinché le informazioni vengano registrate sui file di log binari.

Utilizzare il gruppo di comandi **dscontrol binlog** per configurare la registrazione binaria.

- binlog start
- binlog stop
- binlog set interval <second>
- binlog set retention <hours>
- binlog status

L'opzione start avvia la registrazione delle informazioni sui server sui log binari nella directory dei log. All'inizio di ogni nuova ora viene creato un log, il cui nome è composto dalla data e dall'ora.

L'opzione stop arresta la registrazione delle informazioni sui server sui log binari. Il servizio di registrazione viene arrestato per impostazione predefinita.

L'opzione set interval controlla la frequenza con cui le informazioni vengono scritte sui log. Il gestore invia le informazioni sui server al server di log a ogni intervallo specificato. Le informazioni vengono scritte sui log solo se l'intervallo di registrazione specificato, espresso in secondi, è scaduto dall'ultima volta che un record è stato scritto sul log. Per impostazione predefinita, l'intervallo di registrazione è impostato a 60 secondi. Le impostazioni dell'intervallo di invio delle informazioni da parte del gestore e dell'intervallo di registrazione interagiscono in una certa misura. Poiché la frequenza con cui il server dei log riceve le informazioni non è superiore all'intervallo di invio delle informazioni da parte del gestore, espresso in secondi, impostare l'intervallo di registrazione su un valore inferiore a quello dell'intervallo di invio delle informazioni da parte del gestore significa in pratica impostarlo sul suo stesso valore. Questa tecnica di registrazione consente di acquisire le informazioni sui server a qualsiasi granularità. È possibile acquisire tutte le modifiche alle informazioni sui server di cui viene a conoscenza il gestore per calcolare i pesi dei server. Tuttavia, probabilmente questa quantità di informazioni non è necessaria per analizzare l'utilizzo dei server e i relativi andamenti. La registrazione delle informazioni sui

server ogni 60 secondi consente di ottenere istantanee di informazioni relative ai server nel corso del tempo. L'impostazione dell'intervallo di registrazione su un valore molto basso può generare quantitativi eccessivi di dati.

L'opzione `set retention` controlla per quanto tempo i file di log vengono mantenuti. I file di log, la cui ora di creazione precede il tempo specificato da questa opzione, vengono eliminati dal server dei log. Ciò avviene se il server di log viene richiamato dal gestore; quindi, arrestando il gestore, i vecchi file di log non verranno eliminati.

L'opzione `status` restituisce le impostazioni correnti del servizio di log. Tali impostazioni indicano se il servizio è stato avviato, definiscono l'intervallo e le ore di archiviazione.

Un programma Java e un file dei comandi di esempio sono forniti nella directory **...ibm/edge/lb/servers/samples/BinaryLog**. L'esempio illustra come richiamare tutte le informazioni dai file di log e stamparle sullo schermo. Può essere personalizzato al fine di eseguire qualsiasi tipo di analisi sui dati. Un esempio che utilizza lo script e il programma forniti per dispatcher sarebbe:

```
dslogreport 2001/05/01 8:00 2001/05/01 17:00
```

per ottenere un report delle informazioni sui server del componente Dispatcher dalle 8:00 di mattina alle 5:00 del pomeriggio, nel giorno del primo maggio 2001. (Per CBR, utilizzare **cbrlogreport**.)

Utilizzo di un client posizionato

Solo i sistemi Linux supportano le configurazioni in cui un client si trova sulla stessa macchina di Load Balancer.

Le configurazioni client posizionate potrebbero non funzionare correttamente su altre piattaforme in quanto Load Balancer utilizza tecniche differenti per esaminare i pacchetti in entrata sui diversi sistemi operativi supportati. Nella maggior parte dei casi, su sistemi diversi da Linux, Load Balancer non riceve i pacchetti dalla macchina locale. Esso riceve i pacchetti in entrata solo dalla rete. Per questo motivo, le richieste effettuate all'indirizzo del cluster dalla macchina locale non sono ricevute da Load Balancer e non possono essere soddisfatte.

Capitolo 23. Funzioni avanzate di Controller Cisco CSS e Controller Nortel Alteon

Questo capitolo include le seguenti sezioni:

- “Posizionamento”
- “Disponibilità elevata”
- “Ottimizzazione del bilanciamento del carico in Load Balancer” a pagina 238
- “Advisor” a pagina 240
- “Metric Server” a pagina 245
- “Uso della registrazione binaria per analizzare le statistiche dei server” a pagina 247
- “Uso degli script per generare un avviso o registrare un malfunzionamento dei server” a pagina 249

Nota: in questo capitolo **xxxcontrol** viene utilizzato per indicare **ccocontrol** per Controller Cisco CSS e **nalcontrol** per Controller Nortel Alteon.

Posizionamento

Controller Cisco CSS o Controller Nortel Alteon possono risiedere sulla medesima macchina di un server per cui si sta effettuando il bilanciamento di carico delle richieste. Questa operazione viene comunemente denominata come *posizionamento* di un server. Non sono necessarie ulteriori procedure di configurazione.

Nota: nei periodi di traffico intenso, un server posizionato compete con Load Balancer per l'utilizzo delle risorse. Tuttavia, in assenza di macchine sovraccariche, l'utilizzo di un server posizionato consente di ridurre il numero totale di macchine necessarie per configurare un sito con bilanciamento del carico.

Disponibilità elevata

La funzione di disponibilità elevata è ora disponibile per Controller Cisco CSS e Controller Nortel Alteon.

Per aumentare la tolleranza agli errori del controller, la funzione di disponibilità elevata contiene le seguenti caratteristiche:

- Meccanismo heartbeat per determinare la disponibilità dei controller partner. Gli heartbeat vengono scambiati tra indirizzi configurati sul comando **xxxcontrol highavailability add**. È possibile configurare l'intervallo durante cui vengono scambiati gli impulsi e l'intervallo di takeover, vale a dire quando il controller di backup diventa attivo e il controller attivo diventa di backup.
- Un elenco di destinazioni accessibili a cui ciascun controller deve essere in grado di accedere per calcolare i pesi e aggiornare lo switch. Per ulteriori informazioni, vedere “Rilevamento degli errori” a pagina 237.
- Logica che consente di designare il controller attivo in base alle informazioni sulla disponibilità e sulle destinazioni accessibili.
- Strategia di takeover configurabile utilizzata per determinare le modalità con cui un controller di backup diventa attivo e il suo partner di backup.

- Meccanismo manuale di takeover per la gestione dei controller attivi.
- Report che visualizzano il ruolo, lo stato, la sincronizzazione del controller corrente e varie altre caratteristiche.

Configurazione

Vedere “ccocontrol highavailability — controlla la disponibilità elevata” a pagina 427 e “nalcontrol highavailability — controlla la disponibilità elevata” a pagina 445 per la sintassi completa di **xxxcontrol highavailability**.

Per configurare la disponibilità elevata del controller:

1. Avviare il server controller su entrambe le macchine controller.
2. Applicare a ciascun controller la medesima configurazione.
3. Configurare il ruolo, l'indirizzo e l'indirizzo partner della funzione di disponibilità elevata sul controller locale come indicato di seguito:

```
xxxcontrol highavailability add address 10.10.10.10  
partneraddress 10.10.10.20 port 143 role primary
```

4. Configurare il ruolo, l'indirizzo e l'indirizzo partner della funzione di disponibilità elevata sul controller partner come indicato di seguito:

```
xxxcontrol highavailability add address 10.10.10.20  
partneraddress 10.10.10.10 port 143 role secondary
```

I parametri address e partneraddress sono invertiti sulla macchina primaria e su quella secondaria.

5. Facoltativamente, configurare i parametri della disponibilità elevata sui controller locale e partner, ad esempio:
6. Facoltativamente configurare le destinazioni finali sui controller locale e partner nel modo indicato di seguito:

```
xxxcontrol highavailability set beatinterval 1000  
xxxcontrol highavailability usereach 10.20.20.20
```

Configurare lo stesso numero di destinazioni finali sia sul controller locale che sul controller partner.

7. Avviare il componente di disponibilità elevata e definire la strategia di ripristino sui controller locale e partner nel modo indicato di seguito:
8. Facoltativamente visualizzare le informazioni sulla funzione di disponibilità elevata sui controller locale e partner nel modo indicato di seguito:
9. Facoltativamente, specificare la strategia di takeover in modo che il controller in standby diventi il controller attivo e viceversa nel modo indicato di seguito:

```
xxxcontrol highavailability start auto  
xxxcontrol highavailability report  
xxxcontrol highavailability takeover
```

Necessario solo a fini di gestione.

Note:

1. Per configurare un singolo controller senza la disponibilità elevata, non immettere alcun comando di disponibilità elevata.
2. Per trasformare due controller in un unico controller in una configurazione di disponibilità elevata, arrestare anzitutto la funzione di disponibilità elevata sul controller in standby, quindi arrestarla sul controller attivo.
3. Quando si eseguono due controller in una configurazione di disponibilità elevata, si possono ottenere dei risultati imprevisti se una delle proprietà dei

controller differisce tra uno switch e l'altro; ad esempio, switch consultantid, switch address e così via. Si possono ottenere risultati inaspettati anche quando le proprietà di disponibilità elevata dei controller non corrispondono, ad esempio, port, role, reach targets, beatinterval, takeoverinterval e recovery strategy.

Rilevamento degli errori

Oltre alla mancanza di connettività tra il controller attivo e il controller in standby, che viene rilevata tramite i messaggi di heartbeat, l'*accessibilità* è un altro meccanismo di rilevamento errori.

Quando si configura la funzione di disponibilità elevata dei controller, è possibile fornire un elenco di host a cui i controller devono accedere per poter funzionare correttamente. Occorre almeno un host per ciascuna sottorete che verrà utilizzata dalla macchina controller. Questi host possono essere router, server IP o altri tipi di host.

L'accessibilità degli host è ottenuta grazie all'advisor reach che esegue il ping sull'host. Se i messaggi heartbeat non possono essere trasmessi o se i criteri di accessibilità vengono soddisfatti in maniera ottimale dal controller in standby anziché dal controller attivo, si verifica uno scambio di ruoli. Per prendere questa decisione in base a tutte le informazioni disponibili, il controller attivo invia regolarmente informazioni sulle proprie capacità di accessibilità al controller in standby e viceversa. Quindi, i controller confrontano le proprie informazioni sull'accessibilità con le informazioni del rispettivo partner e decidono chi deve attivarsi.

Strategia di ripristino

I ruoli delle due macchine controller sono configurati come principale e secondario. All'avvio i controller si scambiano informazioni fino a sincronizzare le relative macchine. A questo punto, il controller principale passa allo stato attivo e inizia a calcolare i pesi e ad aggiornare lo switch, mentre la macchina secondaria passa allo stato di standby e monitora la disponibilità della macchina principale.

In qualsiasi momento la macchina in standby rilevi un malfunzionamento della macchina attiva, la macchina in standby assume le funzioni di bilanciamento di carico della macchina attiva (guasta) e diventa essa stessa la macchina attiva. Quando la macchina principale diventa di nuovo operativa, le due macchine stabiliscono quale controller sarà quello attivo in base alla modalità di configurazione della strategia di ripristino.

Sono disponibili due tipi di strategia di ripristino:

Ripristino automatico

Il controller principale passa allo stato attivo, calcolando e aggiornando i pesi, non appena torna ad essere nuovamente operativo. La macchina secondaria passa allo stato di standby dopo che la macchina principale è diventata quella attiva.

Ripristino manuale

Il controller secondario attivo rimane nello stato attivo, anche dopo che il controller principale è diventato operativo.

Il controller principale passa allo stato di standby e richiede un intervento manuale per passare allo stato attivo.

Il parametro relativo alla strategia deve essere impostato sullo stesso valore su entrambe le macchine.

Esempi

Per gli esempi di configurazione della funzione di disponibilità elevata per Controller Cisco CSS, vedere “Esempi” a pagina 429.

Per gli esempi di configurazione della funzione di disponibilità elevata per Controller Nortel Alteon, vedere “Esempi” a pagina 447.

Ottimizzazione del bilanciamento del carico in Load Balancer

La funzione controller di Load Balancer esegue il bilanciamento del carico in base alle seguenti impostazioni:

- “Importanza attribuita alle informazioni metriche”
- “Pesi” a pagina 239
- “Tempi di inattività nel calcolo dei pesi” a pagina 239
- “Tempi di inattività dell’advisor” a pagina 241
- “Soglia di sensibilità” a pagina 239

Queste impostazioni possono essere modificate per ottimizzare il bilanciamento del carico nella rete in uso.

Importanza attribuita alle informazioni metriche

Nelle decisioni relative al calcolo dei pesi, il controller può utilizzare completamente o in parte gli strumenti di raccolta delle metriche elencati di seguito:

- *Connessioni attive*: il numero di connessioni attive su ciascuna macchina server con bilanciamento del carico richiamata dallo switch.
- *Frequenza di connessione*: il numero di nuove connessioni dall’ultima query eseguita su ciascuna macchina server con bilanciamento del carico richiamata dallo switch.
- *CPU*: la percentuale di CPU in uso su ciascuna macchina server con bilanciamento del carico (input dell’agente Metric Server).
- *Memoria*: la percentuale di memoria in uso (input dell’agente Metric Server) su ciascun server con bilanciamento del carico.
- *Metriche del sistema*: l’input degli strumenti di monitoraggio del sistema, ad esempio Metric Server o WLM.
- *Specifici dell’applicazione*: l’input degli advisor in ascolto sulla porta.

Le metriche predefinite sono *activeconn* e *connrate*.

È possibile modificare la proporzione di importanza da attribuire ai vari valori metrici. È opportuno considerare la proporzione come percentuale; la somma delle proporzioni deve essere uguale al 100%. Per impostazione predefinita, vengono utilizzate le metriche delle connessioni attive e le metriche delle nuove connessioni, in un rapporto pari a 50/50. Nell’ambiente in uso, può essere necessario tentare combinazioni diverse delle proporzioni attribuite alle varie metriche per individuare la combinazione che offra le prestazioni migliori.

Per impostare i valori delle proporzioni:

Per Cisco CSS Controller

cococontrol ownercontent metrics *metricName1 proportion1 metricName2 proportion2*

Per Controller Nortel Alteon

nalcontrol service metrics *metricName1 proportion1 metricName2 proportion2*

Pesi

I pesi vengono impostati in base ai tempi di risposta e alla disponibilità dell'applicazione, alle informazioni restituite dagli advisor e alle informazioni restituite dal programma di monitoraggio del sistema, ad esempio Metric Server. Per impostare i pesi manualmente, specificare l'opzione **fixedweight** per il server. Per una descrizione dell'opzione **fixedweight**, vedere "Pesi fissi dei controller".

I pesi vengono applicati a tutti i server che forniscono un servizio. Per ogni particolare porta, le richieste vengono distribuite tra i servizi in base ai loro pesi rispettivi. Ad esempio, se un server è impostato su un peso pari a 10 e l'altro su un peso pari a 5, il server impostato a 10 riceverà il doppio delle richieste del server impostato a 5.

Se un advisor rileva che un server è inattivo, il peso per tale server viene impostato a -1. Per Cisco CSS Controller e Controller Nortel Alteon, lo switch viene informato che il server non è disponibile e arresta l'assegnazione di connessioni al server.

Pesi fissi dei controller

Senza il controller, gli advisor non possono essere eseguiti e non possono rilevare se un server è inattivo. Se si sceglie di eseguire gli advisor, ma *non* si desidera che il controller aggiorni il peso impostato per un determinato server, utilizzare l'opzione **fixedweight** sul comando **cococontrol service** per Cisco CSS Controller o sul comando **nalcontrol server** per Controller Nortel Alteon.

Utilizzare il comando **fixedweight** per impostare il peso sul valore desiderato. Il valore del peso del server rimane fisso mentre il controller è in esecuzione finché non si immette un altro comando con **fixedweight** impostato su no.

Tempi di inattività nel calcolo dei pesi

Per ottimizzare le prestazioni complessive, è possibile limitare la frequenza di raccolta delle informazioni metriche.

Il tempo di inattività del consultant specifica la frequenza con cui il consultant aggiorna i pesi del server. Se il tempo di inattività del consultant è impostato su un valore troppo basso, le prestazioni possono ridursi notevolmente come conseguenza delle continue interruzioni dello switch da parte del consultant. Se il tempo di inattività del consultant è impostato su un valore troppo alto, il bilanciamento del carico dello switch non si basa su informazioni precise e aggiornate.

Ad esempio, per impostare il tempo di inattività del consultant su 1 secondo:

xxxcontrol consultant set *consultantID sleeptime interval*

Soglia di sensibilità

Per ottimizzare il bilanciamento del carico sui server, sono disponibili altri metodi. Per garantire la massima velocità, gli aggiornamenti dei pesi dei server vengono

eseguiti solo se i pesi sono stati modificati significativamente. Un aggiornamento continuo dei pesi quando lo stato dei server non viene sottoposto a modifiche di entità considerevole creerebbe solo un sovraccarico superfluo. Quando la variazione percentuale del peso complessivo di tutti i server che forniscono un servizio supera la soglia di sensibilità, i pesi utilizzati dal programma di bilanciamento del carico per distribuire le connessioni vengono aggiornati. Supporre, ad esempio, che il peso totale passi da 100 a 105. La variazione è del 5%. Se la soglia di sensibilità predefinita è 5, i pesi utilizzati dal programma di bilanciamento del carico non vengono aggiornati, in quanto la variazione in percentuale non **supera** la soglia. Tuttavia, se la variazione del peso totale passa da 100 a 106, i pesi vengono aggiornati. Per impostare la soglia di sensibilità del consultant su un valore diverso da quello predefinito, immettere il seguente comando:

```
xxxcontrol consultant set consultantID sensitivity percentageChange
```

Nella maggior parte dei casi, non è necessario modificare questo valore.

Advisor

Gli advisor sono agenti di Load Balancer. Il loro scopo è valutare lo stato e il carico delle macchine server. Questa operazione viene eseguita con uno scambio proattivo del tipo client con i server. Considerare gli advisor come client leggeri dei server delle applicazioni.

Nota: per un elenco dettagliato degli advisor, vedere “Elenco di advisor” a pagina 184.

Funzionamento degli advisor

Gli advisor aprono periodicamente una connessione TCP con ciascun server e inviano un messaggio di richiesta al server. Il contenuto del messaggio è specifico del protocollo in esecuzione sul server. Ad esempio, l’advisor HTTP invia una richiesta HTTP “HEAD” al server.

Quindi, gli advisor restano in ascolto di una risposta dal server. Dopo aver ricevuto la risposta, l’advisor esegue una valutazione del server. Per calcolare questo valore di *carico*, la maggior parte degli advisor misura il tempo impiegato dal server per rispondere, quindi utilizza questo valore, espresso in millisecondi, come valore del carico.

Gli advisor notificano il valore del carico alla funzione consultant, dove viene visualizzato nel report del consultant. Il consultant calcola i valori dei pesi aggregati provenienti da tutte le fonti, in base alle relative proporzioni, e invia tali valori dei pesi allo switch. Lo switch utilizza questi pesi per bilanciare il carico delle nuove connessioni client in arrivo.

Se l’advisor stabilisce che un server è attivo e funzionante, notifica al consultant un numero di carico positivo, diverso da zero. Se l’advisor stabilisce che un server non è attivo, restituisce un valore di carico particolare pari a meno uno (-1) per informare lo switch che il server è inattivo. Di conseguenza, lo switch non inoltra ulteriori connessioni a quel server finché il server non è tornato attivo.

Tempi di inattività dell'advisor

Nota: le impostazioni predefinite dell'advisor funzionano efficacemente nella maggior parte degli scenari possibili. Prestare massima attenzione quando si specificano dei valori diversi da quelli predefiniti.

Il tempo di inattività dell'advisor consente di impostare la frequenza con cui un advisor chiede lo stato dei server sulla porta su cui esegue il monitoraggio e notifica i risultati al consultant. Se il tempo di inattività dell'advisor è impostato su un valore troppo basso, le prestazioni possono ridursi notevolmente come conseguenza delle continue interruzioni dei server da parte dell'advisor. Se il tempo di inattività dell'advisor è impostato su un valore troppo alto, le decisioni relative ai pesi effettuate dal consultant non si basano su informazioni precise e aggiornate.

Ad esempio, per impostare l'intervallo dell'advisor HTTP a 3 secondi, immettere il seguente comando:

```
xxxcontrol metriccollector set consultantID:HTTP sleeptime 3
```

Timeout di connessione e timeout di ricezione dell'advisor per i server

È possibile impostare il tempo a disposizione di un advisor per individuare il malfunzionamento di una porta sul server o su un servizio. I valori di timeout per i server che non hanno funzionato correttamente, connecttimeout e receivetimeout, stabiliscono per quanto tempo l'advisor deve rimanere in attesa prima di notificare che l'operazione di connessione o l'operazione di ricezione non ha avuto buon esito.

Per ottenere il rilevamento più rapido dei server che non hanno funzionato correttamente, impostare i timeout di connessione e di ricezione dell'advisor sul valore più piccolo (un secondo) e impostare il tempo di inattività dell'advisor e del consultant sul valore più piccolo (un secondo).

Nota: se nell'ambiente di lavoro si osserva un volume di traffico medio-alto e il tempo di risposta del server aumenta, non impostare i valori di timeoutconnect e timeoutreceive su valori troppo piccoli. Se questi valori sono troppo piccoli, l'advisor potrebbe prematuramente contrassegnare come non funzionante un server occupato.

Per impostare il valore di timeoutconnect dell'advisor HTTP a 9 secondi, immettere il seguente comando:

```
xxxcontrol metriccollector set consultantID:HTTP timeoutconnect 9
```

Il valore predefinito del timeout di connessione e di ricezione è 3 volte il valore specificato per il tempo di inattività dell'advisor.

Tentativi dell'advisor

Gli advisor possono tentare nuovamente una connessione prima di contrassegnare come inattivo un server. L'advisor non contrassegna un server come inattivo finché la query eseguita sul server non ha avuto esito negativo per il numero di tentativi più 1. Se non specificato altrimenti, il valore predefinito del numero di tentativi è 0.

Per Cisco CSS Controller, impostare il valore dei **tentativi** tramite il comando **ccocontrol ownercontent set**. Per ulteriori informazioni, vedere “ccocontrol ownercontent — controlla il nome proprietario e la regola di contenuto” a pagina 432.

Per Nortel Alteon Controller, impostare il valore dei **tentativi** tramite il comando **nalcontrol service set**. Per ulteriori informazioni, vedere “nalcontrol service — configura un servizio” a pagina 452.

Creazione di advisor personalizzati

Nota: in questa sezione il termine **server** viene utilizzato genericamente per fare riferimento a un servizio di Cisco CSS Controller o a un server di Controller Nortel Alteon.

L’advisor personalizzato è una piccola parte di codice Java che l’utente deve fornire come file di classe e viene richiamato dal codice di base. Il codice di base fornisce tutti i servizi amministrativi, quali:

- Avvio e arresto di un’istanza dell’advisor personalizzato
- Fornitura dello stato e dei report
- Registrazione della cronologia in un file di log

Inoltre, notifica i risultati al consultant. Periodicamente, il codice di base esegue un ciclo di advisor, durante il quale valuta singolarmente lo stato di tutti i server della configurazione. Per prima cosa, apre una connessione a una macchina server. Se il socket viene aperto, il codice di base richiama il metodo (funzione) `getLoad` nell’advisor personalizzato. L’advisor personalizzato quindi esegue i passi necessari per valutare lo stato del server. In genere, invia al server un messaggio definito dall’utente e aspetta quindi una risposta. (L’accesso al socket aperto viene fornito all’advisor personalizzato.) Il codice di base chiude il socket con il server e notifica le informazioni sul carico al consultant.

Il codice di base e l’advisor personalizzato possono funzionare in modalità normale o in modalità di sostituzione. La scelta della modalità di funzionamento viene specificata nel file dell’advisor personalizzato come un parametro nel metodo del costruttore.

In modalità normale, l’advisor personalizzato scambia i dati con il server, il codice dell’advisor di base programma lo scambio e calcola il valore del carico. Il codice di base notifica quindi questo valore del carico al consultant. L’advisor personalizzato deve solo restituire uno zero (esito positivo) o meno uno (-1) (errore). Per specificare la modalità normale, l’indicatore di sostituzione nel costruttore è impostato su `false`.

In modalità di sostituzione, il codice di base non esegue alcuna misurazione temporizzata. Il codice dell’advisor personalizzato esegue qualsiasi operazione desiderata per i relativi requisiti univoci e restituisce un numero di carico effettivo. Il codice di base accetta il numero e lo notifica al consultant. Per ottenere risultati migliori, normalizzare i numeri del carico tra 10 e 1000; 10 indica un server veloce e 1000 indica un server lento. Per specificare la modalità di sostituzione, l’indicatore di sostituzione nel costruttore è impostato su `true`.

Questa funzione consente di scrivere i propri advisor in modo da fornire le informazioni precise sui server che sono necessarie. Un advisor personalizzato di esempio, **ADV_ctlrsample.java**, viene fornito per i controller. Dopo aver installato

Load Balancer, è possibile trovare il codice di esempio nella directory di installazione **...ibm/edge/lb/servers/samples/CustomAdvisors**.

Le directory di installazione predefinite sono:

- Su sistemi AIX, HP-UX, Linux e Solaris: `/opt/ibm/edge/lb`
- Su sistemi Windows: `C:\Program Files\IBM\ibm\edge\lb`

Nota: Se si aggiunge un advisor personalizzato a Cisco CSS Controller o Controller Nortel Alteon, è necessario arrestare e riavviare **ccoserver** o **nalserver** (per Windows, utilizzare Servizi) per consentire al processo Java di leggere i file di classe del nuovo advisor personalizzato. I file di classe dell'advisor personalizzato vengono caricati solo all'avvio.

Convenzione di denominazione

Il nome di file dell'advisor personalizzato deve essere scritto nel formato `ADV_myadvisor.java`. Il prefisso `ADV_` posto all'inizio deve essere scritto in maiuscolo. I restanti caratteri devono essere tutti in minuscolo.

In base alle convenzioni Java, il nome della classe definita nel file deve corrispondere al nome del file. Se si copia il codice di esempio, accertarsi di modificare tutte le istanze di `ADV_ctrlsample` all'interno del file in base al nuovo nome di classe.

Compilazione

Gli advisor personalizzati vengono scritti in linguaggio Java. Utilizzare il compilatore Java installato con Load Balancer. Durante la compilazione si fa riferimento ai seguenti file:

- File dell'advisor personalizzato
- I file di classe di base, `ibmlb.jar`, presenti nella directory di installazione **...ibm/edge/lb/servers/lib**.

Durante la compilazione, il percorso classe deve indicare il file dell'advisor personalizzato e il file delle classi di base.

Sulla piattaforma Windows, un comando di compilazione potrebbe essere:

```
dir_install/java/bin/javac -classpath  
dir_install\lb\servers\lib\ibmlb.jar ADV_pam.java
```

dove:

- Il file dell'advisor è denominato `ADV_pam.java`
- Il file dell'advisor è memorizzato nella directory corrente

L'output della compilazione è un file di classe, ad esempio:

`ADV_pam.class`

Prima di avviare l'advisor, copiare il file di classe sulla directory di installazione **...ibm/edge/lb/servers/lib/CustomAdvisors**.

Nota: se desiderato, gli advisor personalizzati possono essere compilati su un sistema operativo ed eseguiti su un altro sistema. Ad esempio, è possibile compilare l'advisor su un sistema Windows, copiare il file di classe (in formato binario) su una macchina AIX ed eseguirvi quindi l'advisor personalizzato.

Su sistemi AIX, HP-UX, Linux e Solaris, la sintassi è simile.

Esecuzione

Per eseguire l'advisor personalizzato, è necessario anzitutto copiare il file di classe sulla directory di installazione appropriata:

```
...ibm/edge/lb/servers/lib/CustomAdvisors/ADV_pam.class
```

Avviare il consultant, quindi immettere questo comando per avviare l'advisor personalizzato:

Per Controller Cisco CSS

```
cococontrol ownercontent metrics consultantID:ownerContentID pam 100
```

Per Controller Nortel Alteon

```
nalcontrol service metrics consultantID:serviceID pam 100
```

dove:

- pam è il nome dell'advisor, come in ADV_pam.java
- 100 è la proporzione del peso fornito a questo advisor

Routine richieste

Come tutti gli advisor, un advisor personalizzato estende la funzione dell'advisor di base, definito ADV_Base. L'advisor di base esegue la maggior parte delle funzioni dell'advisor, come ad esempio la notifica dei carichi al consultant affinché li utilizzi nell'algoritmo di valutazione. Inoltre, l'advisor di base effettua le operazioni di connessione e chiusura del socket e fornisce i metodi di invio e di ricezione che saranno utilizzati dall'advisor. L'advisor in sé viene utilizzato unicamente per l'invio e la ricezione dei dati sulla porta specifica del server esaminato. I metodi TCP interni all'advisor di base sono programmati per calcolare il carico. Se desiderato, un'indicatore all'interno del costruttore dell'advisor di base sostituisce il carico esistente con il nuovo carico restituito dall'advisor.

Nota: in base al valore impostato nel costruttore, l'advisor di base fornisce il carico all'algoritmo di valutazione a intervalli specificati. Se l'advisor effettivo non ha completato l'elaborazione e non può restituire un carico valido, l'advisor di base utilizza il carico inviato precedentemente.

I metodi di classe di base sono:

- Una routine **constructor**. Il costruttore richiama il costruttore della classe di base (vedere il file dell'advisor di esempio)
- Un metodo **ADV_AdvisorInitialize**. Questo metodo fornisce una possibile soluzione in caso siano necessarie ulteriori operazioni dopo che la classe di base ha completato la propria inizializzazione.
- Una routine **getLoad**. La classe dell'advisor di base esegue il socket aperto; quindi per completare il ciclo dell'advisor, getLoad deve generare soltanto le richieste di invio e di ricezione appropriate.

Ordine di ricerca

I controller consultano anzitutto l'elenco fornito di advisor nativi; se non vi trovano un determinato advisor, consultano l'elenco di advisor personalizzati.

Denominazione e percorso

- La classe dell'advisor personalizzato deve trovarsi all'interno della directory secondaria **...ibm/edge/lb/servers/lib/CustomAdvisors/** nella directory base di Load Balancer. I valori predefiniti di questa directory variano a seconda del sistema operativo:
 - Su sistemi AIX, HP-UX, Linux o Solaris
`/opt/ibm/edge/lb/servers/lib/CustomAdvisors/`
 - Sistemi Windows
`C:\Program Files\IBM\edge\lb\servers\lib\CustomAdvisors`
- È consentito utilizzare solo caratteri alfabetici in minuscolo. Ciò semplifica l'immissione dei comandi sulla riga comandi. Il nome del file dell'advisor deve essere preceduto dal prefisso **ADV_**.

Advisor di esempio

Il listato del programma di un advisor di esempio di un controller è riportato in "Advisor di esempio" a pagina 473. Dopo l'installazione, questo advisor di esempio può essere trovato nella directory **...ibm/edge/lb/servers/samples/CustomAdvisors**.

Metric Server

Metric Server fornisce informazioni sul carico dei server a Load Balancer sotto forma di metriche specifiche del sistema notificando lo stato dei server. Il consultant di Load Balancer interroga l'agente Metric Server che risiede su ciascun server, assegnando pesi al processo di bilanciamento del carico utilizzando le metriche raccolte dagli agenti. I risultati vengono quindi inseriti nel report servizio per Cisco CSS Controller o nel report server per Controller Nortel Alteon.

Prerequisiti

L'agente Metric Server deve essere installato e in esecuzione su tutti i server che sono sottoposti al bilanciamento del carico.

Modalità d'uso di Metric Server

Di seguito vengono riportati i passi necessari per configurare Metric Server per i controller.

- Lato controller
 1. Avviare **ccoserver** o **nalserver**.
 2. Per Controller Cisco CSS, aggiungere uno switch del consultant, quindi aggiungere ownercontent.
Per Controller Nortel Alteon, aggiungere uno switch del consultant, quindi aggiungere un service.
 3. Specificare la porta su cui l'agente Metric Server resta in ascolto. La porta specificata deve corrispondere alle informazioni immesse nel file `metricserver.cmd`. La porta predefinita è 10004. Utilizzare il seguente comando:

Per Controller Cisco CSS

```
ccocontrol service set consultantID:ownerContentID:serverID  
metricserverport portNumber
```

Per Controller Nortel Alteon

nalcontrol server set *consultantID:serviceID:serverID metricserverport
portNumber*

4. Immettere il comando delle metriche del sistema:

Per Controller Cisco CSS

cococontrol ownercontent metrics *consultantID:ownerContentID
metricName importance*

Per Controller Nortel Alteon

nalcontrol service metrics *consultantID:serviceID metricName
importance*

dove *metricName* è il nome dello script del server delle metriche.

Lo script delle metriche del sistema risiede sul server di backend e viene eseguito su ciascun server della configurazione nell'ownercontent o nel service specificati. È possibile utilizzare i due script forniti, **cpuload** e **memload**, oppure creare degli script personalizzati. Lo script contiene un comando che deve restituire un valore numerico. Questo valore numerico rappresenta una misura del carico e non un valore di disponibilità.

Limitazione: su sistemiWindows, se il nome dello script delle metriche del sistema ha un'estensione diversa da .exe, è necessario specificare il nome completo del file, ad esempio mySystemScript.bat. Si tratta di una limitazione Java.

5. Immettere il comando per il controller nel modo indicato di seguito:

Per Controller Cisco CSS

cococontrol consultant start

Per Controller Nortel Alteon

nalcontrol consultant start

Nota: garantire la sicurezza —

- Sulla macchina controller, creare dei file di chiavi utilizzando il comando **lbkeys create**. Per ulteriori informazioni su lbkeys, vedere "RMI (Remote Method Invocation)" a pagina 254.
 - Sulla macchina server, copiare il file di chiavi risultante nella directory **...ibm/edge/lb/admin/key**. Verificare che le autorizzazioni del file di chiavi consentano la lettura del file da parte della root.
- Agente Metric Server (lato macchina server)
 1. Installare il pacchetto Metric Server dall'installazione di Load Balancer.
 2. Controllare lo script **metricserver** nella directory **/usr/bin** per verificare che venga utilizzata la porta RMI desiderata. (Per sistemi Windows, la directory è C:\WINNT\SYSTEM32.) La porta RMI predefinita è 10004.

Nota: il valore della porta RMI specificata deve corrispondere al valore della porta RMI specificata per Metric Server sulla macchina controller.

3. Vengono forniti i due seguenti script: **cpuload** (restituisce la percentuale di CPU in uso con un valore compreso tra 0 e 100) e **memload** (restituisce la percentuale di memoria in uso con un valore compreso tra 0 e 100). Questi script risiedono nella directory **...ibm/edge/lb/ms/script**.

Facoltativamente, è possibile scrivere dei file script delle metriche personalizzati che definiscano il comando che Metric Server invierà alle macchine server. Accertarsi che gli script personalizzati siano eseguibili e posizionati nella directory **...ibm/edge/lb/ms/script**. Gli script personalizzati **devono** restituire un valore del carico numerico.

Nota: uno script delle metriche personalizzato deve essere un programma o script valido con estensione .bat o .cmd. In particolare, su Sistemi Linux e UNIX, gli script devono iniziare con la dichiarazione shell; altrimenti potrebbero non essere eseguiti correttamente.

4. Avviare l'agente immettendo il comando **metricsserver**.
5. Per arrestare l'agente Metric Server, immettere il comando **metricsserver stop**.

Per eseguire Metric Server su un indirizzo diverso dall'host locale, modificare il file **metricsserver** sulla macchina server con bilanciamento del carico. Nel file **metricsserver**, dopo **java**, inserire quanto segue:

```
-Djava.rmi.server.hostname=OTHER_ADDRESS
```

Inoltre, prima delle istruzioni "if" nel file **metricsserver**, aggiungere: **hostname OTHER_ADDRESS**.

Su sistemi Windows: creare l'alias di **OTHER_ADDRESS** sullo stack Microsoft. Per creare l'alias di un indirizzo sullo stack Microsoft, vedere a pagina 204.

Advisor WLM (Workload Manager)

WLM è il codice che viene eseguito sui mainframe MVS. È possibile eseguire delle query sul carico sulla macchina MVS.

Quando Workload Management MVS è stato configurato sul sistema OS/390, i controller possono accettare le informazioni sulla capacità provenienti da WLM e utilizzarle nel processo di bilanciamento del carico. Utilizzando l'advisor WLM, i controller aprono periodicamente le connessioni tramite la porta WLM su ciascun server nella tabella host del consultant e accettano i numeri interi sulla capacità che vengono restituiti. Poiché tali numeri interi rappresentano la capacità ancora disponibile e i consultant si aspettano al contrario i valori dei carichi di ciascuna macchina, i numeri interi della capacità vengono invertiti dall'advisor e normalizzati in valori del carico (ad esempio, un numero intero grande che rappresenta la capacità e un numero piccolo che rappresenta il carico indicano entrambi un server in buono stato di funzionamento). Numerose importanti differenze distinguono l'advisor WLM dagli altri advisor dei controller:

1. Gli altri advisor aprono delle connessioni ai server sulla stessa porta utilizzata per l'abituale traffico del client. L'advisor WLM apre le connessioni ai server su una porta diversa da quella utilizzata per il traffico abituale. L'agente WLM di ciascuna macchina server deve essere configurato per restare in ascolto sulla stessa porta su cui è stato avviato l'advisor WLM. La porta WLM predefinita è 10007.
2. È possibile utilizzare entrambi gli advisor specifici del protocollo con l'advisor WLM. Gli advisor specifici del protocollo eseguiranno la scansione ciclica dei server sulle porte su cui si svolge il traffico abituale, l'advisor WLM eseguirà la scansione ciclica del carico del sistema utilizzando la porta WLM.

Uso della registrazione binaria per analizzare le statistiche dei server

La funzione di registrazione binaria consente di memorizzare le informazioni sui server in file binari. È quindi possibile elaborare tali file per analizzare le informazioni sui server che sono state raccolte nel corso del tempo.

Nel log binario di ciascun server definito nella configurazione vengono memorizzate le seguenti informazioni.

- parent (ownercontentID per Cisco CSS Controller; serviceID per Controller Nortel Alteon)
- ID del server
- indirizzo del server
- porta del server
- peso del server
- numero di metriche configurate per questo server
- elenco dei valori delle metriche

Per poter registrare le informazioni sui log binari, il consultant deve essere in esecuzione.

Utilizzare il gruppo di comandi **xxxcontrol consultant binarylog** per configurare la registrazione binaria.

- binarylog start
- binarylog stop
- binarylog report
- binarylog set interval <seconds>
- binarylog set retention <hours>

L'opzione start avvia la registrazione delle informazioni sui server sui log binari nella directory dei log. All'inizio di ogni nuova ora viene creato un log, il cui nome è composto dalla data e dall'ora.

L'opzione stop arresta la registrazione delle informazioni sui server sui log binari. Il servizio di registrazione viene arrestato per impostazione predefinita.

L'opzione set interval controlla la frequenza con cui le informazioni vengono scritte sui log. Il consultant invia le informazioni sui server al server dei log a ogni intervallo specificato. Le informazioni vengono scritte sui log solo se l'intervallo di registrazione specificato, espresso in secondi, è scaduto dall'ultima volta che un record è stato scritto sul log. Per impostazione predefinita, l'intervallo di registrazione è impostato a 60 secondi.

Le impostazioni dell'intervallo di invio delle informazioni da parte del consultant e dell'intervallo di registrazione interagiscono in una certa misura. Poiché la frequenza con cui il server dei log riceve le informazioni non è superiore all'intervallo di invio delle informazioni da parte del consultant, espresso in secondi, impostare l'intervallo di registrazione su un valore inferiore a quello dell'intervallo di invio delle informazioni da parte del consultant significa in pratica impostarlo sul suo stesso valore.

Questa tecnica di registrazione consente di acquisire le informazioni sui server a qualsiasi granularità. È possibile acquisire tutte le modifiche alle informazioni sui server di cui viene a conoscenza il consultant per calcolare i pesi dei server; tuttavia, probabilmente questa quantità di informazioni non è necessaria per analizzare l'utilizzo dei server e i relativi andamenti. La registrazione delle informazioni sui server ogni 60 secondi consente di ottenere delle istantanee delle informazioni nel corso del tempo. L'impostazione dell'intervallo di registrazione su un valore molto basso può generare quantitativi eccessivi di dati.

L'opzione set retention controlla per quanto tempo i file di log vengono mantenuti. I file di log, la cui ora di creazione precede il tempo specificato da questa opzione,

vengono eliminati dal server dei log. Questa eliminazione viene eseguita solo se il server dei log viene richiamato dal consultant; quindi se si arresta il consultant, i file di log vecchi non vengono cancellati.

Un programma Java e un file dei comandi di esempio sono forniti nella directory **...ibm/edge/lb/servers/samples/BinaryLog**. L'esempio illustra come richiamare tutte le informazioni dai file di log e stamparle sullo schermo. Può essere personalizzato al fine di eseguire qualsiasi tipo di analisi desiderato sui dati.

Di seguito viene riportato un esempio che utilizza lo script e il programma forniti:

```
xxxlogreport 2002/05/01 8:00 2002/05/01 17:00
```

Ciò genera un report delle informazioni sui server da parte del controller dalle 8:00 della mattina alle 5:00 del pomeriggio, nel giorno del primo maggio 2002.

Uso degli script per generare un avviso o registrare un malfunzionamento dei server

Load Balancer fornisce uscite utente che attivano script personalizzabili. È possibile creare gli script per eseguire azioni automatizzate, quali avvisare un amministratore quando i server sono contrassegnati come inattivi o semplicemente registrare l'evento del malfunzionamento. Gli script di esempio, personalizzabili, si trovano nella directory di installazione **...ibm/edge/lb/servers/samples**. Per eseguire i file, copiarli sulla directory **...ibm/edge/lb/servers/bin**, quindi rinominare ciascun file in base alle istruzioni contenute nello script.

Vengono forniti i seguenti script di esempio, dove **xxx** sta per **cco** per Cisco CSS Controller e **nal** per Controller Nortel Alteon:

- **xxxserverdown** — un server è contrassegnato come inattivo dal controller.
- **xxxserverUp** — un server è contrassegnato come server di backup dal controller.
- **xxxallserversdown** — tutti i server sono contrassegnati come inattivi per un determinato servizio.

Parte 8. Gestione e risoluzione dei problemi di Load Balancer

Questa sezione contiene informazioni sulla gestione e sulla risoluzione dei problemi di Load Balancer. Contiene i seguenti capitoli:

- Capitolo 24, "Funzionamento e gestione di Load Balancer", a pagina 253
- Capitolo 25, "Risoluzione dei problemi", a pagina 273

Capitolo 24. Funzionamento e gestione di Load Balancer

Nota: se, durante la lettura di questo capitolo, nelle sezioni generali non specifiche di un particolare componente, *non* si sta utilizzando il componente Dispatcher, sostituire "dscontrol" e "dsserver" con quanto segue:

- Per CBR, utilizzare **cbrcontrol** e **cbrserver**
- Per Site Selector, utilizzare **sscontrol** e **ssserver**
- Per Cisco CSS Controller, utilizzare **ccocontrol** e **ccoserver**
- Per Nortel Alteon Controller, utilizzare **nalcontrol** e **nalserver**

IMPORTANTE: se si sta utilizzando l'installazione di Load Balancer per IPv4 e IPv6, consultare Capitolo 8, "Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6", a pagina 79 per evidenziare le limitazioni e le differenze di configurazione prima di esaminare i contenuti di questo capitolo.

Questo capitolo illustra il funzionamento e la gestione di Load Balancer e comprende le seguenti sezioni:

- "Amministrazione remota di Load Balancer"
 - "RMI (Remote Method Invocation)" a pagina 254
 - "Amministrazione basata sul Web" a pagina 255
- "Uso dei log di Load Balancer" a pagina 257
 - "Per Dispatcher, CBR e Site Selector" a pagina 257
 - "Per Cisco CSS Controller e Controller Nortel Alteon" a pagina 258
- "Uso del componente Dispatcher" a pagina 259
 - "Uso del protocollo SNMP (Simple Network Management Protocol) con il componente Dispatcher" a pagina 261
- "Uso del componente CBR (Content Based Routing)" a pagina 268
- "Uso del componente Site Selector" a pagina 269
- "Uso del componente Controller Cisco CSS" a pagina 269
- "Uso del componente Controller Nortel Alteon" a pagina 270

Amministrazione remota di Load Balancer

Load Balancer fornisce due diverse modalità per eseguire i programmi di configurazione su una macchina separata da quella in cui risiede Load Balancer. La comunicazione tra i programmi di configurazione (dscontrol, cbrcontrol, sscontrol, ccocontrol, nalcontrol) e il server (dsserver, cbrserver e così via) può essere stabilita utilizzando uno dei seguenti metodi:

- Java RMI (Remote Method Invocation)
- Amministrazione basata sul Web

Il vantaggio dell'uso dell'amministrazione remota con RMI rispetto all'amministrazione basata sul Web è rappresentato dalle prestazioni più veloci.

I vantaggi dell'uso dell'amministrazione basata sul Web consistono nel fatto che forniscono un'amministrazione remota, protetta e autenticata, in grado di comunicare con la macchina Load Balancer anche se è presente un firewall. Inoltre,

questo metodo di amministrazione *non* richiede l'installazione e l'uso di chiavi di autenticazione (lbkeys) sulla macchina client remota in comunicazione con la macchina Load Balancer.

RMI (Remote Method Invocation)

Per RMI, il comando per il collegamento a una macchina Load Balancer per l'amministrazione remota è **dscontrol host:remote_host**.

Se la chiamata RMI proviene da una macchina diversa da quella locale, deve verificarsi una sequenza di autenticazione della chiave pubblica/chiave privata la sequenza di autenticazione deve verificarsi prima di accettare il comando di configurazione.

La comunicazione tra i programmi di controllo in esecuzione sulla stessa macchina dei server del componente non viene autenticata.

Utilizzare il seguente comando per generare chiavi pubbliche e private da utilizzare per l'autenticazione remota:

lbkeys [create | delete]

Questo comando viene eseguito solo sulla stessa macchina di Load Balancer.

L'uso dell'opzione **create** crea una chiave privata nella directory delle chiavi dei server (...**ibm/edge/lb/servers/key/**) e crea le chiavi pubbliche nella directory delle chiavi di amministrazione (...**ibm/edge/lb/admin/keys/**) per ciascun componente Load Balancer. Il nome file della chiave pubblica è: *component-ServerAddress-RMIport*. Queste chiavi pubbliche devono quindi essere trasportate sui client remoti e inserite nella directory delle chiavi di amministrazione.

In una macchina Load Balancer con indirizzo nome host 10.0.0.25 che utilizza la porta RMI predefinita per ciascun componente, il comando **lbkeys create** genera i seguenti file:

- La chiave privata: ...**ibm/edge/lb/servers/key/authorization.key**
- Le chiavi pubbliche:
 - ...**ibm/edge/lb/admin/keys/dispatcher-10.0.0.25-10099.key**
 - ...**ibm/edge/lb/admin/keys/cbr-10.0.0.25-11099.key**
 - ...**ibm/edge/lb/admin/keys/ss-10.0.0.25-12099.key**
 - ...**ibm/edge/lb/admin/keys/cco-10.0.0.25-13099.key**
 - ...**ibm/edge/lb/admin/keys/na1-10.0.0.25-14099.key**

Il fileset di amministrazione è stato installato su un'altra macchina. I file delle chiavi pubbliche devono essere inseriti nella directory ...**ibm/edge/lb/admin/keys** sulla macchina client remota.

Il client remoto sarà, quindi, autorizzato a configurare Load Balancer su 10.0.0.25.

Le stesse chiavi devono essere utilizzate su tutti i client remoti che si desidera autorizzare per configurare Load Balancer su 10.0.0.25.

Se si dovesse eseguire nuovamente il comando **lbkeys create**, verrebbe generato un nuovo gruppo di chiavi pubbliche/private. Ciò significherebbe che tutti i client remoti a cui si tentasse di connettersi utilizzando le chiavi precedenti non

sarebbero autorizzati. La nuova chiave dovrebbe essere inserita nella directory corretta di quei client che si desidera autorizzare nuovamente.

Il comando **lbkeys delete** cancella le chiavi private e pubbliche sulla macchina server. Se queste chiavi vengono cancellate, non verrà autorizzato il collegamento dei client remoti ai server.

Per entrambi i comandi **lbkeys create** e **lbkeys delete** è disponibile un'opzione **force**. L'opzione **force** elimina i prompt dei comandi che richiedono se si desidera sovrascrivere o cancellare le chiavi esistenti.

Una volta stabilita la connessione RMI, è possibile comunicare tra i programmi di configurazione con i comandi **dscontrol**, **cbrcontrol**, **sscontrol**, **ccocontrol**, **nalcontrol**, **dswizard**, **cbrwizard** e **sswizard** da un prompt dei comandi. Inoltre, è possibile configurare Load Balancer dalla GUI, digitando **lbadmin** da un prompt dei comandi.

Nota: a causa delle modifiche apportate ai pacchetti di protezione nella versione Java, le chiavi Load Balancer generate per le release precedenti a v5.1.1 potrebbero non essere compatibili con le chiavi della release corrente, quindi è necessario generare nuovamente le chiavi al momento dell'installazione della nuova release.

Amministrazione basata sul Web

Requisiti

Per utilizzare l'amministrazione basata sul Web, la **macchina client** che esegue l'amministrazione remota deve disporre di quanto segue:

- JRE 1.3.0 (o superiore)
- Per informazioni sui browser supportati, fare riferimento alla seguente pagina Web: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>

Nota: Se si sta utilizzando Netscape, non ridimensionare la finestra del browser Netscape (riduzione, ingrandimento, ripristino in basso e così via) in cui viene visualizzata la GUI di Load Balancer. Poiché ogni volta che le finestre browser vengono ridimensionate Netscape ricarica una pagina, queste operazioni causeranno una disconnessione dall'host. Ogni volta che si ridimensionerà la finestra, sarà necessario riconnettersi all'host.

Quanto segue è necessario sulla **macchina host** a cui si accede per eseguire l'amministrazione remota basata sul Web:

- Caching Proxy V6
- Perl 5.5 (o superiore)

Configurazione di Caching Proxy

- Nel Caching Proxy, per creare certificati server SSL, è necessario il programma di utilità iKeyman (IBM Key Management) o altri programmi di utilità. (Per informazioni sulla modalità di creazione dei certificati, vedere *Caching Proxy Administration Guide*.)
- Nella sezione "Amministrazione basata sul Web di Load Balancer" del file di configurazione Caching Proxy (**ibmp proxy.conf**), aggiungere le seguenti direttive dopo aver definito i domini di protezione ma prima delle regole di mappatura:
Per i sistemi Windows —

```
Protect /lb-admin/lbwebaccess PROT-ADMIN
Exec /lb-admin/lbwebaccess C:\PROGRA~1\IBM\edge\lb\admin\lbwebaccess.pl
Pass /lb-admin/help/* C:\PROGRA~1\IBM\edge\lb\admin\help\*
Pass /lb-admin/*.jar C:\PROGRA~1\IBM\edge\lb\admin\lib\*.jar
Pass /lb-admin/* C:\PROGRA~1\IBM\edge\lb\admin\*
Pass /documentation/lang/* C:\PROGRA~1\IBM\edge\lb\documentation\lang/*
```

dove *lang* è la directory secondaria della lingua (ad esempio, en_US)

Sui Sistemi Linux e UNIX —

```
Protect /lb-admin/lbwebaccess PROT-ADMIN
Exec /lb-admin/lbwebaccess /opt/ibm/edge/lb/admin/lbwebaccess.pl
Pass /lb-admin/help/* /opt/ibm/edge/lb/admin/help/*
Pass /lb-admin/*.jar /opt/ibm/edge/lb/admin/lib/*.jar
Pass /lb-admin/* /opt/ibm/edge/lb/admin/*
Pass /documentation/lang/* /opt/ibm/edge/lb/documentation/lang/*
```

Nota: sui sistemi HP-UX, lo script lbwebaccess.pl presuppone che il file binario Perl si trovi nella directory /usr/bin/. (La prima riga dello script contiene `#!/usr/bin/perl`.) Aggiornare questo percorso directory con qualsiasi posizione in cui si trovi l'applicazione Perl. Un'altra opzione consiste nel creare un collegamento simbolico. Ad esempio, se Perl è installato in /opt/perl/bin/perl, emettere il comando:

```
ln -s /opt/perl/bin/perl /usr/bin/perl
```

Esecuzione e accesso all'amministrazione basata sul Web

Per eseguire l'amministrazione basata sul Web, è necessario avviarla sulla macchina host Load Balancer: immettere **lbwebaccess** dal prompt dei comandi della macchina host.

Sono necessari, inoltre, l'ID utente e la password della macchina host a cui si sta accendendo in modalità remota. L'ID utente e la password sono gli stessi dell'amministrazione Caching Proxy.

Per visualizzare l'amministrazione basata sul Web di Load Balancer, accedere al seguente URL sul browser Web dalla posizione remota:

```
http://host_name/lb-admin/lbadmin.html
```

Dove *host_name* è il nome della macchina a cui si sta accedendo per comunicare con Load Balancer.

Dopo aver caricato la pagina Web, verrà visualizzata la GUI di Load Balancer nella finestra browser per eseguire l'amministrazione basata sul Web.

Dalla GUI di Load Balancer è possibile, inoltre, immettere i comandi di controllo della configurazione. Per immettere un comando dalla GUI:

1. evidenziare il nodo Host dalla struttura ad albero della GUI
2. selezionare **Send command...** dal menu a comparsa Host
3. nel campo di immissione dei comandi, digitare il comando che si desidera eseguire. Ad esempio: **executor report**. I risultati e la cronologia dei comandi in esecuzione nella sessione corrente vengono visualizzati nella finestra fornita.

Aggiornamento della configurazione in modalità remota

Con l'amministrazione remota basata sul Web, se sono presenti più amministratori che aggiornano la configurazione Load Balancer da altre posizioni, sarà necessario aggiornare la configurazione per visualizzare (ad esempio) il cluster, la porta o il

server aggiunti (o eliminati) da un altro amministratore. La GUI dell'amministrazione remota basata sul Web fornisce le funzioni **Refresh Configuration** e **Refresh all Configurations**.

Dalla GUI basata sul Web, per aggiornare la configurazione

- di un Host: fare clic con il tasto destro del mouse su un nodo **Host** nella struttura ad albero della GUI e selezionare **Refresh Configuration**
- di tutti gli Host: selezionare **File** dal menu, quindi, selezionare **Refresh All Configurations**

Uso dei log di Load Balancer

Per Dispatcher, CBR e Site Selector

Load Balancer invia le voci a un log del server, a un log del gestore, a un log di monitoraggio delle metriche (registrazione delle comunicazioni con gli agenti Metric Server) e a un log di ciascun advisor utilizzato.

Nota: inoltre, solo per il componente Dispatcher, le voci possono essere generate su un log dell'agente secondario (SNMP).

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l'uso di Caching Proxy. Per ulteriori informazioni, vedere "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

È possibile impostare il livello di registrazione per definire l'estensione dei messaggi scritti sul log. A livello 0, gli errori vengono registrati e Load Balancer registra anche le intestazioni e i record degli eventi che si sono verificati una volta sola (ad esempio, un messaggio relativo all'inizio della scrittura dell'advisor sul log del gestore). Il livello 1 include le informazioni in fase di sviluppo e così via fino al livello 5 che include tutti i messaggi prodotti per facilitare, se necessario, il debug di un problema. Il valore predefinito per i log del gestore, dell'advisor, del server o dell'agente secondario è 1.

È possibile, inoltre, impostare la dimensione massima di un log. Se si imposta la dimensione massima del file di log, il file ripartirà dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive verranno scritte all'inizio del file, sovrascrivendo quindi le precedenti voci di log. Non è possibile impostare la dimensione del log su un valore inferiore a quello corrente. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte.

Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log. A livello 0, è probabilmente più sicuro lasciare la dimensione del log sul valore predefinito di 1MB; tuttavia, durante la registrazione a livello 3 e superiore, è necessario limitare la dimensione senza renderla troppo piccola per essere utile.

- Per configurare il livello di registrazione o la dimensione massima per un log del server, utilizzare il comando **dscontrol set**. (Per visualizzare le impostazioni del log del server, utilizzare il comando **dscontrol logstatus**.)
- Per configurare il livello di registrazione o la dimensione massima per un log del gestore, utilizzare il comando **dscontrol manager**.

- Per configurare il livello di registrazione o la dimensione massima per un log di monitoraggio delle metriche che registra le comunicazioni con gli agenti Metric Server, utilizzare il comando **dscontrol manager metric set**.
- Per configurare il livello di registrazione o la dimensione massima per un log dell'advisor, utilizzare il comando **dscontrol advisor**.
- Per configurare il livello di registrazione o la dimensione massima per un log dell'agente secondario, utilizzare il comando **dscontrol subagent**. (Il componente Dispatcher utilizza solo l'agente secondario SNMP.)

Modifica dei percorsi file di log

Per impostazione predefinita, i log generati da Load Balancer verranno memorizzati nella directory dei log dell'installazione Load Balancer. Per modificare questo percorso, impostare la variabile *lb_logdir* nello script dserver.

Su sistemi **AIX, HP-UX, Linux e Solaris**: lo script dserver si trova nella directory /usr/bin. In questo script, la variabile *lb_logdir* è impostata sulla directory predefinita. È possibile modificare questa variabile per specificare la directory di log. Esempio:

```
LB_LOGDIR=/path/to/my/logs/
```

Su sistemi **Windows**: il file dserver si trova nella directory di sistema Windows C:\WINNT\SYSTEM32, in Windows 2003. Nel file dserver, la variabile *lb_logdir* è impostata sulla directory predefinita. È possibile modificare questa variabile per specificare la directory di log. Esempio:

```
set LB_LOGDIR=c:\path\to\my\logs\
```

In tutti i sistemi operativi, verificare che non ci siano spazi ai lati del segno uguale e che il percorso termini con una barra ("/" o "\" come appropriato).

Registrazione binaria

Nota: la registrazione binaria non si applica al componente Site Selector.

La funzione di registrazione binaria di Load Balancer utilizza la stessa directory di log degli altri file di log. Vedere "Uso della registrazione binaria per analizzare le statistiche dei server" a pagina 232.

Per Cisco CSS Controller e Controller Nortel Alteon

È possibile impostare il livello di registrazione per definire l'estensione dei messaggi scritti sul log. A livello 0, gli errori vengono registrati e Load Balancer registra anche le intestazioni dei log e i record degli eventi che si sono verificati una volta sola (ad esempio, un messaggio relativo all'inizio della scrittura dell'advisor sul log del consultant). Il livello 1 include le informazioni in fase di sviluppo e così via fino al livello 5 che include tutti i messaggi prodotti per facilitare, se necessario, il debug di un problema. Il valore predefinito per il log è 1.

È possibile, inoltre, impostare la dimensione massima di un log. Se si imposta la dimensione massima del file di log, il file ripartirà dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive verranno scritte all'inizio del file, sovrascrivendo quindi le precedenti voci di log. Non è possibile impostare la dimensione del log su un valore inferiore a quello corrente. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte.

Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log. A livello 0, è probabilmente più sicuro lasciare la dimensione del log sul valore predefinito di 1MB; tuttavia, durante la registrazione a livello 3 e superiore, è necessario limitare la dimensione senza renderla troppo piccola per essere utile.

Log controller

Controller Cisco CSS e Controller Nortel Alteon hanno i seguenti log:

- log del controller (comando **controller set**)
- log del consultant (comando **consultant set**)
- log disponibilità elevata (comando **highavailability set**)
- log degli strumenti di raccolta (comando **metriccollector set**)
- log binario (comando **consultant binarylog**)

Quanto segue è un esempio di configurazione del livello di registrazione e della dimensione massima per un log di monitoraggio delle metriche che registra le comunicazioni con gli agenti Metric Server:

```
xxxcontrol metriccollector set consultantID:serviceID:metricName  
loglevel x logsize y
```

Modifica dei percorsi file di log

Per impostazione predefinita, i log generati dai controller verranno memorizzati nella directory dei log dell'installazione del controller. Per modificare questo percorso, impostare la variabile *xxx_logdir* nello script *xxxserver*.

Su sistemi **AIX, HP-UX, Linux e Solaris**: lo script *xxxserver* si trova nella directory */usr/bin*. In questo script, la variabile *xxx_logdir* è impostata sulla directory predefinita. È possibile modificare questa variabile per specificare la directory di log. Esempio:

```
xxx_LOGDIR=/path/to/my/logs/
```

Su sistemi **Windows**: il file *xxxserver* si trova nella directory del sistema Windows, generalmente *C:\WINNT\SYSTEM32*. Nel file *xxxserver*, la variabile *xxx_logdir* è impostata sulla directory predefinita. È possibile modificare questa variabile per specificare la directory di log. Esempio:

```
set xxx_LOGDIR=c:\path\to\my\logs\
```

In tutti i sistemi operativi, verificare che non ci siano spazi ai lati del segno uguale e che il percorso termini con una barra ("*/*" o "**" come appropriato).

Registrazione binaria

La funzione di registrazione binaria di Load Balancer utilizza la stessa directory di log degli altri file di log. Vedere "Uso della registrazione binaria per analizzare le statistiche dei server" a pagina 232.

Uso del componente Dispatcher

Questo capitolo illustra il funzionamento e la gestione del componente Dispatcher.

Avvio e arresto di Dispatcher

- Digitare **dsserver** su una riga comandi per avviare Dispatcher.
- Digitare **dsserver stop** su una riga comandi per arrestare Dispatcher.

Uso del valore timeout di inattività

In Load Balancer, le connessioni sono considerate inattive quando non ci sono attività su tale connessione per il numero di secondi specificato nel timeout di inattività. Se il numero di secondi è stato superato senza attività, Load Balancer rimuoverà quel record di connessioni dalle tabelle e il traffico successivo non verrà eliminato.

A livello della porta, ad esempio, è possibile specificare il valore di timeout di inattività sul comando **dscontrol port set staletimeout**.

Il timeout di inattività può essere impostato sui livelli executor, cluster e porta. Ai livelli dell'executor e del cluster, il valore predefinito è 300 secondi ed eseguirà il filtro sulla porta. A livello della porta, il valore predefinito dipende dalla porta. Alcune porte correttamente definite hanno diversi valori di timeout di inattività predefiniti. Ad esempio, la porta telnet 23 ha un valore predefinito di 259,200 secondi.

Alcuni servizi potrebbero avere propri valori di timeout di inattività. Ad esempio, LDAP (Lightweight Directory Access Protocol) ha un parametro di configurazione denominato **idletimeout**. Quando i secondi **idletimeout** vengono superati, la connessione client inattiva verrà chiusa. **Idletimeout** potrebbe essere impostato su 0, che indica che la connessione non verrà mai chiusa.

I problemi di connettività possono verificarsi quando il valore di timeout di inattività di Load Balancer è inferiore al valore di timeout del servizio. Nel caso di LDAP, il valore predefinito di **staletimeout** di Load Balancer è 300 secondi. In assenza di attività sulla connessione per 300 secondi, Load Balancer rimuoverà il record di connessione dalle tabelle. Se il valore **idletimeout** è maggiore di 300 secondi (o impostato su 0), il client potrà ritenere di avere una connessione con il server. Quando il client invia pacchetti, questi vengono eliminati da Load Balancer. Questo causerà la sospensione dell'LDAP quando viene effettuata una richiesta al server. Per evitare il problema, impostare **idletimeout** di LDAP su un valore diverso da zero inferiore o pari al valore **staletimeout** di Load Balancer.

Uso di **fintimeout** e **staletimeout** per controllare la pulizia dei record di connessioni

Un client invia un pacchetto FIN dopo aver inviato tutti i pacchetti in modo che il server rilevi il termine della transazione. Quando Dispatcher riceve il pacchetto FIN, contrassegna la transazione dallo stato attivo allo stato FIN. Quando una transazione è contrassegnata FIN, la memoria riservata alla connessione può essere cancellata.

Per migliorare le prestazioni dell'assegnazione dei record di connessione e del riutilizzo, utilizzare il comando **executor set fintimeout** per controllare il periodo durante il quale Dispatcher deve mantenere le connessioni nello stato FIN attive nelle tabelle Dispatcher e accettare il traffico. Una volta che la connessione nello stato FIN supera **fintimeout**, verrà rimossa dalle tabelle Dispatcher e sarà pronta per il nuovo uso. È possibile modificare il timeout FIN utilizzando il comando **dscontrol executor set fincount**.

Utilizzare il comando **dscontrol executor set staletimeout** per controllare il periodo durante il quale Dispatcher deve mantenere le connessioni nello stato Established (stabilita) quando non è stato rilevato traffico attivo nelle tabelle Dispatcher e accettare il traffico. Per ulteriori informazioni, consultare "Uso del valore timeout di inattività" a pagina 260.

Notifica GUI — Opzione del menu Monitor

In base alle informazioni ricevute dall'executor e ritrasmesse al gestore, è possibile visualizzare diversi grafici. (L'opzione del menu Monitor della GUI richiede che la funzione gestore sia in esecuzione):

- Connessioni al secondo per server (possono essere visualizzati più server sullo stesso grafico)
- Valori di calcolo dei pesi relativi per server su una porta particolare
- Durata di connessione media per server su una porta particolare

Uso del protocollo SNMP (Simple Network Management Protocol) con il componente Dispatcher

Un sistema di gestione della rete è un programma che viene eseguito in maniera continua ed è utilizzato per monitorare, riflettere lo stato e controllare una rete. Il protocollo SNMP (Simple Network Management Protocol), un protocollo comune utilizzato dai dispositivi di una rete per comunicare tra loro, è lo standard corrente per la gestione della rete. In genere, i dispositivi della rete dispongono di un *agente* SNMP e di uno o più agenti secondari. L'agente SNMP comunica con la *stazione di gestione della rete* o risponde alle richieste SNMP immesse sulla riga comandi. L'*agente secondario* SNMP richiama e aggiorna i dati, quindi li fornisce all'agente SNMP affinché possa rispondere al dispositivo che ha emesso la richiesta.

Dispatcher fornisce una *base dati MIB (Management Information Base)* SNMP (ibmNetDispatcherMIB) e un agente secondario SNMP. Ciò consente di utilizzare un qualsiasi sistema di gestione della rete, quale — Tivoli NetView, Tivoli Distributed Monitoring o HP OpenView — per monitorare lo stato, la velocità di trasmissione e le attività di Dispatcher. I dati MIB descrivono il Dispatcher sottoposto a gestione e riflettono lo stato corrente del Dispatcher. I dati MIB vengono installati nella directory secondaria **..lb/admin/MIB**.

Nota: i dati MIB, ibmNetDispatcherMIB.02, non vengono caricati quando si utilizza il programma Tivoli NetView xnmloadmib2. Per correggere questo problema, trasformare la sezione NOTIFICATION-GROUP del MIB in un commento, vale a dire, inserire "- " all'inizio della riga "indMibNotifications Group NOTIFICATION-GROUP" e delle 6 righe successive.

Il sistema di gestione della rete utilizza i comandi SNMP GET per ricercare i valori MIB sulle altre macchine. Quindi, è in grado di notificare all'utente se i valori di soglia specificati sono stati superati. È quindi possibile influire sulle prestazioni di Dispatcher modificando i dati di configurazione di Dispatcher per ottimizzare in modo proattivo o risolvere i problemi di Dispatcher prima che diventino interruzioni di funzionamento di Dispatcher o dei server Web.

Comandi SNMP e protocollo

Generalmente, il sistema fornisce un agente SNMP per ciascuna stazione di gestione della rete. L'utente invia un comando GET all'agente SNMP. A sua volta, l'agente SNMP invia un comando GET per richiamare i valori variabili dei dati MIB specificati di un agente secondario responsabile per tali variabili MIB.

Dispatcher fornisce un agente secondario che aggiorna e richiama i dati MIB. L'agente secondario risponde con i dati MIB appropriati quando l'agente SNMP invia un comando GET. L'agente SNMP comunica i dati alla stazione di gestione della rete. La stazione di gestione della rete può notificare all'utente se i valori di soglia specificati sono stati superati.

Il supporto SNMP di Dispatcher include un agente secondario SNMP che utilizza la funzione DPI (Distributed Program Interface). DPI è un'interfaccia che consente la comunicazione tra l'agente SNMP e i relativi agenti secondari. Il sistema operativo Windows utilizza l'agente di estensione di Windows come interfaccia tra un agente SNMP e i relativi agenti secondari.

Abilitazione di SNMP su sistemi AIX, HP-UX, Linux e Solaris

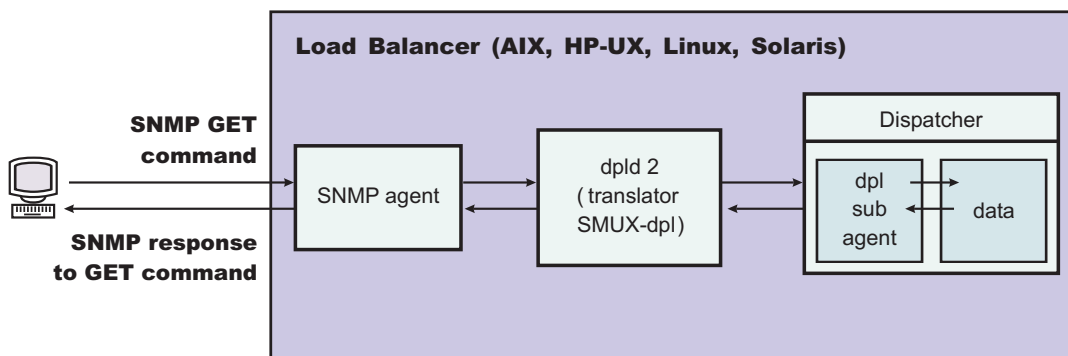


Figura 40. Comandi SNMP in Sistemi Linux e UNIX

AIX fornisce un agente SNMP che utilizza il protocollo SNMP Multiplexer (SMUX) e fornisce DPID2, un ulteriore file eseguibile che funge da convertitore tra DPI e SMUX.

Per i sistemi HP-UX, è necessario ottenere un agente SNMP che sia abilitato a SMUX in quanto HP-UX non ne fornisce uno. Load Balancer fornisce DPID2 per HP-UX.

I sistemi Linux forniscono un agente SNMP che utilizza SMUX. La maggior parte delle versioni Linux (ad esempio, Red Hat) vengono fornite con un pacchetto UCD SNMP. Il pacchetto UCD SNMP versione 4.1 o successive dispone di agenti abilitati a SMUX. Load Balancer fornisce DPID2 per sistemi Linux.

Nota: Per i sistemi SuSE Linux, è necessario ottenere un agente SNMP che sia abilitato a SMUX poiché SuSE non ne fornisce uno.

Per i sistemi Solaris, è necessario ottenere un agente SNMP che sia abilitato al protocollo SMUX in quanto Solaris non ne fornisce uno. Load Balancer fornisce DPID2 per Solaris. nella directory `/opt/ibm/edge/lb/servers/samples/SNMP`.

L'agente DPI deve essere eseguito come utente root. Prima di eseguire il daemon DPID2, aggiornare il file `/etc/snmpd.peers` e il file `/etc/snmpd.conf` nel modo indicato di seguito:

Per sistemi AIX e Solaris:

- Nel file `/etc/snmpd.peers`, aggiungere la voce seguente per `dpid`:
`"dpid2" 1.3.6.1.4.1.2.3.1.2.2.1.1.2 "dpid_password"`
- Nel file `/etc/snmpd.conf`, aggiungere la voce seguente per `dpid`:
`smux 1.3.6.1.4.1.2.3.1.2.2.1.1.2 dpid_password #dpid`

Per sistemi Linux:

- Nel file `/etc/snmpd.peers` (se non esiste nel sistema, crearne uno), aggiungere la voce seguente per `dpid`:
`"dpid2" 1.3.6.1.4.1.2.3.1.2.2.1.1.2 "dpid_password"`
- Nel file `/etc/snmp/snmpd.conf`, aggiungere la voce seguente per `dpid`:
`smuxpeer .1.3.6.1.4.1.2.3.1.2.2.1.1.2 dpid_password`

Inoltre, è necessario trasformare in commento tutte le righe del file `snmpd.conf` che iniziano con le seguenti parole: `com2sec`, `group`, `view` o `access`.

Abilitazione di SNMP su sistemi HP-UX

Per installare il supporto SNMP di HP-UX:

1. Se non si ha una versione di GNU SED installata, scaricarla dal sito Web HP, <http://www.hp.com>.
2. Prelevare il file `ucd-snmp-4.2.4.tar.gz` dalla seguente pagina Web, http://sourceforge.net/project/showfiles.php?group_id=12694.
3. Verificare che "gcc" e "gmake or make" siano installati sulla macchina. In caso contrario, installarli.
4. Decomprimere il file `ucd-snmp-4.2.4.tar.gz`, quindi decomprimere tutti i file di origine della directory.
5. Individuare la directory contenente i file di origine ed effettuare le seguenti operazioni:
 - a. `run ./configure --with-mib-modules=smux`
 - b. `make`
 - c. Eseguire i successivi due comandi come root:
 - 1) `umask 022`
 - 2) `make install`
 - d. `export SNMPCONFPATH=/etc/snmp`
 - e. `start /usr/local/sbin/snmpd -s` (Questo avvia l'agente SNMP)
 - f. `start dpid2` (Questo avvia il convertitore DPI)
 - g. `dscontrol subagent start` (Questo avvia l'agente secondario di Dispatcher)

Abilitazione di SNMP su sistemi SuSE Linux

Per utilizzare il protocollo SNMP di Load Balancer in SuSE Linux, effettuare le seguenti operazioni:

1. Rimuovere `ucd-snmp rpm` installato dalla macchina SuSE.
2. Richiamare `ucd-snmp-4.2.4.tar.gz` da http://sourceforge.net/project/showfiles.php?group_id=12694.
3. Verificare che "gcc" e "gmake or make" siano installati nella macchina SuSE (se non sono presenti, installarli).
4. Decomprimere il file `ucd-snmp-4.2.4.tar.gz`, quindi decomprimere tutti i file di origine della directory.
5. Individuare la directory contenente i file di origine ed effettuare le seguenti operazioni:

- a. `run ./configure --with-mib-modules=smux`
- b. `make`
- c. Eseguire i successivi due comandi come root:
 - 1) `umask 022 #`
 - 2) `make install`
- d. `export SNMPCONFPATH=/etc/snmp`
- e. `start /usr/local/sbin/snmpd -s`
- f. `start dpid2`

Aggiornare snmpd (se è già in esecuzione) in modo che legga nuovamente il file `snmpd.conf`:

```
refresh -s snmpd
```

Avviare il peer di DPID SMUX:

```
dpid2
```

I daemon devono essere avviati nel seguente ordine:

1. Agente SNMP
2. Convertitore DPI
3. Agente secondario di Dispatcher

Abilitazione di SNMP su sistemi Solaris

Per installare il supporto SNMP di Solaris:

1. Arrestare il daemon SNMP di Solaris in esecuzione (`snmpdx` e `snmpXdmid`).
2. Rinominare i file nel modo seguente:


```
da /etc/rc3.d/S76snmpdx a /etc/rc3.d/K76snmpdx
da /etc/rc3.d/S77dmi a /etc/rc3.d/K77dmi
```
3. Scaricare i seguenti pacchetti dall'indirizzo <http://www.sunfreeware.com/>:
 - `libgcc-3.0.3-sol8-sparc-local` (SMClibgcc)
 - `openssl-0.9.6c-sol8-sparc-local` (SMCssl)
 - `popt-1.6.3-sol8-sparc-local` (SMCpopt)
4. Installare i pacchetti scaricati utilizzando `pkgadd`.
5. Scaricare il file `ucd-snmp-4.2.3-solaris8.tar.gz` da http://sourceforge.net/project/showfiles.php?group_id=12694
6. Decomprimere il file `ucd-snmp-4.2.3-solaris8.tar.gz` sulla directory root (/)
7. Immettere i seguenti comandi:


```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH: /usr/local/lib:/usr/local/ssl/lib:/usr/lib
export PATH=/usr/local/sbin:/usr/local/bin:$PATH
export SNMPCONFPATH =/etc/snmp
export MIBDIRS=/usr/local/share/snmp/mibs
cp /opt/ibm/edge/lb/servers/samples/SNMP/dpid2
   /usr/local/sbin/dpid2
```
8. Se non esiste, creare il file `/etc/snmpd.peers`. Inserire quanto segue nel file `snmpd.peers`:


```
"dpid2" 1.3.6.1.4.1.2.3.1.2.2.1.1.2      "dpid_password"
```
9. Se non esiste, creare il file `/etc/snmp/snmpd.conf`. Inserire quanto segue nel file `snmpd.conf`:

smuxpeer 1.3.6.1.4.1.2.3.1.2.2.1.1.2 dpid_password

10. Avviare /usr/local/sbin/snmpd.

11. Avviare /usr/local/sbin/dpid2.

Note:

1. Quanto indicato di seguito è in formato pacchetto.

- libgcc-3.0.3-sol8-sparc-local (SMClibgcc)
- openssl-0.9.6c-sol8-sparc-local (SMCssl)
- popt-1.6.3-sol8-sparc-local (SMCpopt)

Sul sito Web di <http://sunfreeware.com/>, i nomi hanno un'estensione .gz, quindi non cercare di decomprimerli. Al contrario, utilizzare pkgadd *packageName*.

2. Quando si aggiunge la voce smuxpeer nel file /etc/snmp/snmpd.conf, verificare che non vengano aggiunti spazi nella stringa **dpid_password**.

3. La funzione SNMP di Load Balancer è stata testata con ucd-snmp versione 4.2.3 abilitato a SMUX. Le release successive di ucd-snmp con smux dovrebbero funzionare con analoga impostazione.

Abilitazione di SNMP nel sistema operativo di Windows

Per installare il supporto SNMP di Windows:

1. Fare clic su Start > Impostazioni (Windows 2000) > Pannello di controllo > Installazione applicazioni.
2. Fare clic su **Installazione componenti di Windows**.
3. In Aggiunta guidata componenti di Windows, fare clic su **Strumenti di gestione e controllo** (senza selezionare o deselezionare la relativa casella di controllo), quindi fare clic su **Dettagli**
4. Selezionare la casella di controllo **SNMP (Simple Network Management Protocol)**, quindi fare clic su OK.
5. Fare clic su Avanti.

Definizione di un nome comunità per SNMP

Con l'executor in esecuzione, utilizzare il comando **dscontrol subagent start [communityname]** per definire il nome comunità utilizzato tra l'agente di estensione del sistema operativo Windows e l'agente SNMP.

IMPORTANTE: in Windows 2003, per impostazione predefinita SNMP non risponde ai nomi comunità. In tal caso, l'agente secondario SNMP non risponderà ad alcuna richiesta SNMP. Per garantire che l'agente secondario SNMP risponda al nome comunità, impostare le proprietà del servizio SNMP sul nome comunità e sugli host di destinazione appropriati. Configurare le proprietà della sicurezza SNMP nel modo indicato di seguito:

1. Aprire Gestione computer.
2. Nella struttura ad albero, fare clic su **Servizi**
3. Nel riquadro dei dettagli, fare clic su **Servizio SNMP**
4. Dal menu delle azioni, fare clic su **Proprietà**
5. Sulla scheda Sicurezza, in Nomi comunità accettati, fare clic su **Aggiungi**
6. In Diritti comunità, selezionare un livello di autorizzazione per questo host per elaborare le richieste SNMP provenienti dalla comunità selezionata (almeno autorizzazione di **Sola lettura**)

7. In Nome comunità, immettere un nome comunità sensibile al maiuscolo/minuscolo, lo stesso fornito all'agente secondario di Load Balancer (nome comunità predefinito: public), quindi fare clic su **Aggiungi**
8. Specificare se accettare o meno i pacchetti SNMP provenienti da un host. Scegliere una delle seguenti opzioni:
 - Per accettare le richieste SNMP provenienti da un host della rete, a prescindere dall'identità: fare clic su **Accetta pacchetti SNMP da qualsiasi host**. (Se si utilizza questa opzione, è necessario verificare una persona o un'entità tramite autenticazione, in base a criteri quali una password o un certificato.)
 - Per limitare l'accettazione dei pacchetti SNMP: fare clic su **Accetta pacchetti SNMP da questi host**, quindi fare clic su **Aggiungi**. Immettere il nome host, l'indirizzo IP o IPX appropriati, quindi fare clic su **Aggiungi**, dopo ogni immissione.
9. Riavviare il servizio SNMP per applicare le modifiche apportate

Trap

SNMP comunica inviando e ricevendo delle *trap*, messaggi inviati dai dispositivi gestiti per riportare condizioni di eccezione o il verificarsi di eventi significativi, ad esempio una soglia che è stata raggiunta.

L'agente secondario utilizza le trap seguenti:

- indHighAvailStatus
- indSrvrGoneDown
- indDOSAttack
- indDOSAttackDone

La trap **indHighAvailStatus** indica che il valore della variabile dello stato della funzione di disponibilità elevata (hasState) è cambiato. I valori possibili di hasState sono:

- idle Questa macchina sta eseguendo il bilanciamento del carico e non cerca di stabilire un contatto con il Dispatcher partner.
- listen La funzione di disponibilità elevata è stata appena avviata e Dispatcher è in ascolto di eventuali comunicazioni dal partner.
- active Questa macchina sta eseguendo il bilanciamento del carico.
- standby Questa macchina sta controllando la macchina attiva.
- preempt Questa macchina è in uno stato transitorio durante il passaggio dallo stato principale allo stato di backup.
- elect Dispatcher sta negoziando con il partner per stabilire chi assumerà il ruolo principale e chi il ruolo di backup.
- no_exec L'executor non è in esecuzione.

La trap **indSrvrGoneDown** indica che il peso per il server specificato dalla porzione csID (ID cluster), psNum (numero della porta) e ssID (ID server) di Object Identifier ha raggiunto il valore zero. L'ultimo numero noto di connessioni attive per il server viene inviato alla trap. Questa trap indica che, per quanto riguarda il Dispatcher, il server specificato è diventato inattivo.

La trap **indDOSAttack** indica che numhalfopen, il numero di connessioni aperte a metà costituite solo da pacchetti SYN, ha superato la soglia di maxhalfopen per la porta specificata dalla porzione csID (ID cluster) e psNum (numero della porta) di Object Identifier. Il numero di server configurati sulla porta viene inviato alla trap. Questa trap indica che Load Balancer potrebbe aver ricevuto un attacco del tipo "Denial Of Service".

La trap **indDOSAttackDone** indica che numhalfopen, il numero di connessioni aperte a metà costituite solo da pacchetti SYN, ha raggiunto un valore inferiore alla soglia di maxhalfopen per la porta specificata dalla porzione csID e psNum di Object Identifier. Il numero di server configurati sulla porta viene inviato alla trap. Quando Load Balancer stabilisce che l'eventuale attacco "Denial of Service" è terminato, questa trap verrà inviata dopo l'invio di una trap indDOSAttack.

In Sistemi Linux e UNIX, a causa delle limitazioni delle API SMUX, l'identificatore azienda riportato nelle trap dall'agente secondario ibmNetDispatcher potrebbe essere l'identificatore azienda di dpid2, anziché l'identificatore azienda di ibmNetDispatcher, 1.3.6.1.4.1.2.6.144. Tuttavia, i programmi di utilità di gestione del protocollo SNMP saranno in grado di determinare l'origine della trap in quanto i dati contengono un identificatore oggetto proveniente dai dati MIB di ibmNetDispatcher.

Attivazione e disattivazione del supporto SNMP dal comando dscontrol

Il comando **dscontrol subagent start** attiva il supporto SNMP. Il comando **dscontrol subagent stop** disattiva il supporto SNMP.

Per ulteriori informazioni sul comando dscontrol, vedere "dscontrol subagent — configura l'agente secondario SNMP" a pagina 389.

Utilizzo di ipchains o iptables per rifiutare tutto il traffico sulla macchina Load Balancer (sistemi Linux)

Il kernel Linux dispone di una funzione firewall incorporata denominata ipchains. Quando Load Balancer e ipchains vengono eseguiti contemporaneamente, Load Balancer rileva prima i pacchetti, seguiti da ipchains. Ciò consente l'uso di ipchains per rifiutare tutto il traffico sulla macchina Linux Load Balancer, che potrebbe essere, ad esempio, una macchina Load Balancer utilizzata per eseguire il bilanciamento del carico sui firewall.

Quando ipchains o iptables sono configurati come completamente ristretti (nessun traffico in entrata o in uscita consentito), la parte di inoltro del pacchetto di Load Balancer continua a funzionare normalmente.

Notare che ipchains e iptables *non possono* essere utilizzati per filtrare il traffico in entrata prima di aver eseguito il bilanciamento del carico.

Una parte di traffico aggiuntivo deve essere consentito affinché Load Balancer funzioni correttamente. Di seguito sono riportati alcuni esempi di questa comunicazione:

- Comunicazione degli advisor tra la macchina Load Balancer e i server di backend.
- Invio da parte di Load Balancer del ping ai server di backend, alle destinazioni accessibili e alle macchine Load Balancer partner a disponibilità elevata.

- Utilizzo dell'RMI da parte delle interfacce utente (interfaccia utente grafica, riga comandi e procedure guidate).
- I server di backend devono rispondere ai ping provenienti dalla macchina Load Balancer.

In generale, una strategia ipchains appropriata per le macchine Load Balancer consiste nel non consentire tutto il traffico, ad eccezione di quello verso e dai server di backend, partner Load Balancer a disponibilità elevata, qualsiasi destinazione accessibile o qualsiasi host di configurazione.

Si consiglia di non attivare iptables con Load Balancer in esecuzione sul kernel Linux versione 2.4.10.x. L'attivazione su questa versione di kernel Linux, nel tempo, può determinare un peggioramento delle prestazioni.

Per disattivare iptables, elencare i moduli (lsmod) per visualizzare i moduli utilizzati da ip_tables e ip_conntrack, quindi rimuoverli immettendo rmmod ip_tables e rmmod ip_conntrack. Quando viene riavviata la macchina, questi moduli vengono nuovamente aggiunti in modo che sarà necessario ripetere queste operazioni ad ogni riavvio.

Per ulteriori informazioni, vedere "Problema: Linux iptables può interferire con l'instradamento dei pacchetti" a pagina 315.

Uso del componente CBR (Content Based Routing)

Questo capitolo illustra il funzionamento e la gestione del componente CBR di Load Balancer.

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l'uso di Caching Proxy. Per ulteriori informazioni, vedere "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

Avvio e arresto di CBR

- Digitare **cbrserver** su una riga comandi per avviare CBR.
- Digitare **cbrserver stop** su una riga comandi per arrestare CBR.

CBR e Caching Proxy collaborano tramite l'API plugin Caching Proxy per gestire le richieste HTTP e HTTPS (SSL). Affinché CBR possa iniziare il bilanciamento del carico sui server, è necessario che Caching Proxy sia in esecuzione sulla stessa macchina. Configurare CBR e Caching Proxy come descritto in "Esempio di configurazione di CBR" a pagina 116.

Controllo di CBR

Dopo aver avviato CBR, è possibile controllarlo utilizzando uno dei seguenti metodi:

- Configurare CBR tramite il comando **cbrcontrol**. La sintassi completa di questo comando è descritta in Capitolo 27, "Riferimenti sui comandi per Dispatcher e CBR", a pagina 337. Di seguito sono riportati alcuni esempi di utilizzo.
- Configurare CBR tramite l'interfaccia utente grafica (GUI). Digitare **lbadm** sulla riga comandi per aprire la GUI. Per ulteriori informazioni su come configurare CBR tramite la GUI, vedere "GUI" a pagina 109.

Uso dei log di CBR

I log utilizzati da CBR sono simili a quelli utilizzati in Dispatcher. Per ulteriori informazioni, vedere “Uso dei log di Load Balancer” a pagina 257.

Nota:

Nelle release precedenti, per CBR era possibile modificare il percorso della directory dei log nel file di configurazione Caching Proxy. Ora, è possibile modificare il percorso della directory in cui viene memorizzato il log nel file `cbrserver`. Vedere “Modifica dei percorsi file di log” a pagina 259.

Uso del componente Site Selector

Avvio e arresto di Site Selector

- Digitare `sssserver` su una riga comandi per avviare Site Selector.
- Digitare `sssserver stop` su una riga comandi per arrestare Site Selector.

Controllo di Site Selector

Dopo aver avviato Site Selector, è possibile controllarlo utilizzando uno dei seguenti metodi:

- Configurare Site Selector tramite il comando `sscontrol`. La sintassi completa di questo comando è descritta in Capitolo 28, “Riferimenti sui comandi per Site Selector”, a pagina 391. Di seguito sono riportati alcuni esempi di utilizzo.
- Configurare Site Selector tramite l’interfaccia utente grafica (GUI). Digitare `lbadm` sulla riga comandi per aprire la GUI. Per ulteriori informazioni su come configurare Site Selector tramite la GUI, vedere “GUI” a pagina 129.

Uso dei log di Site Selector

I log utilizzati da Site Selector sono simili a quelli utilizzati in Dispatcher. Per una descrizione più dettagliata, vedere “Uso dei log di Load Balancer” a pagina 257.

Uso del componente Controller Cisco CSS

Avvio e arresto di Controller Cisco CSS

1. Digitare `ccoserver` su una riga comandi per avviare Controller Cisco CSS.
2. Digitare `ccoserver stop` su una riga comandi per arrestare Controller Cisco CSS.

Controllo di Controller Cisco CSS

Dopo aver avviato Controller Cisco CSS, è possibile controllarlo utilizzando uno dei seguenti metodi:

- Configurare Controller Cisco CSS tramite il comando `ccocontrol`. La sintassi completa di questo comando è descritta in Capitolo 29, “Riferimenti sui comandi per Cisco CSS Controller”, a pagina 419. Di seguito sono riportati alcuni esempi di utilizzo.
- Configurare Controller Cisco CSS tramite l’interfaccia utente grafica (GUI). Digitare `lbadm` sulla riga comandi per aprire la GUI. Vedere “GUI” a pagina 147, per ulteriori informazioni su come configurare Controller Cisco CSS tramite la GUI.

Uso dei log di Controller Cisco CSS

I log utilizzati da Controller Cisco CSS sono simili a quelli utilizzati in Dispatcher. Per una descrizione più dettagliata, vedere “Uso dei log di Load Balancer” a pagina 257.

Uso del componente Controller Nortel Alteon

Avvio e arresto di Controller Nortel Alteon

1. Digitare **nalserver** su una riga comandi per avviare Controller Nortel Alteon.
2. Digitare **nalserver stop** su una riga comandi per arrestare Controller Nortel Alteon.

Controllo di Controller Nortel Alteon

Dopo aver avviato Controller Nortel Alteon, è possibile controllarlo utilizzando uno dei seguenti metodi:

- Configurare Controller Nortel Alteon tramite il comando **nalcontrol**. La sintassi completa di questo comando è descritta in Capitolo 30, “Riferimenti sui comandi per Controller Nortel Alteon”, a pagina 437. Di seguito sono riportati alcuni esempi di utilizzo.
- Configurare Controller Nortel Alteon tramite l’interfaccia utente grafica (GUI). Digitare **ladmin** sulla riga comandi per aprire la GUI. Vedere “GUI” a pagina 169, per ulteriori informazioni su come configurare Controller Nortel Alteon tramite la GUI.

Uso dei log di Controller Nortel Alteon

I log utilizzati da Controller Nortel Alteon sono simili a quelli utilizzati in Dispatcher. Per una descrizione più dettagliata, vedere “Uso dei log di Load Balancer” a pagina 257.

Uso del componente Metric Server

Avvio e arresto di Metric Server

Metric Server fornisce le informazioni sul carico del server a Load Balancer. Metric Server risiede su ciascun server sottoposto a bilanciamento del carico.

Sistemi Linux e UNIX:

- Su ciascuna macchina server in cui risiede Metric Server, digitare **metricserver start** su una riga comandi per avviare Metric Server.
- Su ciascuna macchina server in cui risiede Metric Server, digitare **metricserver stop** su una riga comandi per arrestare Metric Server.

Sistemi Windows:

Fare clic su Start > Impostazioni (per Windows 2000) > Pannello di controllo > Strumenti di amministrazione > Servizi. Fare clic con il tasto destro del mouse su IBM Metric Server e selezionare Avvia. Per arrestare il servizio, effettuare le stesse operazioni e selezionare Arresta.

Uso dei log di Metric Server

Modificare il livello di log nello script di avvio di Metric Server. È possibile specificare un numero di livello dei log compreso tra 0 e 5, analogamente all'intervallo dei livelli nei log di Load Balancer. In questo modo viene generato un log degli agenti nella directory **...ms/logs**.

Capitolo 25. Risoluzione dei problemi

Questo capitolo aiuta a rilevare e risolvere problemi associati a Load Balancer.

- Prima di contattare l'assistenza IBM, vedere "Raccolta delle informazioni per la risoluzione dei problemi".
- Individuare il sintomo sperimentato in "Tabelle di risoluzione dei problemi" a pagina 277.

Raccolta delle informazioni per la risoluzione dei problemi

Utilizzare le informazioni fornite in questa sezione per raccogliere i dati richiesti dall'assistenza IBM. Le informazioni sono suddivise tra i seguenti argomenti.

- "Informazioni generali (sempre richieste)"
- "Problemi di disponibilità elevata (HA)" a pagina 274
- "Problemi di advisor" a pagina 275
- "Problemi di CBR (Content Based Routing)" a pagina 275
- "Impossibile raggiungere il cluster" a pagina 276
- "Tutte le soluzioni non hanno esito" a pagina 276
- "Aggiornamenti" a pagina 277
- "Link utili" a pagina 277

Informazioni generali (sempre richieste)

Per il solo componente Dispatcher, è disponibile uno strumento per l'individuazione dei problemi che provvede automaticamente alla raccolta dei dati specifici del sistema operativo e dei file di configurazione del componente. Per eseguire questo strumento, digitare **lbpd** dalla directory adeguata:

Per Sistemi Linux e UNIX: /opt/ibm/edge/lb/servers/bin/

Per sistemi Windows: C:\Program Files\IBM\edge\lb\servers\bin

Questo strumento di individuazione dei problemi crea un file archivio dei dati nel modo seguente:

Per Sistemi Linux e UNIX: /opt/ibm/edge/lb/**lbpmr.tar.Z**

Per sistemi Windows: C:\Program Files\IBM\edge\lb**lbpmr.zip**

Nota: È necessario disporre di un programma di utilità per la creazione di file zip da riga comandi per Windows.

Prima di contattare l'assistenza IBM, reperire le seguenti informazioni.

- Solo per Dispatcher, il file **lbpmr** generato dallo strumento di individuazione dei problemi di cuisopra.
- In un ambiente a disponibilità elevata, i file di configurazione di entrambe le macchine Load Balancer. Su tutti i sistemi operativi, utilizzare lo script di cui ci si serve per caricare la configurazione, oppure immettere questo comando:
`dscontrol file save primary.cfg`
Questo comando colloca il file di configurazione nella directory **.../ibm/edge/lb/servers/configuration/componentel**.
- Il sistema operativo in uso e la relativa versione.

- La versione di Load Balancer.
 - Se Load Balancer è in esecuzione, immettere i seguenti comandi:
 - Per il componente Dispatcher: `dscontrol executor report`
 - Per CBR: `cbrcontrol executor status`
 - Per Site Selector, controllare l'inizio del file `server.log`, in `.../ibm/edge/lb/servers/logs/ss/`.
 - Per Cisco CSS Controller e Controller Nortel Alteon: `xxxcontrol controller report`
 - Immettere i seguenti comandi per verificare che Load Balancer sia installato e ottenere il livello corrente di Load Balancer:
 - Su sistemi AIX: `lspp -l | grep ibmlb`
 - Su sistemi HP-UX: `swlist | grep ibmlb`
 - Su sistemi Linux: `rpm -qa | grep ibmlb`
 - Su sistemi Solaris: `pkginfo | grep ibm`

Su sistemi Windows, per verificare che Load Balancer sia installato, fare clic su Start > Impostazioni > Pannello di controllo > Installazione applicazioni.
- Immettere il seguente comando per ottenere il livello corrente di Java:


```
java -fullversion
```
- Si utilizza Token Ring o Ethernet?
- Immettere uno di questi comandi per ottenere le statistiche di protocollo e le informazioni sulle connessioni TCP/IP:
 - Su sistemi AIX, HP-UX, Linux e Solaris: `netstat -ni`
 - Su sistemi Windows: `ipconfig /all`

Questo dato deve essere ottenuto da tutti i server e Load Balancer.
- Immettere uno di questi comandi per ottenere le informazioni della tabella di instradamento:
 - Su sistemi AIX, HP-UX, Linux e Solaris: `netstat -nr`
 - Su sistemi Windows: `route print`

Questo dato deve essere ottenuto da tutti i server e Load Balancer.

Problemi di disponibilità elevata (HA)

Raccogliere le informazioni seguenti, richieste per i problemi in un ambiente HA.

- Impostare `hamon.log` sul livello di log 5: `dscontrol set loglevel 5`.
- Impostare `reach.log` sul livello di log 5: `dscontrol manager reach set loglevel 5`.
- Ottenere gli script, memorizzati nelle posizioni seguenti:
 - Su sistemi AIX, HP-UX, Linux e Solaris: `/opt/ibm/edge/lb/servers/bin`
 - Su sistemi Windows: `C:\Program Files\ibm\edge\lb\servers\bin`

I nomi degli script sono:

 - `goActive`
 - `goStandby`
 - `goIdle` (se presente)
 - `goInOp` (se presente)

Includere anche i file di configurazione. Vedere "Informazioni generali (sempre richieste)" a pagina 273.

Problemi di advisor

Raccogliere le informazioni seguenti, richieste per i problemi di advisor; ad esempio, quando gli advisor contrassegnano erroneamente dei server come inattivi.

- Impostare il log dell'advisor al livello di log 5:

```
dscontrol advisor loglevel http 80 5
```

o

```
dscontrol advisor loglevel nomeAdvisor porta livello di log
```

o

```
dscontrol advisor loglevel nomeAdvisor cluster:porta livello di log
```

o

```
nalcontrol metriccollector set IDconsultant:IDservizio:nomeMetrica  
loglevel valore
```

Questo crea un log denominato ADV_*nomeAdvisor*.log; ad esempio, ADV_http.log. Questo log si trova nella posizione seguente:

Piattaforme AIX, HP-UX, Linux e Solaris: /opt/ibm/edge/lb/servers/logs/
componente

Su piattaforme Windows: C:\Program Files\ibm\edge\lb\servers\logs\
componente

Dove *componente* è:

dispatcher = Dispatcher

cbr = Content Based Routing

cco = Cisco CSS Controller

nal = Controller Nortel Alteon

ss = Site Selector

Nota: Quando si creano advisor personalizzati, è utile servirsi di ADVLOG(*livello di log,messaggio*) per verificare che l'advisor funzioni correttamente.

La chiamata ADVLOG stampa istruzioni nel file di log degli advisor quando il livello è inferiore al livello di log associato agli advisor. Un livello di log 0 comporta che le istruzioni vengono scritte sempre. Non è possibile utilizzare ADVLOG dal costruttore. Il file di log non viene creato fino a subito dopo il completamento del costruttore dell'advisor, dal momento che il nome del file di log dipende da informazioni che vengono impostate nel costruttore.

C'è un altro modo per eseguire il debug di un advisor personalizzato aggirando questa limitazione. È possibile utilizzare istruzioni System.out.println(*messaggio*) per stampare i messaggi in una finestra. Modificare lo script dsserver e sostituire javaw con java per far sì che le istruzioni di stampa appaiano nella finestra. La finestra utilizzata per avviare dsserver deve essere mantenuta aperta per consentire la visualizzazione dei messaggi. Se si utilizza una piattaforma Windows, è necessario arrestare l'esecuzione di Dispatcher come servizio e avviarlo manualmente da una finestra per poter vedere i messaggi.

Vedere *Guida alla programmazione per Edge Components* per ulteriori informazioni su ADVLOG.

Problemi di CBR (Content Based Routing)

Raccogliere le informazioni seguenti, richieste per i problemi di CBR (Content Based Routing).

- Immettere questo comando per ottenere la versione: `cbrcontrol executor status`.
- Ottenere i seguenti file:
 - `ibmproxy.conf`, memorizzato nella posizione seguente:
 Sistemi Linux e UNIX: `/etc/`
 Sistemi Windows: `C:\Program Files\IBM\edge\cp\etc\en_US\`
 - File di configurazione di CBR, memorizzato nelle posizioni seguenti:
 Sistemi Linux e UNIX: `/opt/ibm/edge/lb/servers/configurations/cbr`
 Su sistemi Windows: `C:\Program Files\IBM\edge\lb\servers\configurations\cbr`
 - Accertarsi che siano presenti le voci corrette in `ibmproxy.conf`. Vedere “Fase 1. Configurazione di Caching Proxy per l’uso di CBR” a pagina 111.

Impossibile raggiungere il cluster

Se non è possibile raggiungere il cluster, una o entrambe le macchine Load Balancer potrebbero non disporre di un alias per il cluster. Per determinare a quale macchina appartiene il cluster:

1. Sulla stessa sottorete e *non* su una macchina Load Balancer o server:

```
ping cluster
arp -a
```

Se si utilizzano i metodi di inoltro NAT o CBR di Dispatcher, eseguire un ping anche all’indirizzo mittente.

2. Osservare l’output di `arp` e individuare la corrispondenza tra l’indirizzo MAC (indirizzo esadecimale a 16 cifre) e uno degli output di `netstat -ni` per determinare la macchina a cui appartiene fisicamente il cluster.
3. Utilizzare i comandi che seguono per interpretare l’output di entrambe le macchine e vedere se hanno entrambe l’indirizzo cluster.

Su sistemi AIX e HP-UX: `netstat -ni`

Su sistemi Linux e Solaris: `ifconfig -a`

Su sistemi Windows: `ipconfig /all`

Se non si ottiene una risposta dal ping, è possibile che nessuna delle due macchine abbia un alias per l’indirizzo IP del cluster sulla propria interfaccia, ad esempio `en0`, `tr0` e così via.

Nota: Su sistemi Linux in esecuzione su un’installazione Load Balancer per IPv4 e IPv6, se non si ottiene una risposta dal ping, ciò indica che un server di backend non è disponibile; tuttavia la voce `arp` deve comunque essere aggiornata. In alternativa, è possibile utilizzare la funzione `arp`, se disponibile.

Tutte le soluzioni non hanno esito

Se non si è in grado di risolvere i problemi di instradamento e tutte le altre soluzioni non hanno avuto esito positivo, immettere il comando seguente per eseguire una traccia del traffico di rete:

- Su sistemi AIX, dalla macchina Load Balancer:
`iptrace -a -s IndirizzoIPClientConErrori -d IndirizzoIPCluster -b iptrace.trc`

Eseguire la traccia, ricreare il problema e interrompere il processo.

- Nei sistemi HP-UX:

```
tcpdump -i lan0 host cluster and host client
```

Potrebbe essere necessario scaricare tcpdump da uno dei siti di archivi software GNU per HP-UX.

- Su sistemi Linux:

```
tcpdump -i eth0 host cluster and host client
```

Eseguire la traccia, ricreare il problema e interrompere il processo.

- Su Solaris:

```
snoop -v indirizzoIPclient indirizzoIPdestinazione > snooptrace.out
```

- Su sistemi Windows, è richiesto l'uso di uno sniffer. Utilizzare gli stessi input di un filtro.

È inoltre possibile aumentare diversi livelli di log (quali log del gestore, log dell'advisor e così via) e analizzarne l'output.

Aggiornamenti

Per identificare un problema già risolto in un fix pack di una release di servizio o in una patch, verificare la disponibilità di aggiornamenti. Per ottenere un elenco dei difetti di Edge Components risolti, vedere la pagina di assistenza del sito Web dedicato a WebSphere Application Server: <http://www.ibm.com/software/webservers/appserv/was/support/>. Dalla pagina di assistenza, seguire il link al sito per il download delle correzioni di servizio.

Codice Java

La versione corretta del codice Java viene installata insieme a Load Balancer.

Link utili

Vedere "Informazioni di riferimento" a pagina xvii per link a pagine Web di assistenza e librerie. La pagina Web di assistenza contiene un link a informazioni di "autoassistenza" sotto forma di Technote.

Tabelle di risoluzione dei problemi

Vedere quanto segue per:

- Informazioni per la risoluzione dei problemi di Dispatcher — Tabella 14 a pagina 278
- Informazioni per la risoluzione dei problemi di CBR — Tabella 15 a pagina 284
- Informazioni per la risoluzione dei problemi di Site Selector — Tabella 16 a pagina 285
- Informazioni per la risoluzione dei problemi di Controller Cisco CSS — Tabella 17 a pagina 287
- Informazioni per la risoluzione dei problemi di Controller Nortel Alteon — Tabella 18 a pagina 288
- Informazioni per la risoluzione dei problemi di Metric Server — Tabella 19 a pagina 289

Tabella 14. tabella di risoluzione dei problemi di Dispatcher

Sintomo	Possibile causa	Andare a...
Dispatcher non viene eseguito correttamente	Numeri di porta in conflitto	"Controllo dei numeri di porta di Dispatcher" a pagina 290
È stato configurato un server in co-locazione, che non risponde alle richieste di bilanciamento del carico	Indirizzo errato o in conflitto	"Problema: Dispatcher e il server non rispondono" a pagina 294
Le connessioni dalle macchine client non ottengono risposta alle richieste o scadono	<ul style="list-style-type: none"> • Configurazione errata dell'instradamento • NIC senza alias all'indirizzo cluster • Il server non dispone di un dispositivo loopback con un alias all'indirizzo cluster • Instradamento in eccesso non eliminato • Porta non definita per ciascun cluster 	"Problema: le richieste di Dispatcher non vengono sottoposte a bilanciamento" a pagina 294
Le richieste delle macchine cluster non vengono soddisfatte o scadono	Mancato funzionamento della disponibilità elevata	"Problema: la funzionalità di disponibilità elevata di Dispatcher non funziona" a pagina 295
Impossibile aggiungere heartbeat (piattaforma Windows)	L'indirizzo di origine non è configurato su una scheda	"Problema: impossibile aggiungere heartbeat (piattaforma Windows)" a pagina 295
Il server non soddisfa le richieste (piattaforma Windows)	È stato creato un instradamento in eccesso nella tabella di instradamento	"Problema: instradamenti in eccesso (Windows 2000)" a pagina 295
Gli advisor non funzionano correttamente con Wide Area	Gli advisor non sono in esecuzione sulle macchine in remoto	"Problema: gli advisor non funzionano correttamente" a pagina 296
Dispatcher, Microsoft IIS e SSL non funzionano o si interrompono	Impossibile inviare dati cifrati tra protocolli	"Problema: Dispatcher, Microsoft IIS e SSL non funzionano (piattaforma Windows)" a pagina 296
Connessione alla macchina in remoto rifiutata	Una versione precedente delle chiavi è ancora in uso	"Problema: connessione di Dispatcher a una macchina in remoto" a pagina 296
Il comando dscontrol o lbadmìn provoca un messaggio di errore 'Il server non risponde' o 'Impossibile accedere al server RMI'	<ol style="list-style-type: none"> 1. Il comando non riesce a causa di uno stack abilitato ai socks. Oppure, i comandi non riescono a causa del mancato avvio di dsserver 2. Le porte RMI non sono impostate correttamente 3. L'host locale è errato nel file hosts 	"Problema: esecuzione errata dei comandi dscontrol o lbadmìn" a pagina 296

Tabella 14. tabella di risoluzione dei problemi di Dispatcher (Continua)

Sintomo	Possibile causa	Andare a...
Messaggio di errore "Impossibile trovare il file..." durante l'esecuzione di Netscape come browser predefinito per la visualizzazione della guida in linea (piattaforma Windows)	Impostazione errata per l'associazione dei file HTML	"Problema: messaggio di errore "Impossibile trovare il file..." quando si tenta di visualizzare la guida in linea (piattaforma Windows)" a pagina 297
Interfaccia utente grafica non avviata correttamente	Spazio di paginazione insufficiente	"Problema: l'interfaccia utente grafica (GUI) non viene avviata correttamente" a pagina 297
Errore durante l'esecuzione di Dispatcher con Caching Proxy installato	Dipendenza di file di Caching Proxy	"Problema: errore nell'esecuzione di Dispatcher con Caching Proxy installato" a pagina 297
Interfaccia utente grafica non visualizzata correttamente.	Risoluzione errata.	"Problema: l'interfaccia utente grafica (GUI) non viene visualizzata correttamente" a pagina 298
I pannelli di aiuto a volte scompaiono dietro altre finestre	Limitazione di Java	"Problema: sulla piattaforma Windows, le finestre della guida a volte scompaiono dietro altre finestre aperte" a pagina 298
Load Balancer non può elaborare e inoltrare un frame	È necessario un indirizzo MAC univoco per ciascuna NIC	"Problema: Load Balancer non può elaborare e inoltrare un frame" a pagina 298
Viene visualizzata una schermata blu	Scheda di rete non installata e configurata	"Problema: viene visualizzata una schermata blu quando si avvia l'executor di Load Balancer" a pagina 298
Il percorso di Discovery impedisce il traffico di ritorno	Il cluster ha un alias sul loopback	"Problema: il percorso di Discovery impedisce il traffico di ritorno con Load Balancer" a pagina 298
La disponibilità elevata nella modalità Wide Area di Load Balancer non funziona.	Il Dispatcher in remoto deve essere definito come un server in un cluster sul Dispatcher locale	"Problema: la disponibilità elevata nella modalità Wide Area di Load Balancer non funziona" a pagina 299
La GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni.	Java non ha accesso a memoria sufficiente per gestire un cambiamento della GUI di tale portata	"Problema: la GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni" a pagina 300

Tabella 14. tabella di risoluzione dei problemi di Dispatcher (Continua)

Sintomo	Possibile causa	Andare a...
Gli indirizzi IP non vengono risolti correttamente sulla connessione remota	Quando si utilizza un client remoto su un'implementazione con socks sicuri, i nomi di dominio completi o i nomi host potrebbero non venire risolti sugli indirizzi IP corretti	"Problema: gli indirizzi IP non vengono risolti correttamente sulla connessione remota" a pagina 301
L'interfaccia di Load Balancer in coreano visualizza font sovrapposti o indesiderati su AIX e Linux	Modificare i font predefiniti	"Problema: l'interfaccia di Load Balancer in coreano visualizza font sovrapposti o indesiderati su AIX e Linux" a pagina 301
Su Windows, dopo aver assegnato un alias alla scheda MS Loopback, quando si immettono certi comandi, quale hostname, il sistema operativo risponde in modo non corretto con l'indirizzo alias	Nell'elenco delle connessioni di rete, l'alias appena inserito non deve precedere l'indirizzo locale	"Problema: su Windows, l'indirizzo alias viene restituito al posto dell'indirizzo locale quando si immettono comandi quale hostname" a pagina 301
Comportamento imprevisto della GUI quando si utilizza la piattaforma Windows con una scheda video Matrox AGP	Il problema si verifica quando si utilizzano schede video Matrox AGP durante l'esecuzione della GUI di Load Balancer	"Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP" a pagina 302
Comportamento imprevisto, quale un blocco del sistema, durante l'esecuzione di "rmmod ibmlb" su Linux	Il problema si verifica durante la rimozione manuale del modulo del kernel per Load Balancer (ibmlb).	"Problema: comportamento imprevisto quando si esegue "rmmod ibmlb" (Linux)" a pagina 302
Tempo di risposta eccessivo durante l'esecuzione di comandi sulla macchina Dispatcher	Il tempo di risposta eccessivo può essere dovuto a un sovraccarico della macchina provocato da un elevato volume di traffico client	"Problema: tempo di risposta eccessivo durante l'esecuzione di comandi sulla macchina Dispatcher" a pagina 302
Per il metodo di inoltro MAC di Dispatcher, gli advisor SSL o HTTPS non registrano i carichi del server	Si verificano problemi perché l'applicazione server SSL non è configurata con l'indirizzo IP del cluster	"Problema: per il metodo di inoltro MAC, gli advisor SSL o HTTPS non registrano i carichi del server" a pagina 303
Disconnessione dall'host quando si utilizza l'amministrazione Web in remoto con Netscape	La disconnessione dall'host si verifica quando viene ridimensionata la finestra del browser	"Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web" a pagina 303
Il lotto socket è abilitato e il server Web esegue il bind a 0.0.0.0	Configurare il server Microsoft IIS con bind specifico	"Problema: il lotto socket è abilitato e il server Web esegue il binding a 0.0.0.0" a pagina 303

Tabella 14. tabella di risoluzione dei problemi di Dispatcher (Continua)

Sintomo	Possibile causa	Andare a...
Sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	Modificare le proprietà dei font della finestra del prompt dei comandi	“Problema: su Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti” a pagina 304
Sulla piattaforma HP-UX, viene visualizzato il seguente messaggio: java.lang.OutOfMemoryError impossibile creare un nuovo thread nativo	Alcune installazioni di HP-UX consentono, per impostazione predefinita, 64 thread per processo. Questo valore è insufficiente.	“Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java” a pagina 304
Sulla piattaforma Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi	Task Offload non è disabilitato o può richiedere l'abilitazione di ICMP.	“Problema: su Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi” a pagina 304
Sulla piattaforma Windows, si verificano problemi nella risoluzione di un indirizzo IP in un nome host quando su una scheda sono configurati più indirizzi	L'indirizzo IP desiderato come proprio nome host deve comparire per primo nel registro di configurazione.	“Problema: su Windows, si verificano problemi nella risoluzione di un indirizzo IP in un nome host quando su una scheda sono configurati più indirizzi” a pagina 305
Sulla piattaforma Windows, gli advisor non funzionano in un'installazione a disponibilità elevata dopo un'interruzione della rete	Quando il sistema rileva un'interruzione della rete, cancella la propria cache ARP (Address Resolution Protocol)	“Problema: su Windows, gli advisor non funzionano in un'installazione a disponibilità elevata dopo un'interruzione della rete” a pagina 306
Su Linux, il comando “IP address add” e gli alias loopback per cluster multipli non sono compatibili	Quando si definiscono alias per più di un indirizzo sul dispositivo loopback, utilizzare il comando ifconfig anziché ip address add	“Problema: su Linux, non utilizzare il comando “IP address add” quando si crea un alias per cluster multipli sull'unità loopback” a pagina 307
Messaggio di errore: “Indirizzo router non specificato o non valido per il metodo della porta” quando si tenta di aggiungere un server	Elenco di controllo delle informazioni per individuare il problema che si è verificato durante l'aggiunta di un server	“Problema: messaggio di errore “Indirizzo router non specificato o non valido per il metodo della porta”” a pagina 307
Su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati	Utilizzare il comando nohup per impedire che i processi avviati ricevano un segnale di interruzione all'uscita della sessione di terminale.	“Problema: su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati” a pagina 308
Si verifica un rallentamento durante il caricamento di configurazioni Load Balancer di grandi dimensioni	Il ritardo potrebbe essere dovuto a chiamate Domain Name System (DNS) eseguite per risolvere e verificare l'indirizzo del server.	“Problema: si verifica un ritardo durante il caricamento della configurazione di Load Balancer” a pagina 308

Tabella 14. tabella di risoluzione dei problemi di Dispatcher (Continua)

Sintomo	Possibile causa	Andare a...
Su Windows, viene visualizzato il seguente messaggio di errore: È presente un conflitto di indirizzi IP con un altro sistema sulla rete	Se la disponibilità elevata è configurata, gli indirizzi cluster potrebbero essere configurati su entrambe le macchine per un breve periodo, provocando la visualizzazione di questo messaggio di errore.	“Problema: su Windows, viene visualizzato un messaggio di errore che segnala un conflitto di indirizzi IP” a pagina 308
In una configurazione a disponibilità elevata, sono attive entrambe le macchine, primaria e di riserva	Questo problema può verificarsi quando gli script "go" non vengono eseguiti sulla macchina primaria o di riserva.	“Problema: in una configurazione a disponibilità elevata, sono attive entrambe le macchine, primaria e di riserva” a pagina 309
Le richieste dei client non riescono quando Dispatcher tenta di restituire risposte con pagine di grandi dimensioni	Le richieste client che producono come risposta pagine di grandi dimensioni scadono se l'MTU (Maximum Transmit Unit, unità di trasferimento massima) non è impostata adeguatamente sulla macchina Dispatcher quando si utilizza l'inoltro NAT o CBR.	“Problema: le richieste client hanno esito negativo quando si tenta di restituire risposte con pagine di grandi dimensioni” a pagina 309
Sui sistemi Windows, si verifica un errore "Il server non risponde" quando si immette un comando dscontrol o lbadm	Quando in un sistema Windows esiste più di un indirizzo IP e il file hosts** non specifica l'indirizzo da associare al nome host.	“Problema: sui sistemi Windows, si verifica un errore "Il server non risponde" quando si immette un comando dscontrol o lbadm” a pagina 309
Le macchine Dispatcher a disponibilità elevata potrebbero non sincronizzarsi su Linux per S/390 sui dispositivi qeth	Quando si utilizza la funzione di disponibilità elevata su Linux per S/390 con il driver di rete qeth, i Dispatcher attivo e in sospenso potrebbero non sincronizzarsi.	“Problema: le macchine Dispatcher a disponibilità elevata potrebbero non sincronizzarsi su Linux per S/390 sui driver qeth” a pagina 310
Suggerimenti sulla configurazione della funzione ad alta disponibilità di Load Balancer	Questi suggerimenti consentono di risolvere i problemi legati all'alta disponibilità, quali: <ul style="list-style-type: none"> • Connessioni interrotte in seguito al takeover • Macchine partner che non vengono sincronizzate • Richieste dirette erroneamente alla macchina del partner di backup 	“Problema: suggerimenti sulla configurazione dell'HA (high availability)” a pagina 310

Tabella 14. tabella di risoluzione dei problemi di Dispatcher (Continua)

Sintomo	Possibile causa	Andare a...
Limitazioni della configurazione di inoltro mac del Dispatcher con piattaforme zSeries e S/390	Su Linux, esistono delle limitazioni quando si utilizzano server zSeries o S/390 che hanno schede Open System Adapter (OSA). Sono riportate delle possibili soluzioni alternative.	“Problema: su Linux, esistono delle limitazioni alla configurazione del Dispatcher quando si utilizzano server zSeries o S/390 che utilizzano schede Open System Adapter (OSA)” a pagina 312
Su alcune versioni di Red Hat Linux, si verifica una mancanza di memoria quando si esegue Load Balancer configurato con il gestore e gli advisor	Le versioni di IBM Java SDK della JVM e Native POSIX Thread Library (NPTL) rilasciato con alcune distribuzioni Linux, come Red Hat Enterprise Linux 3.0, possono causare questa mancanza di memoria.	“Problema: su alcune versioni Linux, si verifica una mancanza di memoria quando viene eseguito il Dispatcher con il gestore e gli advisor” a pagina 314
Su SUSE Linux Enterprise Server 9, il prospetto di Dispatcher indica che i pacchetti vengono inoltrati (aumenta il numero di pacchetti), tuttavia i pacchetti non raggiungono il server di backend	Il modulo NAT iptables viene caricato. Esiste un possibile errore (mai confermato) in questa versione di iptables che provoca un funzionamento anomalo quando si utilizza Dispatcher.	“Problema: su SUSE Linux Enterprise Server 9, Dispatcher inoltra i pacchetti, ma i pacchetti non raggiungono il server di backend” a pagina 314
Su sistemi Windows, quando si utilizza la funzione ad alta disponibilità del Dispatcher, si verificano dei problemi durante il takeover	Se lo script goScript che configura l'indirizzo IP del cluster sulla macchina attiva viene eseguito prima dello script goScript per annullare la configurazione dell'indirizzo IP del cluster sulla macchina di backup, è possibile che si verifichino dei problemi.	“Problema: su Windows, un messaggio di conflitto di indirizzi IP viene visualizzato durante un takeover HA” a pagina 315
Su sistemi Linux, iptables può interferire con l'instradamento dei pacchetti	Linux iptables può interferire con il bilanciamento del carico del traffico e deve essere disabilitato sulla macchina Load Balancer.	“Problema: Linux iptables può interferire con l'instradamento dei pacchetti” a pagina 315
Su sistemi Solaris, quando si prova a configurare un server IPv6 sulla macchina del Dispatcher, viene visualizzato il messaggio "impossibile aggiungere il server"	Tale messaggio può essere causato dal modo in cui il sistema operativo Solaris gestisce la richiesta di ping per un indirizzo IPv6.	“Problema: impossibile aggiungere un server IPv6 alla configurazione di Load Balancer su sistemi Solaris” a pagina 316

Tabella 14. tabella di risoluzione dei problemi di Dispatcher (Continua)

Sintomo	Possibile causa	Andare a...
Un messaggio di avvertenza relativo a una serie di file Java viene visualizzato quando si installano le fix dei servizi o quando si utilizzano gli strumenti di assemblaggio del sistema	L'installazione del prodotto è costituita da diversi pacchetti che non devono essere installati sulla stessa macchina, pertanto ognuno di essi installa una serie di file Java. Quando installati sulla stessa macchina, viene visualizzato un messaggio di avvertenza che indica che la serie di file Java è di proprietà anche di un'altra serie di file.	"Messaggio di avvertenza Java visualizzato quando si installano le fix di servizio" a pagina 316
Aggiornamento della serie di file Java fornita con le installazioni di Load Balancer	Se si verifica un problema con la serie di file Java, è necessario riportare il problema all'assistenza IBM in modo da poter ricevere un aggiornamento alla serie di file Java fornita con l'installazione di Load Balancer.	"Aggiornamento della serie di file Java fornita con l'installazione di Load Balancer" a pagina 317

Tabella 15. Tabella di risoluzione dei problemi di CBR

Sintomo	Possibile causa	Andare a...
CBR non viene eseguito correttamente	Numeri di porta in conflitto	"Controllo dei numeri di porta di CBR" a pagina 291
Il comando cbrcontrol o lbadmin provoca un messaggio di errore 'Il server non risponde' o 'Impossibile accedere al server RMI'	Il comando non riesce a causa di uno stack abilitato ai socks. Oppure, i comandi non riescono a causa del mancato avvio di cbrserver	"Problema: esecuzione errata dei comandi cbrcontrol o lbadmin" a pagina 317
Le richieste non vengono sottoposte a bilanciamento del carico	Caching Proxy è stato avviato prima dell'executor	"Problema: le richieste non vengono sottoposte a bilanciamento del carico" a pagina 318
Su Solaris, il comando cbrcontrol executor start genera il messaggio di errore 'Errore: Executor non avviato.'	Il comando non riesce perché potrebbe essere necessario modificare i valori IPC predefiniti del sistema, o perché il collegamento alla libreria è errato.	"Problema: su Solaris, il comando cbrcontrol executor start non riesce" a pagina 318
La regola URL non funziona	Errore di sintassi o di configurazione	"Problema: errore di sintassi o di comunicazione" a pagina 318
Comportamento imprevisto della GUI quando si utilizza un sistema Windows con una scheda video Matrox AGP	Il problema si verifica quando si utilizzano schede video Matrox AGP durante l'esecuzione della GUI di Load Balancer	"Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP" a pagina 318

Tabella 15. Tabella di risoluzione dei problemi di CBR (Continua)

La GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni.	Java non ha accesso a memoria sufficiente per gestire un cambiamento della GUI di tale portata	“Problema: la GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni” a pagina 300
Disconnessione dall’host quando si utilizza l’amministrazione Web in remoto con Netscape	La disconnessione dall’host si verifica quando viene ridimensionata la finestra del browser	“Problema: si verifica una disconnessione dall’host quando si ridimensiona la finestra del browser Netscape durante l’uso della gestione Web” a pagina 318
Sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	Modificare le proprietà dei font della finestra del prompt dei comandi	“Problema: sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti” a pagina 319
Sulla piattaforma HP-UX, viene visualizzato il seguente messaggio: java.lang.OutOfMemoryError impossibile creare un nuovo thread nativo	Alcune installazioni di HP-UX consentono, per impostazione predefinita, 64 thread per processo. Questo valore è insufficiente.	“Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java” a pagina 319
Sulla piattaforma Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi	Task Offload non è disabilitato o può richiedere l’abilitazione di ICMP.	“Problema: su Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi” a pagina 319
Sulla piattaforma Windows, si verificano problemi nella risoluzione di un indirizzo IP su un nome host quando su una scheda sono configurati più indirizzi	L’indirizzo IP desiderato come proprio nome host deve comparire per primo nel registro di configurazione.	“Problema: su Windows, si verificano problemi nella risoluzione di un indirizzo IP su un nome host quando su una scheda sono configurati più indirizzi” a pagina 319
Su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati	Utilizzare il comando nohup per impedire che i processi avviati ricevano un segnale di interruzione all’uscita della sessione di terminale.	“Problema: su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati” a pagina 308

Tabella 16. tabella di risoluzione dei problemi di Site Selector

Sintomo	Possibile causa	Andare a...
Site Selector non viene eseguito correttamente	Numero di porta in conflitto	“Controllo dei numeri di porta di Site Selector” a pagina 292
Site Selector non esegue il round-robin delle richieste in entrata da client Solaris	I sistemi Solaris eseguono un "daemon cache del servizio nomi"	“Problema: Site Selector non esegue il round-robin del traffico dai client Solaris” a pagina 320

Tabella 16. tabella di risoluzione dei problemi di Site Selector (Continua)

Sintomo	Possibile causa	Andare a...
Il comando sscontrol o lbadmin provoca un messaggio di errore 'Il server non risponde' o 'Impossibile accedere al server RMI'	Il comando non riesce a causa di uno stack abilitato ai socks. Oppure, i comandi non riescono a causa del mancato avvio di ssserver.	"Problema: esecuzione errata dei comandi sscontrol o lbadmin" a pagina 320
ssserver non si avvia sulla piattaforma Windows	I sistemi Windows non richiedono che il nome host sia nel DNS.	"Problema: ssserver non si avvia su piattaforma Windows" a pagina 321
Una macchina con instradamenti duplicati non esegue correttamente il bilanciamento del carico — la risoluzione nome sembra non riuscire	Macchina Site Selector con più schede collegate alla stessa sottorete	"Problema: Site Selector con instradamenti duplicati non esegue correttamente il bilanciamento del carico" a pagina 321
Comportamento imprevisto della GUI quando si utilizza la piattaforma Windows con una scheda video Matrox AGP	Il problema si verifica quando si utilizzano schede video Matrox AGP durante l'esecuzione della GUI di Load Balancer	"Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP" a pagina 321
La GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni.	Java non ha accesso a memoria sufficiente per gestire un cambiamento della GUI di tale portata	"Problema: la GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni" a pagina 300
Disconnessione dall'host quando si utilizza l'amministrazione Web in remoto con Netscape	La disconnessione dall'host si verifica quando viene ridimensionata la finestra del browser	"Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web" a pagina 321
Sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	Modificare le proprietà dei font della finestra del prompt dei comandi	"Problema: sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti" a pagina 321
Sulla piattaforma HP-UX, viene visualizzato il seguente messaggio: java.lang.OutOfMemoryError impossibile creare un nuovo thread nativo	Alcune installazioni di HP-UX consentono, per impostazione predefinita, 64 thread per processo. Questo valore è insufficiente.	"Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java" a pagina 322
Sulla piattaforma Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi	Task Offload non è disabilitato o può richiedere l'abilitazione di ICMP.	"Problema: su Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi" a pagina 322

Tabella 16. tabella di risoluzione dei problemi di Site Selector (Continua)

Sintomo	Possibile causa	Andare a...
Su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati	Utilizzare il comando nohup per impedire che i processi avviati ricevano un segnale di interruzione all'uscita della sessione di terminale.	"Problema: su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati" a pagina 308

Tabella 17. tabella di risoluzione dei problemi di Controller per switch Cisco CSS

Sintomo	Possibile causa	Andare a...
mancato avvio di ccoserver	Numeri di porta in conflitto	"Controllo dei numeri di porta di Cisco CSS Controller" a pagina 293
Il comando ccocontrol o lbadmìn provoca un messaggio di errore 'Il server non risponde' o 'Impossibile accedere al server RMI'	Il comando non riesce a causa di uno stack abilitato ai socks. Oppure, i comandi non riescono a causa del mancato avvio di ccoserver.	"Problema: esecuzione errata dei comandi ccocontrol o lbadmìn" a pagina 322
errore di ricezione: Impossibile creare il registro sulla porta 13099	Licenza prodotto scaduta	"Problema: impossibile creare il registro sulla porta 13099" a pagina 323
Comportamento imprevisto della GUI quando si utilizza la piattaforma Windows con una scheda video Matrox AGP	Il problema si verifica quando si utilizzano schede video Matrox AGP durante l'esecuzione della GUI di Load Balancer	"Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP" a pagina 323
Viene ricevuto un errore di connessione durante l'aggiunta di un consultant	Le impostazioni di configurazione non sono corrette sullo switch o sul controller	"Problema: viene ricevuto un errore di connessione durante l'aggiunta di un consultant" a pagina 323
I pesi non vengono aggiornati sullo switch	La comunicazione con il controller o lo switch non è disponibile o è interrotta	"Problema: i pesi non vengono aggiornati sullo switch" a pagina 324
Il comando di aggiornamento non ha aggiornato la configurazione del consultant	La comunicazione tra il controller e lo switch non è disponibile o è interrotta	"Problema: il comando di aggiornamento non ha aggiornato la configurazione del consultant" a pagina 324
La GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni.	Java non ha accesso a memoria sufficiente per gestire un cambiamento della GUI di tale portata	"Problema: la GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni" a pagina 300
Disconnessione dall'host quando si utilizza l'amministrazione Web in remoto con Netscape	La disconnessione dall'host si verifica quando viene ridimensionata la finestra del browser	"Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web" a pagina 324

Tabella 17. tabella di risoluzione dei problemi di Controller per switch Cisco CSS (Continua)

Sintomo	Possibile causa	Andare a...
Sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	Modificare le proprietà dei font della finestra del prompt dei comandi	“Problema: sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti” a pagina 324
Sulla piattaforma HP-UX, viene visualizzato il seguente messaggio: java.lang.OutOfMemoryError impossibile creare un nuovo thread nativo	Alcune installazioni di HP-UX consentono, per impostazione predefinita, 64 thread per processo. Questo valore è insufficiente.	“Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java” a pagina 324
Su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati	Utilizzare il comando nohup per impedire che i processi avviati ricevano un segnale di interruzione all'uscita della sessione di terminale.	“Problema: su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati” a pagina 308

Tabella 18. tabella di risoluzione dei problemi di Controller Nortel Alteon

Sintomo	Possibile causa	Andare a...
Mancato avvio di nalserver	Numeri di porta in conflitto	“Controllo dei numeri di porta di Controller Nortel Alteon” a pagina 293
Il comando nalcontrol o lbadmim provoca un messaggio di errore ‘Il server non risponde’ o ‘Impossibile accedere al server RMI’	Il comando non riesce a causa di uno stack abilitato ai socks. Oppure, i comandi non riescono a causa del mancato avvio di nalserver.	“Problema: esecuzione errata dei comandi nalcontrol o lbadmim” a pagina 325
errore di ricezione: Impossibile creare il registro sulla porta 14099	Licenza prodotto scaduta	“Problema: impossibile creare il registro sulla porta 14099” a pagina 325
Comportamento imprevisto della GUI quando si utilizza la piattaforma Windows con una scheda video Matrox AGP	Il problema si verifica quando si utilizzano schede video Matrox AGP durante l'esecuzione della GUI di Load Balancer	“Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP” a pagina 326
La GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni.	Java non ha accesso a memoria sufficiente per gestire un cambiamento della GUI di tale portata	“Problema: la GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni” a pagina 300
Disconnessione dall'host quando si utilizza l'amministrazione Web in remoto con Netscape	La disconnessione dall'host si verifica quando viene ridimensionata la finestra del browser	“Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web” a pagina 326

Tabella 18. tabella di risoluzione dei problemi di Controller Nortel Alteon (Continua)

Sintomo	Possibile causa	Andare a...
Viene ricevuto un errore di connessione durante l'aggiunta di un consultant	Le impostazioni di configurazione non sono corrette sullo switch o sul controller	"Problema: viene ricevuto un errore di connessione durante l'aggiunta di un consultant" a pagina 326
I pesi non vengono aggiornati sullo switch	La comunicazione con il controller o lo switch non è disponibile o è interrotta	"Problema: i pesi non vengono aggiornati sullo switch" a pagina 326
Il comando di aggiornamento non ha aggiornato la configurazione del consultant	La comunicazione tra il controller e lo switch non è disponibile o è interrotta	"Problema: il comando di aggiornamento non ha aggiornato la configurazione del consultant" a pagina 326
Sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti	Modificare le proprietà dei font della finestra del prompt dei comandi	"Problema: su Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti" a pagina 327
Sulla piattaforma HP-UX, viene visualizzato il seguente messaggio: java.lang.OutOfMemoryError impossibile creare un nuovo thread nativo	Alcune installazioni di HP-UX consentono, per impostazione predefinita, 64 thread per processo. Questo valore è insufficiente.	"Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java" a pagina 327
Su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati	Utilizzare il comando nohup per impedire che i processi avviati ricevano un segnale di interruzione all'uscita della sessione di terminale.	"Problema: su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati" a pagina 308

Tabella 19. Tabella di risoluzione dei problemi di Metric Server

Sintomo	Possibile causa	Andare a...
Metric Server IOException su piattaforma Windows durante l'esecuzione di file di metrica utente .bat o .cmd	È richiesto il nome completo della metrica	"Problema: Metric Server IOException su piattaforma Windows durante l'esecuzione di file di metrica utente .bat o .cmd" a pagina 327
Metric Server non riporta le informazioni sul carico alla macchina Load Balancer	Tra le cause possibili sono incluse: <ul style="list-style-type: none"> • assenza di file di chiave sulla macchina Metric Server • nome host della macchina Metric Server non registrato con il server dei nomi locale • nel file /etc/hosts il nome host locale viene risolto all'indirizzo loopback 127.0.0.1 	"Problema: Metric Server non notifica i carichi alla macchina Load Balancer" a pagina 327

Tabella 19. Tabella di risoluzione dei problemi di Metric Server (Continua)

Sintomo	Possibile causa	Andare a...
Nel log di Metric Server è riportato "La firma è necessaria per l'accesso all'agente" quando i file di chiavi vengono trasferiti sul server	I file di chiavi non vengono autorizzati perché corrotti.	"Problema: nel log di Metric Server è riportato "La firma è necessaria per l'accesso all'agente"" a pagina 328
Su sistemi AIX, quando si esegue Metric Server sotto carichi elevati in un sistema multiprocessore (AIX 4.3.3 o AIX 5.1), l'output del comando ps -vg potrebbe risultare corrotto	APAR IY33804 corregge questo problema noto di AIX	"Problema: su AIX, durante l'esecuzione di Metric Server in condizioni di carico pesante l'output del comando ps -vg può risultare corrotto" a pagina 328
Impostazione di Metric Server in una configurazione a due livelli, con bilanciamento del carico mediante Site Selector tra Dispatcher a disponibilità elevata	Metric Server (residente nel secondo livello) non è configurato per l'ascolto su un nuovo indirizzo IP.	"Problema: impostazione di Metric Server in una configurazione a due livelli, con bilanciamento del carico mediante Site Selector tra Dispatcher a disponibilità elevata" a pagina 328
Gli script (metricserver, cpuload, memload) eseguiti su macchine Solaris multi-CPU producono messaggi console indesiderati	Questo comportamento è dovuto all'uso del comando di sistema VMSTAT per raccogliere le statistiche su CPU e memoria dal kernel.	"Problema: gli script eseguiti su macchine Solaris multi-CPU producono messaggi console indesiderati" a pagina 329
Su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati	Utilizzare il comando nohup per impedire che i processi avviati ricevano un segnale di interruzione all'uscita della sessione di terminale.	"Problema: su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati" a pagina 308
Su sistemi Linux, quando si esegue Load Balancer per IPv6, non è possibile richiamare i valori da Metric Server	Esiste una incompatibilità di selezione degli indirizzi IPv6 quando si utilizzano piattaforme Linux. Come risultato, Metric Monitor prova a comunicare con Metric Server sull'indirizzo IP di origine non corretto.	"Problema: su Load Balancer per IPv6, non è possibile richiamare i valori da Metric Server su sistemi Linux" a pagina 330
Il valore della metrica restituisce -1 dopo aver avviato Metric Server	Questo problema può essere causato dai file delle chiavi che perdono integrità durante il trasferimento dei file al client.	"Problema: dopo oaver avviato Metric Server, il valore della metrica restituisce -1" a pagina 331

Controllo dei numeri di porta di Dispatcher

Se si verificano problemi nell'esecuzione di Dispatcher, questo potrebbe essere dovuto al fatto che una delle applicazioni utilizza un numero di porta normalmente utilizzato da Dispatcher. Tenere presente che il server Dispatcher utilizza i seguenti numeri di porta:

- 10099 per ricevere comandi da dscontrol
- 10004 per inviare query di metrica a Metric Server

- 10199 per la porta del server RMI

Se un'altra applicazione utilizza uno dei numeri di porta di Dispatcher, è possibile modificare i numeri di porta di Dispatcher o il numero di porta dell'applicazione.

Per modificare i numeri di porta di Dispatcher', procedere come indicato di seguito:

- Per modificare la porta utilizzata per la ricezione dei comandi
 - Modificare la variabile LB_RMIPORT all'inizio del file dsserver con la porta su cui si desidera che Dispatcher riceva i comandi.
- Per modificare la porta utilizzata per la ricezione dei report di metrica da Metric Server
 - Modificare la variabile RMI_PORT in metricserver con la porta su cui si desidera che Dispatcher comunichi con Metric Server.
 - Fornire l'argomento metric_port all'avvio del gestore. Vedere la descrizione della sintassi del comando **dscontrol manager start** "dscontrol manager — controlla il gestore" a pagina 363

Per modificare il numero della porta RMI dell'applicazione, procedere come indicato di seguito:

- Per modificare la porta utilizzata dall'applicazione
 - Modificare la variabile LB_RMISERVERPORT nel file dsserver con la porta che si desidera venga utilizzata dall'applicazione. (Il valore predefinito della porta RMI utilizzata dall'applicazione è 10199.)

Nota: Per la piattaforma Windows, i file dsserver e metricserver si trovano nella directory C:\winnt\system32. Per altre piattaforme, questi file si trovano nella directory /usr/bin/.

Controllo dei numeri di porta di CBR

Se si verificano problemi nell'esecuzione di CBR, questo potrebbe essere dovuto al fatto che una delle applicazioni utilizza un numero di porta normalmente utilizzato da CBR. Tenere presente che CBR utilizza i seguenti numeri di porta:

- 11099 per ricevere comandi da cbrcontrol
- 10004 per inviare query di metrica a Metric Server
- 11199 per la porta del server RMI

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l'uso di Caching Proxy. Per ulteriori informazioni, vedere "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

Se un'altra applicazione utilizza uno dei numeri di porta di CBR, è possibile modificare i numeri di porta di CBR o il numero di porta dell'applicazione.

Per modificare i numeri di porta di CBR, procedere come indicato di seguito:

- Per modificare la porta utilizzata per la ricezione dei comandi
 - Modificare la variabile LB_RMIPORT all'inizio del file cbrserver con la porta su cui si desidera che CBR riceva i comandi.

- Per modificare la porta utilizzata per la ricezione dei report di metrica da Metric Server
 - Modificare la variabile RMI_PORT in metricserver con la porta su cui si desidera che CBR comunichi con Metric Server.
 - Fornire l'argomento metric_port all'avvio del gestore. Vedere la descrizione della sintassi del comando **manager start** "dscontrol manager — controlla il gestore" a pagina 363

Per modificare il numero della porta RMI dell'applicazione, procedere come indicato di seguito:

- Per modificare la porta utilizzata dall'applicazione
 - Modificare la variabile LB_RMISERVERPORT all'inizio del file cbrserver con la porta che si desidera venga utilizzata dall'applicazione. (Il valore predefinito della porta RMI utilizzata dall'applicazione è 11199.)

Nota: Per la piattaforma Windows, i file cbrserver e metricserver si trovano nella directory C:\winnt\system32. Per altre piattaforme, questi file si trovano nella directory /usr/bin/.

Controllo dei numeri di porta di Site Selector

Se si verificano problemi nell'esecuzione del componente Site Selector, questo potrebbe essere dovuto al fatto che una delle applicazioni utilizza un numero di porta normalmente utilizzato da Site Selector. Tenere presente che Site Selector utilizza i seguenti numeri di porta:

- 12099 per ricevere comandi da sscontrol
- 10004 per inviare query di metrica a Metric Server
- 12199 per la porta del server RMI

Se un'altra applicazione utilizza uno dei numeri di porta di Site Selector, è possibile modificare i numeri di porta di Site Selector o il numero di porta dell'applicazione.

Per modificare i numeri di porta di Site Selector, procedere come indicato di seguito:

- Per modificare la porta utilizzata per la ricezione dei comandi
 - Modificare la variabile LB_RMIPORT all'inizio del file sssserver con la porta su cui si desidera che Site Selector riceva i comandi.
- Per modificare la porta utilizzata per la ricezione dei report di metrica da Metric Server
 - Modificare la variabile RMI_PORT nel file metricserver con la porta su cui si desidera che Site Selector comunichi con Metric Server.
 - Fornire l'argomento metric_port all'avvio del gestore. Vedere la descrizione della sintassi del comando **manager start** "sscontrol manager — controlla il gestore" a pagina 401

Per modificare il numero della porta RMI dell'applicazione, procedere come indicato di seguito:

- Per modificare la porta utilizzata dall'applicazione
 - Modificare la variabile LB_RMISERVERPORT all'inizio del file sssserver con la porta che si desidera venga utilizzata dall'applicazione. (Il valore predefinito della porta RMI utilizzata dall'applicazione è 12199.)

Nota: Per la piattaforma Windows, i file sserver e metricserver si trovano nella directory C:\winnt\system32. Per altre piattaforme, questi file si trovano nella directory /usr/bin/.

Controllo dei numeri di porta di Cisco CSS Controller

Se si verificano problemi nell'esecuzione del componente Cisco CSS Controller, questo potrebbe essere dovuto al fatto che una delle applicazioni utilizza un numero di porta normalmente utilizzato da ccoserver di Cisco CSS Controller. Tenere presente che Cisco CSS Controller utilizza i seguenti numeri di porta:

- 13099 per ricevere comandi da ccocontrol
- 10004 per inviare query di metrica a Metric Server
- 13199 per la porta del server RMI

Se un'altra applicazione utilizza uno dei numeri di porta di Cisco CSS Controller, è possibile modificare i numeri di porta di Cisco CSS Controller o il numero di porta dell'applicazione.

Per modificare i numeri di porta di Cisco CSS Controller, procedere come indicato di seguito:

- Per modificare la porta utilizzata per la ricezione dei comandi da ccocontrol, modificare la variabile CCO_RMIPORT nel file ccoserver. Sostituire 13099 con la porta su cui si desidera che Cisco CSS Controller riceva i comandi di ccocontrol.
- Per modificare la porta utilizzata per la ricezione dei report di metrica da Metric Server:
 1. Modificare la variabile RMI_PORT nel file metricserver. Sostituire 10004 con la porta su cui si desidera che Cisco CSS Controller comunichi con Metric Server.
 2. Fornire l'argomento metric_port quando si installa il consultant.

Per modificare il numero della porta RMI dell'applicazione, procedere come indicato di seguito:

- Per modificare la porta utilizzata dall'applicazione
 - Modificare la variabile CCO_RMISERVERPORT all'inizio del file ccoserver con la porta che si desidera venga utilizzata dall'applicazione. (Il valore predefinito della porta RMI utilizzata dall'applicazione è 13199.)

Nota: Per la piattaforma Windows, i file ccoserver e metricserver si trovano nella directory C:\winnt\system32. Per altre piattaforme, questi file si trovano nella directory /usr/bin.

Controllo dei numeri di porta di Controller Nortel Alteon

Se si verificano problemi nell'esecuzione del componente Controller Nortel Alteon, questo potrebbe essere dovuto al fatto che una delle applicazioni utilizza un numero di porta normalmente utilizzato da nalserver di Controller Nortel Alteon. Tenere presente che Controller Nortel Alteon utilizza i seguenti numeri di porta:

- 14099 per ricevere comandi da nalcontrol
- 10004 per inviare query di metrica a Metric Server
- 14199 per la porta del server RMI

Se un'altra applicazione utilizza uno dei numeri di porta di Controller Nortel Alteon, è possibile modificare i numeri di porta di Controller Nortel Alteon o i numeri di porta dell'applicazione.

Per modificare i numeri di porta di Controller Nortel Alteon, procedere come indicato di seguito:

- Per modificare la porta utilizzata per la ricezione dei comandi da nalcontrol, modificare la variabile NAL_RMIPORT nel file nalserver. Sostituire 14099 con la porta su cui si desidera che Controller Nortel Alteon riceva i comandi di nalcontrol.
- Per modificare la porta utilizzata per la ricezione dei report di metrica da Metric Server:
 1. Modificare la variabile RMI_PORT nel file metricserver. Sostituire 10004 con la porta su cui si desidera che Controller Nortel Alteon comunichi con Metric Server.
 2. Fornire l'argomento metric_port quando si installa il consultant.

Per modificare il numero della porta RMI dell'applicazione, procedere come indicato di seguito:

- Per modificare la porta utilizzata dall'applicazione
 - Modificare la variabile NAL_RMISERVERPORT all'inizio del file nalserver con la porta che si desidera venga utilizzata dall'applicazione. (Il valore predefinito della porta RMI utilizzata dall'applicazione è 14199.)

Nota: Per la piattaforma Windows, i file nalserver e metricserver si trovano nella directory C:\winnt\system32. Per altre piattaforme, questi file si trovano nella directory /usr/bin.

Risoluzione di problemi comuni—Dispatcher

Problema: mancata esecuzione di Dispatcher

Questo problema può verificarsi quando un'altra applicazione utilizza una delle porte utilizzate da Dispatcher. Per ulteriori informazioni, vedere "Controllo dei numeri di porta di Dispatcher" a pagina 290.

Problema: Dispatcher e il server non rispondono

Questo problema si verifica quando viene utilizzato un indirizzo diverso da quello specificato. Quando si esegue la co-locazione di Dispatcher e server, accertarsi che l'indirizzo del server utilizzato nella configurazione sia l'indirizzo NFA o venga configurato come in co-locazione. Inoltre, verificare che il file hosts contenga l'indirizzo corretto.

Problema: le richieste di Dispatcher non vengono sottoposte a bilanciamento

Questo problema comporta sintomi quali la mancata soddisfazione delle richieste client o la scadenza di connessioni. Per diagnosticare il problema, verificare quanto segue:

1. Sono stati configurati l'indirizzo di non inoltro, i cluster, le porte e i server per l'instradamento? Controllare il file di configurazione.
2. La scheda di interfaccia di rete dispone di un alias per l'indirizzo cluster? Per Sistemi Linux e UNIX, controllare mediante netstat -ni.

3. Il dispositivo loopback su ciascun server dispone dell'alias impostato all'indirizzo cluster? Per Sistemi Linux e UNIX, controllare mediante `netstat -ni`.
4. L'instradamento in eccesso è stato eliminato? Per Sistemi Linux e UNIX, controllare mediante `netstat -nr`.
5. Utilizzare il comando **dscontrol cluster status** per verificare le informazioni per ciascun cluster definito. Accertarsi che ci sia una porta definita per ogni cluster.
6. Utilizzare il comando **dscontrol server report ::** per accertarsi che i server non siano inattivi o impostati a un peso pari a zero.

Per Windows e altre piattaforme, vedere anche "Configurazione delle macchine server per il bilanciamento del carico" a pagina 70.

Problema: la funzionalità di disponibilità elevata di Dispatcher non funziona

Questo problema compare quando un ambiente a disponibilità elevata di Dispatcher è configurato e le richieste delle connessioni dalle macchine client non vengono soddisfatte o scadono. Per correggere o diagnosticare il problema, verificare quanto segue:

- Accertarsi di aver creato gli script `goActive`, `goStandby` e `goInOp` e averli collocati nella directory `bin` in cui è installato Dispatcher. Per ulteriori informazioni su questi script, vedere "Utilizzo di script" a pagina 202
- Per **AIX**, **HP-UX**, **Linux** e **Solaris**, accertarsi che per gli script `goActive`, `goStandby` e `goInOp` siano impostate le autorizzazioni di esecuzione.
- Per Windows, accertarsi di configurare l'indirizzo di non inoltro utilizzando il comando **executor configure**.

La procedura che segue rappresenta un metodo efficace per verificare il corretto funzionamento degli script di disponibilità elevata:

1. ottenere un report immettendo `netstat -an` e `ifconfig -a` dalla macchina
2. eseguire lo script `goActive`
3. eseguire lo script `goStandby`
4. di nuovo, ottenere un report immettendo `netstat -an` e `ifconfig -a`

I due report saranno identici se gli script sono adeguatamente configurati.

Problema: impossibile aggiungere heartbeat (piattaforma Windows)

Questo errore della piattaforma Windows si verifica quando l'indirizzo origine non è configurato su una scheda. Per correggere o diagnosticare il problema, verificare quanto segue.

- Accertarsi di configurare l'indirizzo di non inoltro utilizzando l'interfaccia `token-ring` o `Ethernet` e immettendo uno dei seguenti comandi:
`dscontrol executor configure <indirizzo ip>`

Problema: instradamenti in eccesso (Windows 2000)

Dopo aver impostato le macchine server, ci si può accorgere di aver inavvertitamente creato uno o più instradamenti in eccesso. Se non eliminati, questi impediranno il funzionamento di Dispatcher. Per verificare la loro presenza ed eliminarli, vedere "Configurazione delle macchine server per il bilanciamento del carico" a pagina 70.

Problema: gli advisor non funzionano correttamente

Se si utilizza il supporto Wide Area e gli advisor sembrano non funzionare correttamente, accertarsi che siano avviati su Dispatcher locale e remoto.

Un ping ICMP viene inviato ai server prima della richiesta dell'advisor. Se è presente un firewall tra Load Balancer e i server, accertarsi che questo consenta il passaggio dei ping. Se questa impostazione rappresenta un rischio di sicurezza per la rete, modificare l'istruzione java in dsserver per disattivare tutti i ping ai server aggiungendo la proprietà java:

```
LB_ADV_NO_PING="true"
java -DLB_ADV_NO_PING="true"
```

Vedere "Utilizzo di advisor remoti con il supporto rete geografica di Dispatcher" a pagina 223.

Problema: Dispatcher, Microsoft IIS e SSL non funzionano (piattaforma Windows)

Quando si utilizza Dispatcher, Microsoft IIS e SSL, il loro mancato funzionamento congiunto potrebbe essere dovuto a un problema di abilitazione della sicurezza SSL. Per ulteriori informazioni sulla generazione di una coppia di chiavi, l'acquisizione di un certificato, l'installazione di un certificato con una coppia di chiavi e la configurazione di una directory perché richieda SSL, vedere la documentazione di *Microsoft Information and Peer Web Services*.

Problema: connessione di Dispatcher a una macchina in remoto

Dispatcher utilizza chiavi per consentire la connessione a una macchina in remoto e la sua configurazione. Le chiavi specificano una porta RMI per la connessione. È possibile modificare la porta RMI, qualora questo sia richiesto per ragioni di sicurezza o a causa della presenza di conflitti. Quando si modificano le porte RMI, il nome file della chiave cambia. Se si dispone di più chiavi per la stessa macchina in remoto nella directory delle chiavi, e queste specificano diverse porte RMI, la riga comandi tenta di utilizzare solo la prima chiave trovata. Se questa non è corretta, la connessione verrà rifiutata. La connessione non avviene finché la chiave errata non viene eliminata.

Problema: esecuzione errata dei comandi dscontrol o lbadmin

1. Il comando dscontrol restituisce: **Errore: il server non risponde**. Oppure, il comando lbadmin restituisce: **Errore: impossibile accedere al server RMI**. Questi errori possono verificarsi quando la macchina ha uno stack abilitato ai socks. Per correggere il problema, modificare il file socks.cnf in modo che contenga le righe seguenti:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```
2. Le console di gestione per le interfacce Load Balancer (riga comandi, interfaccia utente grafica e procedure guidate) comunicano con dsserver mediante RMI (Remote Method Invocation). La comunicazione predefinita sfrutta tre porte, ciascuna delle quali è impostata nello script di avvio di dsserver:
 - 10099 per ricevere comandi da dscontrol
 - 10004 per inviare query di metrica a Metric Server
 - 10199 per la porta del server RMI

Questo può causare problemi quando una delle console di gestione viene eseguita sulla stessa macchina di un firewall, oppure attraverso un firewall. Ad esempio, quando Load Balancer viene eseguito sulla stessa macchina di un firewall, e si immettono comandi di dscontrol, potrebbero comparire errori quale **Errore: il server non risponde**.

Per evitare questo problema, modificare il file script di dsserver per impostare la porta utilizzata da RMI per il firewall (o altra applicazione). Modificare la riga: `LB_RMISERVERPORT=10199` in `LB_RMISERVERPORT=propriaPorta`. Dove *propriaPorta* è una porta diversa.

Al termine dell'operazione, riavviare dsserver e aprire il traffico per le porte 10099, 10004, 10199 e 10100, oppure per la porta prescelta per l'indirizzo host da cui verrà eseguita la console di gestione.

3. Questi errori possono inoltre verificarsi se non è stato già avviato **dsserver**.
4. In presenza di più schede di rete su una stessa macchina, è necessario specificare quale scheda dovrà essere utilizzata da dsserver aggiungendo quanto segue allo script di dsserver: `java.rmi.server.hostname=<nome_host o indirizzoIP>`

Ad esempio: `java -Djava.rmi.server.hostname="10.1.1.1"`

Problema: messaggio di errore “Impossibile trovare il file...” quando si tenta di visualizzare la guida in linea (piattaforma Windows)

Per Windows, quando si utilizza Netscape come browser predefinito, potrebbe venire visualizzato il seguente messaggio di errore: “Impossibile trovare il file’<nomefile>.html’ (o uno dei suoi componenti). Verificare che il percorso e il nome file siano corretti e che tutte le librerie necessarie siano disponibili.”

Questo problema è dovuto a un'impostazione errata per l'associazione dei file HTML. La soluzione è la seguente:

1. Fare clic su **Risorse del computer**, fare clic su **Strumenti**, selezionare **Opzioni cartella**, quindi fare clic sulla scheda **Tipi di file**
2. Selezionare “Netscape Hypertext Document”
3. Fare clic sul pulsante **Avanzate**, selezionare **open**, fare clic sul pulsante **Modifica**
4. Immettere *NSShell* nel campo **Applicazione**: (non il campo Applicazione utilizzata per eseguire l'operazione:), quindi fare clic su **OK**

Problema: l'interfaccia utente grafica (GUI) non viene avviata correttamente

L'interfaccia utente grafica (GUI), lbadmin, richiede un adeguato spazio di paginazione per funzionare correttamente. Se lo spazio di paginazione disponibile è insufficiente, potrebbe non avviarsi completamente. In tal caso, controllare ed, eventualmente, aumentare lo spazio di paginazione.

Problema: errore nell'esecuzione di Dispatcher con Caching Proxy installato

Se si disinstalla Load Balancer per reinstallare un'altra versione e si ottiene un errore quando si tenta di avviare il componente Dispatcher, verificare se è installato Caching Proxy. Caching Proxy ha una dipendenza da uno dei file di Dispatcher; questo file viene disinstallato solo all'atto di disinstallare Caching Proxy.

Per evitare questo problema:

1. Disinstallare Caching Proxy.
2. Disinstallare Load Balancer.
3. Reinstallare sia Load Balancer che Caching Proxy.

Problema: l'interfaccia utente grafica (GUI) non viene visualizzata correttamente

Se si riscontra un problema nell'aspetto della GUI di Load Balancer, verificare l'impostazione della risoluzione del desktop del sistema operativo. La visualizzazione ottimale della GUI avviene a una risoluzione di 1024x768 pixel.

Problema: sulla piattaforma Windows, le finestre della guida a volte scompaiono dietro altre finestre aperte

Sulla piattaforma Windows, quando si aprono per la prima volta le finestre della guida, a volte queste scompaiono dietro le finestre esistenti. In tal caso, fare clic sulla finestra per riportarla in primo piano.

Problema: Load Balancer non può elaborare e inoltrare un frame

Su Solaris ciascuna scheda di rete ha, per impostazione predefinita, lo stesso indirizzo MAC. Questo funziona correttamente quando ogni scheda si trova su una sottorete IP diversa; tuttavia, in un ambiente dotato di switch, quando più NIC con lo stesso MAC e lo stesso indirizzo di sottorete IP comunicano con lo stesso switch, quest'ultimo invia tutto il traffico associato al singolo MAC (e a entrambi gli IP) lungo lo stesso cavo. Solo la scheda che ha inserito per ultima un frame sul cavo vede i pacchetti IP associati per entrambe le schede. Solaris potrebbe scartare i pacchetti per un indirizzo IP valido ma giunti sull'interfaccia "sbagliata".

Se tutte le interfacce di rete non sono destinate a Load Balancer come configurato in `ibmlb.conf`, e se la NIC non definita in `ibmlb.conf` riceve un frame, Load Balancer non è in grado di elaborarlo, né di inoltrarlo.

Per evitare questo problema, sovrascrivere il valore predefinito e impostare un indirizzo MAC univoco per ciascuna interfaccia. Utilizzare questo comando:

```
ifconfig interfaccia ether indirizzoMAC
```

Ad esempio:

```
ifconfig eri0 ether 01:02:03:04:05:06
```

Problema: viene visualizzata una schermata blu quando si avvia l'executor di Load Balancer

Sulla piattaforma Windows, è necessario disporre di una scheda di rete installata e configurata prima di avviare l'executor.

Problema: il percorso di Discovery impedisce il traffico di ritorno con Load Balancer

Il sistema operativo AIX contiene un parametro di rete denominato rilevazione percorso MTU. Durante una transazione con un client, se il sistema operativo determina che è necessario utilizzare un valore di MTU (Maximum Transmission Unit) minore per i pacchetti in uscita, questo parametro consente ad AIX di creare

un instradamento per memorizzare questo dato. Il nuovo instradamento riguarda l'IP dello specifico client e registra il valore di MTU necessario per raggiungerlo.

Quando viene creato l'instradamento, potrebbe verificarsi un problema sui server, a causa dell'impostazione dell'alias del cluster sul loopback. Se l'indirizzo gateway dell'instradamento rientra nella sottorete/netmask del cluster, AIX crea l'instradamento sul loopback. Ciò avviene perché questa è l'ultima interfaccia per cui è stato creato un alias con tale sottorete.

Ad esempio, se il cluster è 9.37.54.69 e viene utilizzata una netmask 255.255.255.0 e il gateway desiderato è 9.37.54.1, AIX utilizza il loopback per l'instradamento. Le risposte del server, in questo modo, non lasciano mai la macchina, e il client supera il timeout di attesa. Il client di norma vede una risposta dal cluster, dopodiché viene creato l'instradamento e non riceve nient'altro.

Sono disponibili due soluzioni a questo problema.

1. Disabilitare la rilevazione percorso MTU in modo che AIX non aggiunga instradamenti in modo dinamico. Utilizzare i seguenti comandi.

no -a elenca le impostazioni di rete di AIX

no -o option=value

imposta i parametri TCP su AIX

2. Creare un alias per l'IP del cluster sul loopback con netmask 255.255.255.255. Ciò significa che la sottorete con alias è costituita dal solo IP del cluster. Quando AIX crea gli instradamenti dinamici, l'IP del gateway di destinazione non corrisponde a quella sottorete, per cui viene creato un instradamento che utilizza l'interfaccia di rete corretta. Quindi, eliminare il nuovo instradamento lo0 creato durante la fase di attribuzione dell'alias. A tale scopo, individuare l'instradamento sul loopback con una destinazione di rete dell'IP del cluster ed eliminarlo. Questa operazione dev'essere eseguita ogni volta che si assegna un alias al cluster.

Note:

1. La rilevazione percorso MTU è disabilitata per impostazione predefinita in AIX 4.3.2 e versioni precedenti, ma è abilitata per impostazione predefinita in AIX 4.3.3 e versioni successive.
2. I comandi che seguono disattivano la rilevazione percorso MTU e devono essere eseguiti a ciascun avvio del sistema. Aggiungere questi comandi al file /etc/rc.net.
 - -o udp_pmtu_discover=0
 - -o tcp_pmtu_discover=0

Problema: la disponibilità elevata nella modalità Wide Area di Load Balancer non funziona

Quando si imposta un Load Balancer Wide Area, è necessario definire il Dispatcher remoto come server in un cluster sul Dispatcher locale. Normalmente, si utilizza l'indirizzo di non inoltra (NFA, Non-Forwarding Address) del Dispatcher remoto come indirizzo destinazione del server remoto. Se si esegue questa operazione e, successivamente, si imposta la disponibilità elevata sul Dispatcher remoto, non funzionerà. Questo avviene perché il Dispatcher locale punta sempre all'elemento primario sul lato remoto quando si utilizza il suo NFA per accedervi.

Per aggirare il problema:

1. Definire un cluster aggiuntivo sul Dispatcher remoto. Non è necessario definire porte o server per questo cluster.
2. Aggiungere l'indirizzo di questo cluster agli script goActive e goStandby.
3. Sul Dispatcher locale, definire l'indirizzo di questo cluster come un server, anziché l'NFA del Dispatcher remoto primario.

Quando il Dispatcher remoto primario si attiva, crea un alias a questo indirizzo sulla propria scheda, consentendo di accettare il traffico. In caso di guasti, l'indirizzo passa alla macchina di riserva, che continua ad accettare traffico per lo stesso indirizzo.

Problema: la GUI si blocca (o presenta un altro comportamento imprevisto) quando si tenta di caricare un file di configurazione di grandi dimensioni

Quando si utilizza lbadm o l'amministrazione Web (lbwebaccess) per caricare un file di configurazione di grandi dimensioni (circa 200 o più comandi **add**), la GUI potrebbe bloccarsi o mostrare un comportamento imprevisto, ad esempio rispondere alle modifiche delle schermate con estrema lentezza.

Ciò si verifica perché Java non ha accesso a una quantità di memoria sufficiente a gestire una configurazione di queste dimensioni.

L'ambiente di runtime prevede un'opzione, che può essere specificata per aumentare il lotto di allocazione della memoria disponibile per Java.

Si tratta dell'opzione `-Xmxn` dove *n* rappresenta la dimensione massima, in byte, del lotto di allocazione della memoria. *n* dev'essere un multiplo di 1024 e avere un valore superiore a 2MB. Il valore *n* può essere seguito da *k* o *K* a indicare kilobyte, oppure *m* o *M* a indicare megabyte. Ad esempio, `-Xmx128M` e `-Xmx81920k` sono entrambi validi. Il valore predefinito è 64M. Solaris 8 prevede un valore massimo di 4000M.

Ad esempio, per aggiungere questa opzione, modificare il file script di lbadm, sostituendo "javaw" con "javaw -Xmxn" come indicato di seguito. (Per AIX, sostituire "java" con "java -Xmxn"):

- **Sistemi AIX**

```
javaw -Xmx256m -cp $LB_CLASSPATH $LB_INSTALL_PATH $LB_CLIENT_KEYS
com.ibm.internet.nd.framework.FWK_Main 1>/dev/null 2>&1 &
```

- **Sistemi HP-UX**

```
java -Xmx256m -cp $LB_CLASSPATH $LB_INSTALL_PATH $LB_CLIENT_KEYS
com.ibm.internet.nd.framework.FWK_Main 1>/dev/null 2>&1 &
```

- **Sistemi Linux**

```
javaw -Xmx256m -cp $LB_CLASSPATH $LB_INSTALL_PATH $LB_CLIENT_KEYS
com.ibm.internet.nd.framework.FWK_Main 1>/dev/null 2>&1 &
```

- **Sistemi Solaris**

```
java -Xmx256m -cp $LB_CLASSPATH $LB_INSTALL_PATH $LB_CLIENT_KEYS
com.ibm.internet.nd.framework.FWK_Main 1>/dev/null 2>&1 &
```

- **Sistemi Windows**

```
START javaw -Xmx256m -cp %LB_CLASSPATH% %LB_INSTALL_PATH%
%LB_CLIENT_KEYS% com.ibm.internet.nd.framework.FWK_Main
```

Non è previsto un valore consigliato per *n*, ma dovrebbe essere maggiore dell'opzione predefinita. Un buon punto di partenza è rappresentato dal doppio del valore predefinito.

Problema: lbadmìn si scollega dal server dopo l'aggiornamento della configurazione

Se la gestione di Load Balancer (lbadmìn) si scollega dal server dopo l'aggiornamento della configurazione, verificare la versione di dsserver sul server che si sta tentando di configurare e accertarsi che coincida con quella di lbadmìn o dscontrol.

Problema: gli indirizzi IP non vengono risolti correttamente sulla connessione remota

Quando si utilizza un client remoto su un'implementazione con socks sicuri, i nomi di dominio completi o i nomi host potrebbero non venire risolti sugli indirizzi IP corretti nella notazione in formato indirizzo IP. L'implementazione socks potrebbe aggiungere dati specifici, relativi a socks, alla risoluzione DNS.

Se gli indirizzi IP non vengono risolti correttamente sulla connessione remota, si consiglia di specificare l'indirizzo IP nella notazione in formato indirizzo IP.

Problema: l'interfaccia di Load Balancer in coreano visualizza font sovrapposti o indesiderati su AIX e Linux

Per correggere i font sovrapposti o indesiderati nell'interfaccia di Load Balancer in coreano:

Su sistemi AIX

1. Arrestare tutti i processi Java sul sistema AIX.
2. Aprire il file font.properties.ko in un editor. Questo file si trova in *home/jre/lib* dove *home* è la directory home di Java.
3. Ricercare la stringa:

```
-Monotype-TimesNewRomanWT-medium-r-normal  
--*-%d-75-75-*--ksc5601.1987-0
```

4. Sostituire tutte le occorrenze della stringa con:

```
-Monotype-SansMonoWT-medium-r-normal  
--*-%d-75-75-*--ksc5601.1987-0
```

5. Salvare il file.

Su sistemi Linux

1. Arrestare tutti i processi Java sul sistema.
2. Aprire il file font.properties.ko in un editor. Questo file si trova in *home/jre/lib* dove *home* è la directory home di Java.
3. Ricercare la stringa seguente (senza spazi):

```
-monotype-  
timesnewromanwt-medium-r-normal---%d-75-75-p-*--microsoft-symbol
```

4. Sostituire tutte le occorrenze della stringa con:

```
-monotype-sansmonowt-medium-r-normal---%d-75-75-p-*--microsoft-symbol
```

5. Salvare il file.

Problema: su Windows, l'indirizzo alias viene restituito al posto dell'indirizzo locale quando si immettono comandi quale hostname

Su Windows, dopo aver assegnato un alias alla scheda MS Loopback, quando si immettono certi comandi, quale hostname, il sistema operativo risponde in modo non corretto con l'indirizzo alias anziché l'indirizzo locale. Per correggere questo

problema, nell'elenco delle connessioni di rete, l'alias appena inserito non deve essere elencato al di sotto dell'indirizzo locale. In questo modo, si garantisce che l'accesso avvenga prima all'indirizzo e poi all'alias loopback.

Per controllare l'elenco delle connessioni di rete:

1. Fare clic su **Start > Impostazioni > Connessioni di rete e Accesso remoto**
2. Dall'opzione di menu **Avanzate**, selezionare **Impostazioni avanzate...**
3. Accertarsi che **Connessione alla rete locale** sia la prima voce in elenco nella casella **Connessioni**
4. Se necessario, utilizzare i pulsanti di ordinamento sulla destra per spostare le voci nell'elenco verso l'alto o verso il basso

Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP

Sulla piattaforma Windows, quando si utilizza una scheda Matrox AGP, potrebbero verificarsi comportamenti imprevisti della GUI di Load Balancer. Quando si fa clic con il mouse, un blocco leggermente più grande del puntatore può corrompersi, provocando un'evidenziazione inversa o lo spostamento delle immagini sullo schermo. Questo comportamento è stato riscontrato nelle schede Matrox meno recenti. Non è disponibile una correzione nota in caso di utilizzo di schede Matrox AGP.

Problema: comportamento imprevisto quando si esegue "rmmod ibmlb" (Linux)

Su Linux, se dsserver è ancora in esecuzione durante la rimozione manuale del modulo del kernel per Load Balancer, può verificarsi un comportamento imprevisto, quale un blocco del sistema o javacore. Per la rimozione manuale del modulo del kernel per Load Balancer, è necessario arrestare prima dsserver.

Se "dsserver stop" non funziona, arrestare il processo java con SRV_KNDConfigServer. Arrestare il processo individuandone l'identificatore mediante il comando `ps -ef | grep SRV_KNDConfigServer` e quindi terminando il processo mediante il comando `kill id_processo`.

A questo punto, è possibile eseguire senza problemi il comando "rmmod ibmlb" per rimuovere il modulo di Load Balancer dal kernel.

Problema: tempo di risposta eccessivo durante l'esecuzione di comandi sulla macchina Dispatcher

Se si esegue il componente Dispatcher per il bilanciamento del carico, è possibile che il computer venga sovraccaricato di traffico client. Il modulo del kernel per Load Balancer ha la massima priorità e se questogestisce costantemente pacchetti client, il resto del sistema potrebbe smettere di rispondere. L'esecuzione di comandi nello spazio utente potrebbe richiedere molto tempo per il completamento, o non venire mai completata.

In tal caso, è opportuno ristrutturare l'impostazione generale per evitare di sovraccaricare di traffico la macchina Load Balancer. Le alternative comprendono la distribuzione del carico tra più macchine Load Balancer o la sostituzione della macchina con una più veloce e robusta.

Quando si determina se la risposta lenta sulla macchina è dovuta a un elevato traffico client, tenere in considerazione se questo si verifica durante i momenti di picco del traffico client. Anche sistemi non adeguatamente configurati che provocano loop di instradamento possono essere all'origine degli stessi sintomi. Prima di modificare l'impostazione di Load Balancer, stabilire se i sintomi sono dovuti a un elevato carico client.

Problema: per il metodo di inoltro MAC, gli advisor SSL o HTTPS non registrano i carichi del server

Quando si utilizza il metodo di inoltro basato su MAC, Load Balancer invia pacchetti ai server utilizzando l'indirizzo cluster con alias sul loopback. Alcune applicazioni server, quale SSL, richiedono che le informazioni di configurazione, quali i certificati, siano basate sull'indirizzo IP. L'indirizzo IP deve essere l'indirizzo cluster configurato sul loopback per la corrispondenza con i contenuti dei pacchetti in entrata. Se l'indirizzo IP del cluster non viene utilizzato durante la configurazione dell'applicazione server, la richiesta del client non verrà inoltrata adeguatamente al server.

Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web

Se si sta utilizzando la gestione Web remota, per configurare Load Balancer, non ridimensionare la finestra del browser Netscape (riduzione, ingrandimento, ripristino in basso e così via) in cui viene visualizzata la GUI di Load Balancer. Poiché Netscape ricarica una pagina ogni volta che le finestre del browser vengono ridimensionate, questo provoca la disconnessione dall'host. Sarà necessario riconnettersi all'host ogni volta che si ridimensiona una finestra. Se si esegue la gestione Web da remoto su una piattaforma Windows, utilizzare Internet Explorer.

Problema: il lotto socket è abilitato e il server Web esegue il binding a 0.0.0.0

Quando si esegue il server Microsoft IIS, versione 5.0 sui server backend Windows, è necessario configurare il server Microsoft IIS con un bind specifico. Altrimenti, il lotto socket viene abilitato per impostazione predefinita e il server Web esegue il binding a 0.0.0.0 e rimane in ascolto di tutto il traffico, anziché eseguire il binding all'indirizzo IP virtuale configurato come identità multiple per il sito. Se un'applicazione sull'host locale si arresta mentre il lotto socket è abilitato, gli advisor dei server ND AIX o Windows lo rilevano; tuttavia, se un'applicazione su un host virtuale si arresta mentre l'host locale rimane attivo, gli advisor non rilevano il malfunzionamento e Microsoft IIS continua a rispondere a tutto il traffico, compreso quello destinato all'applicazione che non è più attiva.

Per determinare se il lotto socket è abilitato e il server Web esegue il binding a 0.0.0.0, immettere il seguente comando:

```
netstat -an
```

Le istruzioni per la configurazione del server Microsoft IIS per un bind specifico (disattivazione del lotto socket) si trovano sul sito Web di assistenza per prodotti e servizi Microsoft. È inoltre possibile consultare uno dei seguenti URL per ottenere queste informazioni:

IIS5: Hardware Load Balance Does Not Detect a Stopped Web Site (Q300509)

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q300509>

Problema: su Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti

In una finestra del prompt dei comandi sul sistema operativo Windows, alcuni caratteri nazionali della famiglia Latin-1 potrebbero risultare corrotti. Ad esempio, la lettera "a" con la tilde potrebbe essere visualizzata come un simbolo di pi greco. Per risolvere questo problema, è necessario modificare le proprietà dei font della finestra del prompt dei comandi. Per modificare il font, procedere come indicato di seguito:

1. Fare clic sull'icona nell'angolo superiore sinistro della finestra del prompt dei comandi
2. Selezionare Proprietà, quindi fare clic sulla scheda Tipo di carattere
3. L'impostazione predefinita è Caratteri raster; sostituirla con Lucida Console e fare clic su OK

Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java

Alcune installazioni di HP-UX 11i sono preconfigurate per consentire solo 64 thread per processo. Tuttavia, alcune configurazioni di Load Balancer richiedono una quantità superiore. Per i sistemi HP-UX, impostare i thread per processo almeno su 256. Per aumentare il valore, servirsi dell'utilità "sam" per impostare il parametro del kernel `max_thread_proc`. Se si prevede un utilizzo intensivo, potrebbe essere necessario aumentare `max_thread_proc` oltre 256.

Per aumentare il valore di `max_thread_proc`, procedere come indicato di seguito:

1. Dalla riga comandi, digitare: `sam`
2. Selezionare **Configurazione kernel > Parametri configurabili**
3. Dalla barra di scorrimento, selezionare **max_thread_proc**
4. Premere la barra spaziatrice per evidenziare **max_thread_proc**
5. Premere Tab una volta, quindi premere il tasto freccia a destra fino a selezionare **Azioni**
6. Premere Invio per visualizzare il menu **Azioni**, quindi premere **M** per selezionare Modifica parametro configurabile. (Se l'opzione non è visualizzata, evidenziare **max_thread_proc**)
7. Premere Tab fino a selezionare il campo **Formula/Valore**
8. Immettere un valore di 256 o superiore.
9. Fare clic su **OK**
10. Premere Tab una volta, quindi selezionare **Azioni**
11. Premere **K** per Elaborare nuovo kernel..
12. Selezionare **Sì**
13. Riavviare il sistema

Problema: su Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi

Durante la configurazione della scheda su una macchina Load Balancer, è necessario accertarsi che le due impostazioni seguenti siano corrette, per consentire il funzionamento dell'advisor:

- Disabilitare Task Offload, generalmente utilizzato nelle schede di rete 3Com.
 - Per disattivare Task Offload: andare in Start > Impostazioni > Pannello di controllo > Rete e connessioni remote e selezionare la scheda.
 - Nella finestra a comparsa, fare clic su Proprietà.
 - Fare clic su Configura, quindi selezionare la scheda Avanzate.
 - Nel riquadro delle proprietà, selezionare la proprietà Task Offload e scegliere "disable" nel campo Valore.
- Abilitare Protocol 1 (ICMP) per i protocolli IP se si abilita il filtro TCP/IP. Se ICMP non è abilitato, la prova ping al server di backend non riesce. Per controllare se ICMP è abilitato:
 - Andare in Start > Impostazioni > Pannello di controllo > Rete e connessioni remote e selezionare la scheda.
 - Nella finestra a comparsa, fare clic su Proprietà.
 - Nel riquadro dei componenti, selezionare Protocollo Internet (TCP/IP) e fare clic su Proprietà.
 - Fare clic su Avanzate, quindi selezionare la scheda Opzioni.
 - Selezionare Filtro TCP/IP nel riquadro delle opzioni, quindi fare clic su Proprietà.
 - Se è stato selezionato **Attiva filtro TCP/IP** e **Autorizza solo** per i protocolli IP, è necessario aggiungere il Protocollo IP 1. Questo deve andare ad aggiungersi alle porte TCP e UDP già abilitate.

Problema: su Windows, si verificano problemi nella risoluzione di un indirizzo IP in un nome host quando su una scheda sono configurati più indirizzi

Sulla piattaforma Windows, quando si configura una scheda perché abbia più indirizzi IP, configurare l'indirizzo IP che si desidera associare al nome host come primo nel registro.

Poiché Load Balancer dipende da `InetAddress.getLocalHost()` in molti casi (ad esempio, per `lbkeys create`), più indirizzi IP con alias su una singola scheda possono causare problemi. Per evitare questo problema, collocare per primo nell'elenco del registro l'indirizzo IP sul quale si desidera venga risolto il nome host. Ad esempio:

1. Avviare Regedit
2. Modificare i nomi di valore seguenti come indicato:
 - HKEY_LOCAL_MACHINE -> SYSTEM -> ControlSet001 -> Services -> *IndirizzoInterfaccia* -> Parameters -> Tcpip -> IPAddress
 - Collocare per primo l'indirizzo IP sul quale si desidera venga risolto il nome host.
 - HKEY_LOCAL_MACHINE -> SYSTEM -> ControlSet001 -> Services -> Tcpip -> Parameters -> Interfaces -> *IndirizzoInterfaccia* -> IPAddress
 - Collocare per primo l'indirizzo IP sul quale si desidera venga risolto il nome host.
 - HKEY_LOCAL_MACHINE -> SYSTEM -> ControlSet002 -> Services -> *IndirizzoInterfaccia* -> Parameters -> Tcpip -> IPAddress
 - Collocare per primo l'indirizzo IP sul quale si desidera venga risolto il nome host.
 - HKEY_LOCAL_MACHINE -> SYSTEM -> ControlSet002 -> Services -> Tcpip -> Parameters -> Interfaces -> *IndirizzoInterfaccia* -> IPAddress

- Collocare per primo l'indirizzo IP sul quale si desidera venga risolto il nome host.
 - HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Services-> *IndirizzoInterfaccia* -> Parameters -> Tcpip -> IPAddress
 - Collocare per primo l'indirizzo IP sul quale si desidera venga risolto il nome host.
 - HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Services-> Tcpip -> Parameters -> Interfaces -> *IndirizzoInterfaccia* -> IPAddress
 - Collocare per primo l'indirizzo IP sul quale si desidera venga risolto il nome host.
3. Riavviare
 4. Controllare che il nome host venga risolto sull'indirizzo IP corretto. Ad esempio, eseguire un ping a *nomehost*.

Problema: su Windows, gli advisor non funzionano in un'installazione a disponibilità elevata dopo un'interruzione della rete

Per impostazione predefinita, quando il sistema operativo Windows rileva un'interruzione della rete, cancella la propria cache ARP (Address Resolution Protocol), comprese tutte le voci statiche. Dopo il ripristino della rete, la cache ARP viene ripopolata mediante richieste ARP inviate sulla rete.

Con una configurazione a disponibilità elevata, entrambi i server intraprendono operazioni primarie quando sono interessati tutti e due da un problema di connettività di rete. Quando viene inviata la richiesta ARP per ripopolare la cache ARP, entrambi i server rispondono, cosicché la cache ARP contrassegna la voce come non valida. Di conseguenza, gli advisor non sono in grado di creare un socket ai server di riserva.

Per risolvere questo problema, impedire al sistema operativo Windows di cancellare la cache ARP quando viene persa connettività. Microsoft ha pubblicato un articolo che spiega come eseguire questa operazione. L'articolo si trova sul sito Web di Microsoft, nella Microsoft Knowledge Base, numero articolo 239924: <http://support.microsoft.com/default.aspx?scid=kb;en-us;239924>.

Di seguito viene fornito un riepilogo dei passi descritti nell'articolo di Microsoft per impedire al sistema di cancellare la cache ARP:

1. Utilizzare l'editor del registro di configurazione (regedit o regedit32) per aprire il registro.
2. Visualizzare la seguente chiave nel registro:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
3. Aggiungere il seguente valore di registro: Nome valore:
DisableDHCPMediaSense Tipo valore: REG_DWORD.
4. Dopo aver aggiunto la chiave, modificare il valore impostandolo a 1.
5. Riavviare la macchina per rendere effettiva la modifica.

Nota: Questo influisce sulla cache ARP a prescindere dall'impostazione di DHCP.

Problema: su Linux, non utilizzare il comando "IP address add" quando si crea un alias per cluster multipli sull'unità loopback

È necessario fare alcune considerazioni quando si utilizzano server con kernel Linux 2.4.x e il metodo di inoltro MAC di Dispatcher. Se il server ha un indirizzo cluster configurato sul dispositivo loopback mediante il comando `ip address add`, è possibile creare un alias per un solo indirizzo cluster.

Quando si creano alias per cluster multipli sul dispositivo loopback, utilizzare il comando `ifconfig`, ad esempio:

```
ifconfig lo:num indirizzoCluster netmask 255.255.255.255 up
```

Inoltre, ci sono delle incompatibilità tra il metodo `ifconfig` e il metodo `ip` per la configurazione delle interfacce. Come pratica ottimale, è bene scegliere un metodo e utilizzare esclusivamente quello.

Problema: messaggio di errore "Indirizzo router non specificato o non valido per il metodo della porta"

Quando si aggiungono server alla configurazione di Dispatcher, può venire generato il seguente messaggio di errore: "Errore: indirizzo router non specificato o non valido per il metodo della porta".

Utilizzare questo elenco di controllo per individuare il problema:

- Accertarsi di aver applicato il più recente livello di manutenzione.
- Accertarsi di utilizzare una distribuzione IBM di Java (tranne che su piattaforme Solaris).
- Accertarsi di non aver configurato l'uso di DHCP su Windows.
- Se il metodo di inoltro è MAC (impostazione predefinita), il server, il cluster e almeno una NIC supportata devono trovarsi sulla stessa sottorete. Ad esempio, non è possibile definire un cluster 10.1.1.1 e un server 130.2.3.4 perché non si trovano sulla stessa sottorete.

Nota: Se il metodo di inoltro è NAT o CBR, non è necessario che i server siano sulla stessa sottorete del cluster.

- Se tutti gli elementi si trovano sulla stessa sottorete ed è stato creato un alias per il cluster, verificare che questo sia su una NIC che consente l'instradamento a questa sottorete. Ad esempio, se `en0` è definito per 13.2.3.4 e `en1` è definito per 9.1.2.3 e la definizione del cluster è 9.5.7.3, è necessario configurare il cluster su `en1`. L'interfaccia predefinita è `en0`.
- Sulle piattaforme Linux, accertarsi di aver caricato il kernel corretto controllando il file `loadoutput.log` nella directory `/usr/lpp/ibm/internet/nd/logs/dispatcher`. Verificare se nel file sono riportati errori.

Il valore predefinito del parametro `router` è 0, che indica un server locale. Quando si imposta l'indirizzo del router del server a un valore diverso da 0, si indica che si tratta di un server remoto, su un'altra sottorete. Per ulteriori informazioni sul parametro `router` del comando `server add`, vedere "dscontrol server — configura i server" a pagina 381.

Se il server che si sta aggiungendo si trova su un'altra sottorete, il parametro `router` dovrà essere l'indirizzo del router da utilizzare sulla sottorete locale per comunicare con il server remoto.

Problema: su Solaris, i processi di Load Balancer si interrompono quando si chiude la sessione di terminale da cui sono stati avviati

Su Solaris, dopo l'avvio degli script di Load Balancer (quale `dsserver` o `lbadm`) da una finestra di terminale, se si esce dalla finestra viene interrotto anche il processo di Load Balancer.

Per risolvere questo problema, avviare gli script di Load Balancer con il comando **nohup**. Ad esempio: **nohup dsserver**. Questo comando impedisce che i processi avviati da una sessione di terminale ricevano un segnale di interruzione dal terminale quando questo viene chiuso, consentendo loro di continuare anche dopo la fine della sessione di terminale. Utilizzare il comando **nohup** antepoendolo a qualsiasi script di Load Balancer che si desidera far proseguire oltre la fine di una sessione di terminale.

Problema: si verifica un ritardo durante il caricamento della configurazione di Load Balancer

Il ritardo nel caricamento della configurazione di Load Balancer potrebbe essere dovuto a chiamate Domain Name System (DNS) eseguite per risolvere e verificare l'indirizzo del server.

Se il DNS della macchina Load Balancer non è configurato adeguatamente o se le operazioni DNS in generale richiedono tempi lunghi, questo si aggiunge al ritardo, poiché Java invia richieste DNS sulla rete.

Una soluzione temporanea consiste nell'aggiunta degli indirizzi e dei nomi host dei server al file `/etc/hosts` locale.

Problema: su Windows, viene visualizzato un messaggio di errore che segnala un conflitto di indirizzi IP

Se la disponibilità elevata è configurata, gli indirizzi cluster potrebbero essere configurati su entrambe le macchine per un breve periodo, provocando la visualizzazione del seguente messaggio di errore: È presente un conflitto di indirizzi IP con un altro sistema sulla rete. In questo caso, è possibile ignorare il messaggio. Un indirizzo cluster potrebbe essere configurato, per un breve tempo, su entrambe le macchine a disponibilità elevata contemporaneamente, in particolare all'avvio di una delle due macchine o quando viene iniziato un takeover.

Controllare gli script `go*` per verificare che configurino e deconfigurino correttamente gli indirizzi cluster. Se è stato richiamato un file di configurazione e sono installati gli script `go*`, accertarsi che il file di configurazione non contenga comandi "executor configure" per gli indirizzi cluster, dal momento che questo sarà in conflitto con i comandi `configure` e `unconfigure` negli script `go*`.

Per ulteriori informazioni sugli script `go*` nella configurazione della disponibilità elevata, vedere "Utilizzo di script" a pagina 202.

Problema: in una configurazione a disponibilità elevata, sono attive entrambe le macchine, primaria e di riserva

Questo problema può verificarsi quando gli script "go" non vengono eseguiti sulla macchina primaria o di riserva. Gli script "go" non possono essere eseguiti se dsserver non è avviato su entrambe le macchine. Verificare che dsserver sia in esecuzione su entrambe le macchine.

Problema: le richieste client hanno esito negativo quando si tenta di restituire risposte con pagine di grandi dimensioni

Le richieste client che producono come risposta pagine di grandi dimensioni scadono se l'MTU (Maximum Transmit Unit, unità di trasferimento massima) non è impostata adeguatamente sulla macchina Dispatcher. Per i metodi di inoltro CBR e NAT del componente Dispatcher, questo può verificarsi perché Dispatcher utilizza il valore MTU predefinito, anziché negoziarlo.

L'impostazione del valore di MTU avviene su ciascun sistema operativo in base al tipo di supporto di comunicazione, ad esempio Ethernet o Token-Ring. I router del segmento locale potrebbero avere un valore MTU inferiore se si collegano a un tipo di supporto di comunicazione diverso. Con il normale traffico TCP, si verifica una negoziazione MTU durante l'impostazione della connessione e viene utilizzato il valore minimo per l'invio di dati tra le macchine.

Dispatcher non supporta la negoziazione MTU per i metodi di inoltro CBR o NAT perché è attivamente coinvolto come endpoint per le connessioni TCP. Per l'inoltro CBR e NAT, Dispatcher utilizza il valore MTU predefinito di 1500. Questo rappresenta le dimensioni MTU tipiche per le reti Ethernet standard, per cui la maggior parte dei clienti non dovrà modificarlo.

Quando si utilizza il metodo di inoltro CBR o NAT di Dispatcher, se un router al segmento locale ha un valore MTU inferiore, è necessario impostare lo stesso valore sulla macchina Dispatcher.

Per risolvere questo problema, utilizzare il comando seguente per impostare il valore di MSS (Maximum Segment Size): `dscontrol executor set mss nuovo_valore`

Ad esempio:

```
dscontrol executor set mss 1400
```

Il valore predefinito di MSS è 1460.

L'impostazione di MSS non si applica per il metodo di inoltro MAC di Dispatcher o per eventuali componenti di Load Balancer diversi da Dispatcher.

Problema: sui sistemi Windows, si verifica un errore "Il server non risponde" quando si immette un comando dscontrol o lbadmin

Quando in un sistema Windows esiste più di un indirizzo IP e il file **hosts** non specifica l'indirizzo da associare al nome host, il sistema operativo sceglie l'indirizzo più breve da associare al nome host.

Per risolvere questo problema, aggiornare il file `c:\Windows\system32\drivers\etc\hosts` con il nome host della macchina e l'indirizzo IP che si desidera vi venga associato.

IMPORTANTE: l'indirizzo IP non può essere un indirizzo cluster.

Problema: le macchine Dispatcher a disponibilità elevata potrebbero non sincronizzarsi su Linux per S/390 sui driver qeth

Quando si utilizza la funzione di disponibilità elevata su Linux per S/390 con il driver di rete qeth, i Dispatcher attivo e in sospenso potrebbero non sincronizzarsi. Questo problema potrebbe essere limitato al kernel Linux 2.6.

Se si verifica questo problema, adottare la seguente soluzione temporanea:

Definire un dispositivo di rete CTC (channel-to-channel) tra le immagini Dispatcher attivo e in standby e aggiungere un heartbeat tra gli indirizzi IP dei due endpoint CTC.

Problema: suggerimenti sulla configurazione dell'HA (high availability)

Con la funzione di alta disponibilità (HA, high availability) per Load Balancer, una macchina partner può eseguire il bilanciamento del carico se la macchina primaria riporta un errore o viene terminata. Per mantenere le connessioni tra le varie macchine, i record delle connessioni vengono inviati tra le macchine. Quando la macchina di backup utilizza la funzione di bilanciamento del carico, l'indirizzo IP del cluster viene rimosso dalla macchina di backup e viene aggiunto alla nuova macchina primaria. Esistono numerose considerazioni sulla sincronizzazione e sulla configurazione che possono influenzare questa operazione di takeover.

Per suggerimenti su come risolvere i problemi legati alla configurazione HA (high availability) come:

- Connessioni interrotte in seguito al takeover
- Macchine partner che non vengono sincronizzate
- Richieste dirette erroneamente alla macchina del partner di backup

I seguenti suggerimenti sono utili per una corretta configurazione dell'alta disponibilità sulle macchine Load Balancer.

- La posizione dei comandi HA nei file script può fare una differenza notevole.

Tra gli esempi di comandi HA vi sono:

```
dscontrol highavailability heartbeat add ...
dscontrol highavailability backup add ...
dscontrol highavailability reach add ...
```

Nella maggior parte dei casi, è necessario posizionare le definizioni HA alla fine del file. Le istruzioni del cluster, della porta e del server devono essere inserite prima delle istruzioni HA. Ciò perché quando l'alta disponibilità viene sincronizzata, quando viene ricevuto un record di connessione vengono ricercate le definizioni del cluster, della porta e del server.

Se il cluster, la porta o il server non esiste, il record della connessione viene eliminato. Se si verifica un takeover e il record non è stato replicato sulla macchina, la connessione riporterà un errore.

L'eccezione a questa regola è l'utilizzo di server posizionati configurati con il metodo di inoltro MAC. In questo caso, le istruzioni HA devono essere inserite prima delle istruzioni del server posizionato. Se le istruzioni HA non si trovano prima delle istruzioni del server collocato, Load Balancer riceve una richiesta per il server che sembra essere uguale alla richiesta in entrata per il cluster, quindi viene bilanciata. Ciò può portare a un loop di pacchetti sulla rete e a un traffico eccessivo. Quando le istruzioni HA vengono inserite prima del server posizionato, Load Balancer riconosce che non va inoltrato il traffico in entrata fino a che lo stato è ACTIVE.

- Su sistemi operativi z/OS o OS/390, l'hypervisor controlla l'interfaccia ed esegue il multiplex dell'interfaccia reale tra i sistemi operativi ospiti. Esso consente soltanto la registrazione di un guest alla volta per un indirizzo IP e viene visualizzata una finestra di aggiornamento. Ciò significa che quando l'IP del cluster viene rimosso dalla macchina di backup, è necessario aggiungere un ritardo prima di provare ad aggiungere l'IP del cluster alla macchina primaria; in caso contrario, verrà restituito un errore e le connessioni in entrata non verranno elaborate.

Per correggere questo problema, aggiungere un ritardo sleep nello script goActive. Il tempo del ritardo dipende dalla distribuzione. Si consiglia di impostare questo ritardo su 10.

- I partner HA devono essere in grado di eseguire un ping reciprocamente e devono trovarsi sulla stessa sottorete.

Per impostazione predefinita, le macchine provano a comunicare tra loro ogni mezzo secondo e rileveranno un errore dopo quattro tentativi non riusciti. Se la macchina è occupata, è possibile che si verifichino dei failover mentre il sistema funziona correttamente. È possibile aumentare il numero di tentativi emettendo il comando:

```
dscontrol executor set hatimeout <valore>
```

- Quando le macchine vengono sincronizzate, tutti i record di connessione vengono inviati dalla macchina attiva alla macchina di backup. La sincronizzazione deve essere completata nel limite predefinito di 50 secondi.

Perché ciò sia possibile, le vecchie connessioni non devono rimanere in memoria per troppo tempo. In particolare, si sono verificati dei problemi con le porte LDAP e periodi elevati di staletimeout (superiori a un giorno). L'impostazione di un valore elevato per staletimeout implica che le vecchie connessioni restano in memoria, il che causa l'invio di un numero maggiore di record di connessione durante la sincronizzazione e un maggiore utilizzo di memoria su entrambe le macchine.

Se la sincronizzazione non riesce entro un periodo staletimeout ragionevole, è possibile aumentare il valore di timeout della sincronizzazione emettendo il comando:

```
e xm 33 5 new_timeout
```

Questo comando non viene memorizzato nel file di configurazione quando viene salvato, pertanto è necessario aggiungerlo manualmente al file di configurazione se si desidera che questa impostazione venga conservata in seguito a un riavvio.

Il valore di timeout è memorizzato su un secondo e mezzo; per questo motivo, il valore predefinito per new_timeout è 100 (50 secondi).

- Quando una macchina ha un carico di lavoro elevato, emette una risposta ARP gratuita per indicare alle macchine sulla stessa sottorete del nuovo indirizzo hardware associato all'indirizzo IP del cluster. È necessario garantire che i router utilizzino queste risposte ARP e aggiornino la cache altrimenti le richieste verranno inviate al partner inattivo.

Nota: Per ulteriori informazioni sulla configurazione della funzione HA, fare riferimento a “Disponibilità elevata” a pagina 198.

Problema: su Linux, esistono delle limitazioni alla configurazione del Dispatcher quando si utilizzano server zSeries o S/390 che utilizzano schede Open System Adapter (OSA)

In generale, quando si utilizza il metodo di inoltro MAC, i server nella configurazione di Load Balancer devono trovarsi tutti sullo stesso segmento di rete, indipendentemente dalla piattaforma. I dispositivi di rete attivi come router, bridge e firewall, interferiscono con Load Balancer. Ciò si verifica in quanto le funzioni di Load Balancer come un router specializzato, modificano solo le intestazioni a livello di collegamento sull'hop successivo e su quello finale. Qualsiasi topologia di rete in cui l'hop successivo non è l'hop finale non è valida per Load Balancer.

Nota: I tunnel, come CTC (channel-to-channel) o IUCV (inter-user communication vehicle) sono spesso supportati. Tuttavia, Load Balancer deve passare attraverso il tunnel direttamente alla destinazione finale e non può pertanto essere un tunnel tra reti.

Esiste una limitazione per i server zSeries e S/390 che condividono la scheda OSA in quanto questo adattatore opera in maniera differente dalla maggior parte delle schede di rete. La scheda OSA ha la propria implementazione a livello di collegamento virtuale, che non ha niente a che vedere con Ethernet, presentato agli host Linux e z/OS. In effetti, ogni scheda OSA assomiglia a un host ethernet-to-ethernet (e non agli host OSA) e gli host che la utilizzano risponderanno come se fosse una scheda Ethernet.

La scheda OSA esegue inoltre determinate funzioni relative direttamente al livello IP. La risposta alle richieste ARP (address resolution protocol) è un esempio di funzione eseguita. un altro esempio è che la scheda OSA condivisa indirizza i pacchetti IP in base all'indirizzo IP di destinazione invece che in base a un indirizzo Ethernet come un commutatore di livello 2. In effetti, la scheda OSA è un segmento di rete con bridge su sé stessa.

Il Load Balancer che viene eseguito su un host S/390 Linux o zSeries Linux può inoltrare a host sulla stessa scheda OSA o a host sulla scheda Ethernet. Tutti gli host sulla stessa scheda OSA condivisa si trovano sullo stesso segmento.

Load Balancer può *inoltrare* su una scheda OSA condivisa a causa della natura del bridge OSA. Il bridge riconosce la porta OSA che possiede l'IP del cluster. Il bridge riconosce anche l'indirizzo MAC degli host direttamente connessi al segmento Ethernet. Pertanto, Load Balancer può eseguire un inoltro MAC su un unico bridge OSA.

Tuttavia, Load Balancer non può eseguire un inoltro in una scheda OSA condivisa. Tra questi vi è il Load Balancer su S/390 Linux quando il server di backend si trova su una scheda OSA differente da quella di Load Balancer. La scheda OSA per il server di backend identifica l'indirizzo MAC OSA per l'IP del server, ma quando un pacchetto arriva all'indirizzo di destinazione Ethernet dell'OSA del server e all'indirizzo IP del cluster, la scheda OSA del server non riconosce l'host che deve ricevere il pacchetto. Gli stessi principi che consentono il funzionamento dell'inoltro MAC OSA-to-ethernet di una delle schede OSA condivise non valgono quando si prova a eseguire un inoltro su una scheda OSA condivisa.

Soluzione alternativa:

nelle configurazioni di Load Balancer che utilizzano server zSeries o S/390 che hanno delle schede OSA, esistono due approcci che consentono di risolvere il problema appena descritto.

1. Mediante le funzioni della piattaforma

se i server nella configurazione di Load Balancer si trovano sullo stesso tipo di piattaforma zSeries o S/390, è possibile definire connessioni point-to-point (CTC o IUCV) tra Load Balancer e ogni server. Impostare gli endpoint con indirizzi IP privati. La connessione point-to-point viene utilizzata solo per il traffico tra Load Balancer e il server. Aggiungere quindi i server con l'indirizzo IP dell'endpoint del server del tunnel. con questa configurazione, il traffico del cluster passa attraverso la scheda OSA di Load Balancer e viene inoltrato sulla connessione point-to-point su cui il server risponde mediante l'instradamento predefinito. La risposta utilizza la scheda OSA del server da lasciare, che potrebbe essere o no la stessa scheda.

2. Mediante la funzione GRE di Load Balancer

Nota: Nota: la funzione GRE non è disponibile nell'ambiente a doppio protocollo di Load Balancer per IPv4 e IPv6.

Se i server nella configurazione di Load Balancer non si trovano sullo stesso tipo di piattaforma zSeries o S/390 oppure se non è possibile definire una connessione point-to-point tra Load Balancer e ogni server, si consiglia di utilizzare la funzione GRE (Generic Routing Encapsulation) di Load Balancer, che è un protocollo che consente a Load Balancer di eseguire un inoltro attraverso i router.

Quando si utilizza la funzione GRE, il pacchetto IP client->cluster viene ricevuto da Load Balancer, viene integrato e quindi inviato al server. Sul server, il pacchetto IP client->cluster originale viene incapsulato e il server risponde direttamente al client. Il vantaggio dell'utilizzo della funzione GRE sta nel fatto che Load Balancer vede soltanto il traffico client-server e non quello server-client. Lo svantaggio sta nel fatto che riduce la dimensione massima del segmento (maximum segment size, MSS) della connessione TCP a causa del sovraccarico di integrazione.

Per configurare Load Balancer in modo che utilizzi la funzione GRE, aggiungere i server mediante il seguente comando:

```
dscontrol server add cluster_add:port:server_backend router
server_backend
```

dove router server_backend è valido se Load Balancer e il server di backend sono sulla stessa sottorete IP. In caso contrario, specificare l'indirizzo IP dell'hop successivo valido come router.

Per configurare i sistemi Linux in modo da eseguire l'integrazione GRE nativa, per ogni server di backend, emettere i seguenti comandi:

```
modprobe ip_gre
ip tunnel add grelb0 mode gre ikey 3735928559
ip link set grelb0 up
ip addr add indirizzo_cluster dev grelb0
```

Nota: Non definire l'indirizzo del cluster sul loopback dei server di backend. Quando si utilizzano i server di backend z/OS, è necessario utilizzare i comandi specifici di z/OS per configurare i server per eseguire l'integrazione GRE.

Problema: su alcune versioni Linux, si verifica una mancanza di memoria quando viene eseguito il Dispatcher con il gestore e gli advisor

Quando si esegue Load Balancer configurato con le funzioni del gestore e degli advisor, si verifica una mancanza di memoria su alcune versioni di Red Hat Linux. La mancanza di memoria Java aumenta se si configura un'impostazione time-interval troppo piccola per l'advisor.

Le versioni di IBM Java SDK della JVM e Native POSIX Thread Library (NPTL) rilasciato con alcune distribuzioni Linux, come Red Hat Enterprise Linux 3.0, possono causare questa mancanza di memoria. La libreria di thread avanzati NPTL rilasciata con alcune distribuzioni di sistemi Linux come Red Hat Enterprise Linux 3.0 supporta NPTL.

Fare riferimento a <http://www.ibm.com/developerworks/java/jdk/linux/tested.html> per le informazioni più recenti sui sistemi Linux e su IBM Java SDK rilasciato con tali sistemi.

Come strumento di determinazione dei problemi, utilizzare il comando `vmstat` o `ps` per rilevare la mancanza di memoria.

Per risolvere questo problema, emettere il seguente comando prima di eseguire Load Balancer per disabilitare la libreria NPTL:

```
export LD_ASSUME_KERNEL=2.4.10
```

Problema: su SUSE Linux Enterprise Server 9, Dispatcher inoltra i pacchetti, ma i pacchetti non raggiungono il server di backend

Su Suse Linux Enterprise Server 9, quando si utilizza il metodo di inoltro MAC, il prospettodel Dispatcher indica che il pacchetto è stato inoltrato (il numero di pacchetti aumenta) ma il pacchetto non raggiunge il server di backend.

È possibile che si verifichi quanto riportato di seguito:

- Sulla macchina del Dispatcher viene visualizzato il seguente messaggio:
`ip_finish_output2: Nessuna cache di intestazione e nessun elemento vicino.`
- Sul cliente, viene visualizzato il seguente messaggio:
`Destinazione ICMP non raggiungibile: è necessaria una frammentazione`

Questo problema si verifica a causa del modulo NAT iptables che viene caricato. Su SLES 9, esiste un possibile errore (mai confermato) in questa versione di iptables che provoca un funzionamento anomalo quando si utilizza Dispatcher.

Soluzione:

Caricare il modulo NAT iptables e il modulo di traccia delle connessioni.

Ad esempio:

```
# lsmod | grep ip
iptables_filter      3072  0
iptables_nat         22060  0
ip_conntrack         32560  1 iptable_nat
ip_tables            17280  2
```



```

iptables_filter,iptable_nat
    ipv6                236800  19
    # rmmod iptable_nat
    # rmmod ip_conntrack

```

Rimuovere i moduli nello stesso ordine di utilizzo. In particolare, è possibile rimuovere un modulo solo se il numero di riferimenti (l'ultima colonna nell'output `lsmod`) è zero. Se sono state configurate delle regole in `iptables`, è necessario rimuoverle. Ad esempio: `iptables -t nat -F`.

Il modulo `iptables_nat` utilizza `ip_conntrack`, pertanto è necessario prima rimuovere il modulo `iptables_nat module`, e quindi `ip_conntrack module`.

Nota: La visualizzazione delle regole configurate su una tabella carica il modulo corrispondente, ad esempio `iptables -t nat -L`. Verificare che non venga eseguito nulla in seguito alla rimozione dei moduli.

Problema: su Windows, un messaggio di conflitto di indirizzi IP viene visualizzato durante un takeover HA

Su sistemi Windows, se si esegue la funzione HA di Load Balancer, gli script `goScripts` vengono utilizzati per configurare l'indirizzo IP del cluster sul Load Balancer attivo e per annullare la configurazione dell'IP del cluster sul sistema di backup quando viene eseguito un takeover. Se lo script `goScript` che configura l'indirizzo IP del cluster sulla macchina attiva viene eseguito prima dello script `goScript` per annullare la configurazione dell'indirizzo IP del cluster sulla macchina di backup, è possibile che si verifichino dei problemi. Viene visualizzata una finestra a comparsa che indica che il sistema ha rilevato un conflitto di indirizzi IP. Se si esegue il comando `ipconfig /all` è possibile che sulla macchina venga visualizzato l'indirizzo IP 0.0.0.0.

Soluzione:

emettere il seguente comando per annullare manualmente la configurazione dell'indirizzo IP del cluster dalla macchina primaria:

```
dscontrol executor unconfigure clusterIP
```

Tale comando rimuove l'indirizzo 0.0.0.0 dallo stack IP Windows.

Quando il partner HA rilascia l'indirizzo IP del cluster, emettere il seguente comando per aggiungere manualmente di nuovo l'indirizzo IP del cluster:

```
dscontrol executor configure clusterIP
```

Dopo aver emesso questo comando, ricercare l'indirizzo IP del cluster sullo stack IP di Windows emettendo il seguente comando:

```
ipconfig /all
```

Problema: Linux iptables può interferire con l'instradamento dei pacchetti

Linux `iptables` può interferire con il bilanciamento del carico del traffico e deve essere disabilitato sulla macchina Dispatcher.

Emettere il seguente comando per determinare se `iptables` sono state caricate:

```
lsmod | grep ip_tables
```

L'output del comando precedente può essere simile al seguente:

```
ip_tables          22400    3
iptables_mangle, iptable_nat, iptable_filter
```

Emettere il seguente comando per ogni iptable riportata nell'output per visualizzare le regole per le tabelle:

```
iptables -t <short_name> -L
```

For example:

```
iptables -t mangle -L
iptables -t nat -L
iptables -t filter -L
```

Se iptable_nat viene caricata, allora questa deve essere scaricata. Poiché iptable_nat ha una dipendenza su iptable_conntrack, è necessario anche rimuovere iptable_conntrack. Emettere il seguente comando per scaricare queste due iptables:

```
rmmod iptable_nat iptable_conntrack
```

Problema: impossibile aggiungere un server IPv6 alla configurazione di Load Balancer su sistemi Solaris

Su sistemi Solaris, quando si prova a configurare un server IPv6 su una installazione Load Balancer per IPv4 e IPv6, viene visualizzato il messaggio impossibile aggiungere il server. Tale messaggio può essere causato dal modo in cui il sistema operativo Solaris gestisce la richiesta di ping per un indirizzo IPv6.

Su sistemi Solaris, quando si aggiunge un server alla configurazione, Load Balancer prova a eseguire il ping al server per ottenere l'indirizzo MAC del server. La macchina Solaris può scegliere l'indirizzo del cluster configurato come indirizzo di origine della richiesta ping invece che utilizzare l'indirizzo NFA della macchina. Se l'indirizzo del cluster è configurato sul loopback del server, la risposta al ping non viene ricevuta sulla macchina Load Balancer e pertanto il server non viene aggiunto alla configurazione.

La soluzione sta nel configurare un altro indirizzo IPv6 sulla macchina Load Balancer prima o dopo la configurazione dell'indirizzo del cluster IPv6. Questo indirizzo deve essere un indirizzo senza alias sul loopback del server di backend che si sta provando ad aggiungere alla configurazione di Load Balancer. Quindi aggiungere il server alla configurazione di Load Balancer.

Messaggio di avvertenza Java visualizzato quando si installano le fix di servizio

Load Balancer fornisce una serie di file Java insieme all'installazione del prodotto. L'installazione del prodotto è costituita da diversi pacchetti che non devono essere installati sulla stessa macchina. Tra questi pacchetti vi sono il pacchetto Metric Server, il pacchetto di gestione e il pacchetto di base. Tutti questi pacchetti di codice richiedono una serie di file Java funzionante ma ognuno di questi tre pacchetti può essere installato su una macchina separata. Pertanto, ognuno di questi pacchetti installa una serie di file Java. Se installata sulla stessa macchina, la serie di file Java sarà di proprietà di ognuna di queste serie di file. Quando si installa la seconda e la terza serie di file Java, verrà visualizzato un messaggio di avvertenza che indica che la serie di file Java è di proprietà di un'altra serie di file.

Quando si installa il codice mediante i metodi di installazione nativi (ad esempio, installp su AIX), è necessario ignorare i messaggi di avvertenza.

Aggiornamento della serie di file Java fornita con l'installazione di Load Balancer

Durante il processo di installazione di Load Balancer, viene installata una serie di file Java. Load Balancer sarà l'unica applicazione che utilizza la versione Java che installa il prodotto. Non è necessario aggiornare questa versione della serie di file Java. Se si verifica un problema che richiede un aggiornamento della serie di file Java, è necessario riportare il problema all'assistenza IBM in modo da poter ricevere un aggiornamento alla serie di file Java fornita con l'installazione di Load Balancer.

Risoluzione di problemi comuni—CBR

Problema: mancata esecuzione di CBR

Questo problema può verificarsi quando un'altra applicazione utilizza una delle porte utilizzate da CBR. Per ulteriori informazioni, vedere "Controllo dei numeri di porta di CBR" a pagina 291.

Problema: esecuzione errata dei comandi `cbrcontrol` o `lbadmin`

1. Il comando `cbrcontrol` restituisce: **Errore: il server non risponde**. Oppure, il comando `lbadmin` restituisce: **Errore: impossibile accedere al server RMI**. Questi errori possono verificarsi quando la macchina ha uno stack abilitato ai socks. Per correggere il problema, modificare il file `socks.cnf` in modo che contenga le righe seguenti:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```

2. Le console di gestione per le interfacce Load Balancer (riga comandi, interfaccia utente grafica e procedure guidate) comunicano con `cbrserver` mediante RMI (Remote Method Invocation). La comunicazione predefinita sfrutta tre porte, ciascuna delle quali è impostata nello script di avvio di `cbrserver`:
 - 11099 per ricevere comandi da `cbrcontrol`
 - 10004 per inviare query di metrica a Metric Server
 - 11199 per la porta del server RMI

Questo può causare problemi quando una delle console di gestione viene eseguita sulla stessa macchina di un firewall, oppure attraverso un firewall. Ad esempio, quando Load Balancer viene eseguito sulla stessa macchina di un firewall, e si immettono comandi di `cbrcontrol`, potrebbero comparire errori quale **Errore: il server non risponde**.

Per evitare questo problema, modificare il file script di `cbrserver` per impostare la porta utilizzata da RMI per il firewall (o altra applicazione). Modificare la riga: `LB_RMISERVERPORT=11199` in `LB_RMISERVERPORT=propriaPorta`. Dove *propriaPorta* è una porta diversa.

Al termine dell'operazione, riavviare `cbrserver` e aprire il traffico per le porte 11099, 10004, 11199 e 11100, oppure per la porta prescelta per l'indirizzo host da cui verrà eseguita la console di gestione.

3. Questi errori possono inoltre verificarsi se non è stato già avviato **`cbrserver`**.

Problema: le richieste non vengono sottoposte a bilanciamento del carico

Caching Proxy e CBR sono stati avviati, ma le richieste non vengono sottoposte a bilanciamento del carico. Questo errore può verificarsi se si avvia Caching Proxy prima dell'executor. In tal caso, il log stderr di Caching Proxy conterrà il seguente messaggio di errore: "ndServerInit: impossibile stabilire collegamento all'executor." Per evitare questo problema, avviare l'executor prima di Caching Proxy.

Problema: su Solaris, il comando **cbrcontrol executor start** non riesce

Su Solaris, il comando **cbrcontrol executor start** restituisce: "Errore: executor non avviato." Questo errore si verifica se non si configura IPC (Inter-process Communication) per il sistema in modo che la dimensione massima di un segmento di memoria condivisa e gli ID semaforo sono più grandi del valore predefinito del sistema operativo. Per aumentare la dimensione del segmento di memoria condivisa e gli ID semaforo, è necessario modificare il file **/etc/system**. Per ulteriori informazioni su come configurare questo file vedere la pagina 111.

Problema: errore di sintassi o di comunicazione

Il mancato funzionamento della regola URL può dipendere da un errore di sintassi o di configurazione. Per risolvere il problema, controllare quanto segue:

- Verificare che la regola sia configurata correttamente. Vedere Appendice B, "Sintassi della regola di contenuto (modello)", a pagina 463 per i dettagli.
- Immettere un comando **cbrcontrol rule report** per questa regola e controllare la colonna 'Times Fired' per verificare se il suo valore è incrementato in base al numero di richieste effettuate. Se è incrementato correttamente, ricontrollare la configurazione del server.
- Se la regola non viene attivata, aggiungere una regola 'sempre true'. Immettere un comando **cbrcontrol rule report** sulla regola 'sempre true' per verificare che venga attivata.

Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP

Sulla piattaforma Windows, quando si utilizza una scheda Matrox AGP, potrebbero verificarsi comportamenti imprevisti della GUI di Load Balancer. Quando si fa clic con il mouse, un blocco leggermente più grande del puntatore può corrompersi, provocando un'evidenziazione inversa o lo spostamento delle immagini sullo schermo. Questo comportamento è stato riscontrato nelle schede Matrox meno recenti. Non è disponibile una correzione nota in caso di utilizzo di schede Matrox AGP.

Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web

Se si sta utilizzando la gestione Web remota, per configurare Load Balancer, non ridimensionare la finestra del browser Netscape (riduzione, ingrandimento, ripristino in basso e così via) in cui viene visualizzata la GUI di Load Balancer. Poiché Netscape ricarica una pagina ogni volta che le finestre del browser vengono ridimensionate, questo provoca la disconnessione dall'host. Sarà necessario

riconnettersi all'host ogni volta che si ridimensiona una finestra. Se si esegue la gestione Web da remoto su una piattaforma Windows, utilizzare Internet Explorer.

Problema: sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti

In una finestra del prompt dei comandi sul sistema operativo Windows, alcuni caratteri nazionali della famiglia Latin-1 potrebbero risultare corrotti. Ad esempio, la lettera "a" con la tilde potrebbe essere visualizzata come un simbolo di pi greco. Per risolvere questo problema, è necessario modificare le proprietà dei font della finestra del prompt dei comandi. Per modificare il font, procedere come indicato di seguito:

1. Fare clic sull'icona nell'angolo superiore sinistro della finestra del prompt dei comandi
2. Selezionare Proprietà, quindi fare clic sulla scheda Tipo di carattere
3. L'impostazione predefinita è Caratteri raster; sostituirla con Lucida Console e fare clic su OK

Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java

Alcune installazioni di HP-UX 11i sono preconfigurate per consentire solo 64 thread per processo. Tuttavia, alcune configurazioni di Load Balancer richiedono una quantità superiore. Per i sistemi HP-UX, impostare i thread per processo almeno su 256. Per aumentare il valore, servirsi dell'utilità "sam" per impostare il parametro del kernel `max_thread_proc`. Se si prevede un utilizzo intensivo, potrebbe essere necessario aumentare `max_thread_proc` oltre 256.

Per aumentare il valore di `max_thread_proc`, procedere come indicato in 304.

Problema: su Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi

Durante la configurazione della scheda su una macchina Load Balancer, è necessario accertarsi che le due impostazioni seguenti siano corrette, per consentire il funzionamento dell'advisor:

- Disabilitare Task Offload, generalmente utilizzato nelle schede di rete 3Com.
- Abilitare Protocol 1 (ICMP) per i protocolli IP se si abilita il filtro TCP/IP. Se ICMP non è abilitato, la prova ping al server di backend non riesce.

Fare riferimento a 304 per istruzioni sulla configurazione di questa impostazione.

Problema: su Windows, si verificano problemi nella risoluzione di un indirizzo IP su un nome host quando su una scheda sono configurati più indirizzi

Sulla piattaforma Windows, quando si configura una scheda perché abbia più indirizzi IP, configurare l'indirizzo IP che si desidera associare al nome host come primo nel registro.

Poiché Load Balancer dipende da `InetAddress.getLocalHost()` in molti casi (ad esempio, per `lbkeys create`), più indirizzi IP con alias su una singola scheda possono causare problemi. Per evitare questo problema, collocare per primo nell'elenco del registro l'indirizzo IP sul quale si desidera venga risolto il nome host.

Fare riferimento a pagina 305 per le fasi di configurazione del nome host come primo nel registro.

Risoluzione di problemi comuni—Site Selector

Problema: mancata esecuzione di Site Selector

Questo problema può verificarsi quando un'altra applicazione utilizza una delle porte utilizzate da Site Selector. Per ulteriori informazioni, vedere "Controllo dei numeri di porta di Site Selector" a pagina 292.

Problema: Site Selector non esegue il round-robin del traffico dai client Solaris

Sintomo: Site Selector non esegue il round-robin delle richieste in entrata da client Solaris.

Causa possibile: i sistemi Solaris eseguono un daemon cache del servizio nomi. Se questo daemon è in esecuzione, alla richiesta seguente di resolver verrà fornita risposta da questa cache anziché da un'interrogazione di Site Selector.

Soluzione: disattivare il daemon cache del servizio nomi sulla macchina Solaris.

Problema: esecuzione errata dei comandi sscontrol o lbadmin

1. Il comando sscontrol restituisce: **Errore: il server non risponde**. Oppure, il comando lbadmin restituisce: **Errore: impossibile accedere al server RMI**. Questi errori possono verificarsi quando la macchina ha uno stack abilitato ai socks. Per correggere il problema, modificare il file socks.cnf in modo che contenga le righe seguenti:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```
2. Le console di gestione per le interfacce Load Balancer (riga comandi, interfaccia utente grafica e procedure guidate) comunicano con ssserver mediante RMI (Remote Method Invocation). La comunicazione predefinita sfrutta tre porte, ciascuna delle quali è impostata nello script di avvio di ssserver:
 - 12099 per ricevere comandi da sscontrol
 - 10004 per inviare query di metrica a Metric Server
 - 12199 per la porta del server RMI
 - 53 per inviare e ricevere traffico DNS

Questo può causare problemi quando una delle console di gestione viene eseguita sulla stessa macchina di un firewall, oppure attraverso un firewall. Ad esempio, quando Load Balancer viene eseguito sulla stessa macchina di un firewall, e si immettono comandi di sscontrol, potrebbero comparire errori quale **Errore: il server non risponde**.

Per evitare questo problema, modificare il file script di ssserver per impostare la porta utilizzata da RMI per il firewall (o altra applicazione). Modificare la riga: `LB_RMISERVERPORT=10199` in `LB_RMISERVERPORT=propriaPorta`. Dove *propriaPorta* è una porta diversa.

Al termine dell'operazione, riavviare ssserver e aprire il traffico per le porte 12099, 10004, 12199 e 12100, oppure per la porta prescelta per l'indirizzo host da cui verrà eseguita la console di gestione.

3. Questi errori possono inoltre verificarsi se non è stato già avviato ssserver.

Problema: ssserver non si avvia su piattaforma Windows

Site Selector deve poter partecipare a un DNS. Tutte le macchine coinvolte nella configurazione dovrebbero partecipare anch'esse al sistema. I sistemi Windows non richiedono che il nome host sia nel DNS. Per avviarsi correttamente, Site Selector richiede che il proprio nome host sia definito nel DNS.

Verificare che questo host sia definito nel DNS. Modificare il file ssserver.cmd ed eliminare "w" da "javaw". Questo dovrebbe fornire ulteriori informazioni sugli errori.

Problema: Site Selector con instradamenti duplicati non esegue correttamente il bilanciamento del carico

Il server dei nomi di Site Selector non si associa ad alcun indirizzo sulla macchina. Risponderà alle richieste destinate a qualsiasi IP valido sulla macchina. Site Selector si affida al sistema operativo per inoltrare le risposte al client. Se la macchina Site Selector dispone di più schede e qualsiasi numero di queste è collegato alla stessa sottorete, il sistema operativo potrebbe inviare la risposta al client da un indirizzo diverso rispetto a quello su cui è stata ricevuta la richiesta. Alcune applicazioni client non accettano una risposta da un indirizzo diverso da quello a cui è stata inviata la richiesta. Di conseguenza, la risoluzione nome sembra non riuscire.

Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP

Sulla piattaforma Windows, quando si utilizza una scheda Matrox AGP, potrebbero verificarsi comportamenti imprevisti della GUI di Load Balancer. Quando si fa clic con il mouse, un blocco leggermente più grande del puntatore può corrompersi, provocando un'evidenziazione inversa o lo spostamento delle immagini sullo schermo. Questo comportamento è stato riscontrato nelle schede Matrox meno recenti. Non è disponibile una correzione nota in caso di utilizzo di schede Matrox AGP.

Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web

Se si sta utilizzando la gestione Web remota, per configurare Load Balancer, non ridimensionare la finestra del browser Netscape (riduzione, ingrandimento, ripristino in basso e così via) in cui viene visualizzata la GUI di Load Balancer. Poiché Netscape ricarica una pagina ogni volta che le finestre del browser vengono ridimensionate, questo provoca la disconnessione dall'host. Sarà necessario riconnettersi all'host ogni volta che si ridimensiona una finestra. Se si esegue la gestione Web da remoto su una piattaforma Windows, utilizzare Internet Explorer.

Problema: sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti

In una finestra del prompt dei comandi sul sistema operativo Windows, alcuni caratteri nazionali della famiglia Latin-1 potrebbero risultare corrotti. Ad esempio, la lettera "a" con la tilde potrebbe essere visualizzata come un simbolo di pi greco.

Per risolvere questo problema, è necessario modificare le proprietà dei font della finestra del prompt dei comandi. Per modificare il font, procedere come indicato di seguito:

1. Fare clic sull'icona nell'angolo superiore sinistro della finestra del prompt dei comandi
2. Selezionare Proprietà, quindi fare clic sulla scheda Tipo di carattere
3. L'impostazione predefinita è Caratteri raster; sostituirla con Lucida Console e fare clic su OK

Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java

Alcune installazioni di HP-UX 11i sono preconfigurate per consentire solo 64 thread per processo. Tuttavia, alcune configurazioni di Load Balancer richiedono una quantità superiore. Per i sistemi HP-UX, impostare i thread per processo almeno su 256. Per aumentare il valore, servirsi dell'utilità "sam" per impostare il parametro del kernel max_thread_proc. Se si prevede un utilizzo intensivo, potrebbe essere necessario aumentare max_thread_proc oltre 256.

Per aumentare il valore di max_thread_proc, procedere come indicato in 304.

Problema: su Windows, gli advisor e le destinazioni finali contrassegnano tutti i server come inattivi

Durante la configurazione della scheda su una macchina Load Balancer, è necessario accertarsi che le due impostazioni seguenti siano corrette, per consentire il funzionamento dell'advisor:

- Disabilitare Task Offload, generalmente utilizzato nelle schede di rete 3Com.
- Abilitare Protocol 1 (ICMP) per i protocolli IP se si abilita il filtro TCP/IP. Se ICMP non è abilitato, la prova ping al server di backend non riesce.

Fare riferimento a 304 per istruzioni sulla configurazione di questa impostazione.

Risoluzione di problemi comuni—Controller Cisco CSS

Problema: mancato avvio di ccoserver

Questo problema può verificarsi quando un'altra applicazione utilizza una delle porte utilizzate da Cisco CSS Controller ccoserver. Per ulteriori informazioni, vedere "Controllo dei numeri di porta di Cisco CSS Controller" a pagina 293.

Problema: esecuzione errata dei comandi ccocontrol o lbadmin

1. Il comando ccocontrol restituisce: **Errore: il server non risponde**. Oppure, il comando lbadmin restituisce: **Errore: impossibile accedere al server RMI**. Questi errori possono verificarsi quando la macchina ha uno stack abilitato ai socks. Per correggere il problema, modificare il file socks.cnf in modo che contenga le righe seguenti:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```
2. Le console di gestione per le interfacce di Load Balancer (riga comandi e interfaccia utente grafica) comunicano con ccoserver mediante RMI (Remote Method Invocation). La comunicazione predefinita sfrutta tre porte, ciascuna delle quali è impostata nello script di avvio di ccoserver:

- 13099 per ricevere comandi da ccocontrol
- 10004 per inviare query di metrica a Metric Server
- 13199 per la porta del server RMI

Questo può causare problemi quando una delle console di gestione viene eseguita sulla stessa macchina di un firewall, oppure attraverso un firewall. Ad esempio, quando Load Balancer viene eseguito sulla stessa macchina di un firewall, e si immettono comandi di ccocontrol, potrebbero comparire errori quale **Errore: il server non risponde**.

Per evitare questo problema, modificare il file script di ccoserver per impostare la porta utilizzata da RMI per il firewall (o altra applicazione). Modificare la riga: `CCO_RMISERVERPORT=14199` in `CCO_RMISERVERPORT=propriaPorta`. Dove *propriaPorta* è una porta diversa.

Al termine dell'operazione, riavviare ccoserver e aprire il traffico per le porte 13099, 10004, 13199 e 13100, oppure per la porta prescelta per l'indirizzo host da cui verrà eseguita la console di gestione.

3. Questi errori possono inoltre verificarsi se non è stato già avviato **ccoserver**.

Problema: impossibile creare il registro sulla porta 13099

Questo problema può verificarsi quando manca una licenza del prodotto valida. Quando si tenta di avviare ccoserver, si riceve il seguente messaggio:

La licenza è scaduta. Contattare il rappresentante
o il distributore autorizzato IBM locale.

Per correggere questo problema:

1. Se si è già tentato di avviare ccoserver, digitare **ccoserver stop**.
2. Copiare la licenza valida nella directory `...ibm/edge/lb/servers/conf`.
3. Digitare **ccoserver** per avviare il server.

Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP

Sulla piattaforma Windows, quando si utilizza una scheda Matrox AGP, potrebbero verificarsi comportamenti imprevisti della GUI di Load Balancer. Quando si fa clic con il mouse, un blocco leggermente più grande del puntatore può corrompersi, provocando un'evidenziazione inversa o lo spostamento delle immagini sullo schermo. Questo comportamento è stato riscontrato nelle schede Matrox meno recenti. Non è disponibile una correzione nota in caso di utilizzo di schede Matrox AGP.

Problema: viene ricevuto un errore di connessione durante l'aggiunta di un consultant

Durante l'aggiunta di un consultant, potrebbe verificarsi un errore di connessione, dovuto a una configurazione errata. Per correggere questo problema:

- Accertarsi che l'indirizzo o la community specificati corrispondano esattamente ai valori configurati sullo switch.
- Accertarsi che sia disponibile connettività tra il controller e lo switch.
- Accertarsi che la community abbia le autorizzazioni di lettura-scrittura sullo switch. Il controller tenterà di abilitare la variabile `ApSvcLoadEnable` (SNMP) durante la verifica dell'accesso in scrittura alla connessione.

Problema: i pesi non vengono aggiornati sullo switch

Per correggere questo problema

- Se si utilizzano le metriche Active connections o Connection rate, immettere ccocontrol service SWID:OCID:serviceIO report. Verificare che i valori di metrica cambino in conformità con il traffico in transito sullo switch.
- Aumentare il livello di log di consultant e ricercare le occorrenze di SNMP TimeOut. Se si verificano timeout, le soluzioni possibili comprendono:
 - Riduzione del carico dello switch.
 - Riduzione del ritardo di rete tra lo switch e il controller.
- Arresto e riavvio del consultant.

Problema: il comando di aggiornamento non ha aggiornato la configurazione del consultant

Aumentare il livello di log di consultant e riprovare il comando. Se fallisce nuovamente, ricercare SNMP timeout o altri errori di comunicazione SNMP nel log.

Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web

Se si sta utilizzando la gestione Web remota, per configurare Load Balancer, non ridimensionare la finestra del browser Netscape (riduzione, ingrandimento, ripristino in basso e così via) in cui viene visualizzata la GUI di Load Balancer. Poiché Netscape ricarica una pagina ogni volta che le finestre del browser vengono ridimensionate, questo provoca la disconnessione dall'host. Sarà necessario riconnettersi all'host ogni volta che si ridimensiona una finestra. Se si esegue la gestione Web da remoto su una piattaforma Windows, utilizzare Internet Explorer.

Problema: sulla piattaforma Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti

In una finestra del prompt dei comandi sul sistema operativo Windows, alcuni caratteri nazionali della famiglia Latin-1 potrebbero risultare corrotti. Ad esempio, la lettera "a" con la tilde potrebbe essere visualizzata come un simbolo di pi greco. Per risolvere questo problema, è necessario modificare le proprietà dei font della finestra del prompt dei comandi. Per modificare il font, procedere come indicato di seguito:

1. Fare clic sull'icona nell'angolo superiore sinistro della finestra del prompt dei comandi
2. Selezionare Proprietà, quindi fare clic sulla scheda Tipo di carattere
3. L'impostazione predefinita è Caratteri raster; sostituirla con Lucida Console e fare clic su OK

Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java

Alcune installazioni di HP-UX 11i sono preconfigurate per consentire solo 64 thread per processo. Tuttavia, alcune configurazioni di Load Balancer richiedono una quantità superiore. Per i sistemi HP-UX, impostare i thread per processo almeno su 256. Per aumentare il valore, servirsi dell'utilità "sam" per impostare il parametro del kernel max_thread_proc. Se si prevede un utilizzo intensivo, potrebbe essere necessario aumentare max_thread_proc oltre 256.

Risoluzione di problemi comuni—Controller Nortel Alteon

Problema: mancato avvio di `nalserver`

Questo problema può verificarsi quando un'altra applicazione utilizza una delle porte utilizzate da Controller Nortel Alteon `nalserver`. Per ulteriori informazioni, vedere "Controllo dei numeri di porta di Controller Nortel Alteon" a pagina 293.

Problema: esecuzione errata dei comandi `nalcontrol` o `lbadm`

1. Il comando `nalcontrol` restituisce: **Errore: il server non risponde**. Oppure, il comando `lbadm` restituisce: **Errore: impossibile accedere al server RMI**. Questi errori possono verificarsi quando la macchina ha uno stack abilitato ai socks. Per correggere il problema, modificare il file `socks.cnf` in modo che contenga le righe seguenti:

```
EXCLUDE-MODULE java
EXCLUDE-MODULE javaw
```

2. Le console di gestione per le interfacce Load Balancer (riga comandi e interfaccia utente grafica) comunicano con `nalserver` mediante RMI (Remote Method Invocation). La comunicazione predefinita sfrutta tre porte, ciascuna delle quali è impostata nello script di avvio di `nalserver`:

- 14099 per ricevere comandi da `nalcontrol`
- 10004 per inviare query di metrica a Metric Server
- 14199 per la porta del server RMI

Questo può causare problemi quando una delle console di gestione viene eseguita sulla stessa macchina di un firewall, oppure attraverso un firewall. Ad esempio, quando Load Balancer viene eseguito sulla stessa macchina di un firewall, e si immettono comandi di `nalcontrol`, potrebbero comparire errori quale **Errore: il server non risponde**.

Per evitare questo problema, modificare il file script di `nalserver` per impostare la porta utilizzata da RMI per il firewall (o altra applicazione). Modificare la riga: `NAL_RMISERVERPORT=14199` in `NAL_RMISERVERPORT=propriaPorta`. Dove *propriaPorta* è una porta diversa.

Al termine dell'operazione, riavviare `nalserver` e aprire il traffico per le porte 14099, 10004, 14199 e 14100, oppure per la porta prescelta per l'indirizzo host da cui verrà eseguita la console di gestione.

3. Questi errori possono inoltre verificarsi se non è stato già avviato **`nalserver`**.

Problema: impossibile creare il registro sulla porta 14099

Questo problema può verificarsi quando manca una licenza del prodotto valida. Quando si tenta di avviare `nalserver`, si riceve il seguente messaggio:

La licenza è scaduta. Contattare il rappresentante
o il distributore autorizzato IBM locale.

Per correggere questo problema:

1. Se si è già tentato di avviare `nalserver`, digitare **`nalserver stop`**.
2. Copiare la licenza valida nella directory `...ibm/edge/lb/servers/conf`.
3. Digitare **`nalserver`** per avviare il server.

Problema: sulla piattaforma Windows, si verifica un comportamento imprevisto della GUI quando si utilizzano schede video Matrox AGP

Sulla piattaforma Windows, quando si utilizza una scheda Matrox AGP, potrebbero verificarsi comportamenti imprevisti della GUI di Load Balancer. Quando si fa clic con il mouse, un blocco leggermente più grande del puntatore può corrompersi, provocando un'evidenziazione inversa o lo spostamento delle immagini sullo schermo. Questo comportamento è stato riscontrato nelle schede Matrox meno recenti. Non è disponibile una correzione nota in caso di utilizzo di schede Matrox AGP.

Problema: si verifica una disconnessione dall'host quando si ridimensiona la finestra del browser Netscape durante l'uso della gestione Web

Se si sta utilizzando la gestione Web remota, per configurare Load Balancer, non ridimensionare la finestra del browser Netscape (riduzione, ingrandimento, ripristino in basso e così via) in cui viene visualizzata la GUI di Load Balancer. Poiché Netscape ricarica una pagina ogni volta che le finestre del browser vengono ridimensionate, questo provoca la disconnessione dall'host. Sarà necessario riconnettersi all'host ogni volta che si ridimensiona una finestra. Se si esegue la gestione Web da remoto su una piattaforma Windows, utilizzare Internet Explorer.

Problema: viene ricevuto un errore di connessione durante l'aggiunta di un consultant

Durante l'aggiunta di un consultant, potrebbe verificarsi un errore di connessione, dovuto a una configurazione errata. Per correggere questo problema:

- Accertarsi che l'indirizzo o la community specificati corrispondano esattamente ai valori configurati sullo switch.
- Accertarsi che sia disponibile connettività tra il controller e lo switch.
- Accertarsi che la community abbia le autorizzazioni di lettura-scrittura sullo switch. Il controller tenterà di abilitare la variabile `ApSvcLoadEnable` (SNMP) durante la verifica dell'accesso in scrittura alla connessione.

Problema: i pesi non vengono aggiornati sullo switch

Per correggere questo problema

- Se si utilizzano le metriche Active connections o Connection rate, immettere `ccocontrol service SWID:OCID:serviceIO report`. Verificare che i valori di metrica cambino in conformità con il traffico in transito sullo switch.
- Aumentare il livello di log di consultant e ricercare le occorrenze di SNMP Timeout. Se si verificano timeout, le soluzioni possibili comprendono:
 - Riduzione del carico dello switch.
 - Riduzione del ritardo di rete tra lo switch e il controller.
- Arresto e riavvio del consultant.

Problema: il comando di aggiornamento non ha aggiornato la configurazione del consultant

Aumentare il livello di log di consultant e riprovare il comando. Se fallisce nuovamente, ricercare SNMP timeout o altri errori di comunicazione SNMP nel log.

Problema: su Windows, al prompt dei comandi vengono visualizzati caratteri nazionali Latin-1 corrotti

In una finestra del prompt dei comandi sul sistema operativo Windows, alcuni caratteri nazionali della famiglia Latin-1 potrebbero risultare corrotti. Ad esempio, la lettera "a" con la tilde potrebbe essere visualizzata come un simbolo di pi greco. Per risolvere questo problema, è necessario modificare le proprietà dei font della finestra del prompt dei comandi. Per modificare il font, procedere come indicato di seguito:

1. Fare clic sull'icona nell'angolo superiore sinistro della finestra del prompt dei comandi
2. Selezionare Proprietà, quindi fare clic sulla scheda Tipo di carattere
3. L'impostazione predefinita è Caratteri raster; sostituirla con Lucida Console e fare clic su OK

Problema: su HP-UX, si verifica un errore di esaurimento memoria / thread di Java

Alcune installazioni di HP-UX 11i sono preconfigurate per consentire solo 64 thread per processo. Tuttavia, alcune configurazioni di Load Balancer richiedono una quantità superiore. Per i sistemi HP-UX, impostare i thread per processo almeno su 256. Per aumentare il valore, servirsi dell'utilità "sam" per impostare il parametro del kernel `max_thread_proc`. Se si prevede un utilizzo intensivo, potrebbe essere necessario aumentare `max_thread_proc` oltre 256.

Per aumentare il valore di `max_thread_proc`, procedere come indicato in 304.

Risoluzione di problemi comuni—Metric Server

Problema: Metric Server IOException su piattaforma Windows durante l'esecuzione di file di metrica utente .bat o .cmd

È necessario utilizzare il nome metrica completo per le metriche scritte dall'utente su Metric Server in esecuzione sulla piattaforma Windows. Ad esempio, è necessario specificare **usermetric.bat** anziché **usermetric**. Il nome **usermetric** è valido sulla riga comandi, ma non funziona quando viene eseguito nell'ambiente di runtime. Se non si utilizza il nome metrica completo, verrà generata una IOException di Metric Server. Impostare la variabile `LOG_LEVEL` a un valore 3 nel file dei comandi `metricserver`, quindi controllare l'output del log. In questo esempio, l'eccezione appare come:

```
... java.io.IOException: CreateProcess: usermetric error=2
```

Problema: Metric Server non notifica i carichi alla macchina Load Balancer

Le ragioni per cui Metric Server non notifica le informazioni sui carichi a Load Balancer possono essere diverse. Per individuare la causa, eseguire questi controlli:

- Accertarsi che i file di chiavi siano stati trasferiti a Metric Server.
- Verificare che il nome host della macchina Metric Server sia registrato nel server dei nomi locale.

È inoltre possibile risolvere questo problema specificando il nome host nella proprietà Java `java.rmi.server.hostname` nello script `metricserver`.

- Riavviare con un livello di log superiore e ricercare errori.

- Sulla macchina Load Balancer, aumentare il livello di log per Metric Monitor utilizzando il comando **dscontrol manager metric set**. Ricercare errori nel file MetricMonitor.log.

Problema: nel log di Metric Server è riportato "La firma è necessaria per l'accesso all'agente"

Questo messaggio di errore compare nel log di Metric Server dopo che i file di chiavi sono stati trasferiti al server.

Questo errore viene registrato quando il file di chiavi non supera l'autorizzazione con la coppia di chiavi a causa di una corruzione nella coppia. Per correggere questo problema, provare quanto segue:

- Trasferire nuovamente il file di chiavi tramite FTP utilizzando il metodo di trasferimento binario.
- Creare una nuova chiave e ridistribuirla.

Problema: su AIX, durante l'esecuzione di Metric Server in condizioni di carico pesante l'output del comando ps -vg può risultare corrotto

Quando si esegue Metric Server sotto carichi elevati in un sistema multiprocessore con piattaforma AIX (4.3.3, 5.1 a 32 bit o 5.1 a 64 bit), l'output del comando ps -vg potrebbe risultare corrotto. Ad esempio:

```
55742 - A 88:19 42 18014398509449680 6396 32768 22 36 2.8 1.0 java -Xms
```

I campi SIZE e/o RSS del comando ps potrebbero indicare un uso eccessivo della memoria.

Si tratta di un problema noto del kernel AIX. L'APAR IY33804 correggerà questo problema. Ottenere la correzione dall'assistenza AIX all'indirizzo <http://techsupport.services.ibm.com/server/fixes>, o contattare il rappresentante dell'assistenza AIX locale.

Problema: impostazione di Metric Server in una configurazione a due livelli, con bilanciamento del carico mediante Site Selector tra Dispatcher a disponibilità elevata

In una configurazione Load Balancer a due livelli, se Site Selector (primo livello) esegue il bilanciamento del carico tra una coppia di partner Dispatcher a disponibilità elevata (secondo livello), è necessario completare alcuni passaggi per configurare il componente Metric Server. Metric Server deve essere configurato per rimanere in ascolto su un nuovo indirizzo IP, ad esso specificamente destinato. Sulle due macchine Dispatcher a disponibilità elevata, Metric Server è attivo solo sul Dispatcher attivo.

Per configurare correttamente questa impostazione, completare le seguenti operazioni:

- Configurare Metric Server in modo che sia in ascolto sul nuovo IP locale. Non dovrà essere consentito che risponda sull'indirizzo NFA locale. Per informazioni sulla configurazione, fare riferimento a "Metric Server" a pagina 191.
- Poiché Site Selector deve comunicare solo con il Dispatcher attivo, è necessario avviare e arrestare Metric Server negli script "go" a disponibilità elevata. Per avviare o arrestare correttamente Metric Server, creare un alias al nuovo indirizzo IP specifico di Metric Server sulla macchina. Modificare gli script "go"

per spostare l'indirizzo IP di Metric Server (operazione analoga allo spostamento degli indirizzi cluster) in modo che lo script goActive sposti l'IP di Metric Server dal loopback a una scheda fisica e lo script goStandby faccia l'inverso. Dopo aver spostato l'indirizzo IP, lo script goActive deve eseguire il comando **metricserver** per avviare Metric Server. Lo script goStandby deve eseguire **metricserver stop** per impedire che Metric Server comunichi con Site Selector durante la modalità standby.

- Sulla piattaforma Windows, fare riferimento a “Utilizzo di script” a pagina 202 per lo spostamento dell'indirizzo IP specifico di Metric Server.
- Le modifiche eseguite dallo script goStandby comprendono istruzioni specifiche dei sistemi operativi, nel modo seguente:
 - **HP-UX, Linux e Solaris:** nella sezione dello script goStandby in cui l'indirizzo cluster viene spostato sul loopback, inserire comandi per spostare l'IP specifico di Metric Server sul loopback. Quindi, inserire il comando **metricserver stop** per interrompere le risposte di Metric Server a Site Selector.
 - **Sistemi AIX:** nella sezione all'interno dello script goStandby in cui l'indirizzo del cluster è spostato sul loopback, inserire i comandi per spostare l'indirizzo IP specifico di metric server sul loopback. Quindi, aggiungere un instradamento per consentire la comunicazione con l'alias loopback. Eseguire il comando **route add IPmetricserver 127.0.0.1**. Quindi, inserire il comando **metricserver stop** per impedire che Metric Server risponda ulteriormente a Site Selector. Dopo l'arresto di Metric Server, l'ultima operazione consiste nella rimozione dell'instradamento loopback. Per impedire confusione in futuro, inserire **route delete IPmetricserver**.

Ad esempio:

```
ifconfig en0 delete 9.27.23.61
ifconfig lo0 alias 9.27.23.61 netmask 255.255.255.0
route add 9.27.23.61 127.0.0.1
metricserver stop
# inattività massima di 60 secondi o fino all'arresto di metricserver
let loopcount=0
while [[ "$loopcount" -lt "60" && 'ps -ef | grep AgentStop|
      grep -c -v gr ep' -eq "1"]]
do
  sleep 1
  let loopcount=$loopcount+1
done
route delete 9.27.23.61
```

- **Windows:** per prima cosa, installare la scheda loopback di Metric Server (denominata Connessione alla rete locale 2 nell'esempio seguente) sulla macchina con un indirizzo IP. Aggiungere un tipo di indirizzo di rete privata non utilizzato, ad esempio 10.1.1.1. Dopo aver configurato il loopback, modificare gli script "go". Lo script goStandby comprenderà il comando netsh per spostare l'IP di Metric Server sulla relativa scheda loopback. Quindi, eseguire il comando **metricserver stop**.

Ad esempio:

```
call netsh interface ip delete address "Connessione alla rete locale" addr=9.27.23.61
call netsh interface ip add address "Connessione alla rete locale 2" addr=9.27.2.3.61
mask = 255.255.255.0
sleep 3
metricserver stop
```

Problema: gli script eseguiti su macchine Solaris multi-CPU producono messaggi console indesiderati

Quando vengono eseguiti su macchine Solaris multi-CPU, gli script metricserver, cpuload e memload possono produrre messaggi console indesiderati. Questo

comportamento è dovuto all'uso del comando di sistema VMSTAT per raccogliere le statistiche su CPU e memoria dal kernel. Alcuni messaggi restituiti da VMSTAT indicano che lo stato del kernel è cambiato. Gli script non sono in grado di gestire questi messaggi, per cui vengono visualizzati messaggi console non necessari dalla shell.

Esempi di questi messaggi console sono:

```
/opt/ibm/edge/lb/ms/script/memload[29]: TOTAL=: syntax error
/opt/ibm/edge/lb/ms/script/memload[31]: LOAD=4*100/0: divide by zero
/opt/ibm/edge/lb/ms/script/memload[29]: TOTAL=659664+: more tokens expected
```

Questi messaggi possono essere ignorati.

Problema: su Load Balancer per IPv6, non è possibile richiamare i valori da Metric Server su sistemi Linux

Esiste una incompatibilità di selezione degli indirizzi IPv6 quando si utilizzano piattaforme Linux. Come risultato, Metric Monitor prova a comunicare con Metric Server sull'indirizzo IP di origine non corretto.

Su sistemi Linux, la selezione dell'indirizzo di origine IPv6 per un determinato instradamento fa riferimento all'ultimo indirizzo configurato che corrisponde alla parte di rete dell'instradamento.

Se l'ultima interfaccia configurata è un cluster IPv6 e tale interfaccia corrisponde alla porzione di rete di un'instradamento nella tabella di routing, allora l'interfaccia viene utilizzata come indirizzo IP di origine predefinito per l'instradamento. Se tale instradamento viene utilizzato tra Load Balancer e Metric Server, la comunicazione tra i due nodi non verrà stabilita.

La comunicazione non viene stabilita poiché il nodo di Load Balancer prova a comunicare con Metric Server mediante l'indirizzo del cluster come indirizzo IP di origine. Quando il cluster viene configurato sul loopback del nodo di Metric Server, la risposta da Metric Server va al loopback e la comunicazione non viene stabilita.

Soluzione:

Per determinare l'indirizzo utilizzato dal nodo Linux per il determinato instradamento e l'interfaccia utilizzata per le comunicazioni RMI tra Metric Monitor e Metric Server, emettere il seguente comando:

```
ip -6 route get your_ipv6_route
```

Ad esempio, quando si emette il comando:

```
ip -6 route get fec0::/64
```

viene restituito:

```
fec0:: via fec0:: dev eth0 src fec0::4 metric 0 cache mtu 1500 advmss 1383
```

Se fec0::4 è un indirizzo del cluster, è necessario aggiungere un'altra interfaccia al dispositivo in modo da evitare che il cluster venga utilizzato come origine predefinita altrimenti una precedente interfaccia non cluster non potrà essere rimossa e quindi aggiunta di nuovo.

Ad esempio:

```
ip -6 addr add fec0::5/64 dev eth0
```


Problema: dopo aver avviato Metric Server, il valore della metrica restituisce -1

Questo problema può essere il risultato della perdita di integrità dei file delle chiavi durante il trasferimento al client.

Se si utilizza FTP per trasferire i file delle chiavi dalla macchina di Load Balancer al server di backend verificare di utilizzare la modalità binaria per eseguire il put o il get dei file delle chiavi sul server FTP.

Parte 9. Riferimenti sui comandi

Questa sezione fornisce informazioni di riferimento sui comandi di tutti i componenti di Load Balancer. Contiene i seguenti capitoli:

- Capitolo 26, "Come leggere un diagramma della sintassi", a pagina 335
- Capitolo 27, "Riferimenti sui comandi per Dispatcher e CBR", a pagina 337
- Capitolo 28, "Riferimenti sui comandi per Site Selector", a pagina 391
- Capitolo 29, "Riferimenti sui comandi per Cisco CSS Controller", a pagina 419
- Capitolo 30, "Riferimenti sui comandi per Controller Nortel Alteon", a pagina 437

Capitolo 26. Come leggere un diagramma della sintassi

Il diagramma delle sintassi mostra come specificare un comando in modo che il sistema interpreti correttamente ciò che è stato digitato. Leggere il diagramma delle sintassi da sinistra verso destra e dall'alto verso il basso, seguendo la riga orizzontale (il percorso principale).

Simboli e punteggiatura

Nei diagrammi della sintassi vengono utilizzati i seguenti simboli:

Simbolo

Descrizione

- »» Contrassegna l'inizio della sintassi del comando.
- «« Contrassegna la fine della sintassi del comando.

Inserire tutta la punteggiatura, ad esempio, due punti, virgolette e segni di sottrazione, come mostrato nel diagramma della sintassi.

Parametri

Nei diagrammi della sintassi vengono utilizzati i seguenti parametri

Parameter

Descrizione

Required

I parametri obbligatori vengono visualizzati nel percorso principale.

Optional

I parametri facoltativi vengono visualizzati nel percorso principale.

I parametri sono classificati come parole chiave o variabili. Le parole chiave sono visualizzate in minuscolo e quindi possono essere inserite in minuscolo. Ad esempio, un nome di un comando è una parola chiave. Le variabili sono in corsivo e rappresentano i nomi o i valori forniti.

Esempi di sintassi

Nell'esempio riportato di seguito, il comando `user` è una parola chiave. La variabile obbligatoria è `user_id` e la variabile facoltativa è `password`. Sostituire le variabili con i propri valori.

»»—`user`—`user_id`—`password`—««

Parole chiave obbligatorie: le parole chiave e le variabili obbligatorie vengono visualizzate nella riga del percorso principale.

»»—`required_keyword`—««

È necessario codificare le parole chiave e i valori obbligatori.

Scegliere una delle voci obbligatorie da uno stack: se è disponibile più di una parola chiave o variabile obbligatoria la cui presenza esclude la presenza di un'altra, queste vengono raggruppate in verticale nell'ordine alfanumerico.



Valori facoltativi: le parole chiave e le variabili facoltative vengono visualizzate sotto la riga del percorso principale.



È possibile scegliere di non codificare le parole chiave e le variabili facoltative.

Scegliere una parola chiave facoltativa da uno stack: se è disponibile più di una parola chiave o variabile facoltativa la cui presenza esclude la presenza di un'altra, queste vengono raggruppate in verticale in ordine alfanumerico sotto la riga del percorso principale.



Variabili: una parola interamente in corsivo è una *variabile*. Quando è presente una variabile nella sintassi, sostituirla con uno dei nomi o dei valori possibili, come indicato nel testo.



Caratteri non alfanumerici: se un diagramma mostra un carattere non alfanumerico (punti, virgolette o segni di sottrazione) è necessario codificare il carattere come parte della sintassi. In questo esempio, codificare *cluster:port*.



Capitolo 27. Riferimenti sui comandi per Dispatcher e CBR

Questo capitolo descrive come utilizzare i comandi **dscontrol** del Dispatcher oltre a essere un riferimento ai comandi di CBR.

Per le versioni precedenti, quando il prodotto era noto come Network Dispatcher, il nome del comando per il controllo del Dispatcher era **ndcontrol**. Il nome del comando per il controllo del Dispatcher è ora **dscontrol**. Accertarsi di aver aggiornato tutti i file script precedenti in modo da utilizzare **dscontrol** (e non **ndcontrol**) per configurare il Dispatcher.

CBR utilizza una serie secondaria dei comandi Dispatcher, elencata in questo riferimento sui comandi. Quando si utilizzano questi diagrammi della sintassi per **CBR**, specificare **cbrcontrol** al posto di **dscontrol**. Per ulteriori informazioni, vedere “Differenze di configurazione tra CBR e Dispatcher” a pagina 338.

IMPORTANTE: se si sta utilizzando l’installazione Load Balancer per IPv4 e IPv6 di questo prodotto, è disponibile solo il componente Dispatcher. Il Dispatcher di questo tipo di installazione utilizza una serie secondaria di comandi **dscontrol** elencata in questo riferimento sui comandi. Quando si utilizzano questi diagrammi di sintassi, utilizzare il carattere at (@) al posto del carattere due punti (:) come delimitatore nel comando **dscontrol**. Per ulteriori informazioni fare riferimento a “Differenze di sintassi dei comandi” a pagina 89 e a “Comandi **dscontrol** supportati” a pagina 90 per l’installazione Load Balancer per IPv4 e IPv6.

L’elenco riportato di seguito contiene i comandi descritti in questo capitolo:

- “**dscontrol advisor** — controlla l’advisor” a pagina 339
- “**dscontrol binlog** — controlla il file di log binario” a pagina 344
- “**dscontrol cluster** — configura i cluster” a pagina 345
- “**dscontrol executor** — controlla l’executor” a pagina 349
- “**dscontrol file** — gestisce i file di configurazione” a pagina 354
- “**dscontrol help** — visualizza o stampa la guida per il comando in questione” a pagina 356
- “**dscontrol highavailability** — controlla la disponibilità elevata” a pagina 357
- “**dscontrol host** — configura una macchina remota” a pagina 361
- “**dscontrol logstatus** — visualizza le impostazioni log del server” a pagina 362
- “**dscontrol manager** — controlla il gestore” a pagina 363
- “**dscontrol metric** — configura le metriche di sistema” a pagina 368
- “**dscontrol port** — configura le porte” a pagina 369
- “**dscontrol rule** — configura le regole” a pagina 375
- “**dscontrol server** — configura i server” a pagina 381
- “**dscontrol set** — configura il log del server” a pagina 387
- “**dscontrol status** — mostra se il gestore e gli advisor sono in esecuzione” a pagina 388
- “**dscontrol subagent** — configura l’agente secondario SNMP” a pagina 389

È possibile immettere una versione ridotta dei parametri del comando **dscontrol**. È sufficiente inserire le lettere che designano in modo univoco i parametri. Ad

esempio, per visualizzare la guida del comando di salvataggio file, è possibile immettere **dscontrol he f** anziché **dscontrol help file**.

Per attivare l'interfaccia della riga comandi: emettere **dscontrol** per ricevere un prompt dei comandi dscontrol.

Per chiudere l'interfaccia della riga comandi: emettere **exit** o **quit**.

i valori dei parametri del comando devono essere immessi utilizzando l'alfabeto inglese. Le uniche eccezioni sono i nomi host (utilizzati in cluster, server e comandi highavailability) e i nomi file (utilizzati in comandi file).

Differenze di configurazione tra CBR e Dispatcher

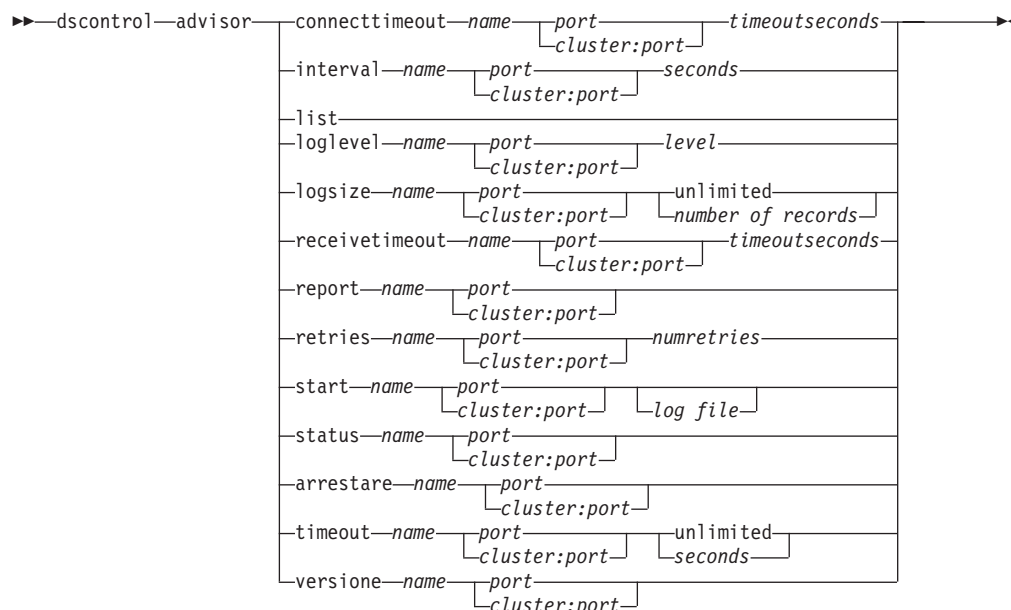
L'interfaccia della riga comandi CBR è una serie secondaria dell'interfaccia della riga comandi del Dispatcher. Per CBR, specificare il comando **cbrcontrol** al posto del comando dscontrol per configurare il componente.

Nota: Il componente Content Based Routing (CBR) è disponibile su tutte le piattaforme supportate eccetto quelle in esecuzione su una JVM a 64-bit. In alternativa è possibile utilizzare il metodo di inoltro cbr del componente Dispatcher di Load Balancer, per instradare i contenuti senza l'uso di Caching Proxy. Per ulteriori informazioni, vedere "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

Alcuni comandi *omessi* in CBR sono elencati di seguito.

1. highavailability
2. subagent
3. executor
 - report
 - set nfa <valore>
 - set fintimeout <valore>
 - set hatimeout <valore>
 - set hasynctimeout <valore>
 - set porttype <valore>
4. cluster
 - report {c}
 - set {c} porttype
5. porta
 - add {c:p} porttype
 - add {c:p} protocol
 - set {c:p} porttype
6. rule add {c:p:r} type port
7. server
 - add {c:p:s} router
 - set {c:p:s} router

dscontrol advisor — controlla l'advisor



connecttimeout

Impostare il tempo che un advisor attende prima di riferire l'interruzione di una connessione a un server relativamente a una specifica porta su un server (un servizio). Per ulteriori informazioni, vedere “Timeout di connessione e timeout di ricezione dell’advisor per i server” a pagina 183.

name

Il nome dell’advisor. Tra i valori possibili vi sono **connect**, **db2**, **dns**, **ftp**, **http**, **https**, **cachingproxy**, **imap**, **ldap**, **nnntp**, **ping**, **pop3**, **self**, **sip**, **smtp**, **ssl**, **ssl2http**, **telnet** e **wlm**.

Consultare “Elenco di advisor” a pagina 184 per ulteriori informazioni sugli advisor forniti da Load Balancer.

I nomi degli advisor personalizzati sono nel formato xxxx, dove per ADV_xxxx si intende il nome della classe che implementa l’advisor personalizzato. Per ulteriori informazioni, consultare “Creazione di advisor personalizzati” a pagina 188.

porta

Il numero della porta monitorata dall’advisor.

cluster:port

Sui comandi advisor il valore cluster è opzionale mentre il valore port è obbligatorio. Se il valore cluster non è specificato, l’advisor inizierà l’esecuzione sulla porta di tutti i cluster. Se si specifica un cluster, l’advisor avvierà l’esecuzione solo sulla porta del cluster specificato. Per ulteriori informazioni, consultare “Avvio e arresto di un adivisor” a pagina 182.

Il cluster è il nome simbolico o l’indirizzo sotto forma di indirizzo IP. La porta è il numero della porta monitorata dall’advisor.

timeoutseconds

Un numero intero positivo che rappresenta il timeout, in secondi, che l’advisor attende prima di riferire l’interruzione di una connessione a un server. Il valore predefinito è pari a 3 volte il valore specificato per l’intervallo dell’advisor.

interval

Impostare la frequenza con cui l'advisor richiederà informazioni ai server.

seconds

Un numero intero positivo che rappresenta il numero di secondi trascorsi tra le richieste ai server, relativamente al loro stato corrente. Il valore predefinito è 7.

list

Mostra l'elenco degli advisor che attualmente forniscono informazioni al gestore.

loglevel

Imposta il livello di registrazione per un log dell'advisor.

level

Il numero del livello (da 0 a 5). Il valore predefinito è 1. Maggiore è il numero, maggiori saranno le informazioni scritte sul log dell'advisor. Di seguito sono riportati i valori possibili: 0 sta per Nessuno, 1 per Minimo, 2 per Base, 3 per Moderato, 4 per Avanzato, 5 per Verbose.

logsize

Impostare la dimensione massima di un log dell'advisor. Se si imposta la dimensione massima del file di log, il file ripartirà dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive verranno scritte all'inizio del file, sovrascrivendo quindi le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora, in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

number of records

La dimensione massima in byte del file di log dell'advisor. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima, prima di iniziare la sovrascrittura, in quanto le voci di log in sé variano, in termini di dimensione. Il valore predefinito è 1 MB.

receivetimeout

Impostare il tempo che un advisor attende prima di riferire l'impossibilità di ricezione da una specifica porta su un server (un servizio). Per ulteriori informazioni, vedere "Timeout di connessione e timeout di ricezione dell'advisor per i server" a pagina 183.

timeoutseconds

Un numero intero positivo che rappresenta il timeout, in secondi, che l'advisor attende prima di riferire l'impossibilità di ricezione da un server. Il valore predefinito è pari a 3 volte il valore specificato per l'intervallo dell'advisor.

report

Visualizza un report sullo stato dell'advisor.

retry

Il parametro retry imposta il numero dei tentativi che un advisor può eseguire prima di contrassegnare un server come inattivo.

numretries

Un numero intero maggiore o uguale a zero. È preferibile che questo valore non sia maggiore di 3. Se la parola chiave retries non è configurata, per il numero di tentativi viene assunto il valore zero.

start

Avvia l'advisor. Sono disponibili advisor per ciascun protocollo. Le porte predefinite sono le seguenti:

Nome advisor	Protocollo	Port
cachingproxy	HTTP (via Caching Proxy)	80
connessione	ICMP	12345
db2	private	50000
dns	DNS	53
ftp	FTP	21
http	HTTP	80
https	SSL	443
imap	IMAP	143
ldap	LDAP	389
nntp	NNTP	119
ping	PING	0
pop3	POP3	110
self	private	12345
sip	SIP	5060
smtp	SMTP	25
ssl	SSL	443
ssl2http	SSL	443
telnet	Telnet	23
WLM	private	10.007

Nota: l'advisor FTP dovrebbe fornire informazioni solo sulla porta di controllo FTP (21). Non avviare un advisor FTP sulla porta dei dati FTP (20).

log file

Nome del file su cui sono registrati i dati di gestione. Ciascun record nel log verrà dotato di un indicatore di data e ora.

Il file predefinito è *advisorname_port.log*, ad esempio, **http_80.log**. Per modificare la directory su cui vengono memorizzati i file di log, consultare "Modifica dei percorsi file di log" a pagina 259. I file di log predefiniti per advisor specifici del cluster (o del sito) vengono creati con l'indirizzo cluster, ad esempio, **http_127.40.50.1_80.log**.

status

Visualizza lo stato corrente di tutti i valori in un advisor che possono essere impostati globalmente, compresi i valori predefiniti.

stop

Arresta l'advisor.

timeout

Imposta il numero di secondi entro il quale il gestore considera valide le informazioni ricevute dall'advisor. Se il gestore rileva che le informazioni dell'advisor sono meno aggiornate rispetto a questo periodo di timeout, non utilizzerà tali informazioni per determinare i pesi dei server sulla porta monitorata dall'advisor. Un'eccezione a questo timeout avviene quando

l'advisor ha informato il gestore dell'inattività di uno specifico server. Il gestore utilizzerà quelle informazioni sul server anche in seguito al timeout delle informazioni dell'advisor.

seconds

Un numero positivo che rappresenta il numero di secondi o la parola **unlimited**. Il valore predefinito è unlimited.

version

Visualizza la versione corrente dell'advisor.

Esempi

- Per avviare l'advisor http sulla porta 80 per il cluster 127.40.50.1:
`dscontrol advisor start http 127.40.50.1:80`
- Per avviare l'advisor http sulla porta 88 di tutti i cluster:
`dscontrol advisor start http 88`
- Per arrestare l'advisor http sulla porta 80 per il cluster 127.40.50.1:
`dscontrol advisor stop http 127.40.50.1:80`
- Per impostare il tempo (30 secondi) che un advisor HTTP per la porta 80 attende prima di riferire l'interruzione di una connessione a un server:
`dscontrol advisor connecttimeout http 80 30`
- Per impostare il tempo (20 secondi) che un advisor HTTP per la porta 80 sul cluster 127.40.50.1 attende prima di riferire l'interruzione di una connessione a un server:
`dscontrol advisor connecttimeout http 127.40.50.1:80 20`
- Per impostare l'intervallo per l'advisor FTP (per la porta 21) su 6 secondi:
`dscontrol advisor interval ftp 21 6`
- Per visualizzare l'elenco degli advisor che attualmente forniscono informazioni al gestore:
`dscontrol advisor list`

Questo comando produce un output simile a:

ADVISOR	CLUSTER:PORT	TIMEOUT
http	127.40.50.1:80	unlimited
ftp	21	unlimited

- Per modificare il livello di log del log dell'advisor su 0, al fine di ottenere migliori prestazioni:
`dscontrol advisor loglevel http 80 0`
- Per modificare la dimensioni di log dell'advisor ftp per la porta 21 su 5000 byte:
`dscontrol advisor logsize ftp 21 5000`
- Per impostare il tempo (60 secondi) che un advisor HTTP (per la porta 80) attende prima di riferire l'impossibilità di ricezione da un server:
`dscontrol advisor receivetimeout http 80 60`
- Per visualizzare un report sullo stato dell'advisor ftp (per la porta 21):
`dscontrol advisor report ftp 21`

Questo comando produce un output simile a:

Advisor Report:

Advisor name Ftp

```

Port number ..... 21

Cluster address ..... 9.67.131.18
Server address ..... 9.67.129.230
Load ..... 8

Cluster address ..... 9.67.131.18
Server address ..... 9.67.131.215
Load ..... -1

```

- Per visualizzare lo stato corrente dei valori associati all'advisor http per la porta 80:

```
dscontrol advisor status http 80
```

Questo comando produce un output simile al seguente:

```

Advisor Status:
-----
Interval (seconds) ..... 7
Timeout (seconds) ..... Unlimited
Connect timeout (seconds).....21
Receive timeout (seconds).....21
Advisor log filename ..... Http_80.log
Log level ..... 1
Maximum log size (bytes) ..... Unlimited
Number of retries ..... 0

```

- Per impostare il valore di timeout per le informazioni dell'advisor ftp sulla porta 21 su 5 secondi:

```
dscontrol advisor timeout ftp 21 5
```

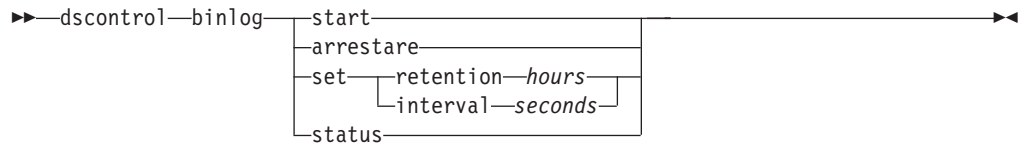
- Per visualizzare il numero della versione corrente dell'advisor ssl per la porta 443:

```
dscontrol advisor version ssl 443
```

Questo comando produce un output simile al seguente:

```
Version: 04.00.00.00 - 07/12/2001-10:09:56-EDT
```

dscontrol binlog — controlla il file di log binario



start

Avvia il log binario.

stop

Arresta il log binario.

set

Imposta i campi per la registrazione binaria. Per ulteriori informazioni sull'impostazione dei campi per la registrazione binaria, consultare "Uso della registrazione binaria per analizzare le statistiche dei server" a pagina 232.

retention

Il numero di ore che vengono conservati i file di log binari. Il valore predefinito di retention è 24.

hours

Il numero di ore.

interval

Il numero di secondi tra le voci di log. Il valore predefinito per interval è 60.

seconds

Il numero di secondi.

status

Mostra il tempo di conservazione in memoria e gli intervalli di scrittura dei file binari di log.

dscontrol cluster — configura i cluster



add

Aggiunge il cluster. È necessario definire almeno un cluster.

cluster

Il nome del cluster o l'indirizzo a cui si collegano i client. Il nome del cluster può essere un nome simbolico o trovarsi nel formato indirizzo IP. Un valore cluster pari a 0.0.0.0 può essere utilizzato per specificare un cluster jolly. Per ulteriori informazioni, consultare "Utilizzo del cluster jolly per combinare le configurazioni di server" a pagina 229.

Ad eccezione del comando dscontrol cluster add, è possibile utilizzare un carattere due punti (:) in modo che funzioni da carattere jolly. Ad esempio, il seguente comando, dscontrol cluster set : weightbound 80, consente di impostare un limite di peso di 80 su tutti i cluster.

Nota: i cluster supplementari vengono separati dal segno più (+).

address

L'indirizzo IP univoco della macchina TCP sotto forma di nome host o di indirizzo IP. Se il valore del cluster non è risolvibile, è necessario specificare questo indirizzo IP sulla macchina fisica.

Nota: il parametro address si applica unicamente al componente Dispatcher.

address

Il valore dell'indirizzo del cluster.

proportions

A livello di cluster, impostare la proporzione di importanza per le connessioni attive (*active*), le nuove connessioni (*new*), le informazioni dagli advisor (*port*) e le informazioni da un programma di monitoraggio del sistema, quale Metric Server (*system*), utilizzate dal gestore per stabilire i pesi dei server. Ciascuno di questi valori, descritti di seguito, sono espressi come una percentuale del totale, perciò la loro somma ammonta sempre a 100. Per ulteriori informazioni, consultare "Proporzione di importanza attribuita alle informazioni sullo stato" a pagina 176.

active

Un numero compreso nell'intervallo 0 – 100 che rappresenta la proporzione del peso da fornire alle connessioni attive. Il valore predefinito è 50.

new

Un numero compreso nell'intervallo 0 – 100 che rappresenta la proporzione del peso da fornire alle nuove connessioni. Il valore predefinito è 50.

porta

Un numero compreso nell'intervallo 0 – 100 che rappresenta la proporzione del peso da fornire alle informazioni dagli advisor. Il valore predefinito è 0.

Nota: quando un advisor viene avviato, e se la proporzione porta è 0, Load Balancer imposta automaticamente questo valore su 1 in modo che il gestore possa utilizzare le informazioni dell'advisor come input per calcolare il peso del server.

system

Un numero compreso nell'intervallo 0 – 100 che rappresenta la proporzione del peso da fornire alle informazioni provenienti dalle metriche di sistema, ad esempio da Metric Server. Il valore predefinito è 0.

maxports

Il numero massimo di porte. Il valore predefinito di maxports è 8.

size

Il numero di porte consentito.

maxservers

Il numero massimo predefinito di server per porta. Questo valore può essere sostituito per le singole porte utilizzando **port maxservers**. Il valore predefinito di maxservers è 32.

size

Il numero di server consentito su una porta.

stickytime

Il valore stickytime predefinito per le porte da creare. Questo valore può essere sostituito per le singole porte utilizzando **port stickytime**. Il valore predefinito di stickytime è 0.

Nota: per il metodo di inoltro cbr del Dispatcher, se si imposta stickytime (su un valore diverso da zero), port stickytime viene abilitato nel caso la porta sia SSL (non HTTP). Se il valore di stickytime per le porte da creare è diverso da zero e la nuova porta aggiunta è SSL, verrà abilitata l'affinità ID SSL per la porta. Per disabilitare l'affinità ID SSL sulla porta, sarà necessario impostare esplicitamente port stickytime su 0.

time

Il valore di stickytime in secondi.

weightbound

Il limite del peso predefinito della porta. Questo valore può essere sostituito per le singole porte utilizzando **port weightbound**. Il valore predefinito di weightbound è 20.

weight

Il valore di weightbound.

porttype

Il tipo di porta predefinito. Questo valore può essere sostituito per le singole porte utilizzando **port porttype**.

type

I valori consentiti sono **tcp**, **udp** e **both**.

primaryhost

L'indirizzo NFA della macchina Dispatcher in questione o l'indirizzo NFA della macchina Dispatcher di backup. In una configurazione di disponibilità elevata reciproca, un cluster viene associato a una macchina principale o di backup.

Se si modifica il valore **primaryhost** di un cluster dopo aver avviato la macchina principale e le macchine di backup, in esecuzione con disponibilità elevata reciproca, è necessario anche forzare il nuovo host principale ad assumere il comando. Inoltre, è necessario aggiornare gli script, quindi deconfigurare e configurare manualmente il cluster in modo corretto. Per ulteriori informazioni, consultare "Disponibilità elevata reciproca" a pagina 58.

address

Il valore dell'indirizzo di **primaryhost**. Il valore predefinito è l'indirizzo NFA di questa macchina.

staletimeout

Il numero di secondi durante il quale è possibile che non vi sia attività su una connessione prima che la connessione venga rimossa. Il valore predefinito per FTP è 900; il valore predefinito per Telnet è 32.000.000. Il valore predefinito per tutti gli altri protocolli è 300. Questo valore può essere sostituito per singole porte utilizzando **port staletimeout**. Per ulteriori informazioni, consultare "Uso del valore timeout di inattività" a pagina 260.

staletimeout

Il valore di **staletimeout**.

sharedbandwidth

La quantità massima di larghezza di banda (in kilobyte al secondo) che può essere condivisa a livello di cluster. Per ulteriori informazioni sulla larghezza di banda condivisa, consultare "Utilizzo delle regole basate sulla larghezza di banda riservata e condivisa" a pagina 209 e "Regola della larghezza di banda condivisa" a pagina 209.

Nota: la larghezza di banda condivisa si applica al componente Dispatcher.

size

La dimensione di **sharedbandwidth** è un valore intero. Il valore predefinito è zero. Se il valore è zero, la larghezza di banda non può essere condivisa a livello di cluster.

set

Imposta le proprietà del cluster.

remove

Elimina il cluster.

report

Mostra i campi interni del cluster.

Nota: il parametro **report** si applica al componente Dispatcher.

status

Mostra lo stato corrente di uno specifico cluster.

Esempi

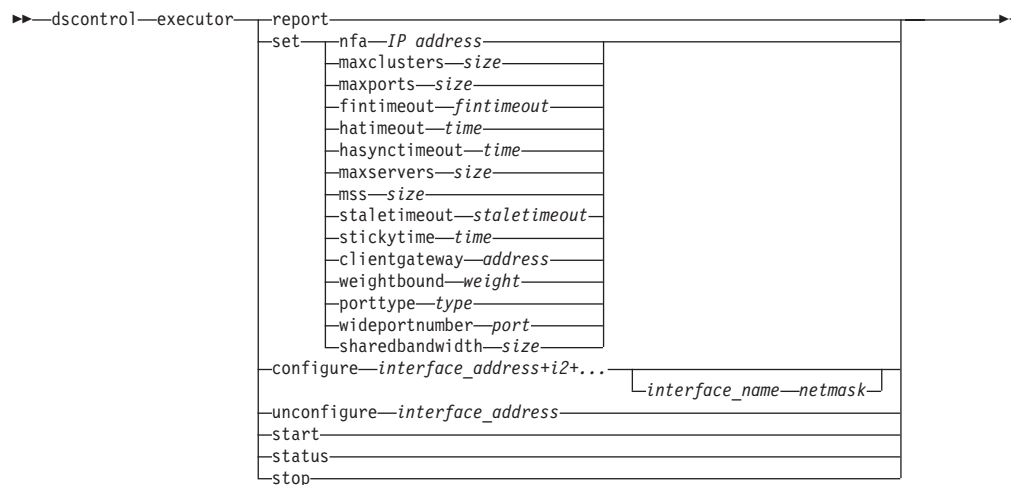
- Per aggiungere l'indirizzo cluster 130.40.52.153:
`dscontrol cluster add 130.40.52.153`

- Per rimuovere l'indirizzo cluster 130.40.52.153:
dscontrol cluster remove 130.40.52.153
- Per impostare l'importanza relativa posizionata sull'input (active, new, port, system) ricevuto dal gestore per i server che risiedono sul cluster 9.6.54.12:
dscontrol cluster set 9.6.54.12 proportions 60 35 5 0
- Per aggiungere un cluster jolly:
dscontrol cluster add 0.0.0.0
- Per configurare la disponibilità elevata reciproca, impostare l'indirizzo cluster 9.6.54.12 con l'NFA della macchina di backup (9.65.70.19) come host principale:
dscontrol cluster set 9.6.54.12 primaryhost 9.65.70.19
- Per visualizzare lo stato dell'indirizzo cluster 9.67.131.167:
dscontrol cluster status 9.67.131.167

Questo comando produce un output simile a:

```
Cluster Status:
-----
Cluster ..... 9.67.131.167
Address ..... 9.67.131.167
Number of target ports ..... 3
Default sticky time ..... 0
Default stale timeout ..... 30
Default port weight bound ..... 20
Maximum number of ports ..... 8
Default port protocol ..... tcp/udp
Default maximum number of servers ..... 32
Proportion given to active connections... 0.5
Proportion given to new connections..... 0.5
Proportion given specific to the port.... 0
Proportion given to system metrics..... 0
Shared bandwidth (KBytes) ..... 0
Primary Host Address ..... 9.67.131.167
```

dscontrol executor — controlla l'executor



report

Visualizza un report di istantanee delle statistiche. Ad esempio: i pacchetti totali ricevuti, i pacchetti eliminati, i pacchetti inoltrati con errori, ecc.

Nota: il parametro `report` si applica al componente Dispatcher.

set

Imposta i campi dell'executor.

nfa

Imposta l'indirizzo di non inoltrare. Qualsiasi pacchetto inviato a questo indirizzo non verrà instradato dalla macchina Dispatcher.

Nota: il parametro NFA si applica al componente Dispatcher.

IP address

L'indirizzo Internet espresso come nome simbolico o in formato decimale puntato.

maxclusters

Il numero massimo di cluster che può essere configurato. Il valore predefinito di `maxclusters` è 100.

size

Il numero massimo di cluster che può essere configurato.

maxports

Il valore predefinito di `maxports` per i cluster da creare. Questo valore può essere sostituito dal comando **cluster set** o **cluster add**. Il valore predefinito di `maxports` è 8.

size

Il numero di porte.

fintimeout

Il numero di secondi entro il quale conservare una connessione in memoria, dopo che la connessione è stata posta nello stato FIN. Il valore predefinito di `fintimeout` è 60.

fintimeout

Il valore di `fintimeout`.

Nota: il parametro `finetimeout` si applica al componente Dispatcher.

hathertimeout

Il numero di secondi che l'executor impiega per stabilire la scadenza degli heartbeat di disponibilità elevata. Il valore predefinito è 2.

Nota: il valore `hathertimeout` si applica al componente Dispatcher.

time

Il valore di `hathertimeout`.

hasynctimeout

Il numero di secondi che l'executor utilizza per la replica di timeout di record di connessione tra la macchina primaria e la macchina di backup. Il valore predefinito è 50.

Il timer viene utilizzato per garantire che la macchina primaria e quella di backup siano sincronizzate. Tuttavia, se è presente un numero troppo elevato di connessioni e la macchina attiva continua a gestire un carico di traffico in entrata significativo, allora la sincronizzazione potrebbe non essere completata nel periodo definito dal timer. Come risultato, Load Balancer proverà a eseguire continuamente la risincronizzazione e le due macchine non saranno mai sincronizzate. In questo caso, impostare `hasynctimeout` su un valore maggiore di quello predefinito in modo da fornire alle due macchine un tempo sufficiente per scambiare le informazioni sulle connessioni esistenti. Per impostare questo timer, il comando `dscontrol executor start` deve essere emesso dopo il comando `dscontrol highavailability`.

Nota: Il valore `hasynctimeout` si applica al componente Dispatcher.

time

Il valore di `hasynctimeout`.

maxservers

Il numero massimo predefinito di server per porta. Questo valore può essere sostituito dal comando **cluster** o **port**. Il valore predefinito di `maxservers` è 32.

mss

Il numero massimo di byte nel segmento dati della connessione TCP/UDP. Il totale del numero di byte nel segmento dati e nell'intestazione deve essere inferiore al numero di byte nell'unità MTU (Maximum Transmission Unit). Il valore predefinito di `mss` è 1460.

Nota: la dimensione massima del segmento si applica esclusivamente al metodo di inoltro nat o cbr del componente Dispatcher.

size

Il numero di server.

staletimeout

Il numero di secondi durante il quale è possibile che non vi sia attività su una connessione prima che la connessione venga rimossa. Il valore predefinito per FTP è 900; il valore predefinito per Telnet è 32.000.000. Il valore predefinito per tutte le altre porte è 300. Questo valore può essere sostituito dal comando **cluster** o **port**. Per ulteriori informazioni, consultare "Uso del valore timeout di inattività" a pagina 260.

staletimeout

Il valore di `staletimeout`.

stickytime

Il valore del tempo di aderenza porta predefinito per tutti i futuri cluster. Questo valore può essere sostituito dal comando **cluster** o **port**. Il valore stickytime predefinito è 0.

time

Il valore di stickytime in secondi.

clientgateway

Clientgateway è un indirizzo IP utilizzato per NAT/NAPT o Instradamento basato sul contenuto di Dispatcher. Si tratta dell'indirizzo del router attraverso il quale il traffico in direzione di ritorno viene inoltrato da Load Balancer ai client. Clientgateway deve essere impostato su un valore diverso da zero prima di aggiungere una porta con un metodo di inoltro NAT/NAPT o Instradamento basato sul contenuto di Dispatcher. Per ulteriori informazioni, consultare "NAT/NAPT del Dispatcher (metodo di inoltro nat)" a pagina 51 e "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

Nota: il parametro clientgateway si applica solo al componente Dispatcher.

address

L'indirizzo clientgateway espresso come nome simbolico o in formato decimale puntato. Il valore predefinito è 0.0.0.0.

weightbound

Il valore weightbound predefinito della porta, per tutte le future porte. Questo valore può essere sostituito dal comando **cluster** o **port**. Il valore predefinito di weightbound è 20.

weight

Il valore di weightbound.

porttype

Il valore porttype predefinito della porta, per tutte le future porte. Questo valore può essere sostituito dal comando **cluster** o **port**.

Nota: il parametro porttype si applica al componente Dispatcher.

type

I valori consentiti sono **tcp**, **udp** e **both**.

wideportnumber

Una porta TCP non utilizzata su ciascuna macchina Dispatcher. Il valore di *wideportnumber* deve essere identico per tutte le macchine Dispatcher. Il valore predefinito di wideportnumber è 0, per indicare che il supporto per wide area non è in uso.

Nota: il parametro wideportnumber si applica al componente Dispatcher.

porta

Il valore di **wideportnumber**.

sharedbandwidth

La quantità massima di larghezza di banda (in kilobyte al secondo) che può essere condivisa a livello di executor. Per ulteriori informazioni sulla larghezza di banda condivisa, consultare "Utilizzo delle regole basate sulla larghezza di banda riservata e condivisa" a pagina 209 e "Regola della larghezza di banda condivisa" a pagina 209.

Nota: la larghezza di banda condivisa si applica al componente Dispatcher.

size

La dimensione di **sharedbandwidth** è un valore intero. Il valore predefinito è zero. Se il valore è zero, la larghezza di banda non può essere condivisa a livello di executor.

configure

Configurare un indirizzo (ad esempio un indirizzo cluster, un indirizzo mittente o un indirizzo heartbeat disponibilità elevata) per la scheda interfaccia di rete della macchina Dispatcher. Questa procedura è nota anche come configurazione di un alias sulla macchina Dispatcher.

Nota: il parametro configure si applica alla macchina Dispatcher.

interface_address

L'indirizzo espresso come nome simbolico o in formato indirizzo IP.

Nota: gli indirizzi interfaccia supplementari sono separati dal segno più (+).

interface_name netmask

Richiesto solo se l'indirizzo non corrisponde ad alcuna sottorete degli indirizzi esistenti. Il valore di *interface_name* può essere uno dei seguenti: en0, eth1, eri0. *netmask* è una maschera a 32 bit utilizzata per identificare i bit dell'indirizzo sottorete nella parte host di un indirizzo IP.

unconfigure

Elimina l'indirizzo alias dalla scheda interfaccia di rete.

Nota: il parametro unconfigure si applica al componente Dispatcher.

start

Avvia l'executor.

status

Visualizza lo stato corrente dei valori nell'executor che possono essere impostati, compresi i valori predefiniti.

stop

Arresta l'executor.

Nota: il parametro stop si applica a Dispatcher e a CBR.

Esempi

- Per visualizzare i contatori interni di Dispatcher:

```
dscontrol executor status
```

```
Executor Status:
```

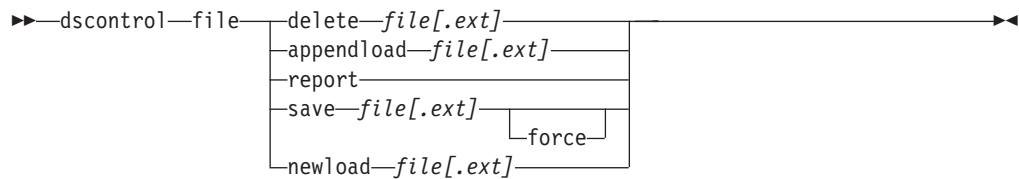
```
-----  
Nonforwarding address ..... 9.67.131.151  
Client gateway address ..... 0.0.0.0  
Fin timeout ..... 60  
Wide area network port number ..... 0  
Shared bandwidth (Kbytes) ..... 0  
Default maximum ports per cluster ... 8  
Maximum number of clusters ..... 100  
Default maximum servers per port .... 32  
Default stale timeout ..... 300  
Default sticky time ..... 0  
Default weight bound ..... 20  
Default port type ..... tcp/udp
```

- Per impostare un indirizzo di non inoltra su 130.40.52.167:

```
dscontrol executor set nfa 130.40.52.167
```

- Per impostare il numero massimo di cluster:
`dscontrol executor set maxclusters 4096`
- Per avviare l'executor:
`dscontrol executor start`
- Per arrestare l'executor:
`dscontrol executor stop`

dscontrol file — gestisce i file di configurazione



delete

Elimina il file.

file[.ext]

Un file di configurazione composto da comandi dscontrol.

L'estensione del file (.ext) è a scelta e può essere omessa.

appendload

Per aggiornare la configurazione corrente, il comando appendload avvia i comandi eseguibili dal file script.

report

Crea il report relativo ai file disponibili.

save

Salva la configurazione corrente di Load Balancer nel file.

Nota: i file vengono salvati e caricati nelle/dalle directory riportate di seguito, dove per *component* si intende dispatcher o cbr:

- Sistemi Linux e UNIX: **/opt/ibm/edge/lb/servers/configurations/*component***
- Windows: **C:\Program Files\ibm\edge\lb\servers\configurations*component***

force

Per salvare il file in un file esistente con nome identico, utilizzare l'opzione **force** per eliminare il file esistente prima di salvare quello nuovo. Se non si utilizza l'opzione force, il file esistente non verrà sovrascritto.

newload

Carica ed esegue un nuovo file di configurazione in Load Balancer. Il nuovo file di configurazione sostituisce la configurazione corrente.

Esempi

- Per eliminare un file:
`dscontrol file delete file3`

File (file3) was deleted.
- Per caricare un nuovo file di configurazione per sostituire la configurazione corrente:
`dscontrol file newload file1.sv`

File (file1.sv) was loaded into the Dispatcher.
- Per aggiungere un file di configurazione alla configurazione corrente e caricarlo:
`dscontrol file appendload file2.sv`

File (file2.sv) was appended to the current configuration and loaded.

- Per visualizzare un report dei file (ossia, dei file precedentemente salvati):

```
dscontrol file report
```

```
FILE REPORT:
```

```
file1.save
```

```
file2.sv
```

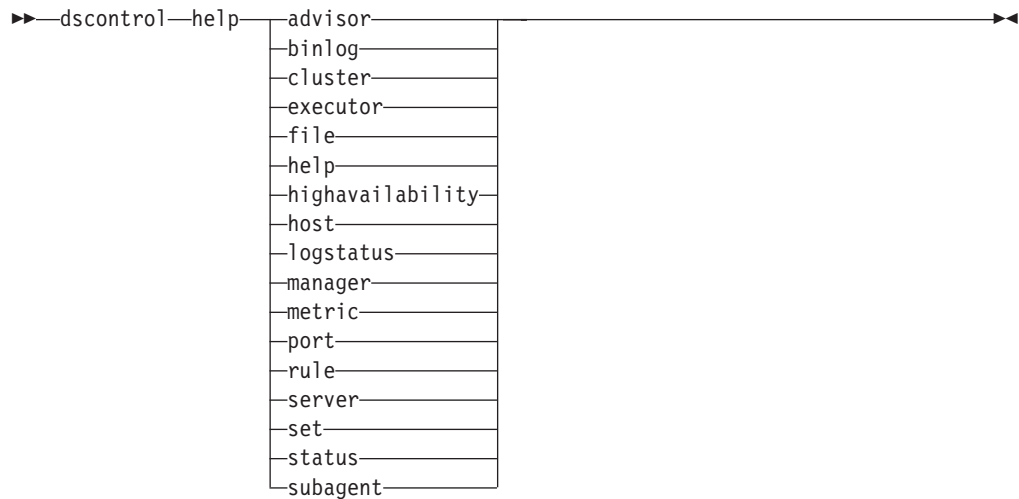
```
file3
```

- Per salvare la configurazione in un file denominato file3:

```
dscontrol file save file3
```

```
The configuration was saved into file (file3).
```

dscontrol help — visualizza o stampa la guida per il comando in questione



Esempi

- Per richiamare la guida sul comando dscontrol:
guida dscontrol

Questo comando produce un output simile a:

```
HELP COMMAND ARGUMENTS:
```

```
-----
```

```
Usage: help <help option>
```

```
Example: help cluster
```

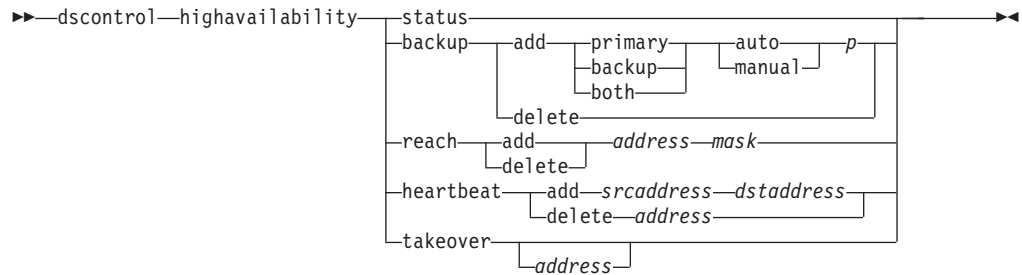
```
help          - print complete help text
advisor       - help on advisor command
cluster       - help on cluster command
executor      - help on executor command
file          - help on file command
host          - help on host command
binlog        - help on binary log command
manager       - help on manager command
metric        - help on metric command
port          - help on port command
rule          - help on rule command
server        - help on server command
set           - help on set command
status        - help on status command
logstatus     - help on server log status
subagent      - help on subagent command
highavailability - help on high availability command
```

Notare che i parametri nelle tag <> sono variabili.

- A volte la guida visualizza le scelte per le variabili utilizzando il carattere | per separare le opzioni:
fintimeout <cluster address>|all <time>
-Change FIN timeout
(Use 'all' to change all clusters)

dscontrol highavailability — controlla la disponibilità elevata

Nota: il diagramma della sintassi di disponibilità elevata dscontrol si applica esclusivamente al componente Dispatcher.



status

Restituisce un report sulla disponibilità elevata. Le macchine vengono identificate come se avessero una delle tre condizioni di stato o stati:

Attivo Una determinata macchina (principale, di backup o di entrambi i tipi) sta instradando pacchetti.

Standby

Una determinata macchina (principale, di backup o di entrambi i tipi) non sta instradando pacchetti; sta monitorando lo stato di un Dispatcher **attivo**.

Inattivo

Una determinata macchina sta instradando pacchetti ma non tenta di stabilire il contatto con il Dispatcher partner.

Inoltre, la parola chiave **status** restituisce informazioni su vari stati secondari:

Sincronizzato

Una determinata macchina ha stabilito il contatto con un altro Dispatcher.

Altri stati secondari

Questa macchina sta tentando di stabilire il contatto con il Dispatcher partner, finora senza successo.

backup

Specifica le informazioni per la macchina principale o di backup.

add

Definisce ed esegue le funzioni di disponibilità elevata per la macchina in questione.

primary

Identifica la macchina Dispatcher con ruolo *primary*.

backup

Identifica la macchina Dispatcher con ruolo *backup*.

both

Identifica la macchina Dispatcher con *entrambi* i ruoli *primary* e *backup*. Si tratta della funzione di disponibilità elevata reciproca, in cui i ruoli *primary* e *backup* sono associati a ciascun cluster. Per ulteriori informazioni, consultare “Disponibilità elevata reciproca” a pagina 58.

auto

Specifica una strategia di recupero *automatica*, in cui la macchina principale riprende a instradare i pacchetti appena torna in servizio.

manual

Specifica una strategia di recupero *manuale*, in cui la macchina principale non riprende a instradare i pacchetti finché l'amministratore non emette un comando **takeover**.

p[port]

Una porta TCP non utilizzata su entrambe le macchine, che deve essere adoperata da Dispatcher per i messaggi heartbeat. Il valore di *port* della macchina principale e di backup deve essere identico.

delete

Rimuove questa macchina dall'opzione di disponibilità elevata, quindi non verrà più utilizzata come macchina di backup o principale.

reach

Aggiunge o elimina l'indirizzo di destinazione dei Dispatcher principali e di backup, l'advisor reach invia *comandi ping* sia dai Dispatcher principali che di backup per determinare se sono accessibili.

Nota: durante la configurazione della destinazione accessibile, è necessario avviare anche l'advisor reach. L'advisor reach viene avviato automaticamente dalla funzione gestore.

add

Aggiunge un indirizzo di destinazione per l'advisor reach.

delete

Elimina un indirizzo di destinazione dall'advisor reach.

address

L'indirizzo IP (simbolico o in formato indirizzo IP) del nodo di destinazione.

mask

Una subnet mask.

heartbeat

Definisce una sessione di comunicazione tra le macchine Dispatcher principali e di backup.

add

Indica il Dispatcher di origine e l'indirizzo del partner (indirizzo di destinazione).

srcaddress

Indirizzo di origine. L'indirizzo (IP o simbolico) della macchina Dispatcher in questione.

dstaddress

Indirizzo di destinazione. L'indirizzo (IP o simbolico) dell'altra macchina Dispatcher.

Nota: i parametri *srcaddress* e *dstaddress* devono essere gli indirizzi NFA delle macchine per almeno una coppia di heartbeat.

delete

Elimina la coppia di indirizzi dalle informazioni heartbeat. È possibile specificare l'indirizzo di origine o di destinazione della coppia di heartbeat.

address

L'indirizzo (IP o simbolico) della destinazione o dell'origine.

takeover

Configurazione di disponibilità elevata semplice (il ruolo delle macchine Dispatcher può essere *primary* o *backup*):

- Il parametro takeover indica a un Dispatcher in standby di diventare attivo e di iniziare a instradare pacchetti. In questo modo, il Dispatcher attualmente attivo verrà forzato nello stato standby. Il comando takeover deve essere emesso sulla macchina in standby e funziona solo quando la strategia è **manual**. Lo stato secondario deve essere *sincronizzato*.

Configurazione di disponibilità elevata reciproca (il ruolo di ciascuna macchina Dispatcher è *both*):

- La macchina Dispatcher con la funzione di disponibilità elevata reciproca contiene due cluster che corrispondono a quelli del partner. Uno dei cluster viene considerato primario (il cluster di backup del partner) e l'altro di backup (il cluster principale del partner). Il parametro takeover indica alla macchina Dispatcher di iniziare a instradare i pacchetti per i cluster dell'altra macchina. Il comando takeover può essere emesso solo quando i cluster della macchina Dispatcher si trovano nello stato *standby* e lo stato secondario è *sincronizzato*. In questo modo, i cluster del partner al momento attivi verranno forzati a passare allo stato standby. Il comando takeover funziona solo quando la strategia è **manual**. Per ulteriori informazioni, consultare "Disponibilità elevata reciproca" a pagina 58.

Note:

1. Notare che i *ruoli* delle macchine (*primary*, *backup*, *both*) non vengono modificati. Cambiano solo gli *stati* relativi (*attivo* o *standby*).
2. Gli *script* takeover possibili sono tre: goActive, goStandby e goInOp. Vedere "Utilizzo di script" a pagina 202.

address

Il valore dell'indirizzo takeover è opzionale e dovrebbe essere utilizzato solo quando la macchina dispone di *entrambi* i ruoli *primary* e *backup* (configurazione di disponibilità elevata reciproca). L'indirizzo specificato è l'NFA della macchina Dispatcher che normalmente instrada il traffico di questo cluster. In caso di takeover di entrambi i cluster, specificare l'indirizzo NFA del proprio Dispatcher.

Esempi

- Per verificare lo stato di disponibilità elevata di una macchina:

```
dscontrol highavailability status
```

Output:

```
High Availability Status:
```

```
-----
```

```
Role .....primary
Recovery Strategy ..... manual
State ..... Active
Sub-state..... Synchronized
Primary host..... 9.67.131.151
Port .....12345
Preferred Target..... 9.67.134.223
```

```
Heartbeat Status:
```

```
-----
```

```
Count ..... 1
Source/destination ..... 9.67.131.151/9.67.134.223
```

Reachability Status:

Count 1

Address 9.67.131.1 reachable

- Per aggiungere le informazioni di backup alla macchina principale utilizzando la strategia di recupero automatico e la porta 80:

`dscontrol highavailability backup add primary auto 80`

- Per aggiungere un indirizzo che possa essere raggiunto dal Dispatcher:

`dscontrol highavailability reach add 9.67.125.18`

- Per aggiungere le informazioni heartbeat per le macchine principali e di backup.

Primary - `highavailability heartbeat add 9.67.111.3 9.67.186.8`

Backup - `highavailability heartbeat add 9.67.186.8 9.67.111.3`

- Per indicare al Dispatcher in standby di diventare attivo, forzando la macchina attiva nello stato standby:

`dscontrol highavailability takeover`

dscontrol host — configura una macchina remota

►►—dscontrol—host:—*remote_host*—◄◄

remote_host

Il nome della macchina Load Balancer remota da configurare. Quando si immette questo comando, assicurarsi che non vi siano spazi tra **host:** e *remote_host*, ad esempio:

```
dscontrol host:remote_host
```

Dopo aver emesso questo comando sul prompt dei comandi, immettere un comando dscontrol valido da inviare alla macchina Load Balancer remota.

dscontrol logstatus — visualizza le impostazioni log del server

►►—dscontrol—logstatus—◄◄

logstatus

Visualizza le impostazioni log del server (nome file di log, livello di registrazione e dimensione log).

Esempi

Per visualizzare logstatus:

```
dscontrol logstatus
```

Questo comando produce un output simile a:

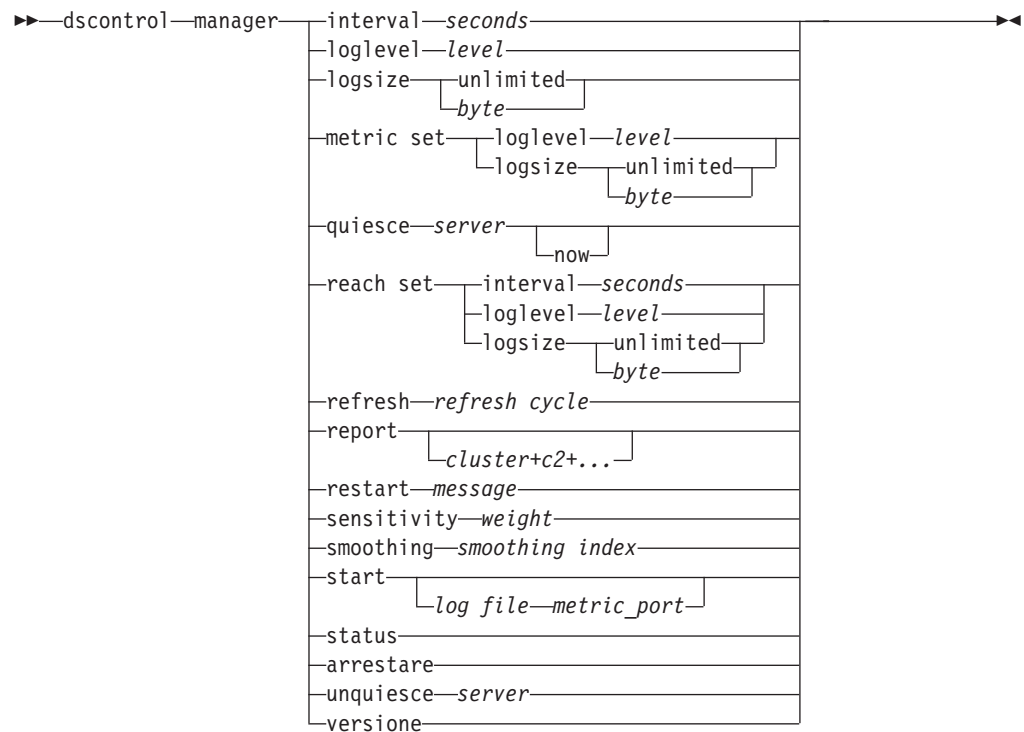
Dispatcher Log Status:

Log filename C:\PROGRA~1\IBM\edge\lb\servers\logs\dispatcher
\server.log

Log level 1

Maximum log size (bytes) ... 1048576

dscontrol manager — controlla il gestore



interval

Imposta la frequenza con cui il gestore aggiornerà i pesi dei server per l'executor, aggiornando il criterio utilizzato dall'executor per instradare le richieste client.

seconds

Un numero positivo che rappresenta, in secondi, la frequenza con cui il gestore aggiornerà i pesi per l'executor. Il valore predefinito è 2.

loglevel

Imposta il livello di registrazione per il log del gestore.

level

Il numero del livello (da 0 a 5). Maggiore è il numero, maggiori saranno le informazioni scritte sul log del gestore. Il valore predefinito è 1. Di seguito sono riportati i valori possibili: 0 sta per Nessuno, 1 per Minimo, 2 per Base, 3 per Moderato, 4 per Avanzato, 5 per Verbose.

logsize

Imposta la dimensione massima del log del gestore. Se si imposta la dimensione massima del file di log, il file ripartirà dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive verranno scritte all'inizio del file, sovrascrivendo quindi le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

bytes

La dimensione massima in byte del file di log del gestore. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima, prima di iniziare la sovrascrittura, in quanto le voci di log in sé variano, in termini di dimensione. Il valore predefinito è 1 MB.

metric set

Imposta **loglevel** e **logsize** per il log di controllo metrica. **loglevel** è il livello di registrazione di controllo metrica (0 - Nessuno, 1 - Minimo, 2 - Base, 3 - Moderato, 4 - Avanzato o 5 - Verbose). Il **loglevel** predefinito è 1. Il **logsize** è il numero massimo di byte da registrare nel file di log di controllo metrica. È possibile specificare un numero positivo maggiore di zero o **unlimited**. Il valore **logsize** predefinito è 1 MB.

quiesce

Specifica di non inviare altre connessioni a un server tranne le successive nuove connessioni dal client al server disattivato, se la connessione è designata come sticky (permanente) e **stickytime** non è scaduto. Il gestore imposta il peso del server su 0 in ogni porta per cui è definito. Utilizzare questo comando se si intende eseguire una veloce manutenzione su un server, quindi attivarlo. Se si elimina un server disattivato dalla configurazione, quindi lo si riaggiunge, il server non conserverà lo stato che aveva prima di essere disattivato. Per ulteriori informazioni, vedere “Gestione della disattivazione delle connessioni server” a pagina 217.

server

L'indirizzo IP del server espresso come nome simbolico o in formato decimale puntato.

Altrimenti, se è stata adoperata la suddivisione in partizioni del server, utilizzare il nome univoco del server logico. Per ulteriori informazioni, consultare “Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)” a pagina 55.

now

Utilizzare **quiesce “now”** solo se **stickytime** è impostato e si intende inviare nuove connessioni a un altro server (diverso dal server disattivato) prima della scadenza di **stickytime**. Per ulteriori informazioni, vedere “Gestione della disattivazione delle connessioni server” a pagina 217.

reach set

Imposta **interval**, **loglevel** e **logsize** per l'advisor reach.

refresh

Imposta il numero di intervalli prima di richiedere all'executor un aggiornamento delle informazioni sulle connessioni nuove e attive.

refresh cycle

Un numero positivo che rappresenta il numero di intervalli. Il valore predefinito è 2.

report

Visualizza un report di istantanee delle statistiche.

cluster

L'indirizzo del cluster da visualizzare nel report. L'indirizzo può essere espresso come nome simbolico o in formato indirizzo IP. Il valore predefinito prevede la visualizzazione del report del gestore per tutti i cluster.

Nota: i cluster supplementari vengono separati dal segno più (+).

restart

Riavvia tutti i server (non disattivi) con i pesi normalizzati (1/2 del peso massimo).

messaggio

Un messaggio che si desidera venga scritto nel file di log del gestore.

sensitivity

Impostare la sensibilità minima su cui aggiornare i pesi. Questa impostazione definisce il momento in cui il gestore deve modificare il peso del server in base alle informazioni esterne.

weight

Un numero da 1 a 100 da utilizzare come percentuale dei pesi. Il valore predefinito 5 crea una sensibilità minima del 5%.

smoothing

Impostare un indice che arrotondi le variazioni del peso durante il bilanciamento del carico. Un indice di arrotondamento più alto fa in modo che i pesi del server subiscano delle variazioni meno drastiche, in caso di cambiamento delle condizioni di rete. Con un indice più basso, i pesi del server subiranno delle variazioni più drastiche.

index

Un numero a virgola mobile positivo. Il valore predefinito è 1,5.

start

Avvia il gestore.

log file

Nome file su cui vengono registrati i dati gestore. Ciascun record nel log verrà dotato di un indicatore di data e ora.

Il file predefinito viene installato nella directory **logs**. Vedere Appendice C, "File di configurazione di esempio", a pagina 467. Per modificare la directory su cui vengono memorizzati i file di log, consultare "Modifica dei percorsi file di log" a pagina 259.

metric_port

La porta utilizzata da Metric Server per creare i report dei carichi di sistema. Se si specifica una porta metrica, è necessario indicare il nome di un file di log. La porta metrica predefinita è la numero 10004.

status

Visualizza lo stato corrente di tutti i valori del gestore che possono essere impostati globalmente, compresi i valori predefiniti.

stop

Arresta il gestore.

unquiesce

Specifica che il gestore può iniziare a fornire un peso maggiore di 0 a un server precedentemente disattivato, in ogni porta in cui è stato definito.

server

L'indirizzo IP del server espresso come nome simbolico o in formato decimale puntato.

version

Visualizza la versione corrente del gestore.

Esempi

- Per impostare l'intervallo di aggiornamento del gestore ogni 5 secondi:
`dscontrol manager interval 5`
- Per impostare il livello di registrazione su 0 per ottenere migliori prestazioni:
`dscontrol manager loglevel 0`
- Per impostare la dimensione del log del gestore su 1.000.000 byte:
`dscontrol manager logsize 1000000`
- Per specificare di non inviare ulteriori connessioni al server all'indirizzo 130.40.52.153:
`dscontrol manager quiesce 130.40.52.153`
- Per impostare il numero degli intervalli di aggiornamento prima dell'aggiornamento dei pesi su 3:
`dscontrol manager refresh 3`
- Per richiamare l'istantanea delle statistiche del gestore:
`dscontrol manager report`

Questo comando produce un output simile a:

SERVER	IP ADDRESS	STATUS
mach14.dmz.com	10.6.21.14	ACTIVE
mach15.dmz.com	10.6.21.15	ACTIVE

MANAGER REPORT LEGEND	
ACTV	Active Connections
NEWC	New Connections
SYS	System Metric
NOW	Current Weight
NEW	New Weight
WT	Weight
CONN	Connections

www.dmz.com 10.6.21.100 PORT: 21	WEIGHT NOW NEW	ACTV 49%	NEWC 50%	PORT 1%	SYS 0%
mach14.dmz.com	10 10	0	0	-1	0
mach15.dmz.com	10 10	0	0	-1	0

www.dmz.com 10.6.21.100 PORT: 80	WEIGHT NOW NEW	ACTV 49%	NEWC 50%	PORT 1%	SYS 0%
mach14.dmz.com	10 10	0	0	23	0
mach15.dmz.com	9 9	0	0	30	0

ADVISOR	CLUSTER:PORT	TIMEOUT
http	80	unlimited
ftp	21	unlimited

- Per riavviare tutti i server con i pesi normalizzati e scrivere un messaggio nel file di log del gestore:

`dscontrol manager restart` Restarting the manager to update code

Questo comando produce un output simile a:

320-14:04:54 Restarting the manager to update code

- Per impostare la sensibilità alle variazioni del peso su 10:
`dscontrol manager sensitivity 10`
- Per impostare l'indice di arrotondamento su 2,0:
`dscontrol manager smoothing 2.0`
- Per avviare il gestore e specificare il file di log denominato `ndmgr.log` (i percorsi non possono essere impostati)
`dscontrol manager start ndmgr.log`
- Per visualizzare lo stato corrente dei valori associati al gestore:
`dscontrol manager status`

Questo comando produce un output simile al seguente esempio.

Manager status:

=====

```
Metric port..... 10004
Manager log filename..... manager.log
Manager log level..... 1
Maximum manager log size (bytes)..... unlimited
Sensitivity level..... 0.05
Smoothing index..... 1.5
Update interval (seconds)..... 2
Weights refresh cycle..... 2
Reach log level..... 1
Maximum reach log size (bytes)..... unlimited
Reach update interval (seconds)..... 7
Metric monitor log file name..... MetricMonitor.log
Metric monitor log level..... 1
Maximum metric monitor log size..... 1048576
```

- Per arrestare il gestore:
`dscontrol manager stop`
- Per specificare di non inviare ulteriori connessioni a un server all'indirizzo 130.40.52.153. (Nota: è sufficiente disattivare il server "immediatamente" (`quiesce now`) se `stickytime` è impostato e si intende inviare le nuove connessioni a un altro server prima della scadenza di `stickytime`.):
`dscontrol manager quiesce 130.40.52.153 now`
- Per specificare di non inviare ulteriori connessioni a un server all'indirizzo 130.40.52.153. (Nota: se `stickytime` è impostato, le successive nuove connessioni dal client verranno inviate a questo server fino alla scadenza di `stickytime`.):
`dscontrol manager quiesce 130.40.52.153`
- Per specificare che il gestore può iniziare a fornire un peso maggiore di 0 a un server all'indirizzo 130.40.52.153, precedentemente disattivato:
`dscontrol manager unquiesce 130.40.52.153`
- Per visualizzare il numero della versione corrente del gestore:
`dscontrol manager version`

dscontrol metric — configura le metriche di sistema

```
➤➤ dscontrol metric — add—cluster+c2+...+cN:metric+metric1+...+metricN —————➤➤
                        — remove—cluster+c2+...+cN:metric+metric1+...+metricN —————
                        — proportions—cluster+c2+...+cN proportion1 prop2 prop3...propN —
                        — status—cluster+c2+...+cN:metric+metric1+...+metricN —————
```

add

Aggiunge la metrica specificata.

cluster

L'indirizzo a cui si collegano i client. L'indirizzo può essere espresso come nome host della macchina o nel formato notazione indirizzo IP. i cluster supplementari vengono separati dal segno più (+).

metric

Il nome della metrica di sistema, che deve essere il nome di un file eseguibile o script nella directory script di Metric Server.

remove

Elimina la metrica specificata.

proportions

Imposta le proporzioni per tutte le metriche associate a questo oggetto.

status

Visualizza i valori correnti della metrica in questione.

Esempi

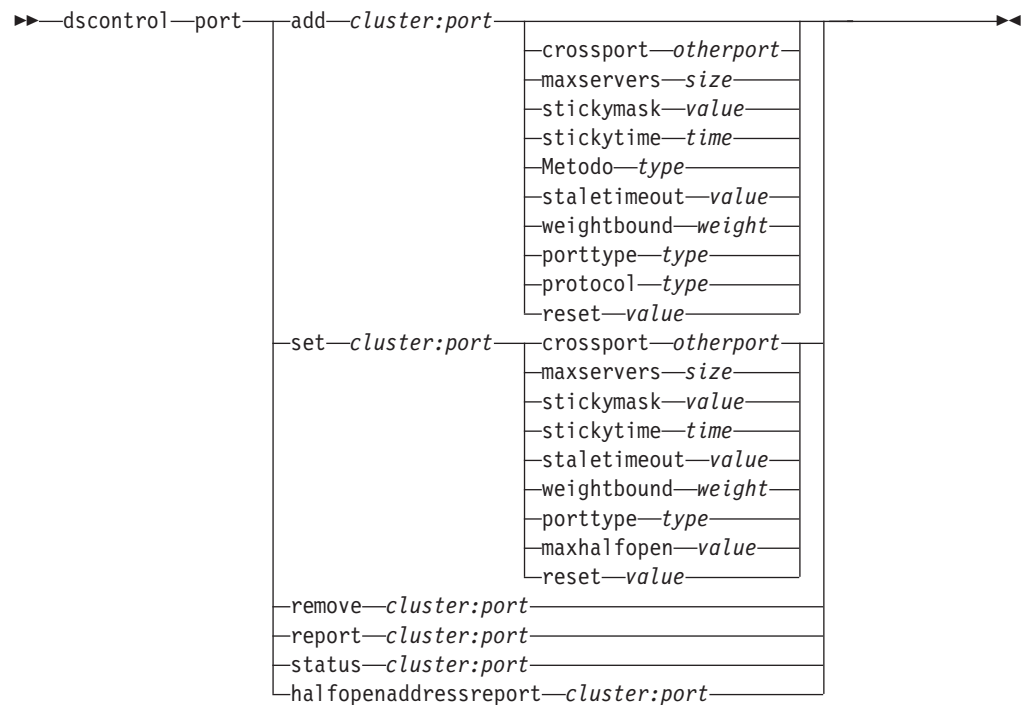
- Per aggiungere una metrica di sistema:
`dscontrol metric add site1:metric1`
- Per impostare le proporzioni di un nome sito (sitename) con due metriche di sistema:
`dscontrol metric proportions site1 0 100`
- Per visualizzare lo stato corrente dei valori associati alla metrica specificata:
`dscontrol metric status site1:metric1`

Questo comando produce un output simile al seguente:

Metric Status:

```
Cluster ..... 10.10.10.20
Metric name ..... metric1
Metric proportion ..... 50
  Server ..... plm3
  Metric data ..... -1
```

dscontrol port — configura le porte



add

Aggiunge una porta a un cluster. È necessario aggiungere una porta a un cluster prima di poter aggiungere server a quella porta. In mancanza di porte per un cluster, tutte le richieste client verranno elaborate localmente. Mediante questo comando, è possibile aggiungere più di una porta contemporaneamente.

cluster

L'indirizzo del cluster come nome simbolico o in formato indirizzo IP. È possibile utilizzare un carattere due punti (:), che funga da carattere jolly. Ad esempio, il seguente comando, `dscontrol port add :80`, consente di aggiungere la porta 80 a tutti i cluster.

Nota: i cluster supplementari vengono separati dal segno più (+).

porta

Il numero della porta. È possibile utilizzare un valore numero di porta pari a 0 (zero) per specificare una porta jolly.

Nota: le porte supplementari vengono separate dal segno più (+).

crossport

Il parametro `crossport` consente di estendere la funzione affinità/permanente a più porte in modo che le richieste di un client ricevute su porte diverse vengano inviate sempre allo stesso server, anche in caso di richieste successive. Per il valore di `crossport`, specificare il numero di *otherport* per cui si desidera condividere la funzione di affinità multiporta. Per utilizzare questa funzione, è importante che le porte:

- condividano lo stesso indirizzo cluster
- condividano gli stessi server
- dispongano dello stesso valore `stickytime` (diverso da zero)

- dispongano dello stesso valore stickymask

Per eliminare la funzione crossport, impostare nuovamente il valore crossport sul numero di porta originale. Per ulteriori informazioni sulla funzione di affinità multiporta, consultare “Affinità multiporta” a pagina 215.

Nota: il parametro crossport si applica esclusivamente ai metodi di inoltro MAC e NAT/NATP del componente Dispatcher.

otherport

Il valore di crossport. Il valore predefinito è identico al numero *port* originale.

maxservers

Il numero massimo di server. Il valore predefinito di maxservers è 32.

size

Il valore di maxservers.

stickymask

La funzione maschera indirizzo affinità raggruppa le richieste client in entrata in base agli indirizzi di sottorete comuni. Quando una richiesta client stabilisce la prima connessione alla porta, tutte le successive richieste dai client con lo stesso indirizzo di sottorete (designato da quella parte dell'indirizzo IP con maschera) verranno indirizzate allo stesso server. Per abilitare stickymask, il valore di port stickytime deve essere diverso da zero. Per ulteriori informazioni, consultare “Maschera indirizzo affinità (stickymask)” a pagina 216.

Nota: la parola chiave stickymask si applica esclusivamente al componente Dispatcher.

value

Il valore stickymask è il numero di bit più significativi dell'indirizzo IP a 32 bit da mascherare. I valori possibili sono: 8, 16, 24 e 32. Il valore predefinito è 32, che disabilita la funzione maschera indirizzo affinità.

stickytime

L'intervallo compreso tra la chiusura di una connessione e l'apertura di una nuova connessione durante il quale un client verrà rinviato allo stesso server utilizzato durante la prima connessione. Dopo questo intervallo, il client potrebbe essere inviato a un server diverso dal primo.

Per il componente Dispatcher:

- Per il metodo cbr del Dispatcher
 - È possibile impostare stickytime (su un valore diverso da zero) solo su una porta SSL (e non HTTP), in quanto l'impostazione di stickytime attiva l'affinità ID SSL.
 - Se si imposta port stickytime, il tipo di affinità sulla regola deve essere none (valore predefinito). L'affinità basata su regole (cookie passivo, URI) non può coesistere quando stickytime è impostato sulla porta.
- Per i metodi di inoltro mac e nat del Dispatcher
 - Se si imposta port stickytime (su un valore diverso da zero), non è possibile impostare un tipo di affinità sulla regola. L'affinità basata su regole non può coesistere quando stickytime è impostato sulla porta.
 - L'impostazione di un valore port stickytime abilita l'affinità indirizzo IP.

Per il componente CBR: se si imposta port stickytime su un valore diverso da zero, il tipo di affinità sulla regola deve essere none (valore predefinito).

L'affinità basata su regole (cookie passivo, URI, cookie attivo) non può coesistere quando stickyttime è impostato sulla porta.

time

Il periodo di permanenza della porta, espresso in secondi. Zero indica che la porta non è permanente.

method

Il metodo di inoltro. I metodi di inoltro possibili sono: mac, nat o cbr (content-based routing). È possibile *non* aggiungere un metodo di inoltro nat o cbr, a meno che non si specifichi inizialmente un indirizzo IP diverso da zero nel parametro clientgateway del comando dscontrol executor. Per ulteriori informazioni, consultare "NAT/NAPT del Dispatcher (metodo di inoltro nat)" a pagina 51 e "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

Note:

1. Il metodo si applica esclusivamente al componente Dispatcher.
2. Se il server di backend si trova sulla stessa sottorete dell'indirizzo mittente e si sta utilizzando il metodo di inoltro cbr o nat, è necessario definire l'indirizzo router da utilizzare come indirizzo server di backend.
3. Se si aggiunge un metodo di inoltro mac, sarà necessario specificare HTTP o SSL per il parametro "protocol".

type

Il tipo di metodo di inoltro. I valori possibili sono: mac, nat o cbr. Il valore predefinito è l'inoltro mac.

staletimeout

Il numero di secondi durante il quale è possibile che non vi sia attività su una connessione prima che la connessione venga rimossa. Per il componente Dispatcher, il valore predefinito è 900 per la porta 21 (FTP) e 32.000.000 per la porta 23 (Telnet). Per tutte le altre porte Dispatcher e CBR, il valore predefinito è 300. Il parametro staletimeout può essere impostato anche a livello di executor o di cluster. Per ulteriori informazioni, consultare "Uso del valore timeout di inattività" a pagina 260.

value

Il valore di **staletimeout** espresso in secondi.

weightbound

Impostare il peso massimo per i server su questa porta. Questa impostazione influisce sulla differenza che può sussistere tra il numero delle richieste che l'executor fornirà a ciascun server. Il valore predefinito è 20.

weight

Un numero compreso nell'intervallo 1 – 100 che rappresenta il limite di peso massimo.

porttype

Il tipo di porta.

Nota: il parametro porttype si applica esclusivamente a Dispatcher.

type

I valori consentiti sono **tcp**, **udp** e **both**. Il valore predefinito è both (tcp/udp).

protocol

Il tipo di protocollo. Per il componente Dispatcher, si tratta di un parametro obbligatorio se si specifica un metodo "cbr" sulla porta. Se si seleziona un protocollo porta di tipo **SSL**, si dovrebbe anche specificare un valore di

stickyttime diverso da zero per abilitare l'affinità ID SSL. Se si seleziona il protocollo **HTTP**, è possibile stabilire l'affinità server utilizzando le regole "content". Per ulteriori informazioni, consultare "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro cbr)" a pagina 53.

Nota: il parametro protocol si applica esclusivamente al metodo di inoltro cbr del Dispatcher.

type

I valori possibili sono **HTTP** o **SSL**.

maxhalfopen

La soglia per il numero massimo di connessioni aperte a metà. Utilizzare questo parametro per rilevare eventuali attacchi di tipo Denial of service da cui deriva un numero considerevole di connessioni TCP aperte a metà sui server.

Un valore positivo indica che verrà effettuato un controllo per determinare se le attuali connessioni aperte a metà superano la soglia. In questo caso, viene effettuata una chiamata a uno script di avvertimento. Per ulteriori informazioni, consultare "Rilevamento attacco di tipo Denial of service" a pagina 231.

Nota: il parametro maxhalfopen si applica esclusivamente a Dispatcher.

value

Il valore di maxhalfopen. Il valore predefinito è zero (non verranno effettuati controlli).

reset

Il parametro reset consente di specificare se Load Balancer invierà i ripristini TCP ai server inattivi sulla porta. Un ripristino TCP chiude immediatamente la connessione. Per ulteriori informazioni, consultare "Invio di un comando TCP reset a un server guasto (solo componente Dispatcher)" a pagina 178.

Nota: il parametro reset si applica solo al componente Dispatcher. Per poter utilizzare la parola chiave reset, il clientgateway sul comando dscontrol executor deve essere impostato su un indirizzo router.

value

I valori possibili per reset sono yes e no. Il valore predefinito è no (non verranno effettuati ripristini TCP per i server inattivi). Se reset è impostato su yes, i ripristini TCP verranno inviati ai server inattivi.

set

Imposta i campi di una porta.

remove

Rimuove la porta.

report

Crea un report sulla porta.

status

Mostra lo stato dei server su questa porta. Se si desidera visualizzare lo stato su tutte le porte, non specificare un valore di *port* con questo comando. Tuttavia, non dimenticare il carattere due punti.

numSeconds

Il tempo, espresso in secondi, prima della reimpostazione delle connessioni aperte a metà.

halfopenaddressreport

Genera voci nel log (halfOpen.log) per tutti gli indirizzi client (fino a 8000 coppie indirizzi circa) che hanno accesso a server con connessioni aperte a metà. Inoltre, i dati statistici come il numero totale, maggiore e medio di connessioni aperte a metà e il tempo medio (in secondi) impiegato per aprire a metà una connessione verranno riportati di nuovo sulla riga comandi. Per ulteriori informazioni, consultare "Rilevamento attacco di tipo Denial of service" a pagina 231.

Esempi

- Per aggiungere la porta 80 e 23 all'indirizzo cluster 130.40.52.153:
dscontrol port add 130.40.52.153:80+23
- Per aggiungere una porta jolly all'indirizzo cluster 130.40.52.153:
dscontrol port set 130.40.52.153:0
- Per impostare il peso massimo 10 sulla porta 80 all'indirizzo cluster 130.40.52.153:
dscontrol port set 130.40.52.153:80 weightbound 10
- Per impostare il valore di stickytime su 60 secondi per la porta 80 e 23 all'indirizzo cluster 130.40.52.153:
dscontrol port set 130.40.52.153:80+23 stickytime 60
- Per impostare l'affinità multiporta della porta 80 sulla porta 23 all'indirizzo cluster 130.40.52.153:
dscontrol port set 130.40.52.153:80 crossport 23
- Per rimuovere la porta 23 dall'indirizzo cluster 130.40.52.153:
dscontrol port remove 130.40.52.153:23
- Per visualizzare lo stato della porta 80 all'indirizzo cluster 9.67.131.153:
dscontrol port status 9.67.131.153:80

Questo comando produce un output simile a:

Port Status:

```
Port number ..... 80
Cluster ..... 9.67.131.153
Stale timeout ..... 300
Weight bound ..... 20
Maximum number of servers ..... 32
Sticky time ..... 0
Port type ..... tcp/udp
Cross Port Affinity ..... 80
Sticky mask bits ..... 32
Max Half Open Connections ..... 0
Send TCP Resets ..... no
```

- Per visualizzare il report della porta 80 all'indirizzo cluster 9.62.130.157:
dscontrol port report 9.62.130.157:80

Questo comando produce un output simile a:

Port Report:

```
Cluster address ..... 9.62.130.157
Port number ..... 80
Number of servers ..... 5
Maximum server weight ..... 10
Total active connections ..... 55
Connections per second ..... 12
KBytes per second ..... 298
```

```
Number half open ..... 0
TCP Resets sent ..... 0
Forwarding method ..... MAC Based Forwarding
```

- Per visualizzare il report degli indirizzi delle connessioni aperte a metà per la porta 80 all'indirizzo cluster 9.67.127.121:

```
dscontrol port halfopenaddressreport 9.67.127.121:80
```

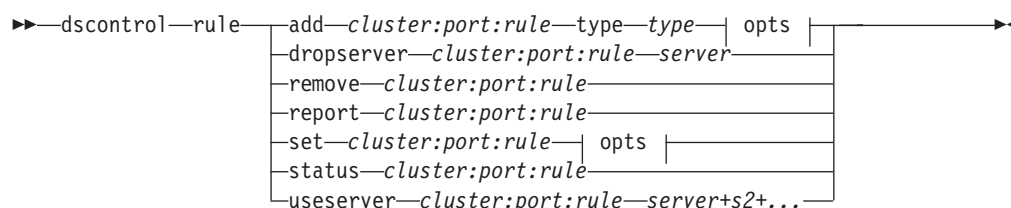
Questo comando produce un output simile a:

```
Half open connection report successfully created:
```

```
-----
```

```
Half Open Address Report for cluster:port = 9.67.127.121:80
Total addresses with half open connections reported ... 0
Total number of half open connections reported ..... 0
Largest number of half open connections reported ..... 0
Average number of half open connections reported ..... 0
Average half open connection time (seconds) reported .. 0
Total half open connections received ..... 0
```

dscontrol rule — configura le regole



opts:

beginrange	low	endrange	high
priority	level		
pattern	pattern		
tos	value		
stickytime	time		
affinity	affinity_type		
cookie name	value		
evaluate	level		
sharelevel	level		

add

Aggiunge la regola a una porta.

cluster

L'indirizzo del cluster come nome simbolico o in formato indirizzo IP. È possibile utilizzare un carattere due punti (:), che funga da carattere jolly. Ad esempio, il seguente comando, `dscontrol rule add :80:RuleA type type`, consente di aggiungere la RuleA alla porta 80 di tutti i cluster.

Nota: i cluster supplementari vengono separati dal segno più (+).

porta

Il numero della porta. È possibile utilizzare un carattere due punti (:), che funga da carattere jolly. Ad esempio, il seguente comando, `dscontrol rule add clusterA::RuleA type type`, consente di aggiungere la RuleA a tutte le porte di ClusterA.

Nota: le porte supplementari vengono separate dal segno più (+).

regola

Il nome scelto per la regola. Questo nome può contenere caratteri alfanumerici, caratteri di sottolineatura, trattini o punti. La lunghezza può variare da 1 a 20 caratteri e gli spazi non sono ammessi.

Nota: le regole supplementari vengono separate dal segno più (+).

tipo

Il tipo di regola.

type

Le scelte per *type* sono:

ip La regola è basata sull'indirizzo IP client.

time La regola è basata sull'ora del giorno.

connection

La regola è basata sul numero di connessioni al secondo della porta. Questa regola funziona solo se il gestore è in esecuzione.

active Questa regola è basata sul numero di connessioni attive totali della porta. Questa regola funziona solo se il gestore è in esecuzione.

port La regola è basata sulla porta client.

Nota: port si applica al componente Dispatcher.

service

Questa regola si basa sul campo byte TOS (type of service) nell'intestazione IP.

Nota: service si applica solo al componente Dispatcher.

reservedbandwidth

Questa regola è basata sulla larghezza di banda (kilobyte al secondo) trasmessa da una serie di server. Per maggiori informazioni, consultare "Utilizzo delle regole basate sulla larghezza di banda riservata e condivisa" a pagina 209 e "Regola della larghezza di banda riservata" a pagina 209.

Nota: reservedbandwidth si applica solo al componente Dispatcher.

sharedbandwidth

Questa regola è basata sulla quantità di larghezza di banda (kilobyte al secondo) che verrà condivisa a livello di executor o di cluster. Per maggiori informazioni, consultare "Utilizzo delle regole basate sulla larghezza di banda riservata e condivisa" a pagina 209 e "Regola della larghezza di banda condivisa" a pagina 209.

Nota: sharedbandwidth si applica esclusivamente al componente Dispatcher.

true Questa regola è sempre true. Considerarla come un'istruzione else nella logica programmatica.

content

Questa regola descrive un'espressione regolare che verrà confrontata con gli URL richiesti dal client. È valida per Dispatcher e CBR.

beginrange

Il valore minimo nell'intervallo utilizzato per determinare se la regola assume o meno il valore true.

low

Dipende dal tipo di regola. Il tipo di valore e le relative impostazioni predefinite vengono qui elencate per tipo di regola:

ip L'indirizzo del client espresso come nome simbolico o nel formato indirizzo IP. Il valore predefinito è 0.0.0.0.

time Numero intero. Il valore predefinito è 0, ossia mezzanotte.

connection

Numero intero. Il valore predefinito è 0.

active Numero intero. Il valore predefinito è 0.

port Numero intero. Il valore predefinito è 0.

reservedbandwidth

Un numero intero (kilobyte al secondo). Il valore predefinito è 0.

endrange

Il valore massimo nell'intervallo utilizzato per determinare se la regola assume o meno il valore true.

high

Dipende dal tipo di regola. Il tipo di valore e le relative impostazioni predefinite vengono qui elencate per tipo di regola:

ip L'indirizzo del client espresso come nome simbolico o nel formato indirizzo IP. Il valore predefinito è 255.255.255.254.

time Numero intero. Il valore predefinito è 24, ossia mezzanotte.

Nota: quando si definiscono i valori beginrange ed endrange degli intervalli di tempo, notare che ciascun valore deve essere un numero intero positivo che rappresenta solo l'ora; non è possibile specificare i minuti. Per questo motivo, per indicare una singola ora — ad esempio, l'ora compresa tra le 3:00 e le 4:00 — specificare 3 per beginrange e nuovamente 3 per endrange. Ciò indica tutti i minuti dalle 3:00 alle 3:59. Specificando 3 per beginrange e 4 per endrange, l'intervallo di tempo stabilito sarà compreso tra le 3:00 e le 4:59.

connections

Numero intero. Il valore predefinito è 2 alla trentaduesima potenza meno 1.

active Numero intero. Il valore predefinito è 2 alla trentaduesima potenza meno 1.

port Numero intero. Il valore predefinito è 65535.

reservedbandwidth

Un numero intero (kilobyte al secondo). Il valore predefinito è 2 alla trentaduesima potenza meno 1.

priority

L'ordine in cui verranno riviste le regole.

level

Numero intero. Se non si specifica la priorità della prima regola aggiunta, il Dispatcher la imposta, per valore predefinito, su 1. Quando si aggiunge una seconda regola, sempre per valore predefinito, la relativa priorità viene calcolata come $10 +$ la priorità attualmente più bassa di una regola esistente. Ad esempio, presupporre di avere una regola con priorità pari a 30. Quindi, viene aggiunta una nuova regola la cui priorità viene impostata su 25 (ossia, una priorità superiore a 30). Infine, si aggiunge una terza regola senza impostarne la priorità. La priorità della terza regola viene calcolata come 40 ($30 + 10$).

pattern

Specifica il modello da utilizzare per una regola tipo content.

pattern

Il modello da utilizzare. Per ulteriori informazioni sui valori validi, consultare Appendice B, "Sintassi della regola di contenuto (modello)", a pagina 463.

tos

Specifica il valore "type of service" (TOS) utilizzato per la regola tipo service.

Nota: TOS si applica unicamente al componente Dispatcher.

value

La stringa da 8 caratteri utilizzata per il valore tos, dove i caratteri validi sono: 0 (zero binario), 1 (uno binario) e x (indifferente). Ad esempio: 0xx1010x. Per ulteriori informazioni, vedere "Utilizzo delle regole basate sul tipo di servizio (TOS, type of service)" a pagina 208.

stickytime

Specifica lo stickytime da utilizzare per una regola. Quando si imposta il parametro di affinità su "activecookie" sul comando rule, stickytime deve essere impostato su un valore diverso da zero per abilitare questo tipo di affinità. Stickytime sulla regola non è applicabile ai tipi di regole di affinità "passivecookie" o "uri".

Per ulteriori informazioni, consultare "Affinità cookie attivo" a pagina 218.

Nota: la regola stickytime si applica unicamente al componente CBR.

time

Tempo in secondi.

affinity

Specifica il tipo di affinità da utilizzare per una regola: cookie attivo, passivo, URI o nessuno.

Un tipo di affinità "activecookie" consente di bilanciare il carico del traffico Web con caratteristiche di affinità con lo stesso server tramite la creazione di cookie da parte di Load Balancer.

Un tipo di affinità "passivecookie" consente di bilanciare il carico del traffico Web con caratteristiche di affinità con lo stesso server tramite la creazione di cookie auto-identificativi da parte dei server. È necessario utilizzare il parametro cookiename insieme all'affinità cookie passivo.

Un tipo di affinità "URI" consente di bilanciare il carico del traffico Web per i server Caching Proxy in una maniera che consente di aumentare efficacemente la dimensione della cache.

Consultare "Affinità cookie attivo" a pagina 218, "Affinità cookie passivo" a pagina 219 e "Affinità URI" a pagina 220 per ulteriori informazioni.

Nota: il parametro affinity si applica alle regole configurate con il metodo di inoltro cbr del componente Dispatcher e al componente CBR.

affinity_type

I valori possibili per il tipo di affinità sono: none (valore predefinito), activecookie, passivecookie o uri.

cookiename

Un nome arbitrario impostato dall'amministratore che funge da identificativo per Load Balancer. Si tratta del nome che Load Balancer deve ricercare nella richiesta intestazione HTTP del client. Il nome del cookie, insieme al valore, funge da identificativo per Load Balancer e consente a Load Balancer di inviare le richieste successive di un sito Web alla stessa macchina server. Il nome del cookie è applicabile unicamente all'affinità "cookie passivo".

Per ulteriori informazioni, consultare "Affinità cookie passivo" a pagina 219.

Nota: il nome del cookie si applica alle regole configurate con il metodo di inoltro cbr del componente Dispatcher e al componente CBR.

value

Il valore nome del cookie.

evaluate

Questa opzione è disponibile solo nel componente Dispatcher. Specifica se valutare la condizione della regola tra tutti i server nella porta o tra i server nella regola. Questa opzione è valida solo per le regole che prendono decisioni in base alle caratteristiche dei server, come le regole connection, active e reservedbandwidth. Per ulteriori informazioni, vedere “Opzione di valutazione dei server per le regole” a pagina 213.

Per la regola di tipo connection, è possibile specificare anche un’opzione evaluate — upserversonrule. Specificando upserversonrule, i server che rimangono all’interno della regola non verranno sovraccaricati, se alcuni dei server del gruppo non sono attivi.

level

I valori possibili sono port, rule o upserversonrule. Il valore predefinito è port. Il valore upserversonrule è disponibile unicamente per la regola di tipo connection.

sharelevel

Il parametro è specifico per la regola shared bandwidth. Specifica se condividere la larghezza di banda a livello di cluster o di executor. La condivisione della larghezza di banda a livello di cluster consente a una o più porte di condividere una quantità massima di larghezza di banda tra diverse porte nello stesso cluster. La condivisione della larghezza di banda a livello di executor consente a uno o più cluster all’interno della configurazione Dispatcher totale di condividere una quantità massima di larghezza di banda. Per ulteriori informazioni, consultare “Regola della larghezza di banda condivisa” a pagina 209.

level

I valori possibili sono executor o cluster.

dropserver

Rimuove un server da un insieme di regole.

server

L’indirizzo IP della macchina server TCP espresso come nome simbolico o in formato indirizzo IP.

Altrimenti, se è stata adoperata la suddivisione in partizioni del server, utilizzare il nome univoco del server logico. Per ulteriori informazioni, consultare “Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)” a pagina 55.

Nota: i server supplementari vengono separati dal segno più (+).

remove

Rimuove una o più regole, separate l’un l’altra dai più (+).

report

Visualizza i valori interni di una o più regole.

set

Imposta i valori per questa regola.

status

Visualizza i valori impostabili di una o più regole.

useserver

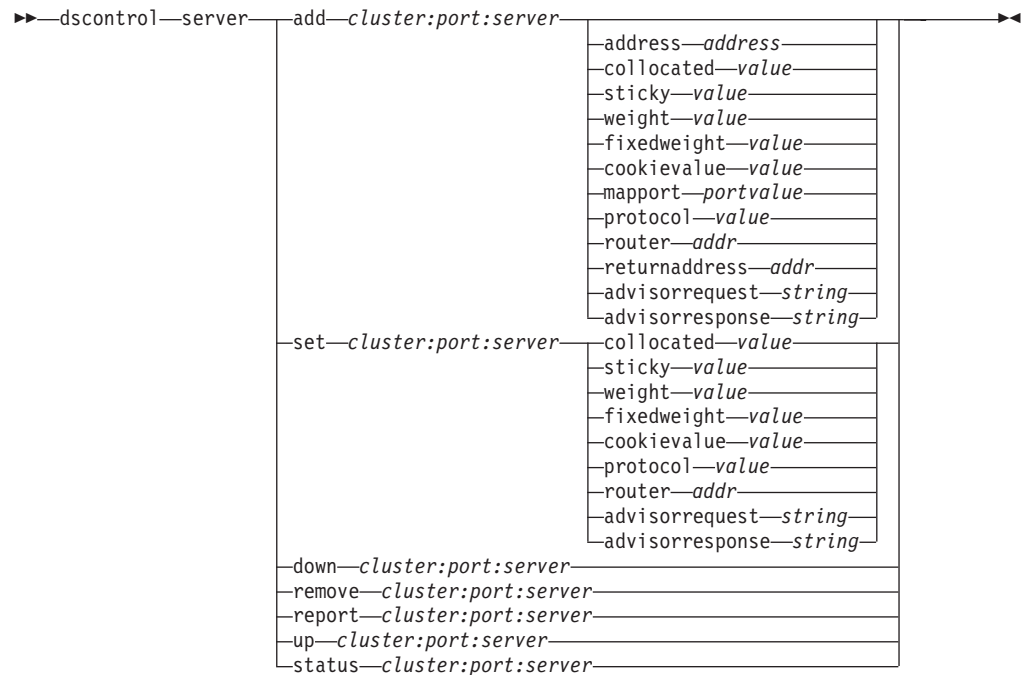
Inserisce i server in un insieme di regole.

Esempi

- Per aggiungere una regola il cui valore sarà sempre true, non specificare il valore di inizio o di fine:
`dscontrol rule add 9.37.67.100:80:trule type true priority 100`
- Per creare una regola che vieta l'accesso a un intervallo di indirizzi IP, in questo caso, gli indirizzi IP che iniziano con "9:"
`dscontrol rule add 9.37.131.153:80:ni type ip b 9.0.0.0 e 9.255.255.255`
- Per creare una regola che specificherà l'uso di un determinato server dalle 11:00 a.m. alle 3:00 p.m.:
`dscontrol rule add cluster1:80:timerule type time beginrange 11 endrange 14`
`dscontrol rule useserver cluster1:80:timerule server05`
- Per creare una regola basata sul contenuto del campo byte TOS nell'intestazione IP:
`dscontrol rule add 9.67.131.153:80:tosrule type service tos 0xx1001x`
- Per creare una regola basata su una larghezza di banda riservata che assegnerà un insieme di server (valutati all'interno della regola) per distribuire i dati con una velocità fino a 100 kilobyte al secondo:
`dscontrol rule add 9.67.131.153:80:rbwrule type reservedbandwidth`
`beginrange 0 endrange 100 evaluate rule`
- Per creare una regola basata su una larghezza di banda che impiegherà la larghezza di banda inutilizzata a livello di cluster. (Nota: per prima cosa, è necessario specificare la quantità massima di larghezza di banda (kilobyte al secondo) che può essere condivisa a livello di cluster utilizzando il comando `dscontrol cluster`):
`dscontrol cluster set 9.67.131.153 sharedbandwidth 200`

`dscontrol rule add 9.67.131.153:80:shbwrule type sharedbandwidth`
`sharelevel cluster`

dscontrol server — configura i server



add

Aggiunge il server.

cluster

L'indirizzo del cluster come nome simbolico o in formato indirizzo IP. È possibile utilizzare un carattere due punti (:), che funga da carattere jolly. Ad esempio, il seguente comando, `dscontrol server add :80:ServerA`, aggiunge ServerA alla porta 80 su tutti i cluster.

Nota: i cluster supplementari vengono separati dal segno più (+).

porta

Il numero della porta. È possibile utilizzare un carattere due punti (:), che funga da carattere jolly. Ad esempio, il seguente comando, `dscontrol server add ::ServerA`, aggiunge ServerA a tutti i cluster su tutte le porte.

Nota: le porte supplementari vengono separate dal segno più (+).

server

Il parametro **server** è l'indirizzo IP univoco della macchina server TCP espresso come nome simbolico o in formato indirizzo IP.

Altrimenti, se si utilizza un nome univoco che non si risolve in un indirizzo IP, è necessario specificare il parametro **address** del server sul comando **dscontrol server add**. Per ulteriori informazioni, consultare "Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)" a pagina 55.

Nota: i server supplementari vengono separati dal segno più (+).

address

L'indirizzo IP univoco della macchina server TCP, sotto forma di nome host o di indirizzo IP. Se il server non è risolvibile, è necessario specificare l'indirizzo

della macchina server fisica. Per ulteriori informazioni, consultare “Suddivisione in partizioni dei server: server logici configurati su un server fisico (indirizzo IP)” a pagina 55.

address

Valore dell’indirizzo del server.

collocated

Il parametro *collocated* consente di specificare se il Dispatcher è installato o meno su una delle macchine server su cui sta eseguendo il bilanciamento del carico.

Nota: il parametro *collocated* è valido quando si utilizzano i metodi di inoltro *mac*, *nat* o *cbr* del Dispatcher. Site Selector e CBR possono essere posizionati su tutte le piattaforme ma non richiedono questa parola chiave. Per ulteriori informazioni, vedere “Utilizzo dei server posizionati” a pagina 196.

value

Valore del parametro *collocated*: *yes* o *no*. Il valore predefinito è *no*.

sticky

Consente a un server di ignorare l’impostazione *stickytime* su questa porta. Con il valore predefinito “*yes*,” il server mantiene la normale affinità definita sulla porta. Con il valore “*no*,” il client *non* viene reindirizzato allo stesso server quando emette un’altra richiesta su tale porta, indipendentemente dall’impostazione *stickytime* della porta stessa. Questa impostazione è utile in determinate situazioni in cui si utilizzano le regole. Per ulteriori informazioni, vedere “ignora affinità di porta” a pagina 213.

value

Il valore di *sticky*: *yes* o *no*. Il valore predefinito è *yes*.

weight

Un numero compreso nell’intervallo 0 – 100 (che non deve superare il valore *weightbound* della porta) che rappresenta il peso per questo server. L’impostazione del peso su zero impedisce di inviare al server eventuali nuove richieste ma non chiude le connessioni attive a quel server. Il valore predefinito è la metà del valore *weightbound* massimo della porta specificato. Se il gestore è in esecuzione, questa impostazione verrà velocemente sovrascritta.

value

Il valore del peso del server.

fixedweight

L’opzione *fixedweight* consente di specificare se si desidera che il gestore modifichi o meno il peso del server. Se si imposta il valore *fixedweight* su *yes*, il gestore non potrà modificare il peso del server quando è in esecuzione. Per ulteriori informazioni, vedere “Pesi fissi del gestore” a pagina 178.

value

Il valore di *fixedweight*: *yes* o *no*. Il valore predefinito è *no*.

cookievalue

Il parametro *cookievalue* è un valore arbitrario che rappresenta il lato server della coppia nome/valore del cookie. Il valore del cookie, insieme al nome del cookie, funge da identificativo e consente a Load Balancer di inviare le richieste client successive allo stesso server. Per ulteriori informazioni, consultare “Affinità cookie passivo” a pagina 219.

Nota: il parametro `cookievalue` è valido per Dispatcher (con il metodo di inoltro `cbr`) e per CBR.

value

Il valore è arbitrario. L'impostazione predefinita non prevede valori cookie.

mapport

Mappa il numero di porta (specifico per il Dispatcher) di destinazione della richiesta client sul numero di porta del server che il Dispatcher utilizza per bilanciare il carico delle richieste del client. Consente a Load Balancer di ricevere una richiesta del client su una porta e di trasmetterla a una porta differente sulla macchina server. Con il parametro `mapport` è possibile bilanciare il carico delle richieste di un client su un server che dispone di più daemon server attivi.

Nota: il parametro `mapport` si applica a Dispatcher (con i metodi di inoltro `nat` o `cbr`) e a CBR. Per il Dispatcher, consultare "NAT/NAPT del Dispatcher (metodo di inoltro `nat`)" a pagina 51 e "Instradamento basato sul contenuto di Dispatcher (metodo di inoltro `cbr`)" a pagina 53. Per CBR, consultare "Bilanciamento del carico client-proxy in SSL e proxy-server in HTTP" a pagina 106.

protocol

I valori validi per `protocol` sono HTTP e HTTPS. Il valore predefinito è HTTP.

Nota: il parametro `protocol` si applica unicamente al componente CBR.

portvalue

Valore del numero `mapport`. Il valore predefinito è il numero di porta di destinazione della richiesta client.

router

Se si sta impostando una rete WAN (wide area network), l'indirizzo del router al server remoto. Il valore predefinito è 0, che indica un server locale. Notare che, una volta impostato l'indirizzo router di un server su un valore diverso da zero (che indica un server remoto), tale indirizzo non potrà più essere ripristinato su 0 per rendere nuovamente il server locale. Il server deve essere invece rimosso e riaggiunto senza specificare un indirizzo router. Allo stesso modo, un server definito come locale (indirizzo router = 0) non può diventare remoto modificando l'indirizzo router. Il server deve essere rimosso, quindi riaggiunto. Per ulteriori informazioni, consultare "Configurazione del supporto di Dispatcher per una rete geografica" a pagina 221.

Nota: il parametro `router` si applica unicamente a Dispatcher. Se si stanno utilizzando i metodi di inoltro `nat` o `cbr`, quando si aggiunge un server alla configurazione, è necessario specificare l'indirizzo router.

addr

Il valore dell'indirizzo del router.

returnaddress

Un nome host o un indirizzo IP univoco. Si tratta di un indirizzo configurato sulla macchina Dispatcher e che il Dispatcher utilizza come indirizzo di origine quando bilancia il carico delle richieste del client al server. In questo modo, il server restituisce il pacchetto alla macchina Dispatcher, che elabora il contenuto della richiesta, anziché inviarlo direttamente al client. (Il Dispatcher inoltra quindi il pacchetto IP al client.) Quando il server viene aggiunto, è necessario specificare il valore dell'indirizzo mittente. L'indirizzo mittente non può essere

modificato, a meno che il server non venga rimosso e riaggiunto. L'indirizzo mittente non può essere uguale all'indirizzo cluster, server o NFA.

Nota: il parametro `returnaddress` si applica esclusivamente al Dispatcher. Se si stanno utilizzando i metodi di inoltro `nat` o `cbr`, quando si aggiunge un server alla configurazione, è necessario specificare l'indirizzo `returnaddress`.

addr

Il valore dell'indirizzo mittente.

advisorrequest

L'advisor HTTP o HTTPS utilizza la stringa di richiesta advisor per verificare lo stato dei server. È valida solo per i server notificati dall'advisor HTTP o HTTPS. Per abilitare questo valore, è necessario avviare l'advisor HTTP o HTTPS. Per ulteriori informazioni, consultare "Configurazione dell'advisor HTTP o HTTPS utilizzando l'opzione richiesta/risposta (URL)" a pagina 186.

Nota: il parametro `advisorrequest` si applica solo ai componenti Dispatcher e CBR.

string

Il valore della stringa utilizzata dall'advisor HTTP o HTTPS. Il valore predefinito è `HEAD / HTTP/1.0`.

Nota: se la stringa contiene uno spazio —

- Quando si emette il comando dal prompt della shell **dscontrol**>>, è necessario racchiudere la stringa tra virgolette. Ad esempio: **server set cluster:port:server advisorrequest "head / http/1.0"**
- Quando si emette il comando **dscontrol** dal prompt del sistema operativo, il testo deve essere preceduto da `"\"` e seguito da `\"`. Ad esempio: **dscontrol server set cluster:port:server advisorrequest "\"head / http/1.0\""**

advisorresponse

La stringa di risposta advisor ricercata dall'advisor HTTP o HTTPS nella risposta HTTP. È valida solo per i server notificati dall'advisor HTTP o HTTPS. Per abilitare questo valore, è necessario avviare l'advisor HTTP o HTTPS. Per ulteriori informazioni, consultare "Configurazione dell'advisor HTTP o HTTPS utilizzando l'opzione richiesta/risposta (URL)" a pagina 186.

Nota: il parametro `advisorresponse` si applica ai componenti Dispatcher e CBR.

string

Il valore della stringa utilizzata dall'advisor HTTP o HTTPS. Il valore predefinito è `null`.

Nota: se la stringa contiene uno spazio —

- Quando si emette il comando dal prompt della shell **dscontrol**>>, è necessario racchiudere la stringa tra virgolette.
- Quando si emette il comando **dscontrol** dal prompt del sistema operativo, il testo deve essere preceduto da `"\"` e seguito da `\"`.

down

Contrassegna il server come disattivo. Questo comando interrompe tutte le connessioni attive al server e impedisce di inviare al server altre connessioni o pacchetti.

Quando il comando del server inattivo (`dscontrol server down`) viene utilizzato per porre un server offline, se il valore dell'intervallo è diverso da zero per tale server, i client esistenti continuano a funzionare sul server fino a che viene raggiunto l'intervallo. Il server non sarà reso inattivo fino a che non viene raggiunto il valore dell'intervallo.

remove

Rimuove il server.

report

Crea un report sul server. Per ciascun server, il report contiene le seguenti informazioni: numero corrente di connessioni al secondo (CPS), kilobyte trasferiti nell'intervallo di un secondo (KBPS), numero totale di connessioni (Total), numero di connessioni in stato attivo (Active), numero di connessioni in stato FIN (FINed) e numero di connessioni completate (Comp).

set

Imposta i valori per il server.

status

Mostra lo stato dei server.

up Contrassegna il server come attivo. A questo punto, il Dispatcher invierà le nuove connessioni al server.

Esempi

- Per aggiungere il server all'indirizzo 27.65.89.42 alla porta 80 sull'indirizzo cluster 130.40.52.153:
`dscontrol server add 130.40.52.153:80:27.65.89.42`
- Per impostare il server all'indirizzo 27.65.89.42 come non permanente (nonsticky) (funzione ignora affinità di porta):
`dscontrol server set 130.40.52.153:80:27.65.89.42 sticky no`
- Per contrassegnare il server all'indirizzo 27.65.89.42 come disattivo:
`dscontrol server down 130.40.52.153:80:27.65.89.42`
- Per rimuovere il server all'indirizzo 27.65.89.42 su tutte le porte su tutti i cluster:
`dscontrol server remove ::27.65.89.42`
- Per impostare il server all'indirizzo 27.65.89.42 come posizionato (collocated) (il server risiede nella stessa macchina di Load Balancer):
`dscontrol server set 130.40.52.153:80:27.65.89.42 collocated yes`
- Per impostare il peso su 10 per il server 27.65.89.42 sulla porta 80 all'indirizzo cluster 130.40.52.153:
`dscontrol server set 130.40.52.153:80:27.65.89.42 weight 10`
- Per contrassegnare il server all'indirizzo 27.65.89.42 come attivo:
`dscontrol server up 130.40.52.153:80:27.65.89.42`
- Per aggiungere un server remoto:
`dscontrol server add 130.40.52.153:80:130.60.70.1 router 130.140.150.0`
- Per consentire all'advisor HTTP di estrapolare una richiesta URL HTTP HEAD / HTTP/1.0 per il server 27.65.89.42 sulla porta HTTP 80:
`dscontrol server set 130.40.52.153:80:27.65.89.42
advisorrequest "\"HEAD / HTTP/1.0\""`
- Per visualizzare lo stato del server 9.67.143.154 sulla porta 80:
`dscontrol server status 9.67.131.167:80:9.67.143.154`

Questo comando produce un output simile a:

Server Status:

Server	9.67.143.154
Port number	80
Cluster	9.67.131.167
Cluster address	9.67.131.167
Quiesced	N
Server up	Y
Weight	10
Fixed weight	N
Sticky for rule	Y
Remote server	N
Network Router address	0.0.0.0
Collocated	N
Advisor request.....	HEAD / HTTP/1.0
Advisor response.....	
Cookie value	n/a
Clone ID	n/a

dscontrol set — configura il log del server



loglevel

Il livello su cui dsserver registra le proprie attività.

level

Il valore predefinito di **loglevel** è 0. L'intervallo è compreso tra 0 e 5. Di seguito sono riportati i valori possibili: 0 sta per Nessuno, 1 per Minimo, 2 per Base, 3 per Moderato, 4 per Avanzato, 5 per Verbose.

logsize

Il numero massimo di byte da registrare nel file di log.

size

Il valore predefinito di logsize è 1 MB.

dscontrol status — mostra se il gestore e gli advisor sono in esecuzione

►► dscontrol status ◀◀

Esempi

- Per visualizzare gli elementi in esecuzione:
dscontrol status

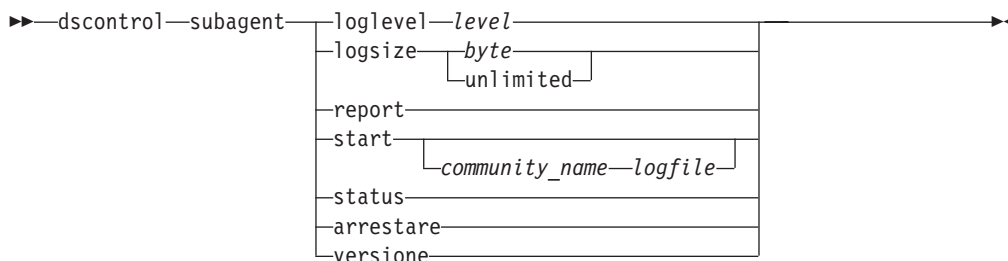
Questo comando produce un output simile a:

Executor has been started.
Manager has been started.

ADVISOR	CLUSTER:PORT	TIMEOUT
reach	0	unlimited
http	80	unlimited
ftp	21	unlimited

dscontrol subagent — configura l'agente secondario SNMP

Nota: i diagrammi della sintassi del comando dscontrol subagent si applicano al componente Dispatcher.



loglevel

Il livello su cui l'agente secondario registra le proprie attività in un file.

level

Il numero del livello (da 0 a 5). Maggiore è il numero, maggiori saranno le informazioni scritte sul log del gestore. Il valore predefinito è 1. Di seguito sono riportati i valori possibili: 0 sta per Nessuno, 1 per Minimo, 2 per Base, 3 per Moderato, 4 per Avanzato, 5 per Verbose.

logsize

Imposta la dimensione massima dei byte da registrare nel log dell'agente secondario. Il valore predefinito è 1 MB. Se si imposta la dimensione massima del file di log, il file ripartirà dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive verranno scritte all'inizio del file, sovrascrivendo quindi le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora, in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

bytes

La dimensione massima in byte del file di log dell'agente secondario. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima, prima di iniziare la sovrascrittura, in quanto le voci di log in sé variano, in termini di dimensione. Il valore predefinito è unlimited.

report

Visualizza un report di istantanee delle statistiche.

start

Avvia l'agente secondario.

community_name

Il nome del valore SNMP del nome comunità che può essere utilizzato come password di sicurezza. Il valore predefinito è public.

Per la piattaforma **Windows**: viene utilizzato il nome comunità del sistema operativo.

log file

Il nome del file su cui vengono registrati i dati dell'agente secondario SNMP.

Ciascun record nel log verrà dotato di un indicatore di data e ora. Il valore predefinito è subagent.log. Il file predefinito viene installato nella directory **logs**. Vedere Appendice C, “File di configurazione di esempio”, a pagina 467. Per modificare la directory su cui vengono memorizzati i file di log, consultare “Modifica dei percorsi file di log” a pagina 259.

status

Visualizza lo stato corrente di tutti i valori dell’agente secondario SNMP che possono essere impostati globalmente, compresi i valori predefiniti.

version

Visualizza la versione corrente dell’agente secondario.

Esempi

- Per avviare l’agente secondario con il nome comunità bigguy:
`dscontrol subagent start bigguy bigguy.log`

Capitolo 28. Riferimenti sui comandi per Site Selector

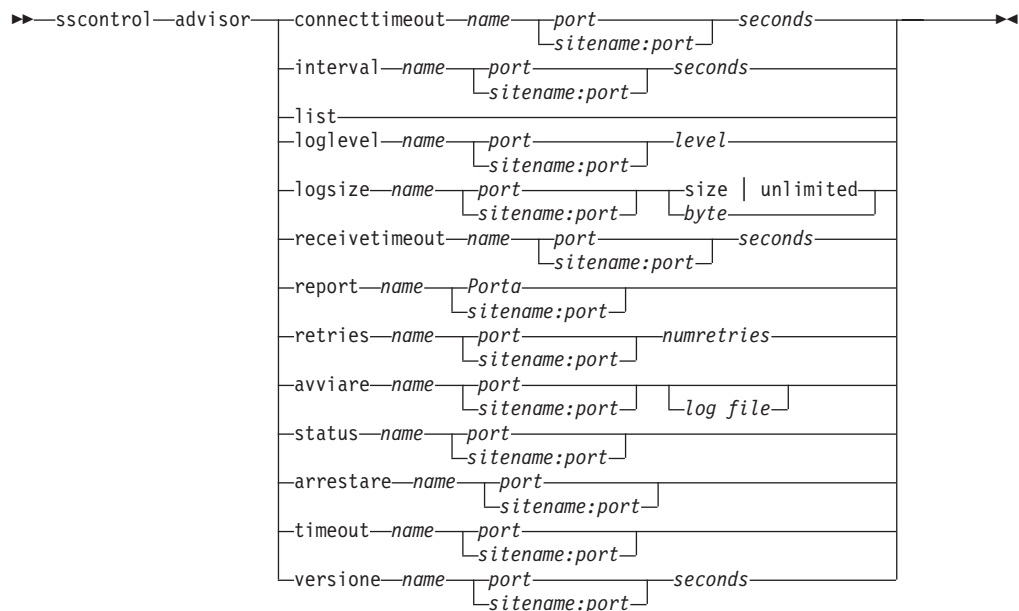
Questo capitolo descrive come utilizzare i seguenti comandi **sscontrol** di Site Selector:

- “sscontrol advisor — controlla l’advisor” a pagina 392
- “sscontrol file — gestisce i file di configurazione” a pagina 397
- “sscontrol help — visualizza o stampa la guida per il comando in questione” a pagina 399
- “sscontrol logstatus — visualizza le impostazioni log del server” a pagina 400
- “sscontrol manager — controlla il gestore” a pagina 401
- “sscontrol metric — configura le metriche di sistema” a pagina 406
- “sscontrol nameserver — controlla il server dei nomi” a pagina 407
- “sscontrol rule — configura le regole” a pagina 408
- “sscontrol server — configura i server” a pagina 411
- “sscontrol set — configura il log del server” a pagina 413
- “sscontrol sitename — configura un sitename” a pagina 414
- “sscontrol status — mostra se il gestore e gli advisor sono in esecuzione” a pagina 417

È possibile immettere una versione ridotta dei parametri del comando **sscontrol**. A tal fine, è sufficiente immettere le lettere che designano in modo univoco i parametri. Ad esempio, per richiamare la guida sul comando di salvataggio file, è possibile digitare **sscontrol he f** invece di **sscontrol help file**.

Nota: i valori dei parametri dei comandi devono essere immessi utilizzando l’alfabeto inglese. Le sole eccezioni sono rappresentate dai nomi host (utilizzati nei comandi dei server e dei cluster) e dai nomi file (utilizzati nei comandi file).

sscontrol advisor — controlla l'advisor



connecttimeout

Impostare il tempo che un advisor attende prima di riferire l'interruzione di una connessione a un server. Per ulteriori informazioni, vedere "Timeout di connessione e timeout di ricezione dell'advisor per i server" a pagina 183.

name

Il nome dell'advisor. Tra i valori possibili vi sono **http**, **https**, **ftp**, **sip**, **ssl**, **smtp**, **imap**, **pop3**, **ldap**, **nntp**, **telnet**, **connect**, **ping**, **WLM** e **WTE**. I nomi degli advisor personalizzati sono nel formato **xxxx**, dove per **ADV_xxxx** si intende il nome della classe che implementa l'advisor personalizzato.

port

Il numero della porta monitorata dall'advisor.

seconds

Un numero intero positivo che rappresenta il tempo, in secondi, che l'advisor attende prima di riferire l'interruzione di una connessione a un server. Il valore predefinito è pari a 3 volte il valore specificato per l'intervallo dell'advisor.

interval

Impostare la frequenza con cui l'advisor richiede informazioni ai server.

seconds

Un numero intero positivo che rappresenta il numero di secondi trascorsi tra le richieste di stato ai server. Il valore predefinito è 7.

list

Mostra l'elenco degli advisor che attualmente forniscono informazioni al gestore.

loglevel

Imposta il livello di registrazione per un log dell'advisor.

level

Il numero del livello (da 0 a 5). Il valore predefinito è 1. Maggiore è il numero, maggiori saranno le informazioni scritte sul log dell'advisor. I valori possibili sono:

- 0 sta per Nessuno
- 1 per Minimo
- 2 per Base
- 3 per Moderato
- 4 per Avanzato
- 5 per Verbose

logsize

Impostare la dimensione massima di un log dell'advisor. Se si imposta la dimensione massima del file di log, il file riparte dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive sovrascrivono le voci di log precedenti. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

size | unlimited

La dimensione massima in byte del file di log dell'advisor. È possibile specificare un numero positivo maggiore di zero o **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima, prima di essere sovrascritto, in quanto le voci di log variano in termini di dimensione. Il valore predefinito è 1 MB.

receivetimeout

Impostare il tempo che un advisor attende prima di riferire l'impossibilità di ricezione da un server. Per ulteriori informazioni, vedere "Timeout di connessione e timeout di ricezione dell'advisor per i server" a pagina 183.

seconds

Un numero intero positivo che rappresenta il tempo, in secondi, che l'advisor attende prima di riferire l'impossibilità di una ricezione da un server. Il valore predefinito è pari a 3 volte il valore specificato per l'intervallo dell'advisor.

report

Visualizza un report sullo stato dell'advisor.

retries

Il numero di tentativi che un advisor può eseguire prima di contrassegnare un server come inattivo.

numretries

Un numero intero maggiore o uguale a zero. È preferibile che questo valore non sia maggiore di 3. Se la parola chiave retries non è configurata, per il numero di tentativi viene assunto il valore zero.

start

Avvia l'advisor. Sono disponibili advisor per ciascun protocollo. Le porte predefinite sono:

Nome advisor	Protocollo	Porta
Connect	n/d	definito dall'utente
db2	private	50000
ftp	FTP	21
http	HTTP	80

Nome advisor	Protocollo	Porta
https	SSL	443
imap	IMAP	143
ldap	LDAP	389
nntp	NNTP	119
PING	PING	N/A
pop3	POP3	110
sip	SIP	5060
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23

name

Il nome dell'advisor.

sitename:port

Sui comandi advisor il valore sitename è opzionale mentre il valore port è obbligatorio. Se il valore sitename non è specificato, l'advisor inizia l'esecuzione su tutti i sitename configurati e disponibili. Se si specifica un sitename, l'advisor inizia l'esecuzione solo per il sitename specificato. i sitename supplementari vengono separati dal segno più (+).

log file

Nome del file su cui sono registrati i dati di gestione. Ciascun record nel log è dotato di un indicatore di data e ora.

Il file predefinito è *advisorname_port.log*, ad esempio, **http_80.log**. Per modificare la directory su cui vengono memorizzati i file di log, consultare "Modifica dei percorsi file di log" a pagina 259.

È possibile avviare un solo advisor per ogni sitename.

status

Visualizza lo stato corrente e le impostazioni predefinite di tutti i valori globali in un advisor.

stop

Arresta l'advisor.

timeout

Imposta il numero di secondi entro il quale il gestore considera valide le informazioni ricevute dall'advisor. Se il gestore rileva che le informazioni dell'advisor sono meno aggiornate rispetto a questo periodo di timeout, non utilizza tali informazioni per determinare i pesi dei server sulla porta monitorata dall'advisor. Un'eccezione a questo timeout avviene quando l'advisor ha informato il gestore dell'inattività di uno specifico server. Il gestore utilizza quelle informazioni sul server anche in seguito al timeout delle informazioni dell'advisor.

seconds

Un numero positivo che rappresenta un numero di secondi o **unlimited**. Il valore predefinito è unlimited.

version

Visualizza la versione corrente dell'advisor.

Esempi

- Per impostare il tempo (30 secondi) che un advisor HTTP (per la porta 80) attende prima di riferire l'interruzione di una connessione a un server:
`sscontrol advisor connecttimeout http 80 30`
- Per impostare l'intervallo per l'advisor FTP (per la porta 21) su 6 secondi:
`sscontrol advisor interval ftp 21 6`
- Per visualizzare l'elenco degli advisor che attualmente forniscono informazioni al gestore:
`sscontrol advisor list`

Questo comando produce un output simile a:

ADVISOR	SITENAME:PORT	TIMEOUT
http	80	unlimited
ftp	21	unlimited

- Per modificare il livello di log del log dell'advisor http, del sitename di mysite, su 0 al fine di ottenere migliori prestazioni:
`sscontrol advisor loglevel http mysite:80 0`
- Per modificare la dimensioni di log dell'advisor ftp per sitename di mysite su 5000 byte:
`sscontrol advisor logsize ftp mysite:21 5000`
- Per impostare il tempo (60 secondi) che un advisor HTTP (per la porta 80) attende prima di riferire l'impossibilità di ricezione da un server:
`sscontrol advisor receivetimeout http 80 60`
- Per visualizzare un report sullo stato dell'advisor ftp (per la porta 21):
`sscontrol advisor report ftp 21`

Questo comando produce un output simile a:

Advisor Report:

```
-----
Advisor name ..... http
Port number ..... 80

sitename ..... mySite
Server address ..... 9.67.129.230
Load ..... 8
```

- Per avviare l'advisor con il file ftpadv.log:
`sscontrol advisor start ftp 21 ftpadv.log`
- Per visualizzare lo stato corrente dei valori associati all'advisor http:
`sscontrol advisor status http 80`

Questo comando produce un output simile al seguente:

Advisor Status:

```
-----
Interval (seconds) ..... 7
Timeout (seconds) ..... Unlimited
Connect timeout (seconds).....21
Receive timeout (seconds).....21
Advisor log filename ..... Http_80.log
Log level ..... 1
Maximum log size (bytes) ..... Unlimited
Number of retries ..... 0
```

- Per arrestare l'advisor http sulla porta 80:

```
sscontrol advisor stop http 80
```

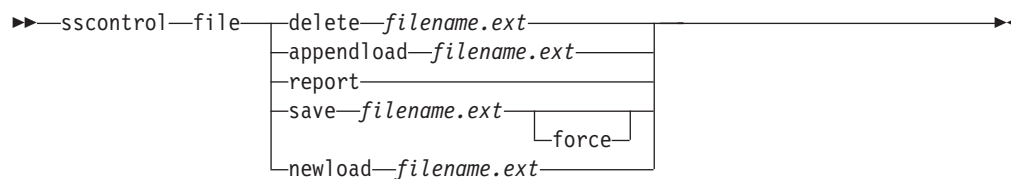
- Per impostare il valore di timeout per le informazioni dell'advisor su 5 secondi:

```
sscontrol advisor timeout ftp 21 5
```

- Per trovare il numero di porta corrente dell'advisor ssl:

```
sscontrol advisor version ssl 443
```

sscontrol file — gestisce i file di configurazione



delete

Elimina il file.

file.ext

Un file di configurazione.

L'estensione del file (*.ext*) è a scelta e facoltativa.

appendload

Aggiunge un file di configurazione alla configurazione corrente e lo carica su Site Selector.

report

Crea il report relativo ai file disponibili.

save

Salva la configurazione corrente di Site Selector nel file.

Nota: I file vengono salvati nelle directory e caricati dalle stesse directory:

- Sistemi Linux e UNIX: **/opt/ibm/edge/lb/servers/configurations/ss**
- Sistemi Windows: **C:\Program Files\ibm\edge\lb\servers\configurations\componente**

force

Per salvare il file in un file esistente con nome identico, utilizzare l'opzione **force** per eliminare il file esistente prima di salvare quello nuovo. Se non si utilizza l'opzione **force**, il file esistente non verrà sovrascritto.

newload

Carica un nuovo file di configurazione in Site Selector. Il nuovo file di configurazione sostituisce la configurazione corrente.

Esempi

- Per eliminare un file:

```
sscontrol file delete file3
```

File (file3) was deleted.
- Per caricare un nuovo file di configurazione per sostituire la configurazione corrente:

```
sscontrol file newload file1.sv
```

File (file1.sv) was loaded into the Dispatcher.
- Per aggiungere un file di configurazione alla configurazione corrente e caricarlo:

```
sscontrol file appendload file2.sv
```

File (file2.sv) was appended to the current configuration and loaded.
- Per visualizzare un report dei file (ossia, dei file precedentemente salvati):

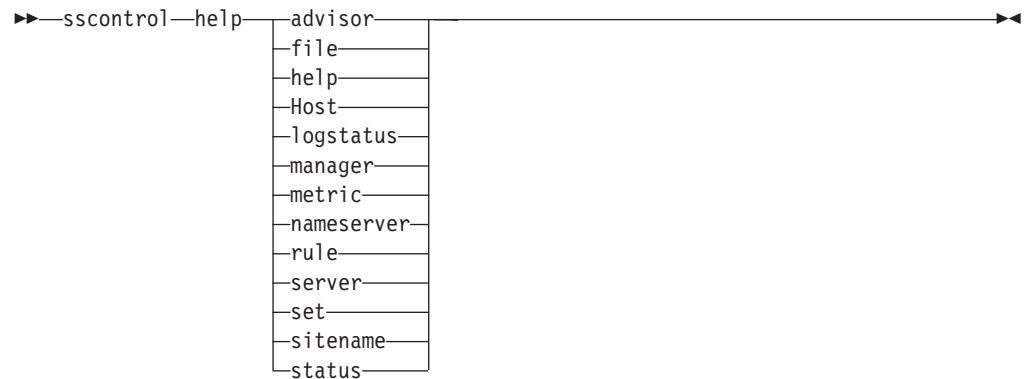
```
sscontrol file report
```

```
FILE REPORT:  
file1.save  
file2.sv  
file3
```

- Per salvare la configurazione in un file denominato file3:
sscontrol file save file3

```
The configuration was saved into file (file3).
```

sscontrol help — visualizza o stampa la guida per il comando in questione



Esempi

- Per richiamare la guida sul comando sscontrol:
sscontrol help

Questo comando produce un output simile a:

```
HELP COMMAND  
ARGUMENTS:  
-----  
Usage: help <help option>  
Example: help name  
  
help          - print complete help text  
advisor       - help on advisor command  
file          - help on file command  
host          - help on host command  
manager       - help on manager command  
metric        - help on metric command  
sitename      - help on sitename command  
nameserver    - help on nameserver command  
rule          - help on rule command  
server        - help on server command  
set           - help on set command  
status        - help on status command  
logstatus     - help on logstatus command
```

I parametri nelle tag < > sono variabili.

- A volte la guida visualizza le scelte per le variabili utilizzando il carattere | per separare le opzioni:
logsize <number of bytes | unlimited>
-Set the maximum number of bytes to be logged in the log file

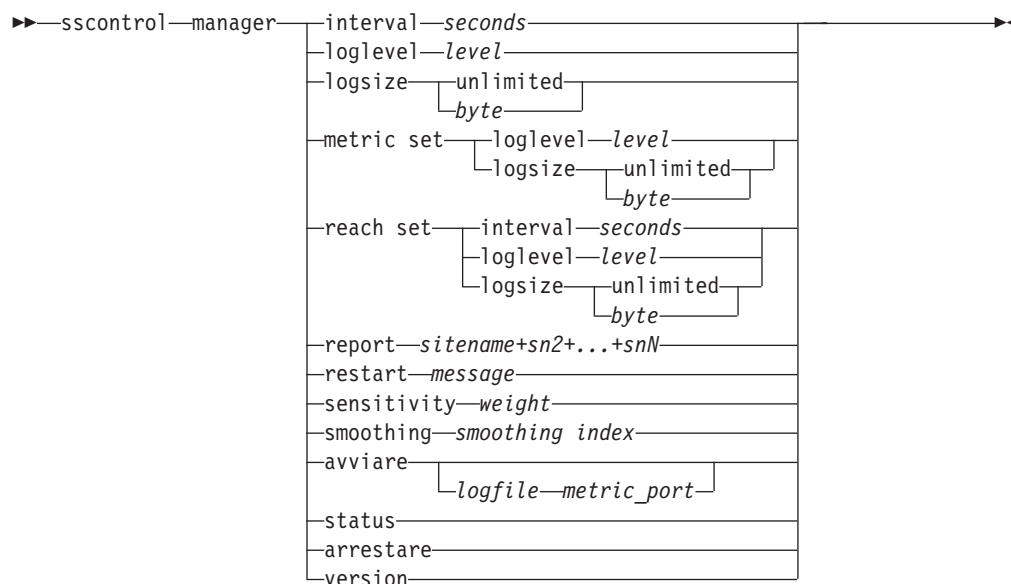
sscontrol logstatus — visualizza le impostazioni log del server

►►—sscontrol—logstatus—◄◄

logstatus

Visualizza le impostazioni log del server (nome file di log, livello di registrazione e dimensione log).

sscontrol manager — controlla il gestore



interval

Imposta la frequenza con cui il gestore aggiorna i pesi del server.

seconds

Un numero intero, in secondi, che indica la frequenza con cui il gestore aggiorna i pesi. Il valore predefinito è 2.

loglevel

Imposta il livello di registrazione per il log del gestore.

level

Il numero del livello (da 0 a 5). Maggiore è il numero, maggiori saranno le informazioni scritte sul log del gestore. Il valore predefinito è 1. I valori possibili sono:

- 0 sta per Nessuno
- 1 per Minimo
- 2 per Base
- 3 per Moderato
- 4 per Avanzato
- 5 per Verbose

logsize

Imposta la dimensione massima del log del gestore. Se si imposta la dimensione massima del file di log, il file riparte dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive vengono scritte partendo dall'inizio del file, sovrascrivendo quindi le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

bytes

La dimensione massima in byte del file di log del gestore. È possibile specificare un numero positivo maggiore di zero o **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima, prima di essere sovrascritto, in quanto le voci di log variano in termini di dimensione. Il valore predefinito è 1 MB.

metric set

Imposta **loglevel** e **logsize** per il log di controllo metrica. Loglevel è il livello di registrazione di controllo metrica (0 - Nessuno, 1 - Minimo, 2 - Base, 3 - Moderato, 4 - Avanzato o 5 - Verbose). Il loglevel predefinito è 1. Il logsize è il numero massimo di byte da registrare nel file di log di controllo metrica. È possibile specificare un numero positivo maggiore di zero o unlimited. Il valore logsize predefinito è 1.

reach set

Imposta interval, loglevel e logsize per l'advisor reach.

report

Visualizza un report di istantanee delle statistiche.

sitename

Il nome del sito da visualizzare nel report. È un nome host non risolvibile che il client richiederà. Il sitename deve essere un nome dominio completo.

Nota: i sitename supplementari vengono separati dal segno più (+).

restart

Riavvia tutti i server (non disattivi) con i pesi normalizzati (1/2 del peso massimo).

messaggio

Un messaggio che si desidera venga scritto nel file di log del gestore.

sensitivity

Impostare la sensibilità minima su cui aggiornare i pesi. Questa impostazione definisce il momento in cui il gestore deve modificare il peso del server in base alle informazioni esterne.

weight

Un numero da 0 a 100 utilizzato come percentuale dei pesi. Il valore predefinito 5 crea una sensibilità minima del 5%.

smoothing

Impostare un indice che arrotondi le variazioni del peso durante il bilanciamento del carico. Un indice di arrotondamento più alto fa in modo che i pesi del server subiscano delle variazioni meno drastiche, in caso di cambiamento delle condizioni di rete. Con un indice più basso, i pesi del server subiscono delle variazioni più drastiche.

index

Un numero a virgola mobile positivo. Il valore predefinito è 1,5.

start

Avvia il gestore.

log file

Il nome del file su cui vengono registrati i dati gestore. Ciascun record nel log è dotato di un indicatore di data e ora.

Il file predefinito viene installato nella directory **logs**. Vedere Appendice C, “File di configurazione di esempio”, a pagina 467. Per modificare la directory su cui vengono memorizzati i file di log, consultare “Modifica dei percorsi file di log” a pagina 259.

metric_port

La porta utilizzata da Metric Server per creare i report dei carichi di sistema. Se si specifica una porta metrica, è necessario indicare il nome di un file di log. La porta metrica predefinita è la numero 10004.

status

Visualizza lo stato corrente e le impostazioni predefinite di tutti i valori globali in un gestore.

stop

Arresta il gestore.

version

Visualizza la versione corrente del gestore.

Esempi

- Per impostare l'intervallo di aggiornamento del gestore ogni 5 secondi:
`sscontrol manager interval 5`
- Per impostare il livello di registrazione su 0 per ottenere migliori prestazioni:
`sscontrol manager loglevel 0`
- Per impostare la dimensione del log del gestore su 1.000.000 byte:
`sscontrol manager logsize 1000000`
- Per richiamare l'istantanea delle statistiche del gestore:
`sscontrol manager report`

Questo comando produce un output simile a:

SERVER	STATUS
9.67.129.221	ACTIVE
9.67.129.213	ACTIVE
9.67.134.223	ACTIVE

MANAGER REPORT LEGEND	
CPU	CPU Load
MEM	Memory Load
SYS	System Metric
NOW	Current Weight
NEW	New Weight
WT	Weight

mySite	WEIGHT	CPU	49%	MEM	50%	PORT	1%	SYS	0%	
	NOW	NEW	WT	LOAD	WT	LOAD	WT	LOAD	WT	LOAD
9.37.56.180	10	10	-99	-1	-99	-1	-99	-1	0	0
TOTALS:	10	10		-1		-1		-1		0

ADVISOR	SITENAME:PORT	TIMEOUT
http	80	unlimited

- Per riavviare tutti i server con i pesi normalizzati e scrivere un messaggio nel file di log del gestore:
sscontrol manager restart Restarting the manager to update code

Questo comando produce un output simile a:

```
320-14:04:54
Restarting the manager to update code
```

- Per impostare la sensibilità alle variazioni del peso su 10:
sscontrol manager sensitivity 10
- Per impostare l'indice di arrotondamento su 2,0:
sscontrol manager smoothing 2.0
- Per avviare il gestore e specificare il file di log denominato ndmgr.log (i percorsi non possono essere impostati)
sscontrol manager start ndmgr.log
- Per visualizzare lo stato corrente dei valori associati al gestore:
sscontrol manager status

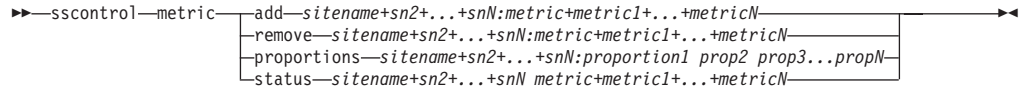
Questo comando produce un output simile al seguente esempio.

```
Manager status:
=====
Metric port..... 10004
Manager log filename..... manager.log
Manager log level..... 1
Maximum manager log size (bytes)..... unlimited
Sensitivity level..... 5
Smoothing index..... 1.5
Update interval (seconds)..... 2
Weights refresh cycle..... 2
```

```
Reach log level..... 1
Maximum reach log size (bytes)..... unlimited
Reach update interval (seconds)..... 7
```

- Per arrestare il gestore:
sscontrol manager stop
- Per visualizzare il numero della versione corrente del gestore:
sscontrol manager version

sscontrol metric — configura le metriche di sistema



add

Aggiunge la metrica specificata.

sitename

Il sitename configurato. i sitename supplementari vengono separati dal segno più (+).

metric

Il nome della metrica di sistema, che deve essere il nome di un file eseguibile o script nella directory script di Metric Server.

remove

Elimina la metrica specificata.

proportions

Determina l'importanza di ciascuna metrica confrontata con le altre se su un singolo server vengono utilizzate più metriche.

status

Visualizza i valori correnti del server della metrica in questione.

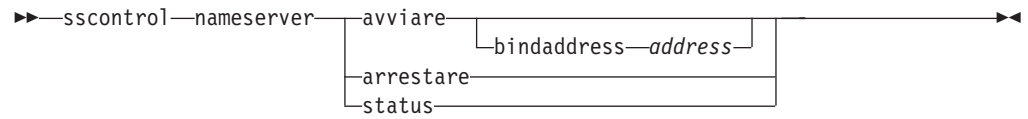
Esempi

- Per aggiungere una metrica di sistema:
`sscontrol metric add sitel:metric1`
- Per impostare le proporzioni di un sitename con due metriche di sistema:
`sscontrol metric proportions sitel 0 100`
- Per visualizzare lo stato corrente dei valori associati alla metrica specificata:
`sscontrol metric status sitel:metric1`

Questo comando produce un output simile al seguente:

```
Metric Status:
-----
sitename ..... sitel
Metric name ..... metric1
Metric proportion ..... 50
  Server ..... 9.37.56.100
  Metric data .... -1
```

sscontrol nameserver — controlla il server dei nomi



start

Avvia il server dei nomi.

bindaddress

Avvia il server dei nomi associato all'indirizzo specifico. Il server dei nomi risponde solo a una richiesta destinata a questo indirizzo.

address

Un indirizzo (IP o simbolico) configurato sulla macchina Site Selector.

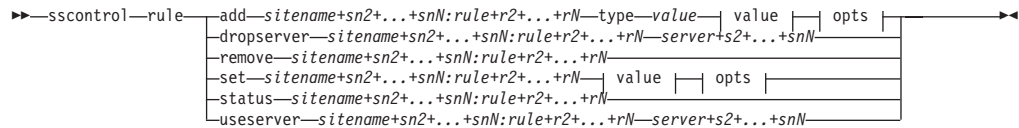
stop

Arresta il server dei nomi.

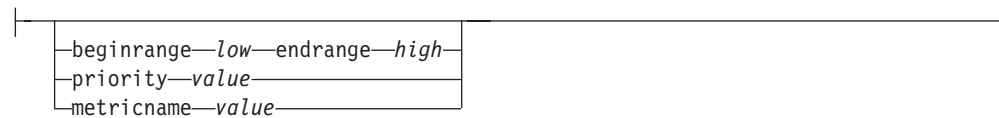
status

Visualizza lo stato del server dei nomi.

sscontrol rule — configura le regole



opts:



add

Aggiunge la regola a un sitename.

sitename

Un nome host non risolvibile che il client richiederà. Il sitename deve essere un nome dominio completo. I sitename supplementari vengono separati dal segno più (+).

regola

Il nome scelto per la regola. Questo nome può contenere caratteri alfanumerici, caratteri di sottolineatura, trattini o punti. La lunghezza può variare da 1 a 20 caratteri e gli spazi non sono ammessi.

Nota: le regole supplementari vengono separate da un segno più (+).

tipo

Il tipo di regola.

type

Le scelte per *type* sono:

ip La regola è basata sull'indirizzo IP client.

metricall

La regola si basa sul valore della metrica attuale per tutti i server all'interno del gruppo.

metricavg

La regola si basa sulla media dei valori di metrica correnti per tutti i server all'interno del gruppo.

time La regola è basata sull'ora del giorno.

true Questa regola è sempre true. Considerarla come un'istruzione else nella logica programmatica.

beginrange

Il valore minimo nell'intervallo utilizzato per determinare se la regola assume o meno il valore true.

low

Dipende dal tipo di regola. Il tipo di valore e le relative impostazioni predefinite vengono qui elencate per tipo di regola:

ip L'indirizzo del client espresso come nome simbolico o nel formato indirizzo IP. Il valore predefinito è 0.0.0.0.

time Numero intero. Il valore predefinito è 0, ossia mezzanotte.

metricall

Numero intero. Il valore predefinito è 100.

metricavg

Numero intero. Il valore predefinito è 100.

endrange

Il valore massimo nell'intervallo utilizzato per determinare se la regola assume o meno il valore true.

high

Dipende dal tipo di regola. Il tipo di valore e le relative impostazioni predefinite vengono qui elencate per tipo di regola:

ip

L'indirizzo del client espresso come nome simbolico o nel formato indirizzo IP. Il valore predefinito è 255.255.255.254.

time

Numero intero. Il valore predefinito è 24, ossia mezzanotte.

Nota: quando si definiscono i valori beginrange ed endrange degli intervalli di tempo, notare che ciascun valore deve essere un numero intero positivo che rappresenta solo l'ora; non è possibile specificare i minuti. Per questo motivo, per indicare una singola ora —ad esempio, l'ora compresa tra le 3:00 e le 4:00— specificare 3 per beginrange e nuovamente 3 per endrange. Ciò indica tutti i minuti dalle 3:00 alle 3:59. Specificando 3 per beginrange e 4 per endrange, l'intervallo di tempo stabilito sarà compreso tra le 3:00 e le 4:59.

metricall

Numero intero. Il valore predefinito è 2 alla trentaduesima potenza meno 1.

metricavg

Numero intero. Il valore predefinito è 2 alla trentaduesima potenza meno 1.

priority

L'ordine in cui verranno riviste le regole.

level

Numero intero. Se non si specifica la priorità della prima regola aggiunta, Site Selector la imposta, per valore predefinito, su 1. Quando si aggiunge una seconda regola, sempre per valore predefinito, la relativa priorità viene calcolata come 10 + la priorità attualmente più bassa di una regola esistente. Ad esempio, presupporre di avere una regola con priorità pari a 30. Quindi, viene aggiunta una nuova regola la cui priorità viene impostata su 25 (ossia, una priorità *superiore* a 30). Infine, si aggiunge una terza regola senza impostarne la priorità. La priorità della terza regola viene calcolata come 40 (30 + 10).

metricname

Nome della metrica misurata per una regola.

dropserver

Rimuove un server da un insieme di regole.

server

L'indirizzo IP della macchina server TCP espresso come nome simbolico o in formato indirizzo IP.

Nota: i sitename supplementari vengono separati dal segno più (+).

remove

Rimuove una o più regole, separate l'un dall'altra l'altra dai segni più (+).

set

Imposta i valori per questa regola.

status

Visualizza tutti i valori di una o più regole.

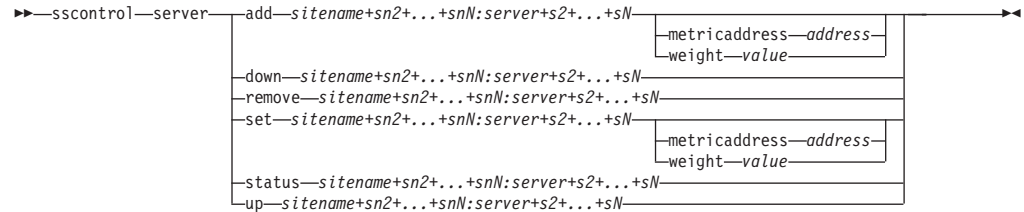
useserver

Inserisce il server in un insieme di regole.

Esempi

- Per aggiungere una regola il cui valore sarà sempre true, non specificare il valore di inizio o di fine:
`sscontrol rule add sitename:rulename type true priority 100`
- Per creare una regola che vieta l'accesso a un intervallo di indirizzi IP, in questo caso, gli indirizzi IP che iniziano con "9" :
`sscontrol rule add sitename:rulename type ip b 9.0.0.0 e 9.255.255.255`
- Per creare una regola che specificherà l'uso di un determinato server dalle 11:00 a.m. alle 3:00 p.m.:
`sscontrol rule add sitename:rulename type time beginrange 11 endrange 14`
`sscontrol rule useserver sitename:rulename server05`

sscontrol server — configura i server



add

Aggiunge il server.

sitename

Un nome host non risolvibile che il client richiede. Il sitename deve essere un nome dominio completo. I sitename supplementari vengono separati dal segno più (+).

server

L'indirizzo IP della macchina server TCP espresso come nome simbolico o in formato indirizzo IP.

Nota: i server supplementari vengono separati da un segno più (+).

metricaddress

L'indirizzo di metric server.

address

L'indirizzo del server espresso come nome simbolico o nel formato indirizzo IP.

weight

Un numero compreso nell'intervallo 0–100 (che non deve superare il valore weightbound massimo del sitename) che rappresenta il peso per questo server. L'impostazione del peso su zero impedisce di inviare al server eventuali nuove richieste. Il valore predefinito è la metà del valore weightbound massimo del sitename specificato. Se il gestore è in esecuzione, questa impostazione verrà velocemente sovrascritta.

value

Il valore del peso del server.

down

Contrassegna il server come disattivo. Questo comando impedisce a qualsiasi richiesta di essere risolta su quel server.

remove

Rimuove il server.

set

Imposta i valori per il server.

status

Mostra lo stato dei server.

up Contrassegna il server come attivo. Site Selector risolverà le nuove richieste su quel server.

Esempi

- Per aggiungere il server all'indirizzo 27.65.89.42 su un sitename di site1:
`sscontrol server add site1:27.65.89.42`
- Per contrassegnare il server all'indirizzo 27.65.89.42 come disattivo:
`sscontrol server down site1:27.65.89.42`
- Per rimuovere il server dall'indirizzo 27.65.89.42 di tutti i sitename:
`sscontrol server remove :27.65.89.42`
- Per contrassegnare il server all'indirizzo 27.65.89.42 come attivo:
`sscontrol server up site1:27.65.89.42`

sscontrol set — configura il log del server



loglevel

Il livello su cui ssserver registra le proprie attività.

level

Il valore predefinito di **loglevel** è 0. I valori possibili sono:

- 0 sta per Nessuno
- 1 per Minimo
- 2 per Base
- 3 per Moderato
- 4 per Avanzato
- 5 per Verbose

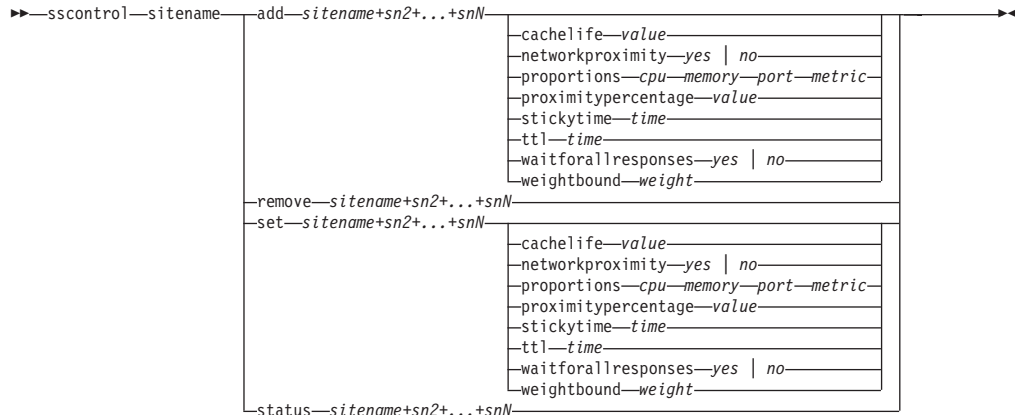
logsize

Il numero massimo di byte da registrare nel file di log.

size

Il valore predefinito di logsize è 1 MB.

sscontrol sitename — configura un sitename



add

Aggiunge un nuovo sitename.

sitename

Un nome host non risolvibile, richiesto dal client. I sitename supplementari vengono separati dal segno più (+).

cachelife

La quantità di tempo durante la quale una risposta di prossimità sarà valida e verrà salvata nella cache. Il valore predefinito è 1800. Per ulteriori informazioni, consultare “Uso della funzione di prossimità della rete” a pagina 126.

value

Un numero positivo che rappresenta il numero di secondi per cui una risposta di prossimità è valida e viene salvata nella cache.

networkproximity

Determina la prossimità della rete di ciascun server al client richiedente. Utilizzare la risposta di prossimità nella decisione di bilanciamento del carico. Impostare la prossimità su on o off. Per ulteriori informazioni, consultare “Uso della funzione di prossimità della rete” a pagina 126.

value

Le scelte sono yes o no. L'impostazione predefinita è no, e indica che la prossimità della rete è disabilitata.

proportions

Imposta la proporzione di importanza per cpu, memoria, porta (informazioni fornite dagli advisor) e metriche di sistema per Metric Server, utilizzate dal gestore per impostare i pesi dei server. Ognuno di questi valori viene espresso come una percentuale del totale e il totale è sempre 100.

cpu

La percentuale di CPU in uso su ciascuna macchina server con bilanciamento del carico (input dell'agente Metric Server).

memoria

La percentuale di memoria in uso (input dell'agente di Metric Server agent) su ciascun server con bilanciamento del carico

porta

l'input degli advisor in ascolto sulla porta.

sistema

L'input di Metric Server.

proximitypercentage

Imposta l'importanza della risposta di prossimità rispetto allo stato del server (peso del gestore). Per ulteriori informazioni, consultare "Uso della funzione di prossimità della rete" a pagina 126.

value

Il valore predefinito è 50.

stickytime

L'intervallo durante il quale un client riceve lo stesso ID server restituito in precedenza, per la prima richiesta. Il valore predefinito di stickytime è 0, e indica che il nome sito (sitename) non è aderente.

time

Un numero positivo, diverso da zero, che rappresenta il numero di secondi durante i quali il client riceve lo stesso ID server restituito in precedenza per la prima richiesta.

ttl Imposta la durata (TTL, time to live). Indica il tempo durante il quale un altro server dei nomi memorizzerà nella cache la risposta risolta. Il valore predefinito è 5.

value

Un numero positivo che rappresenta il numero di secondi per cui il server dei nomi memorizzerà nella cache la risposta risolta.

waitforallresponses

Determina se attendere tutte le risposte di prossimità dai server prima di rispondere alla richiesta del client. Per ulteriori informazioni, consultare "Uso della funzione di prossimità della rete" a pagina 126.

value

Le scelte sono yes o no. Il valore predefinito è yes.

weightbound

Un numero che rappresenta il peso massimo che si può impostare per i server su questo sitename. Il valore weightbound, impostato per il sitename, può essere ignorato per i singoli server mediante il **peso server**. Il valore predefinito di weightbound di sitename è 20.

weight

Il valore di weightbound.

set

Imposta le proprietà di sitename.

remove

Rimuove il sitename.

status

Mostra lo stato corrente di un sitename specifico.

Esempi

- Per aggiungere un sitename:
`sscontrol sitename add 130.40.52.153`
- Per attivare la prossimità della rete:
`sscontrol sitename set mySite networkproximity yes`
- Per impostare la durata della cache su 1900000 secondi:
`sscontrol sitename set mySite cachelife 1900000`
- Per impostare la percentuale di prossimità di 45:

```
sscontrol sitename set mySite proximitypercentage 45
```

- Per impostare un sitename ed evitare che aspetti tutte le risposte prima di rispondere:

```
sscontrol sitename set mySite waitforallresponses no
```

- Per impostare il valore TTL (time to live) su 7 secondi:

```
sscontrol sitename set mySite ttl 7
```

- Per impostare le proporzioni di importanza rispettivamente per CpuLoad, MemLoad, Port e System Metric:

```
sscontrol sitename set mySite proportions 50 48 1 1
```

- Per rimuovere un sitename:

```
sscontrol sitename remove 130.40.52.153
```

- Per visualizzare lo stato del sitename mySite:

```
sscontrol sitename status mySite
```

Questo comando produce un output simile a:

```
SiteName Status:
```

```
-----
```

```
SiteName ..... mySite
WeightBound ..... 20
TTL ..... 5
StickyTime ..... 0
Number of Servers ..... 1
Proportion given to CpuLoad ..... 49
Proportion given to MemLoad ..... 50
Proportion given to Port ..... 1
Proportion given to System metric .. 0
Advisor running on port ..... 80
Using Proximity ..... N
```

sscontrol status — mostra se il gestore e gli advisor sono in esecuzione

►—sscontrol—status—◄◄

Esempi

- Per visualizzare gli elementi in esecuzione, digitare:
`sscontrol status`

Questo comando produce un output simile a:

```
NameServer has been started.  
Manager has been started.
```

```
-----  
| ADVISOR | SITENAME:PORT | TIMEOUT |  
-----  
|   http |           80 | unlimited |  
-----
```

Capitolo 29. Riferimenti sui comandi per Cisco CSS Controller

Questo capitolo descrive come utilizzare i seguenti comandi **ccocontrol** di Cisco CSS Controller:

- “ccocontrol consultant — configura e controlla un consultant” a pagina 420
- “ccocontrol controller — gestione del controller” a pagina 423
- “ccocontrol file — gestisce i file di configurazione” a pagina 425
- “ccocontrol help — Visualizza o stampa la guida per questo comando” a pagina 426
- “ccocontrol highavailability — controlla la disponibilità elevata” a pagina 427
- “ccocontrol metriccollector — configura lo strumento di raccolta delle metriche” a pagina 430
- “ccocontrol ownercontent — controlla il nome proprietario e la regola di contenuto” a pagina 432
- “ccocontrol service — configura un servizio” a pagina 435

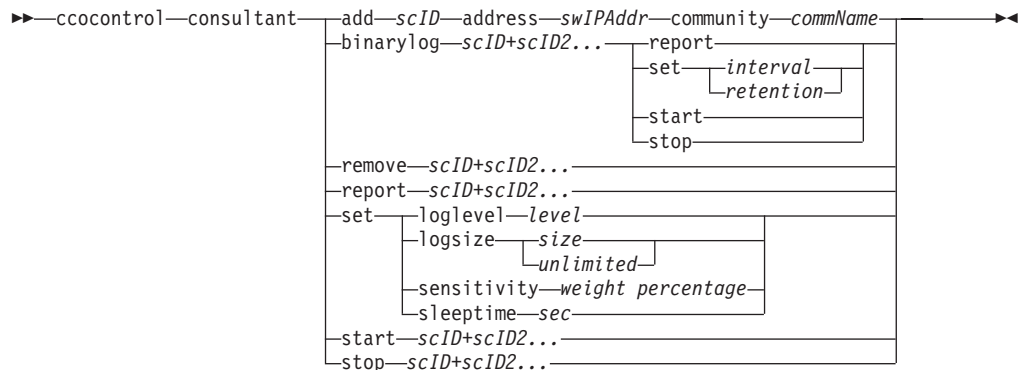
È possibile utilizzare una versione abbreviata dei parametri del comando **ccocontrol** digitando le lettere che designano in modo univoco i parametri. Ad esempio, per visualizzare le informazioni sul comando di salvataggio del file, è possibile digitare **ccocontrol he f** invece di **ccocontrol help file**.

Per richiamare il prompt dei comandi **ccocontrol**: digitare **ccocontrol** .

Per terminare l'interfaccia della riga comandi: digitare **exit** o **quit**.

Nota: Utilizzare i caratteri inglesi per tutti i valori dei parametri dei comandi. Le sole eccezioni sono rappresentate dai nomi host (utilizzati nei comandi **server**) e dai nomi file (utilizzati nei comandi **file**).

cococontrol consultant — configura e controlla un consultant



add

Aggiunge un consultant dello switch.

scID (switchConsultantID)

Una stringa definita dall'utente che fa riferimento al consultant.

address

L'indirizzo IP di Switch Cisco CSS per cui il consultant fornisce i pesi.

swIPAddr (switchIPAddress)

L'indirizzo IP dello switch.

community

Il nome utilizzato in SNMP per richiamare e impostare le comunicazioni con Switch Cisco CSS.

commName

Il nome della comunità di lettura/scrittura di Switch Cisco CSS.

binarylog

Controlla la registrazione binaria di un consultant.

report

Notifica le caratteristiche della registrazione binaria.

set

Imposta la frequenza, espressa in secondi, con la quale le informazioni vengono scritte sui log binari. La funzione di registrazione binaria consente la memorizzazione delle informazioni di servizio nei file di log binari per ciascun servizio definito nella configurazione. Le informazioni vengono scritte sui log solo quando l'intervallo di log specificato, espresso in secondi, è scaduto dall'ultima volta che un record è stato scritto sul log. L'intervallo predefinito di registrazione binaria è 60.

interval

Imposta il numero di secondi che intercorre tra le voci nel log binario.

retention

Imposta il numero delle ore durante il quale i file di log binari vengono conservati.

start

Avvia la registrazione binaria.

stop

Arresta la registrazione binaria.

remove

Rimuove un consultant dello switch.

report

Notifica le caratteristiche dei consultant dello switch.

set

Imposta le caratteristiche dei consultant dello switch.

loglevel

Imposta il livello al quale il consultant dello switch registra le attività. Il valore predefinito è 1.

level

Il numero del livello da 0 a 5. Il valore predefinito è 1. I valori possibili sono:

0 = Nessuno

1 = Minimo

2 = Base

3 = Moderato

4 = Avanzato

5 = Verbose

logsize

Imposta il numero massimo di byte registrati nel file di log. Il valore predefinito è 1048576. Se si imposta la dimensione massima del file di log, il file riparte dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive vengono scritte partendo dall'inizio del file, sovrascrivendo le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

size

Il numero massimo di byte registrato nel log del consultant. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima, prima di iniziare la sovrascrittura, in quanto le voci di log variano, in termini di dimensione.

sensitivity

Indica l'entità della variazione tra i vecchi e i nuovi pesi necessaria affinché un peso possa essere modificato. La differenza tra il vecchio e il nuovo peso deve essere superiore alla percentuale di sensibilità del peso da modificare. Il valore è compreso tra 0 e 100; il valore predefinito è 5.

weight percentage

Un numero intero compreso tra 0 e 100, che rappresenta il valore della sensibilità.

sleeptime

Imposta l'intervallo di inattività in secondi tra i cicli di impostazione dei pesi. Il valore predefinito è 7.

sec Un numero intero che rappresenta il tempo di attesa espresso in secondi. L'intervallo valido è compreso tra 0 e 2,147,460.

start

Avvia la raccolta delle metriche e l'impostazione dei pesi.

stop

Arresta la raccolta delle metriche e l'impostazione dei pesi.

Esempi

- Per aggiungere un consultant dello switch con un identificatore switch sc1, un indirizzo IP 9.37.50.17 e un nome comunità comm1:

```
cococontrol consultant add sc1 address 9.37.50.17 community comm2
```

- Per avviare la registrazione binaria:

```
cococontrol consultant  
binarylog sc1 start
```

- Per visualizzare un report sulle caratteristiche del consultant sullo switch sc1:

```
cococontrol consultant report sc1
```

Questo comando produce un output simile a:

```
Consultant sc1 connected to switch at  
9.37.50.1:cn1  
    Consultant has been started  
    Sleep time   = 7  
    Sensitivity  = 5  
    Log level    = 5  
    Log size     = 1,048,576  
    ownerContent(s):  
        ownerContent oc1
```

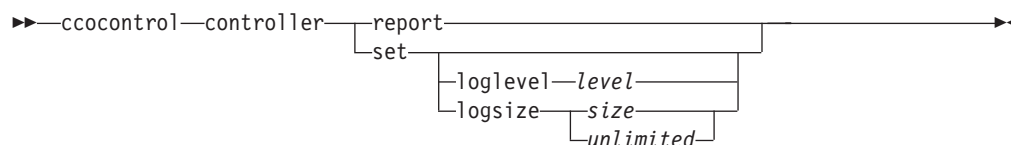
- Per impostare il tempo di inattività tra i cicli di impostazione dei pesi per l'ID dello switch sc1 su 10 secondi:

```
cococontrol  
consultant set sc1 sleeptime 10
```

- Per avviare la raccolta delle metriche e l'impostazione dei pesi per l'ID del consultant sc1:

```
cococontrol consultant start sc1
```

cococontrol controller — gestione del controller



report

Visualizza le caratteristiche del controller. Le informazioni sulla versione vengono visualizzate come parte di questo report.

set

Imposta le caratteristiche del controller.

loglevel

Imposta il livello al quale il controller registra le attività. Il valore predefinito è 1.

level

Il numero del livello da 0 a 5. Il valore predefinito è 1. I valori possibili sono:

- 0 = Nessuno
- 1 = Minimo
- 2 = Base
- 3 = Moderato
- 4 = Avanzato
- 5 = Verbose

logsize

Imposta il numero massimo di byte registrati nel file di log. Il valore predefinito è 1048576. Se si imposta la dimensione massima del file di log, il file riparte dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive vengono scritte partendo dall'inizio del file, sovrascrivendo le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

size | unlimited

Il numero massimo di byte registrato nel log del consultant. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima, prima di iniziare la sovrascrittura, in quanto le voci di log variano, in termini di dimensione.

Esempi

- Per visualizzare un report sul controller:

```
cococontrol controller report
```

Questo comando produce un output simile a:

Controller Report:

Version Version: 05.00.00.00 - 03/21/2002-09:49:57-EST

Logging level 1

Log size. 1048576

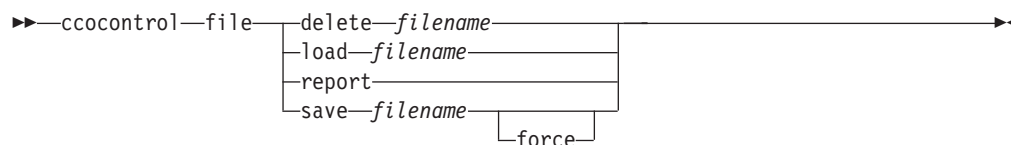
Configuration File. . . . config1.xml

Consultants:

Consultant consult1 -Started

- Per impostare il livello di registrazione su zero per ottenere migliori prestazioni:
ccocontrol set loglevel 0
- Per impostare la dimensione del log del controller su 1.000.000 byte:
ccocontrol controller set logsize 1000000

cococontrol file — gestisce i file di configurazione



delete

Cancella il file di configurazione specificato.

filename

Un file di configurazione. L'estensione del file deve essere .xml. Se questa estensione non è specificata, verrà assunta automaticamente.

load

Carica la configurazione memorizzata nel file specificato.

Nota: il caricamento di un file aggiunge la configurazione memorizzata in quel file alla configurazione in esecuzione. Per caricare una *nuova* configurazione, arrestare e riavviare il server prima di caricare il file.

report

Elenca i file di configurazione.

save

Salva la configurazione corrente nel file specificato.

Nota: i file vengono salvati in e caricati dalle seguenti directory:

- Sistemi AIX: **/opt/ibm/edge/lb/servers/configurations/cco**
- Sistemi Linux: **/opt/ibm/edge/lb/servers/configurations/cco**
- Sistemi Solaris: **/opt/ibm/edge/lb/servers/configurations/cco**
- Sistemi Windows:

directory di installazione (predefinita) **C:\Program Files\ibm\edge\lb\servers\configurations\cco**

force

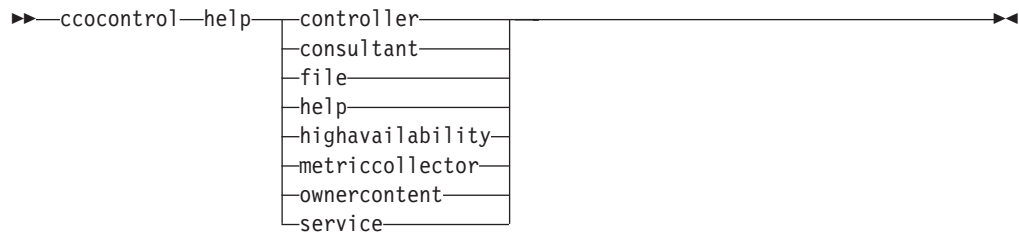
Esegue il salvataggio su un file esistente.

Esempi

- Per eliminare un file denominato file1:
`cococontrol file delete file1`
- Per aggiungere la configurazione nel file alla configurazione corrente:
`cococontrol file load config2`
- Per visualizzare un report di file precedentemente salvato:
`cococontrol file report`
Questo comando produce un output simile a:
FILE REPORT:

file1.xml
file2.xml
file3.xml
- Per salvare il file di configurazione in un file denominato config2.xml:
`cococontrol file save config2`

cococontrol help — Visualizza o stampa la guida per questo comando



Esempi

- Per richiamare la guida sul comando cococontrol, digitare:

```
cococontrol help
```

Questo comando produce un output simile a:

Sono disponibili i
seguenti comandi:

controller	- operate on the controller
consultant	- operate on switch consultants
file	- operate on configuration files
help	- operate on help
highavailability	- operate on high availability
metriccollector	- operate on metric collectors
ownerContent	- operate on ownerContents
service	- operate on services

- Nella sintassi della guida in linea vengono utilizzati i seguenti simboli:

< > Le parentesi graffe racchiudono i parametri o una sequenza di caratteri.

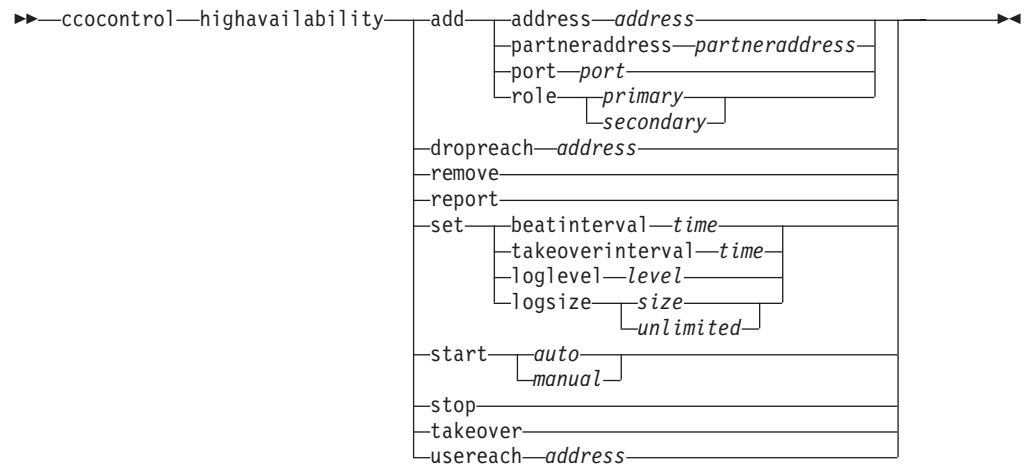
[] Le parentesi quadre racchiudono le voci facoltative.

| Una barra verticale separa le alternative all'interno delle parentesi graffe e quadre.

:

I due punti rappresentano un separatore tra i nomi; ad esempio
consultant1:ownercontent1.

cococontrol highavailability — controlla la disponibilità elevata



add

Configura nodo, partner e destinazioni accessibili di disponibilità elevata.

address

L'indirizzo da cui ricevere heartbeat.

address

L'indirizzo IP del nodo di disponibilità elevata.

partneraddress

L'indirizzo a cui inviare heartbeat. È l'indirizzo IP o il nome host configurato sul nodo partner. Questo indirizzo viene utilizzato per comunicare con la macchina di disponibilità elevata partner.

address

L'indirizzo IP del partner.

port

La porta utilizzata per comunicare con il partner. Il valore predefinito è 12345.

port

Il numero di porta.

role

Il ruolo di disponibilità elevata.

primary | secondary

Il ruolo primario o secondario.

dropreach

Rimuove questa destinazione accessibile dai criteri di disponibilità elevata.

address

L'indirizzo IP della destinazione accessibile.

remove

Rimuove il nodo, il partner e la destinazione accessibile dalla configurazione di disponibilità elevata. Prima di utilizzare questo comando, arrestare la disponibilità elevata.

report

Visualizza le informazioni di disponibilità elevata.

set

Imposta le caratteristiche di disponibilità elevata.

beatinterval

Imposta la frequenza, espressa in millisecondi, con cui gli heartbeat vengono inviati al partner. Il valore predefinito è 500.

time

Un numero intero positivo che rappresenta l'intervallo di beat, espresso in millisecondi.

takeoverinterval

Imposta la quantità di tempo, espressa in millisecondi, che deve trascorrere (durante cui non viene ricevuto nessun heartbeat) prima che si verifichi un takeover. Il valore predefinito è 2000.

time

Un numero intero positivo che rappresenta l'intervallo di takeover, espresso in millisecondi.

loglevel

Imposta il livello al quale vengono registrate le attività. Il valore predefinito è 1.

level

Il numero del livello da 0 a 5. Il valore predefinito è 1. I valori possibili sono:

- 0 = Nessuno
- 1 = Minimo
- 2 = Base
- 3 = Moderato
- 4 = Avanzato
- 5 = Verbose

logsize

Imposta il numero massimo di byte registrati nel file di log di disponibilità elevata. Il valore predefinito è 1048576. Se si imposta la dimensione massima del file di log, il file riparte dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive vengono scritte partendo dall'inizio del file, sovrascrivendo le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

size | unlimited

Il numero massimo di byte registrato nel log di disponibilità elevata. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima, prima di iniziare la sovrascrittura, in quanto le voci di log variano, in termini di dimensione.

start

Avvia l'uso della disponibilità elevata. Un nodo, un partner o una destinazione accessibile di disponibilità elevata devono essere configurati utilizzando questo comando.

auto | *manual*

Determina se avviare la disponibilità elevata con una strategia di ripristino automatica o manuale.

stop

Arresta l'uso della disponibilità elevata.

takeover

Mantiene il controllo dal nodo di disponibilità elevata attivo.

usereach

L'indirizzo di destinazione accessibile che verrà avviato utilizzando la disponibilità elevata. Aggiungere una destinazione accessibile che possa ricevere ping in modo che i partner di disponibilità elevata possano determinare l'accessibilità delle destinazioni.

address

L'indirizzo IP della destinazione accessibile.

Esempi

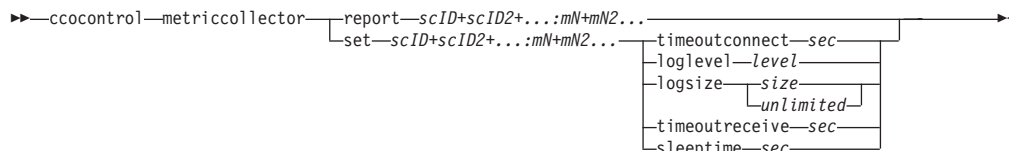
- Per aggiungere un nodo di disponibilità elevata con un indirizzo IP 9.37.50.17 con un ruolo primario sulla porta 12345 e un indirizzo partner 9.37.50.14:
ccocontrol highavailability add
address 9.37.50.17 role primary port 12345 partneraddress 9.37.50.14
- Per aggiungere un indirizzo della destinazione accessibile 9.37.50.9:
ccocontrol highavailability usereach 9.37.50.9
- Per rimuovere un indirizzo della destinazione accessibile 9.37.50.9:
ccocontrol highavailability dropreach 9.37.50.9
- Per avviare la disponibilità elevata con una strategia di ripristino manuale:
ccocontrol highavailability start manual
- Per richiamare un'istantanea della disponibilità elevata:
ccocontrol highavailability report

Questo comando produce un output simile a:

```
High Availability Status:
-----
Node . . . . . primary
Node Address . . . . . 9.37.50.17
Port . . . . . 12345
Partner Address. . . . . 9.37.50.14
Recovery Strategy. . . . . manual
Heartbeat Interval . . . . . 500
Takeover Interval. . . . . 2000
State. . . . . idle
Sub-state. . . . . unsynchronized

Reachability Status : Node/Partner
-----
No reach targets configured
```

cococontrol metriccollector — configura lo strumento di raccolta delle metriche



report

Visualizza le caratteristiche di uno strumento di raccolta delle metriche.

scID (ID consultant dello switch)

Una stringa definita dall'utente che fa riferimento al consultant.

mN (nome della metrica)

Nome che identifica la metrica fornita o personalizzata.

set

Imposta le caratteristiche di uno strumento di raccolta delle metriche.

timeoutconnect

Imposta il tempo che lo strumento di raccolta delle metriche deve attendere prima di segnalare una connessione non riuscita.

sec Un numero interno positivo che rappresenta il tempo, espresso in secondi, che lo strumento di raccolta delle metriche deve attendere prima di segnalare una connessione a un servizio non riuscita.

loglevel

Imposta il livello al quale il consultant specificato registra le attività. Il valore predefinito è 1.

level

Il numero del livello. Il valore predefinito è 1. Maggiore è il numero, maggiori saranno le informazioni scritte sul log del consultant. I valori possibili sono:

- 0 = Nessuno
- 1 = Minimo
- 2 = Base
- 3 = Moderato
- 4 = Avanzato
- 5 = Verbose

logsize

Imposta il numero massimo di byte registrati nel file di log. Il valore predefinito è 1048576. Se si imposta la dimensione massima del file di log, il file riparte dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive vengono scritte partendo dall'inizio del file, sovrascrivendo le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

size | unlimited

Il numero massimo di byte registrato nel log del consultant. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file

di log potrebbe non raggiungere esattamente la dimensione massima, prima di iniziare la sovrascrittura, in quanto le voci di log variano, in termini di dimensione.

timeoutreceive

Imposta il tempo che il consultant attende prima di segnalare una ricezione dal servizio non riuscita.

sec Un numero intero positivo che rappresenta il tempo, espresso in secondi, che il consultant attende prima di segnalare una ricezione da un servizio non riuscita.

sleeptime

Imposta il tempo, espresso in secondi, durante il quale lo strumento di raccolta delle metriche rimane inattivo tra i cicli di raccolta delle metriche.

Un numero intero positivo che rappresenta il numero di secondi del tempo di inattività.

Esempi

- Per visualizzare un report sulle caratteristiche dello strumento di raccolta delle metriche:

```
cococontrol metriccollector report sc1:http
```

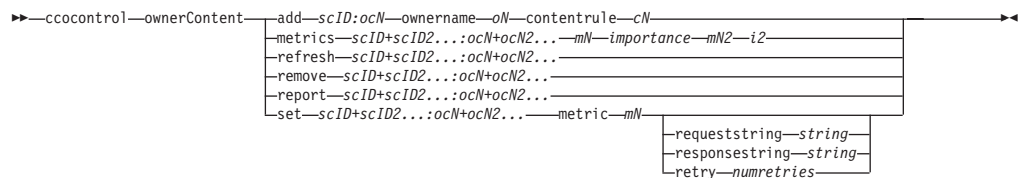
Questo comando produce un output simile a:

```
MetricCollector sc1:http
  collected metric(s).... http
  loglevel..... 5
  logSize..... 1048576
  sleepTimeSeconds..... 7
  timeoutConnectSeconds.. 21
  timeoutReceiveSeconds.. 21
```

- Per impostare un valore di timeoutconnect di 15 secondi e un valore logsize illimitato per il consultant dello switch sc1 e per la metrica http:

```
cococontrol metriccollector set sc1:http timeoutconnect 15 logsize unlimited
```

cococontrol ownercontent — controlla il nome proprietario e la regola di contenuto



add

Aggiunge un ownercontent al consultant specificato.

scID (ID consultant dello switch)

Una stringa definita dall'utente che rappresenta il consultant.

OCName (nome ownercontent)

Una stringa definita dall'utente che rappresenta il nome proprietario e la regola di contenuto sullo switch.

ownername

Il nome configurato sullo switch che identifica la configurazione del proprietario.

oN (ownername)

Una stringa di testo univoca senza spazi. L'ownername deve corrispondere a quello specificato sullo switch Cisco.

contentrule

Il nome configurato sullo switch che identifica la configurazione della regola di contenuto del proprietario.

cN (contentname)

Una stringa di testo univoca senza spazi. Il contentname deve corrispondere a quello specificato sullo switch Cisco.

metrics

Specifica la serie di metriche utilizzate nel calcolo dei pesi e l'importanza di ciascuna metrica. L'importanza è espressa come percentuale del totale. La somma dei valori di importanza deve essere sempre pari a 100. Le metriche possono essere una combinazione di metriche dei dati di connessione, degli advisor delle applicazioni e dei server delle metriche. I valori predefiniti sono le metriche delle connessioni attive (activeconn) e della frequenza di connessione (connrate) con importanza 50/50.

mN (metricname)

Nome che indica lo strumento di raccolta delle metriche che raccoglierà le metriche per determinare il peso del server.

Segue un elenco di nomi di metriche validi e delle porte associate.

Nome advisor	Protocollo	Porta
connect	ICMP	12345
db2	private	50000
dns	DNS	53
ftp	FTP	21
http	HTTP	80

Nome advisor	Protocollo	Porta
https	SSL	443
cachingproxy	HTTP (via Caching Proxy)	80
imap	IMAP	143
ldap	LDAP	389
nntp	NNTP	119
ping	PING	0
pop3	POP3	110
sip	SIP	5060
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23
WLM	private	10,007
activeconn	n/d	n/d
connrate	n/d	n/d
cpuload	n/d	n/d
memload	n/d	n/d

importance

Un numero da 0 a 100 che rappresenta l'importanza di questa metrica nel calcolo dei pesi sul server.

refresh

Aggiorna i servizi configurati con la configurazione di Switch Cisco CSS.

remove

Rimuove un ownercontent

report

Notifica le caratteristiche di ownercontent.

set

Imposta le caratteristiche di ownercontent.

metric

Imposta le caratteristiche di una metrica.

mN

Il nome della metrica desiderata.

requeststring

Imposta una stringa di richiesta per la metrica specificata. Rappresenta la richiesta inviata da uno strumento di raccolta delle metriche per raccogliere le informazioni sulle metriche.

string

La stringa della richiesta inviata dallo strumento di raccolta delle metriche al server.

responsestring

Imposta una stringa di risposta per la metrica specificata. La stringa di risposta specificata viene utilizzata dallo strumento di raccolta delle metriche per confrontare le risposte ricevute dai server e, successivamente, determinare la disponibilità dei server.

string

La stringa di risposta con cui lo strumento di raccolta delle metriche confronta le risposte dei server ricevute.

retry

Imposta il numero dei nuovi tentativi che possono essere eseguiti prima di contrassegnare un server come inattivo.

numretries

Un numero intero maggiore o uguale a zero. È preferibile che questo valore non sia maggiore di 3. Se la parola chiave *the* non è configurata, per il numero di tentativi viene assunto il valore zero.

Esempi

- Per aggiungere un *ownerContent* denominato *oc1* (con un nome proprietario *owner1* e un nome contenuto *content1*) all'ID consultant dello switch *sc1*:
`ccocontrol ownerContent add sc1:oc1 ownername owner1 contentrule content1`
- Per specificare una proporzione di 50 per la metrica *activeconn* e per la metrica *http*:

```
ccocontrol ownerContent metrics sc1:oc1 activeconn 50 http 50
```

- Per visualizzare un report caratteristiche di *ownercontent*:

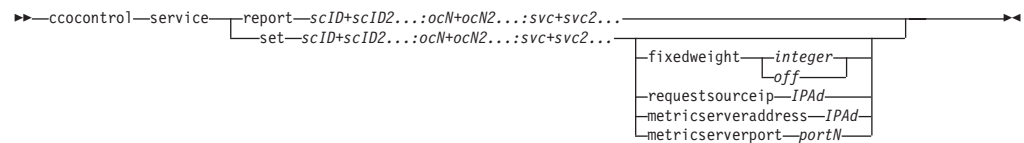
```
ccocontrol ownerContent report sc1:oc1
```

Questo comando produce un output simile a:

```
ownerContent sc1:oc1
  Weightbound = 10
  Metric activeconn has proportion 25
    ResponseString... n/a
    RequestString.... n/a
  Metric http has proportion 50
    ResponseString... n/a
    RequestString.... n/a
  Metric connrate has proportion 25
    ResponseString... n/a
    RequestString.... n/a
  Contains Service t3
  Contains Service t2
  Contains Service t1
```

- Per impostare una stringa di richiesta *http*:
`ccocontrol ownerContent set sc1:oc1 metric http requeststring getCookie`

cococontrol service — configura un servizio



report

Visualizza le caratteristiche dei servizi.

scID (ID consultant dello switch)

Una stringa definita dall'utente che rappresenta il consultant.

OCName (nome ownercontent)

Una stringa definita dall'utente che rappresenta il nome proprietario e la regola di contenuto sullo switch.

svc (servizio)

Una stringa definita dall'utente sullo switch che rappresenta il servizio.

set

Imposta le caratteristiche dei servizi.

fixedweight

Imposta un peso fisso per questo servizio. Il valore predefinito è off.

integer | off

Un numero intero positivo compreso tra 0 e 100, che rappresenta un peso fisso per questo servizio o la parola **off** per non specificare alcun peso fisso.

requestsourceip

Impostare l'indirizzo da cui si desidera contattare il servizio per le richieste di applicazione.

IPAd (indirizzo IP)

L'indirizzo IP da cui contattare il servizio, espresso come nome simbolico o in formato indirizzo IP.

metricserveraddress

Imposta l'indirizzo sul quale contattare il servizio per le richieste di Metric Server.

IPAd (indirizzo IP)

L'indirizzo IP di Metric Server, espresso come nome simbolico o in formato indirizzo IP.

metricserverport

Imposta la porta da utilizzare per contattare Metric Server.

portN (numero porta)

Il numero della porta utilizzato per contattare Metric Server.

Esempi

- Per visualizzare un report sul servizio t1 per il consultant sc1:

```
cococontrol service report sc1:oc1:t1
```

Questo comando produce un output simile a:

```
Service scl:ocl:ta has weight 10
Fixed weight is off
Request Source Ip..... 9.27.24.156
Application port..... 80
MetricServer address.. 1.0.0.1
MetricServer port..... 10004
Metric activeconn has value -99
Metric http has value -99
Metric connrate has value -99
```

- Per impostare un indirizzo Metric Server per il servizio t2:
ccocontrol service set scl:ocl:t2 metricserveraddress 9.37.50.17

Capitolo 30. Riferimenti sui comandi per Controller Nortel Alteon

Questo capitolo descrive come utilizzare i comandi **nalcontrol** riportati di seguito per Controller Nortel Alteon:

- “**nalcontrol consultant** — configura e controlla un consultant” a pagina 438
- “**nalcontrol controller** — gestisce il controller” a pagina 441
- “**nalcontrol file** — gestisce i file di configurazione” a pagina 443
- “**nalcontrol help** — visualizza o stampa la guida del comando” a pagina 444
- “**nalcontrol highavailability** — controlla la disponibilità elevata” a pagina 445
- “**nalcontrol metriccollector** — configura lo strumento di raccolta delle metriche” a pagina 448
- “**nalcontrol service** — configura un servizio” a pagina 452
- “**nalcontrol server** — configura un server” a pagina 450

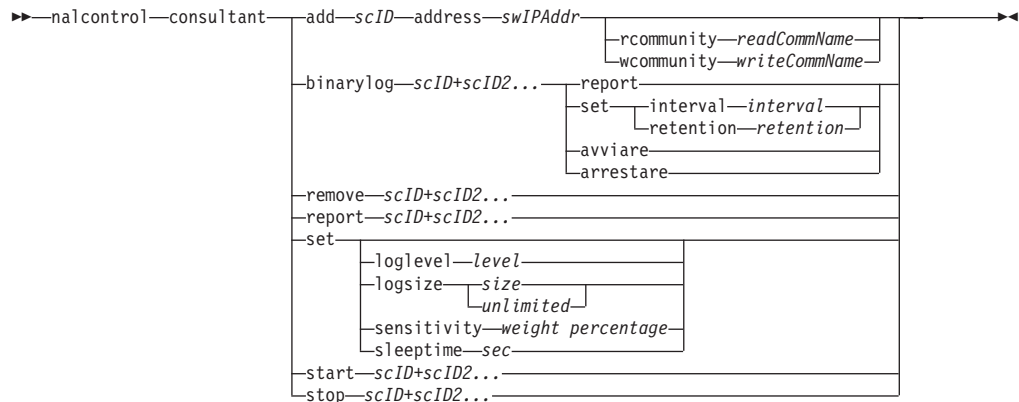
È possibile utilizzare una versione abbreviata dei parametri del comando **nalcontrol**, immettendo le lettere che designano in modo univoco i parametri. Ad esempio, per visualizzare la guida del comando di salvataggio file, è possibile immettere **nalcontrol he f** anziché **nalcontrol help file**.

Per richiamare il prompt dei comandi **nalcontrol**: immettere **nalcontrol**.

Per chiudere l'interfaccia della riga comandi: immettere **exit** o **quit**.

Nota: utilizzare i caratteri inglesi per tutti i valori dei parametri dei comandi. Le uniche eccezioni sono i nomi host (utilizzati in comandi **server**) e i nomi file (utilizzati in comandi **file**).

nalcontrol consultant — configura e controlla un consultant



add

Aggiungere un consultant dello switch.

scID

Una stringa definita dall'utente che si riferisce al consultant.

address

L'indirizzo IP di Switch Nortel Alteon Web a cui il consultant fornisce i pesi.

swIPAddr

L'indirizzo IP dello switch.

rcommunity

Il nome della comunità di lettura utilizzato nelle comunicazioni SNMP get con Switch Nortel Alteon Web. Il valore predefinito è public.

readCommName

La stringa che rappresenta il nome della comunità di lettura configurato su Switch Nortel Alteon Web. Il valore predefinito è public.

wcommunity

Il nome della comunità di scrittura utilizzato nelle comunicazioni SNMP set

writeCommName

La stringa che rappresenta il nome della comunità di scrittura configurato su Switch Nortel Alteon Web. Il valore predefinito è private.

binarylog

Controlla la registrazione binaria di un consultant.

report

Crea un report sulle caratteristiche della registrazione binaria.

set

Imposta la frequenza, in secondi, con cui le informazioni vengono scritte sui log binari. La funzione di registrazione binaria consente di memorizzare le informazioni sul servizio in file di log binari per ciascun servizio definito nella configurazione. Le informazioni vengono scritte nei log solo dopo che sono trascorsi i secondi specificati come intervallo di scrittura nei log, calcolati dall'ultima operazione di scrittura di un record nel log. L'intervallo di registrazione binaria predefinito è 60.

interval

Imposta il numero di secondi tra le voci nel log binario.

retention

Imposta il numero di ore in cui vengono conservati i file di log binari.

start

Avvia la registrazione binaria.

stop

Arresta la registrazione binaria.

remove

Rimuove un consultant dello switch.

report

Crea un report sulle caratteristiche del consultant dello switch.

set

Imposta le caratteristiche del consultant dello switch.

loglevel

Imposta il livello su cui il consultant dello switch registra le attività. Il valore predefinito è 1.

level

Il numero del livello da 0 a 5. Il valore predefinito è 1. I valori possibili sono:

0 = Nessuno

1 = Minimo

2 = Base

3 = Moderato

4 = Avanzato

5 = Verbose

logsize

Imposta il numero massimo di byte registrati nel file di log. Il valore predefinito è 1048576. Se si imposta la dimensione massima del file di log, il file ripartirà dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive verranno scritte partendo dall'inizio del file, sovrascrivendo quindi le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

size

Il numero massimo di byte registrati nel log del consultant. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima prima di iniziare la sovrascrittura, in quanto le voci di log variano in termini di dimensioni.

sensitivity

Indica il numero di modifiche che deve aver luogo tra i pesi vecchi e nuovi, per poter variare il peso. Affinché il peso possa variare, la differenza tra il peso vecchio e nuovo deve essere superiore alla percentuale della sensibilità. L'intervallo valido è compreso tra 0 e 100; il valore predefinito è 5.

weight percentage

Un numero intero tra 0 e 100, che rappresenta il valore della sensibilità.

sleeptime

Imposta il numero di secondi di inattività tra i cicli di impostazione dei pesi. Il valore predefinito è 7.

seconds

Un numero intero che rappresenta il tempo di inattività in secondi. I valori validi sono compresi tra 0 e 2.147.460.

start

Avvia la raccolta delle metriche e l'impostazione dei pesi.

stop

Arresta la raccolta delle metriche e l'impostazione dei pesi.

Esempi

- Per aggiungere a un consultant dello switch un identificativo dello switch sc1 e un indirizzo IP 9.37.50.17:

```
nalcontrol consultant add sc1 address 9.37.50.17
```

- Per avviare la registrazione binaria:

```
nalcontrol consultant binarylog sc1 start
```

- Per visualizzare un report sulle caratteristiche del consultant dello switch sc1:

```
nalcontrol consultant report sc1
```

Questo comando produce un output simile a:

```
Consultant ID: sc1 Switch IP addr: 9.37.50.1
```

```
Read Community: public
```

```
Write Community: private
```

```
Consultant has been started
```

```
Sleep time = 7
```

```
Sensitivity = 5
```

```
Log level = 5
```

```
log size = 1,048,576
```

```
Service(s):
```

```
Service svc1
```

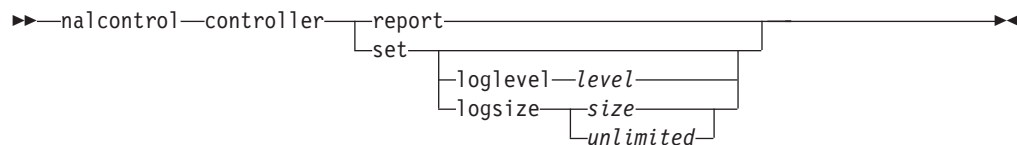
- Per impostare il tempo di inattività tra i cicli di impostazione dei pesi per l'ID switch sc1 su 10 secondi:

```
nalcontrol consultant set sc1 sleeptime 10
```

- Per avviare la raccolta delle metriche e l'impostazione dei pesi per l'ID consultant sc1:

```
nalcontrol consultant start sc1
```

nalcontrol controller — gestisce il controller



report

Visualizza le caratteristiche del controller. Come parte del report, vengono visualizzate le informazioni sulla versione.

set

Imposta le caratteristiche del controller.

loglevel

Imposta il livello su cui il controller registra le attività. Il valore predefinito è 1.

level

Il numero del livello da 0 a 5. Il valore predefinito è 1. I valori possibili sono:

- 0 = Nessuno
- 1 = Minimo
- 2 = Base
- 3 = Moderato
- 4 = Avanzato
- 5 = Verbose

logsize

Imposta il numero massimo di byte registrati nel file di log. Il valore predefinito è 1048576. Se si imposta la dimensione massima del file di log, il file ripartirà dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive verranno scritte partendo dall'inizio del file, sovrascrivendo quindi le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

size | unlimited

Il numero massimo di byte registrati nel log del consultant. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima prima di iniziare la sovrascrittura, in quanto le voci di log variano in termini di dimensioni.

Esempi

- Per visualizzare un report sul controller:

```
nalcontrol controller report
```

Questo comando produce un output simile a:

Controller Report:

```
-----
Version . . . . . Version: 05.00.00.00 - 03/21/2002-09:49:57-EST
Logging level . . . . . 1
Log size. . . . . 1048576
```

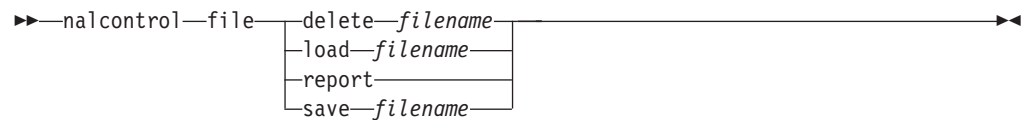
Configuration File. . . . config1.xml

Consultants:

Consultant consult1 -Started

- Per impostare il livello di registrazione su zero per ottenere migliori prestazioni:
nalcontrol set loglevel 0
- Per impostare la dimensione del log del controller su 1.000.000 byte:
nalcontrol controller set logsize 1000000

nalcontrol file — gestisce i file di configurazione



delete

Elimina il file di configurazione specificato.

filename

Un file di configurazione. L'estensione del file deve essere .xml. Se non specificata, l'estensione verrà presupposta.

load

Carica la configurazione memorizzata nel file specificato.

Nota: quando si carica un file, la configurazione in esso memorizzata viene aggiunta alla configurazione in atto. Se si desidera caricare una *nuova* configurazione, è necessario arrestare e riavviare il server prima di caricare il file.

report

Elenca i file di configurazione.

save

Salva la configurazione corrente nel file specificato.

Nota: i file vengono salvati nelle seguenti directory, da cui vengono caricati:

- Sistemi AIX: **/opt/ibm/edge/lb/servers/configurations/nal**
- Sistemi Linux: **/opt/ibm/edge/lb/servers/configurations/nal**
- Sistemi Solaris: **/opt/ibm/edge/lb/servers/configurations/nal**
- Sistemi Windows:

Percorso directory di installazione comune — **C:\Program Files\ibm\edge\lb\servers\configurations\nal**

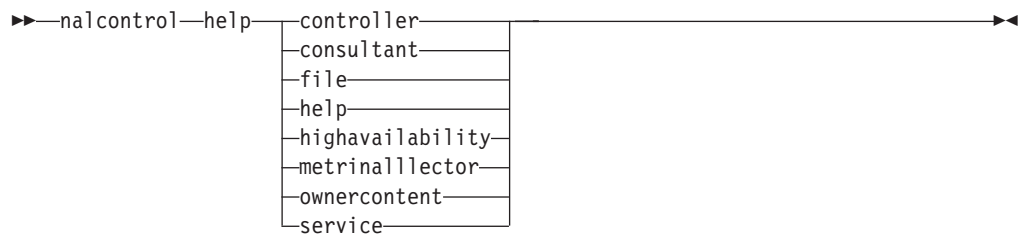
Percorso directory di installazione native — **C:\Program Files\ibm\lb\servers\configurations\nal**

Esempi

- Per eliminare un file denominato file1:
`nalcontrol file delete file1`
- Per caricare un nuovo file di configurazione per sostituire la configurazione corrente:
`nalcontrol file load config2`
- Per visualizzare un report dei file precedentemente salvati:
`nalcontrol file report`
Questo comando produce un output simile a:
FILE REPORT:

file1.xml
file2.xml
file3.xml
- Per salvare il file di configurazione in un file denominato config2:
`nalcontrol file save config2`

nalcontrol help — visualizza o stampa la guida del comando



Esempi

- Per richiamare la guida sul comando nalcontrol, immettere:

```
nalcontrol help
```

Questo comando produce un output simile a:

The following commands are available:

controller	- operate on the controller
consultant	- operate on switch consultants
file	- operate on configuration files
help	- operate on help
highavailability	- operate on high availability
metriccollector	- operate on metric collectors
server	- operate on servers
service	- operate on services

- I simboli riportati di seguito vengono utilizzati nella sintassi della guida in linea:

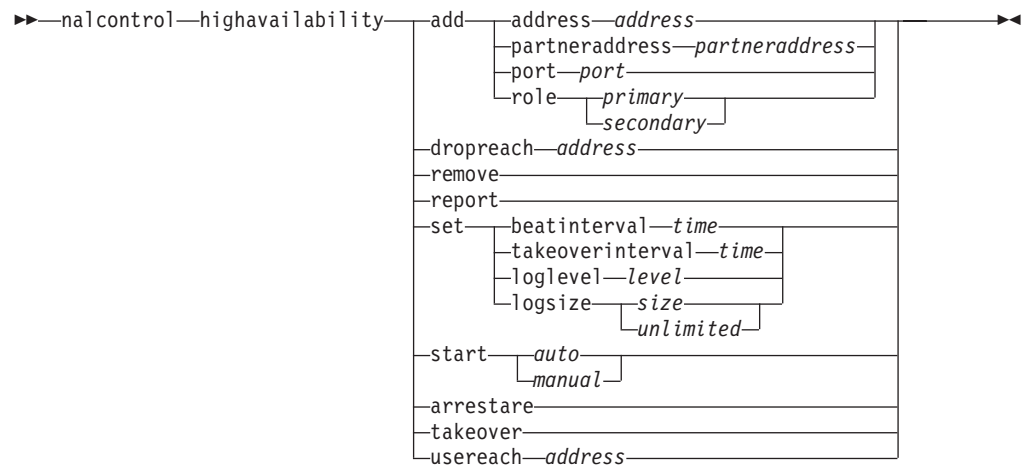
< > Le parentesi graffe racchiudono i parametri o una sequenza di parametri.

[] Le parentesi quadre racchiudono le voci facoltative.

| Una barra verticale separa le alternative racchiuse tra le parentesi.

: Un carattere due punti rappresenta un separatore tra i nomi; ad esempio, **consultant1:service1**.

nalcontrol highavailability — controlla la disponibilità elevata



add

Configura un nodo con disponibilità elevata, un partner e destinazioni accessibili.

address

L'indirizzo da cui ricevere gli heartbeat.

address

L'indirizzo IP del nodo con disponibilità elevata.

partneraddress

L'indirizzo a cui inviare gli heartbeat. Si tratta dell'indirizzo IP o del nome host configurato sul nodo partner. Questo indirizzo viene utilizzato per comunicare con la macchina partner con disponibilità elevata.

address

L'indirizzo IP del partner.

port

La porta utilizzata per comunicare con il partner. Il valore predefinito è 12345.

port

Il numero di porta.

role

Il ruolo di disponibilità elevata.

primary | secondary

Il ruolo principale o secondario.

dropreach

Rimuove questa destinazione accessibile dal criterio di disponibilità elevata.

address

L'indirizzo IP della destinazione accessibile.

remove

Rimuove il nodo, il partner e la destinazione accessibile dalla configurazione di disponibilità elevata. Prima di utilizzare questo comando, arrestare la funzione di disponibilità elevata.

report

Visualizza le informazioni relative alla disponibilità elevata.

set

Imposta le caratteristiche di disponibilità elevata.

beatinterval

Imposta la frequenza, in millisecondi, con cui gli heartbeat vengono inviati al partner. Il valore predefinito è 500.

time

Un numero intero positivo che rappresenta l'intervallo beat, in millisecondi.

takeoverinterval

Imposta l'intervallo di tempo, in millisecondi, che deve trascorrere (durante il quale non vengono ricevuti heartbeat) prima che si verifichi un takeover. Il valore predefinito è 2000.

time

Un numero intero positivo che rappresenta l'intervallo takeover, in millisecondi.

loglevel

Imposta il livello sui cui vengono registrate le attività. Il valore predefinito è 1.

level

Il numero del livello da 0 a 5. Il valore predefinito è 1. I valori possibili sono:

- 0 = Nessuno
- 1 = Minimo
- 2 = Base
- 3 = Moderato
- 4 = Avanzato
- 5 = Verbose

logsize

Imposta il numero massimo di byte registrati nel file di log di disponibilità elevata. Il valore predefinito è 1048576. Se si imposta la dimensione massima del file di log, il file ripartirà dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive verranno scritte partendo dall'inizio del file, sovrascrivendo quindi le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

size | unlimited

Il numero massimo dei byte registrati nel log di disponibilità elevata. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima prima di iniziare la sovrascrittura, in quanto le voci di log variano in termini di dimensioni.

start

Avvia l'uso della funzione di disponibilità elevata. Prima di utilizzare questo comando, è necessario configurare un nodo, un partner e una destinazione accessibile.

auto | manual

Determina se avviare la funzione di disponibilità elevata con una strategia di ripristino automatica o manuale.

stop

Arresta l'uso della funzione di disponibilità elevata.

takeover

Assume il controllo del nodo con disponibilità elevata attivo.

usereach

L'indirizzo della destinazione accessibile che avvierà l'uso della funzione di disponibilità elevata. Aggiungere una destinazione accessibile su cui può essere eseguito il ping, in modo che i partner con disponibilità elevata possano determinare se le destinazioni sono raggiungibili.

address

L'indirizzo IP della destinazione accessibile.

Esempi

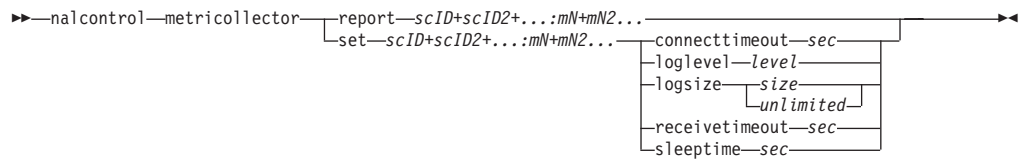
- Per aggiungere a un nodo con disponibilità elevata un indirizzo IP 9.37.50.17 con un ruolo principale sulla porta 12345 e un indirizzo partner 9.37.50.14:
`nalcontrol highavailability add
address 9.37.50.17 role primary port 12345 partneraddress 9.37.50.14`
- Per aggiungere un indirizzo della destinazione accessibile 9.37.50.9:
`nalcontrol highavailability usereach 9.37.50.9`
- Per rimuovere un indirizzo della destinazione accessibile 9.37.50.9:
`nalcontrol highavailability dropreach 9.37.50.9`
- Per avviare la funzione di disponibilità elevata con una strategia di ripristino manuale:
`nalcontrol highavailability start manual`
- Per richiamare un'istantanea delle statistiche di disponibilità elevata:
`nalcontrol highavailability report`

Questo comando produce un output simile a:

```
High Availability Status:
-----
Node . . . . . primary
Node Address . . . . . 9.37.50.17
Port . . . . . 12345
Partner Address. . . . . 9.37.50.14
Recovery Strategy. . . . manual
Heartbeat Interval . . . . 500
Takeover Interval. . . . 2000
Started. . . . . N
State. . . . . idle
Sub-state. . . . . unsynchronized

Reachability Status : Node/Partner
-----
```

nalcontrol metriccollector — configura lo strumento di raccolta delle metriche



report

Visualizza le caratteristiche di uno strumento di raccolta delle metriche.

scID (ID consultant dello switch)

Una stringa definita dall'utente che si riferisce al consultant.

mN (nome metrica)

Il nome che identifica la metrica personalizzata o fornita.

set

Imposta le caratteristiche dello strumento di raccolta delle metriche.

connecttimeout

Imposta il tempo che uno strumento di raccolta delle metriche attende prima di riportare l'interruzione di una connessione.

sec Un numero intero positivo che rappresenta l'intervallo di tempo, in secondi, che uno strumento di raccolta delle metriche attende prima di riportare l'interruzione di una connessione a un servizio.

loglevel

Imposta il livello su cui il consultant specificato registra le attività. Il valore predefinito è 1.

level

Il numero del livello. Il valore predefinito è 1. Maggiore è il numero, maggiori saranno le informazioni scritte sul log del consultant. I valori possibili sono:

- 0 = Nessuno
- 1 = Minimo
- 2 = Base
- 3 = Moderato
- 4 = Avanzato
- 5 = Verbose

logsize

Imposta il numero massimo dei byte registrati nel file di log. Il valore predefinito è 1048576. Se si imposta la dimensione massima del file di log, il file ripartirà dall'inizio; quando il file raggiunge la dimensione specificata, le voci successive verranno scritte partendo dall'inizio del file, sovrascrivendo quindi le precedenti voci di log. La dimensione del log non può essere inferiore alla dimensione corrente del log. Le voci di log sono dotate di un indicatore di data e ora in modo da poter comunicare l'ordine in cui sono state scritte. Tanto maggiore sarà il valore impostato per il livello di log, tanto più attentamente dovrà essere selezionata la dimensione del log, in quanto lo spazio può esaurirsi velocemente quando si esegue la registrazione ai livelli più alti.

size | unlimited

Il numero massimo dei byte registrati nel log del consultant. È possibile specificare un numero positivo maggiore di zero o la parola **unlimited**. Il file di log potrebbe non raggiungere esattamente la dimensione massima prima di iniziare la sovrascrittura, in quanto le voci di log variano in termini di dimensioni.

receivetimeout

Imposta il tempo che il consultant attende prima di riportare la mancata ricezione da un servizio.

sec Un numero intero positivo che rappresenta l'intervallo di tempo, in secondi, che il consultant attende prima di riportare la mancata ricezione da un servizio.

sleeptime

Imposta l'intervallo di tempo, in secondi, in cui uno strumento di raccolta rimane inattivo tra i cicli di raccolta delle metriche.

sec Un numero intero positivo che rappresenta il numero di secondi del tempo di inattività.

Esempi

- Per visualizzare un report sulle caratteristiche di uno strumento di raccolta delle metriche:

```
nalcontrol metrinallector report sc1:http
```

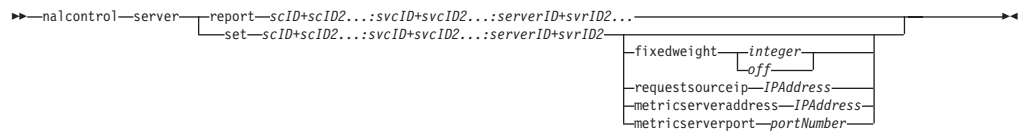
Questo comando produce un output simile a:

```
Metrinallector sc1:http
  collected metric(s).... http
  loglevel..... 5
  logSize..... 1048576
  sleepTimeSeconds..... 7
  timeoutConnectSeconds.. 21
  timeoutReceiveSeconds.. 21
```

- Per impostare un valore connecttimeout di 15 secondi e un valore logsize di unlimited per il consultant dello switch sc1 e la metrica http:

```
nalcontrol metrinallector set sc1:http connecttimeout 15 logsize unlimited
```

nalcontrol server — configura un server



report

Visualizza le caratteristiche dei server.

scID

Una stringa definita dall'utente che rappresenta il consultant.

svcID

Una stringa definita dall'utente che rappresenta l'identificativo di servizio virtuale e il numero di porta virtuale sullo switch.

serverID

Un numero intero che rappresenta il server sullo switch.

set

Imposta le caratteristiche dei server

fixedweight

Imposta un peso fisso per il server. Il valore predefinito è off. Il valore massimo di fixedweight è 48.

integer | off

Un numero intero positivo che rappresenta il peso fisso del server o la parola **off** per specificare l'assenza di un peso fisso.

requestsourceip

Imposta l'indirizzo da cui contattare il server per richieste di applicazioni.

IPAddress

L'indirizzo IP da cui contattare il server, espresso come nome simbolico o sotto forma di indirizzo IP.

metricserveraddress

Imposta l'indirizzo da cui contattare il server per richieste Metric Server.

IPAddress

L'indirizzo IP di Metric Server, espresso come nome simbolico o in formato indirizzo IP.

metricserverport

Imposta la porta da utilizzare per contattare Metric Server.

portNumber

Il numero di porta utilizzato per contattare Metric Server.

Esempi

- Per visualizzare un report su server 1 per il consultant sc1:

```
nalcontrol server report sc1:svc1:1
```

Questo comando produce un output simile a:

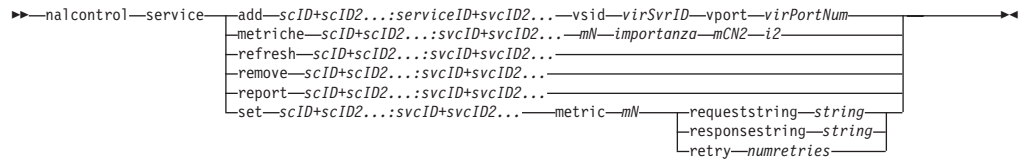
```
Server sc1:svc1:1 has weight -99
Fixed weight is off
Request Source Ip..... 9.27.24.156
Application port..... 99
MetricServer address... 9.99.99.98
```



```
MetricServer port..... 10004
Metric activeconn has value -99
Metric connrate has value -99
```

- Per impostare un indirizzo Metric Server per il servizio 2:
nalcontrol server set scl:svc1:2 metricserveraddress 9.37.50.17

nalcontrol service — configura un servizio



add

Aggiunge un servizio al consultant specificato.

scID (switchConsultantID)

Una stringa definita dall'utente che si riferisce al consultant.

svcID (serviceID)

Una stringa definita dall'utente che identifica il servizio.

vsid

La parola chiave dell'identificativo di servizio virtuale.

virSvrID (virtualServerID)

Il numero sullo switch che rappresenta il server virtuale.

vport

La parola chiave della porta virtuale.

virPortNum (virtualPortNumber)

Il numero di porta per il servizio attualmente configurato sullo switch.

metrics

Specifica l'insieme di metriche utilizzate nel calcolo dei pesi e l'importanza di ciascuna metrica. L'importanza è espressa come percentuale del totale. La somma dei valori di importanza deve essere pari a 100. Le metriche possono essere costituite da qualsiasi combinazione di metriche dei dati di connessione, degli advisor delle applicazioni e dei server delle metriche. I valori predefiniti sono metriche activeconn (connessioni attive) e connrate (frequenza di connessione) con importanza pari a 50/50.

mN (nome metrica)

Il nome che identifica lo strumento di raccolta delle metriche che raccoglierà le misurazioni per determinare il peso del server.

Segue un elenco di nomi metrica validi e delle porte associate.

Nome advisor	Protocollo	Porta
connect	ICMP	12345
db2	private	50000
dns	DNS	53
ftp	FTP	21
http	HTTP	80
https	SSL	443
cachingproxy	HTTP (via Caching Proxy)	80
imap	IMAP	143
ldap	LDAP	389
nntp	NNTP	119

Nome advisor	Protocollo	Porta
ping	PING	0
pop3	POP3	110
sip	SIP	5060
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23
WLM	private	10.007
activeconn	n/d	n/d
connrate	n/d	n/d
cpuload	n/d	n/d
memload	n/d	n/d

importance

Un numero compreso tra 0 e 100 che rappresenta l'importanza di questa metrica nel calcolo dei pesi del server.

refresh

Aggiorna un servizio con le informazioni da Switch Nortel Alteon Web.

remove

Rimuove un servizio.

report

Crea un report delle caratteristiche di un servizio.

set

Imposta le caratteristiche di un servizio.

metric

Imposta le caratteristiche di una metrica configurata.

mN (nome metrica)

Il nome della metrica desiderata.

requeststring

Imposta una stringa di richiesta per la metrica specificata. Ciò rappresenta la richiesta inviata da uno strumento di raccolta delle metriche per raccogliere le informazioni sulle metriche.

string

La stringa di richiesta inviata da uno strumento di raccolta delle metriche al server.

responsestring

Imposta una stringa di risposta per la metrica specificata. La stringa di risposta specificata viene utilizzata dallo strumento di raccolta delle metriche per confrontare le risposte ricevute dai server e, in seguito, determinare la disponibilità dei server.

string

La stringa di risposta con cui lo strumento di raccolta delle metriche confronta le risposte server ricevute.

retry

Il parametro retry imposta il numero dei tentativi che è possibile eseguire prima di contrassegnare un server come inattivo.

numretries

Un numero intero maggiore o uguale a zero. È preferibile che questo valore non sia maggiore di 3. Se la parola chiave *retries* non è configurata, per il numero di tentativi viene assunto il valore zero.

Esempi

- Per aggiungere un servizio denominato *svc1* (con un ID server virtuale 1 e una porta virtuale 80) all'ID consultant dello switch *sc1*:

```
nalcontrol service add sc1:svc1 vsid 1 vport 80
```

- Per specificare una proporzione di 50 ciascuno alle metriche *activeconn* e *http*:

```
nalcontrol service metrics sc1:svc1 activeconn 50 http 50
```

- Per visualizzare un report delle caratteristiche di *ownercontent*:

```
nalcontrol service report sc1:svc1
```

Questo comando produce un output simile a:

```
Service sc1:svc1
  Weightbound = 48
  Metric activeconn has proportion 50
  Metric connrate has rproportion 50
  Contains Server 4
  Contains Server 3
  Contains Server 2
  Contains Server 1
```

- Per impostare una stringa di richiesta *http*:

```
nalcontrol service set sc1:svc1 metric http requeststring getLastErrorCode
```

Appendice A. GUI: istruzioni generali

L'interfaccia utente grafica (GUI) di Load Balancer visualizza sul lato sinistro del pannello la struttura ad albero con Load Balancer nel livello superiore e Dispatcher, Content Based Routing (CBR), Site Selector, Controller Cisco CSS e Controller Nortel Alteon elencati come componenti.

Se si utilizza l'installazione di Load Balancer per IPv4 e IPv6, solo il componente Dispatcher è disponibile. Per ulteriori informazioni, vedere Capitolo 8, "Distribuzione di Dispatcher su Load Balancer per IPv4 e IPv6", a pagina 79.

Per esempi grafici della GUI di Load Balancer che evidenziano ciascuno dei diversi componenti, fare riferimento a quanto indicato di seguito:

- Vedere Figura 41 a pagina 456 per Dispatcher
- Vedere Figura 42 a pagina 457 per CBR
- Vedere Figura 43 a pagina 458 per Site Selector
- Vedere Figura 44 a pagina 459 per Cisco CSS Controller
- Vedere Figura 45 a pagina 460 per Nortel Alteon Controller

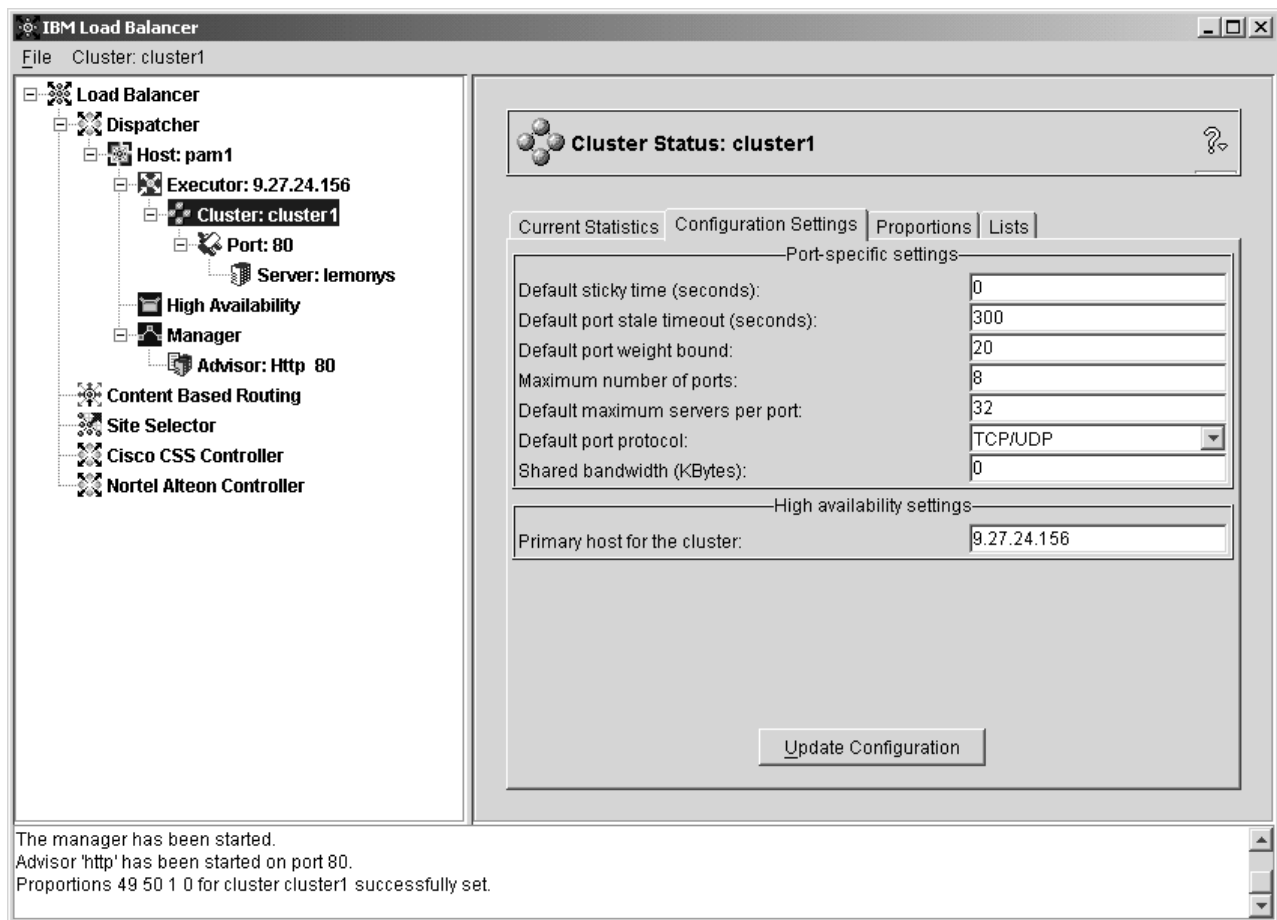


Figura 41. L'interfaccia utente grafica (GUI) con l'espansione del componente Dispatcher visualizzata nella struttura ad albero

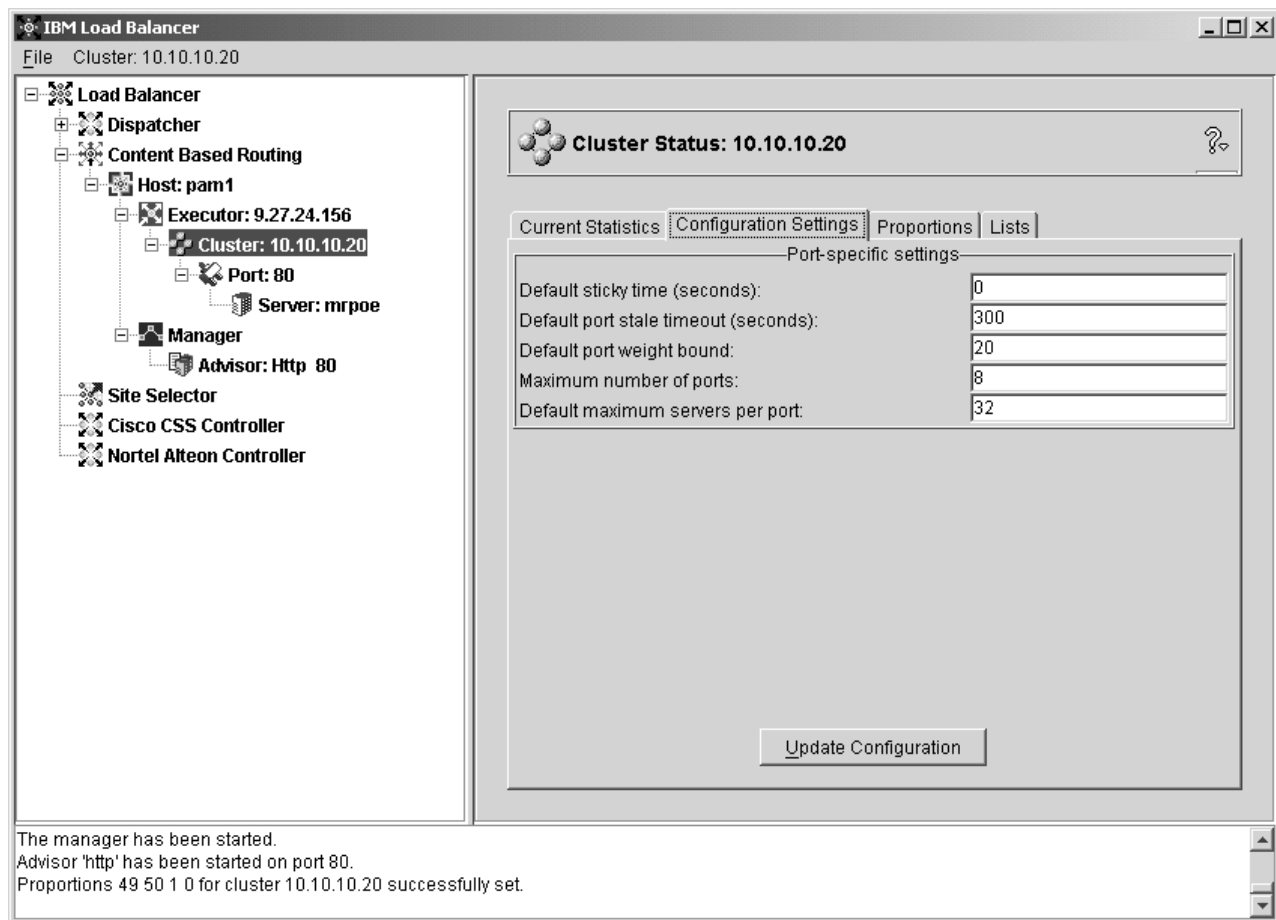


Figura 42. L'interfaccia utente grafica (GUI) con l'espansione del componente CBR visualizzata nella struttura ad albero

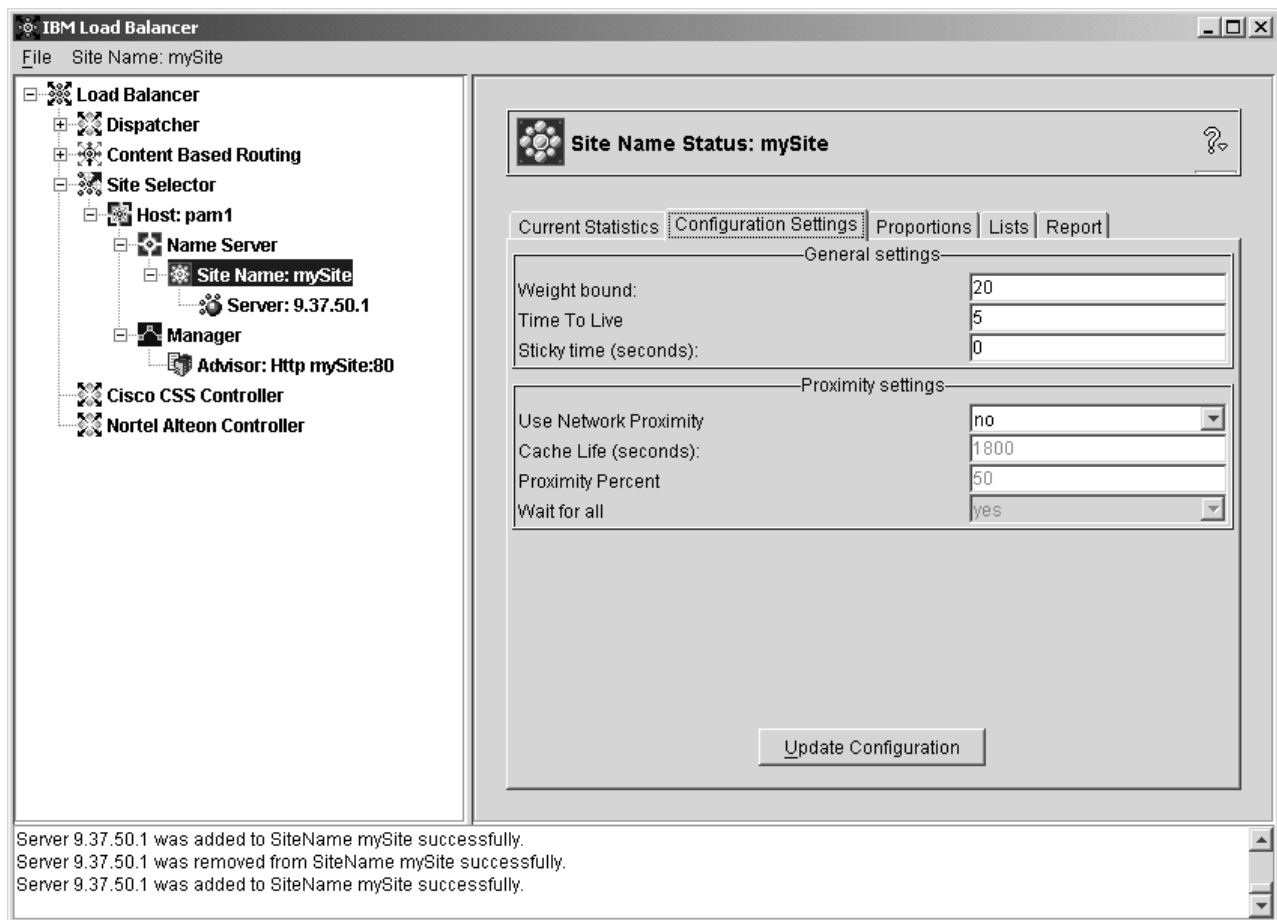


Figura 43. L'interfaccia utente grafica (GUI) con l'espansione del componente Site Selector visualizzata nella struttura ad albero

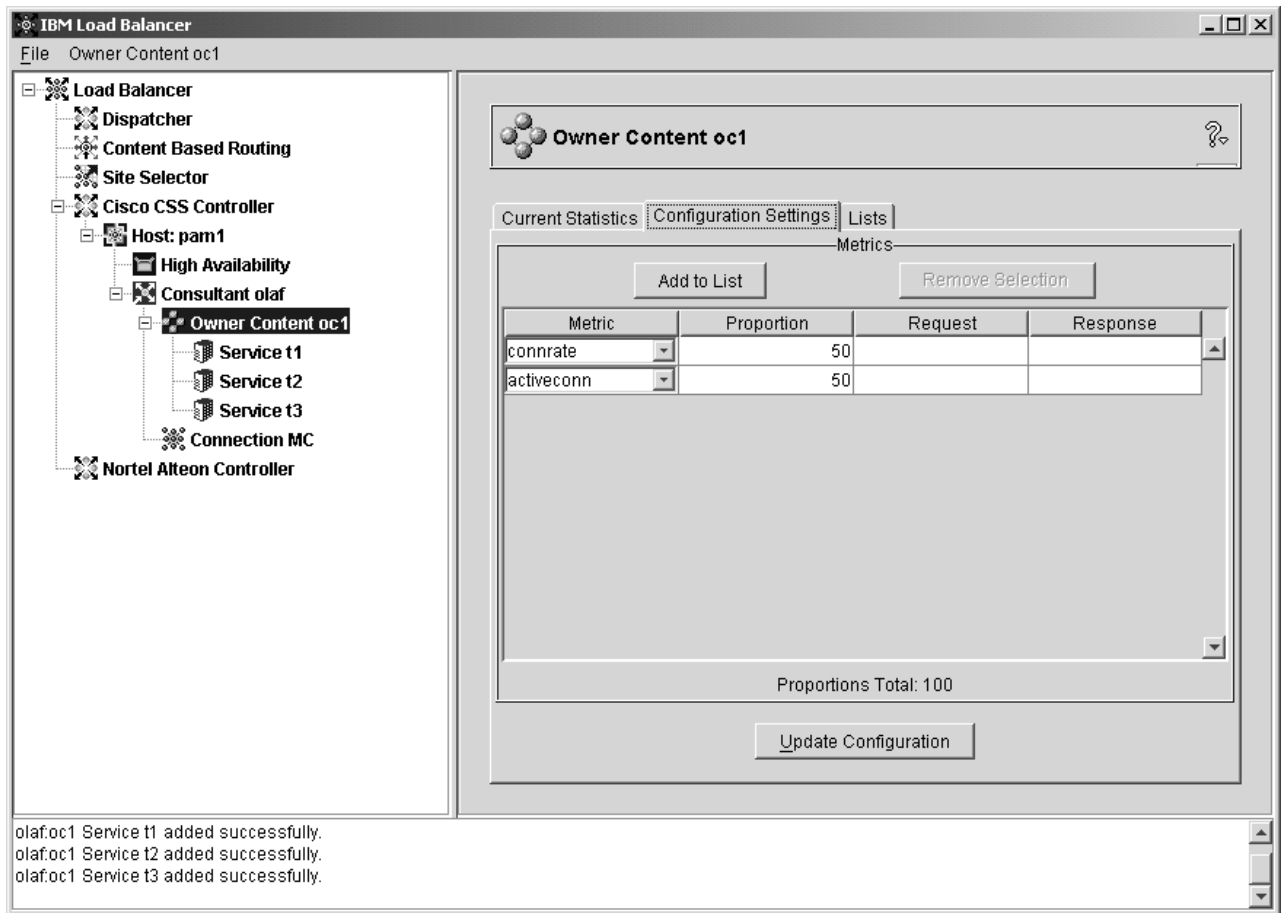


Figura 44. L'interfaccia utente grafica (GUI) con l'espansione del componente Cisco CSS Controller visualizzata nella struttura ad albero

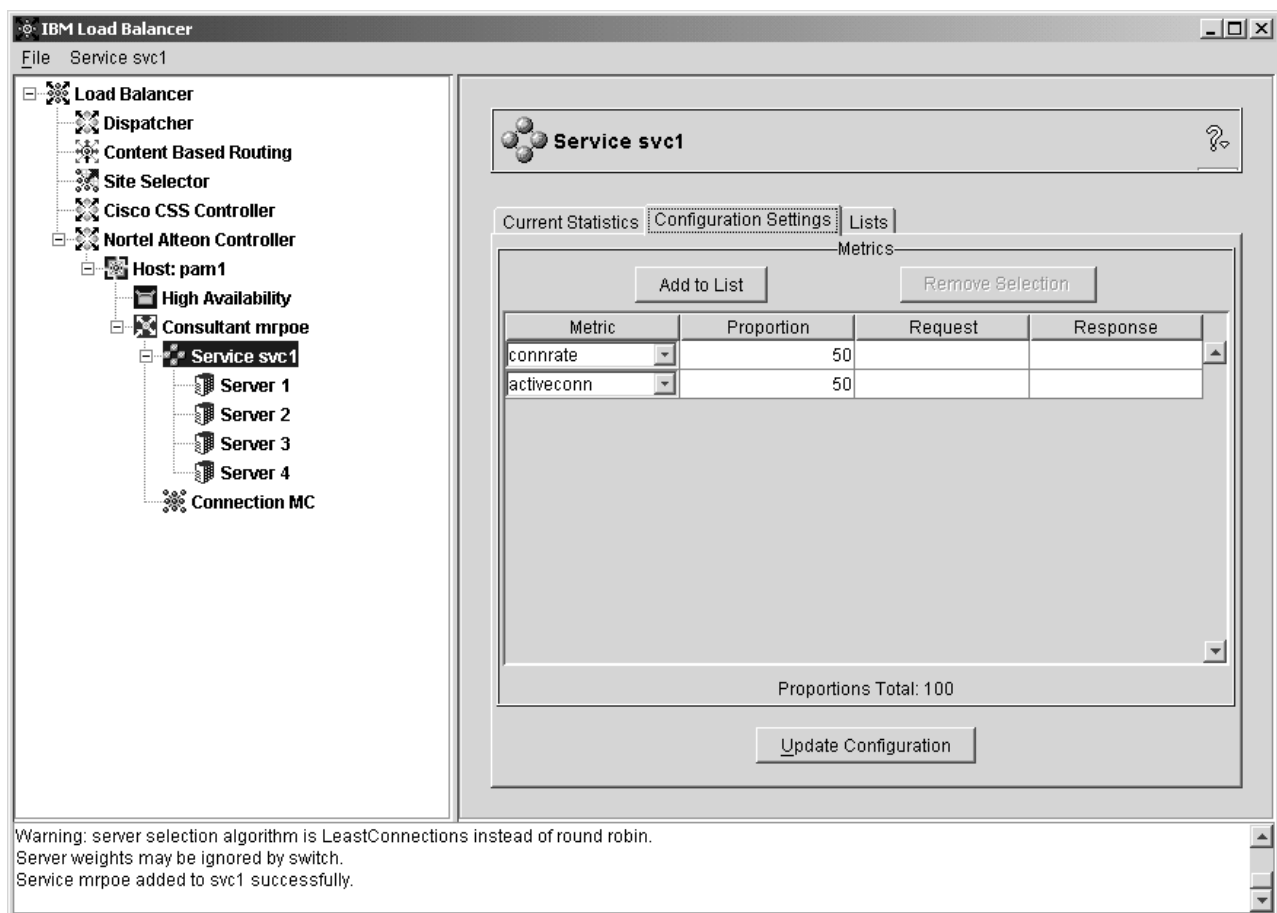


Figura 45. L'interfaccia utente grafica (GUI) con l'espansione del componente Nortel Alteon Controller visualizzata nella struttura ad albero

Tutti i componenti possono essere configurati dalla GUI. È possibile selezionare gli elementi della struttura ad albero con il primo pulsante del mouse (in genere, il pulsante sinistro) e visualizzare i menu a comparsa con l'altro pulsante (in genere, il pulsante destro). I menu a comparsa degli elementi della struttura ad albero sono accessibili anche dalla barra dei menu situata in alto sul pannello.

Fare clic sul segno più (+) o meno (-) per espandere o comprimere gli elementi della struttura ad albero.

Per eseguire un comando dalla GUI: evidenziare il nodo Host dalla struttura ad albero della GUI e selezionare **Send command....** dal relativo menu a comparsa. Nel campo di immissione dei comandi, digitare il comando che si desidera eseguire, ad esempio: **executor report**. I risultati e la cronologia dei comandi in esecuzione nella sessione corrente vengono visualizzati nella finestra fornita.

Sul lato destro del pannello vengono visualizzate le schede degli indicatori di stato per l'elemento correntemente selezionato.

- La scheda **Current Statistics** riporta le informazioni statistiche sull'elemento. Questa scheda non è disponibile per tutti gli elementi della struttura ad albero.
- Il pulsante **Refresh Statistics** consente di visualizzare i dati statistici più aggiornati. Se il pulsante Refresh Statistics non viene visualizzato, le statistiche vengono aggiornate dinamicamente e sono sempre recenti.

- La scheda **Configuration Settings** riporta i parametri di configurazione che possono essere impostati con le procedure descritte nei relativi capitoli dedicati a ciascun componente. Questa scheda non è disponibile per tutti gli elementi della struttura ad albero.
- Il pulsante **Update Configuration** applica le ultime modifiche apportate alla configurazione correntemente in esecuzione.
- La scheda **Proportions** riporta i parametri sulle proporzioni (o pesi) che possono essere impostate utilizzando le informazioni contenute in Capitolo 22, “Funzioni avanzate di Dispatcher, CBR e Site Selector”, a pagina 195. Questa scheda non è disponibile per tutti gli elementi della struttura ad albero.
- La scheda **Lists** riporta ulteriori dettagli sull’elemento della struttura ad albero. Questa scheda non è disponibile per tutti gli elementi della struttura ad albero.
- Il pulsante **Remove** consente di eliminare gli elementi evidenziati dagli elenchi.
- La scheda **Report** riporta le informazioni del report del gestore sull’elemento. Questa scheda non è disponibile per tutti gli elementi della struttura ad albero.
- Il pulsante **Refresh Report** consente di visualizzare i dati più aggiornati del report del gestore.

Per accedere all’**Help**, fare clic sul punto interrogativo (?) nell’angolo superiore destro della finestra di Load Balancer.

- **Help: Field level** — descrive i valori predefiniti di ciascun campo
- **Help: How do I** — elenca le attività possibili dalla schermata corrente
- **InfoCenter** — consente l’accesso alle informazioni sul prodotto, quali panoramica e descrizione delle nuove funzioni, collegamento al sito Web del prodotto, indice dei file della guida, glossario dei termini

Appendice B. Sintassi della regola di contenuto (modello)

Questa appendice descrive come utilizzare la sintassi della regola di contenuto (modello) per il componente CBR e per il metodo di inoltro cbr del componente Dispatcher e contiene scenari ed esempi di uso.

Sintassi della regola di contenuto (modello):

Applicabile solo se È stato selezionato "content" per il tipo di regola.

Immettere la sintassi modello che si desidera utilizzare, con le seguenti restrizioni:

- il modello non supporta l'uso di spazi
- i caratteri speciali possono essere utilizzati solo se preceduti dalla barra rovesciata (\):
 - * carattere jolly (trova da 0 a x corrispondenze di un qualsiasi carattere)
 - (parentesi di apertura utilizzata per il raggruppamento logico
 -) parentesi di chiusura utilizzata per il raggruppamento logico
 - & AND logico
 - | OR logico
 - ! NOT logico

Parole chiave riservate

Le parole chiave riservate sono sempre seguite da un segno di uguale "=".

Method

Metodo HTTP della richiesta, ad esempio GET, POST e così via.

URI Percorso della richiesta URL (sensibile al maiuscolo/minuscolo).

Version

Versione specifica della richiesta, HTTP/1.0 o HTTP/1.1.

Host Valore dall'host: intestazione (non sensibile al maiuscolo/minuscolo)

Nota: facoltativo nei protocolli HTTP/1.0.

<key> Un nome intestazione HTTP valido che può essere cercato da Dispatcher. Esempi di intestazioni HTTP sono User-Agent, Connection, Referer e così via.

Un browser che punta a `http://www.company.com/path/webpage.htm` potrebbe avere valori analoghi a quelli seguenti:

```
Method=GET
URI=/path/webpage.htm
Version=HTTP/1.1
Host=www.company.com
Connection=Keep-Alive
Referer=http://www.company.com/path/parentwebpage.htm
```

Nota: la shell del sistema operativo potrebbe interpretare i caratteri speciali, quali la E commerciale ("&") e trasformarli per alternare il testo prima che **cbrcontrol** li possa valutare.

Ad esempio, il seguente comando È valido solo quando si utilizza il prompt **cbrcontrol**>>.

```
rule add 10.1.203.4:80:cbr_prod_rule_ek type content
  pattern uri=/nipoe/*
```

Quando si utilizzano i caratteri speciali, affinché questo stesso comando funzioni sul prompt del sistema operativo, È necessario aggiungere le doppie virgolette (" ") prima e dopo il modello, come indicato di seguito:

```
cbrcontrol rule add 10.1.203.4:80:cbr_prod_rule_ek type content
  pattern "uri=/nipoe/*"
```

Se non si utilizzano le virgolette, è possibile che il modello venga troncato quando la regola viene salvata nel componente CBR. Notare che le virgolette non sono supportate quando si utilizza il prompt dei comandi cbrcontrol>>.

Di seguito viene riportata una raccolta di scenari possibili e di esempi di uso delle sintassi modello.

Scenario 1

La configurazione per un nome cluster prevede un gruppo di server Web per il contenuto HTML standard, un secondo gruppo di server Web che comprenda WebSphere Application Server per le richieste servlet, un terzo gruppo di server Lotus Notes per i file NSF e così via. È necessario accedere ai dati client per distinguere queste pagine richieste. È anche necessario inviarli ai server appropriati. Le regole di corrispondenza dei contenuti forniscono la separazione necessaria per completare queste attività. Viene inoltre configurata una serie di regole in modo che la necessaria separazione delle richieste venga eseguita automaticamente. Ad esempio, i seguenti comandi consentono di effettuare le tre suddivisioni menzionate:

```
>>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
```

Se a Load Balancer arriva una richiesta per un file NSF, viene controllata per prima la regola dei servlet, che non offre alcuna corrispondenza. La richiesta è quindi controllata dalla regola di Notes che restituisce una corrispondenza. Il carico del client viene bilanciato tra il server3 e il server4.

Scenario 2

Un altro scenario comune È un sito Web principale che controlla numerosi gruppi interni distinti. Ad esempio, www.company.com/software comporta un gruppo di server diversi e il contenuto della sezione www.company.com/hardware. Poiché le richieste si basano tutte sul cluster root www.company.com, le regole di contenuto sono necessarie per trovare le differenze di URI e completare il bilanciamento del carico. La regola dello scenario È simile a quanto segue:

```
>>rule add cluster1:80:div1 type content pattern uri=/software/* priority 1
>>rule uses cluster1:80:div1 server1+server2
>>rule add cluster1:80:div2 type content pattern uri=/hardware/* priority 2
>>rule uses cluster1:80:div2 server3+server4
```

Scenario 3

Alcune combinazioni sono sensibili all'ordine in cui le regole vengono ricercate. Ad esempio, nello scenario 2, i client erano suddivisi in base a una directory del percorso delle rispettive richieste; tuttavia, la directory di destinazione potrebbe comparire a più livelli del percorso e comportare conseguenze diverse nel posizionamento. Ad esempio, `www.company.com/pcs/fixed/software` È una destinazione diversa da `www.company.com/mainframe/fixed/software`. Le regole devono essere definite sull'account per questa possibilità e non prevedere troppi scenari contemporaneamente. Ad esempio, il test `"uri=*/software/*"` in questo caso contiene troppi caratteri jolly e comporterebbe una ricerca troppo vasta. Delle regole alternative potrebbero essere strutturate nel seguente modo:

Una ricerca combinata può restringere il campo di ricerca:

```
>>rule add cluster1:80:pcs type content pattern (uri=/pcs/*)&(uri=*/software/*)
>>rule uses cluster 1:80:pcs server1
```

In caso non sia possibile utilizzare le combinazioni disponibili, diventa importante l'ordine:

```
>>rule add cluster1:80:pc1 type content pattern uri=/pcs/*
>>rule uses cluster1:80:pc1 server2
```

La seconda regola interviene quando "pcs" compare nelle posizioni successive di directory anziché nella prima.

```
>>rule add cluster1:80:pc2 type content pattern uri=*/pcs/*
>>rule uses cluster1:80:pc2 server3
```

In quasi tutti i casi, è possibile completare le regole con una regola **sempre true** predefinita da applicare in tutti i casi in cui non possono essere applicate le altre regole. Questa potrebbe essere anche un server del tipo "Spiacenti, impossibile al momento collegarsi al sito, provare di nuovo" per scenari in cui tutti gli altri server non riescono a soddisfare la richiesta di questo client.

```
>>rule add cluster1:80:sorry type true priority 100
>>rule uses cluster1:80:sorry server5
```

Appendice C. File di configurazione di esempio

Questo appendice contiene i file di configurazione di esempio per il componente Dispatcher di Load Balancer.

IMPORTANTE: se si utilizza l'installazione di Load Balancer per IPv4 e IPv6, ricordarsi di sostituire i due punti (:) con il simbolo at (@) come delimitatore nei comandi dscontrol in questi file di configurazione di esempio.

File di configurazione di Load Balancer di esempio

I file di esempio sono posizionati nella directory ...ibm/edge/lb/servers/samples/.

File di configurazione di Dispatcher — sistemi AIX, Linux e Solaris

```
#!/bin/bash
#
# configuration.sample - File di configurazione di esempio per il
# componente Dispatcher
#
#
# Accertarsi che l'utente root sia l'utente che esegue lo script.
#
# iam=`whoami`

# if [ "$iam" != "root" ]if [ "$iam" != "root" ]
# then
#   echo "You must login as root to run this script"
#   exit 2
# fi

#
# In primo luogo, avviare il server
#
# dsserver start
# sleep 5

#
# Quindi, avviare l'executor
#
# dscontrol executor start

#
# Il Dispatcher può essere eliminato in qualsiasi momento utilizzando
# i comandi "dscontrol executor stop" e "dsserver stop" per
# arrestare rispettivamente l'executor e il server prima di rimuovere
# il software di Dispatcher.
#
# Il passo successivo nella configurazione di Dispatcher è impostare
# l'indirizzo NFA (indirizzo di non inoltrare) e gli indirizzi cluster.
#
# L'NFA viene utilizzato per accedere in remoto alla macchina Dispatcher
# a scopi di amministrazione o configurazione. Questo
# indirizzo è necessario in quanto il Dispatcher inoltrerà i pacchetti
# agli indirizzi cluster.
#
# L'indirizzo CLUSTER è il nome host (o l'indirizzo IP) a cui
# si collegano i client remoti.
#
```

```

# In qualunque punto di questo file, i nomi host e gli
# indirizzi IP sono intercambiabili.
#

# NFA=hostname.domain.name
# CLUSTER=www.yourcompany.com

# echo "Loading the non-forwarding address"
# dscontrol executor set nfa $NFA

#
# Il passo successivo nella configurazione di Dispatcher è creare
# un cluster. Il Dispatcher instrada le richieste inviate
# all'indirizzo cluster alle macchine server corrispondenti
# definite per quel cluster. È possibile configurare e utilizzare
# più indirizzi cluster tramite Dispatcher.

# Utilizzare una configurazione simile per CLUSTER2, CLUSTER3 ecc.
#

# echo "Loading first CLUSTER address "
# dscontrol cluster add $CLUSTER

#
# Ora occorre definire le porte che saranno utilizzate da questo cluster.
# Qualsiasi richiesta ricevuta da Dispatcher su una porta definita verrà
# inoltrata alla porta corrispondente di una delle macchine
# server.
#

# echo "Creating ports for CLUSTER: $CLUSTER"

# dscontrol port add $CLUSTER:20+21+80

#
# L'ultimo passo consiste nell'aggiungere ciascuna macchina server
# alle porte di questo cluster.
# Anche in questo caso, è possibile utilizzare il nome host o
# l'indirizzo IP delle macchine server.
#

# SERVER1=server1name.domain.name
# SERVER2=server2name.domain.name
# SERVER3=server3name.domain.name

# echo "Adding server machines"
# dscontrol server add $CLUSTER:20+21+80:
# $SERVER1+$SERVER2+$SERVER3

#
# Si avviano ora i componenti di bilanciamento del carico di
# Dispatcher. Il componente principale viene definito
# gestore e i componenti secondari advisor.
# Se il gestore e gli advisor non sono in esecuzione,
# Dispatcher invia le richieste in formato round-robin. Dopo aver
# avviato il gestore, vengono prese le decisioni sul calcolo dei pesi,
# in base al numero di connessioni nuove e di connessioni attive, e le richieste
# in entrata sono inviate al server considerato più adatto. Gli advisor
# forniscono al gestore ulteriori informazioni sulla capacità di un
# server di ricevere le richieste e rilevano se un server è attivo.
# Se un advisor rileva un server inattivo, lo contrassegna
# come tale (a condizione che le proporzioni del gestore siano state impostate
# in modo da includere l'input dell'advisor) e nessuna ulteriore richiesta
# sarà instradata verso quel server.

# L'ultimo passo nella configurazione dei componenti di bilanciamento
# del carico consiste nell'impostare le proporzioni del gestore. Il gestore

```

```

# aggiorna il peso di ciascun server in base a quattro politiche:
# 1. Il numero delle connessioni attive su ciascun server.
# 2. Il numero delle nuove connessioni a ciascun server.
# 3. L'input proveniente dagli advisor.
# 4. L'input proveniente dagli advisor del sistema.
# La somma di tali proporzioni deve essere 100. Ad esempio,
# se si impostano le proporzioni del gestore su
# dscontrol manager proportions 48 48 0 0
# le connessioni attive e nuove rappresenteranno il 48% nella
# decisione sul calcolo dei pesi, gli advisor contribuiranno nella
# misura del 4% e l'input del sistema non verrà preso in considerazione.
#
# NOTA: per impostazione predefinita, le proporzioni del gestore sono impostate a 50 50 0 0
#

# echo "Starting the manager..."
# dscontrol manager start

# echo "Starting the FTP advisor on port 21 ..."
# dscontrol advisor start ftp 21
# echo "Starting the HTTP advisor on port 80 ..."
# dscontrol advisor start http 80
# echo "Starting the Telnet advisor on port 23 ..."
# dscontrol advisor start telnet 23
# echo "Starting the SMTP advisor on port 25 ..."
# dscontrol advisor start smtp 25
# echo "Starting the POP3 advisor on port 110 ..."
# dscontrol advisor start pop3 110
# echo "Starting the NNTP advisor on port 119 ..."
# dscontrol advisor start nntp 119
# echo "Starting the SSL advisor on port 443 ..."
# dscontrol advisor start ssl 443
#

# echo "Setting the manager proportions..."
# dscontrol manager proportions 58 40 2 0

#
# Il passo finale nella configurazione della macchina Dispatcher è creare
# l'alias della scheda di interfaccia di rete(NIC).
#
# NOTA: NON utilizzare questo comando in un ambiente con la funzione
# di disponibilità elevata abilitata. Gli script go* configureranno
# la NIC e il loopback come necessario.
# dscontrol executor configure $CLUSTER

# Se l'indirizzo cluster si trova su una NIC o sottorete diversa
# da quella di NFA utilizzare il seguente formato per il comando
# di configurazione del cluster.
# dscontrol executor configure $CLUSTER tr0 0xfffff800
# dove tr0 è la NIC (tr1 per la seconda scheda token ring,
# en0 per la prima scheda ethernet) e 0xfffff800 è una
# subnet mask valida per questo sito.
#

#
# I seguenti comandi sono impostati sui valori predefiniti.
# Utilizzare questi comandi come guida per modificare i valori predefiniti.
# dscontrol manager loglevel 1
# dscontrol manager logsize 1048576
# dscontrol manager sensitivity 5
# dscontrol manager interval 2
# dscontrol manager refresh 2
#
# dscontrol advisor interval ftp 21 5
# dscontrol advisor loglevel ftp 21 1
# dscontrol advisor logsize ftp 21 1048576

```

```
# dscontrol advisor timeout ftp 21 unlimited
# dscontrol advisor interval telnet 23 5
# dscontrol advisor loglevel telnet 23 1
# dscontrol advisor logsize telnet 23 1048576
# dscontrol advisor timeout telnet 23 unlimited
# dscontrol advisor interval smtp 25 5
# dscontrol advisor loglevel smtp 25 1
# dscontrol advisor logsize smtp 25 1048576
# dscontrol advisor timeout smtp 25 unlimited
# dscontrol advisor interval http 80 5
# dscontrol advisor loglevel http 80 1
# dscontrol advisor logsize http 80 1048576
# dscontrol advisor timeout http 80 unlimited
# dscontrol advisor interval pop3 110 5
# dscontrol advisor loglevel pop3 110 1
# dscontrol advisor logsize pop3 110 1048576
# dscontrol advisor timeout pop3 110 unlimited
# dscontrol advisor interval nntp 119 5
# dscontrol advisor loglevel nntp 119 1
# dscontrol advisor logsize nntp 119 1048576
# dscontrol advisor timeout nntp 119 unlimited
# dscontrol advisor interval ssl 443 5
# dscontrol advisor loglevel ssl 443 1
# dscontrol advisor logsize ssl 443 1048576
# dscontrol advisor timeout ssl 443 unlimited
#
```

File di configurazione di Dispatcher — sistemi Windows

Di seguito viene riportato un file di configurazione di esempio di Load Balancer denominato **configuration.cmd.sample** da utilizzare in Windows.

```
@echo off
rem configuration.cmd.sample - File di configurazione di esempio per il
rem componente Dispatcher.
rem

rem dsserver deve essere avviato dal pannello Servizi

rem

rem
rem Quindi, avviare l'executor
rem
rem call dscontrol executor start

rem

rem Il passo successivo nella configurazione di Dispatcher è impostare
rem l'indirizzo NFA (indirizzo di non inoltrare) e impostare gli
rem indirizzi cluster.
rem

rem L'NFA viene utilizzato per accedere in remoto alla macchina Dispatcher
rem a scopi di amministrazione o configurazione. Questo
rem indirizzo è necessario in quanto il Dispatcher inoltrerà
rem i pacchetti agli indirizzi cluster.

rem
rem L'indirizzo CLUSTER è il nome host (o l'indirizzo IP) a cui
rem si collegano i client remoti.
rem

rem In qualunque punto di questo file, i nomi host e gli
rem indirizzi IP sono intercambiabili.
rem NFA=[Non-forwarding address]
rem CLUSTER=[your clustername]
```

```

rem

rem set NFA=hostname.domain.name
rem set CLUSTER=www.yourcompany.com

rem echo "Loading the non-forwarding address"
rem call dscontrol executor set nfa %NFA%

rem
rem I seguenti comandi sono impostati sui valori predefiniti.
rem Utilizzare questi comandi per modificare i valori predefiniti.

rem call dscontrol executor set fintimeout 30
rem
rem Il passo successivo nella configurazione di Dispatcher è creare
rem un cluster. Il Dispatcher instrada le richieste inviate
rem all'indirizzo cluster alle macchine server corrispondenti
rem definite per quel cluster. È possibile configurare e utilizzare
rem più indirizzi cluster tramite Dispatcher.
rem Utilizzare una configurazione simile per CLUSTER2, CLUSTER3 ecc.
rem

rem echo "Loading first CLUSTER address "
rem call dscontrol cluster add %CLUSTER%

rem
rem Ora occorre definire le porte che saranno utilizzate da questo cluster.
rem Qualsiasi richiesta ricevuta da Dispatcher su una porta definita verrà
rem inoltrata alla porta corrispondente
rem di una delle macchine server.
rem

rem echo "Creating ports for CLUSTER: %CLUSTER%"
rem call dscontrol port add %CLUSTER%:20+21+80

rem
rem L'ultimo passo consiste nell'aggiungere ciascuna macchina server
rem alle porte di questo cluster. Anche in questo caso, è possibile utilizzare
rem il nome host o l'indirizzo IP delle macchine server.
rem

rem set SERVER1=server1name.domain.name
rem set SERVER2=server2name.domain.name
rem set SERVER3=server3name.domain.name

rem echo "Adding server machines"
rem call dscontrol server add %CLUSTER%:20+21+80:
rem %SERVER1%+%SERVER2%+%SERVER3%

rem
rem Si avviano ora i componenti di bilanciamento del carico di
rem Dispatcher. Il componente principale viene definito
rem gestore e i componenti secondari advisor.
rem Se il gestore e gli advisor non sono in esecuzione,
rem Dispatcher invia le richieste in formato round-robin. Dopo aver
rem avviato il gestore, vengono prese le decisioni sul calcolo dei pesi,
rem in base al numero di connessioni nuove e di connessioni attive, e le richieste
rem in entrata sono inviate al server considerato più adatto. Gli advisor
rem forniscono al gestore ulteriori informazioni
rem ulteriori informazioni sulla capacità di un
rem server di ricevere le richieste e rilevano se un server è attivo.
rem Se un advisor rileva un server inattivo, lo contrassegna come tale
rem (a condizione che le proporzioni del gestore siano state impostate
rem in modo da includere l'input dell'advisor) e nessuna ulteriore richiesta sarà
rem instradata verso quel server.
rem L'ultimo passo nella configurazione dei componenti di bilanciamento
rem del carico consiste nell'impostare le proporzioni del gestore. Il

```

```

rem gestore aggiorna il peso di ciascun server in base
rem a quattro politiche:

rem 1. Il numero delle connessioni attive su ciascun server.
rem 2. Il numero delle nuove connessioni a ciascun server.
rem 3. L'input proveniente dagli advisor.
rem 4. L'input proveniente dagli advisor del sistema.
rem
rem La somma di tali proporzioni deve essere 100. Ad esempio,
rem impostando le proporzioni del cluster mediante
rem dscontrol cluster set <cluster> proportions 48 48 4 0
rem le connessioni attive e nuove rappresenteranno il 48% nella
rem decisione sul calcolo dei pesi, l'advisor contribuirà nella
rem misura del 4% e l'input del sistema non verrà preso in considerazione.
rem
rem NOTA: per impostazione predefinita, le proporzioni del gestore sono impostate a
rem 50 50 0 0

rem echo "Starting the manager..."
rem call dscontrol manager start

rem echo "Starting the FTP advisor on port 21 ..."
rem call dscontrol advisor start ftp 21
rem echo "Starting the HTTP advisor on port 80 ..."
rem call dscontrol advisor start http 80
rem echo "Starting the Telnet advisor on port 23 ..."
rem call dscontrol advisor start telnet 23
rem echo "Starting the SMTP advisor on port 25 ..."
rem call dscontrol advisor start smtp 25
rem echo "Starting the POP3 advisor on port 110 ..."
rem call dscontrol advisor start pop3 110
rem echo "Starting the NNTP advisor on port 119 ..."
rem call dscontrol advisor start nntp 119
rem echo "Starting the SSL advisor on port 443 ..."
rem call dscontrol advisor start ssl 443
rem

rem echo "Setting the cluster proportions..."
rem call dscontrol cluster set %CLUSTER% proportions 58 40 2 0

rem
rem Il passo finale nella configurazione della macchina Dispatcher è creare
rem l'alias della scheda di interfaccia di rete (NIC).
rem
rem NOTA: NON utilizzare questo comando in un ambiente con la funzione
rem di disponibilità elevata abilitata. Gli script go* configureranno
rem la NIC e il loopback come necessario.
rem
rem dscontrol executor configure %CLUSTER%

rem Se l'indirizzo cluster si trova su una NIC o sottorete diversa
rem da quella di NFA utilizzare il seguente formato per il comando
rem di configurazione del cluster.
rem dscontrol executor configure %CLUSTER% tr0 0xfffff800
rem dove tr0 è la NIC (tr1 per la seconda scheda token ring,
rem en0 per la prima scheda ethernet) e 0xfffff800 è una
rem subnet mask valida per questo sito.
rem

rem
rem I seguenti comandi sono impostati sui valori predefiniti.
rem Utilizzare questi comandi come guida per modificare i valori predefiniti.
rem call dscontrol manager loglevel 1
rem call dscontrol manager logsize 1048576
rem call dscontrol manager sensitivity 5
rem call dscontrol manager interval 2
rem call dscontrol manager refresh 2

```

```

rem
rem call dscontrol advisor interval ftp 21 5
rem call dscontrol advisor loglevel ftp 21 1
rem call dscontrol advisor logsize ftp 21 1048576
rem call dscontrol advisor timeout ftp 21 unlimited
rem call dscontrol advisor interval telnet 23 5
rem call dscontrol advisor loglevel telnet 23 1
rem call dscontrol advisor logsize telnet 23 1048576
rem call dscontrol advisor timeout telnet 23 unlimited
rem call dscontrol advisor interval smtp 25 5
rem call dscontrol advisor loglevel smtp 25 1
rem call dscontrol advisor logsize smtp 25 1048576
rem call dscontrol advisor timeout smtp 25 unlimited
rem call dscontrol advisor interval http 80 5
rem call dscontrol advisor loglevel http 80 1
rem call dscontrol advisor logsize http 80 1048576
rem call dscontrol advisor timeout http 80 unlimited
rem call dscontrol advisor interval pop3 110 5
rem call dscontrol advisor loglevel pop3 110 1
rem call dscontrol advisor logsize pop3 110 1048576
rem call dscontrol advisor timeout pop3 110 unlimited
rem call dscontrol advisor interval nntp 119 5
rem call dscontrol advisor loglevel nntp 119 1
rem call dscontrol advisor logsize nntp 119 1048576
rem call dscontrol advisor timeout nntp 119 unlimited
rem call dscontrol advisor interval ssl 443 5
rem call dscontrol advisor loglevel ssl 443 1
rem call dscontrol advisor logsize ssl 443 1048576
rem call dscontrol advisor timeout ssl 443 unlimited
rem

```

Advisor di esempio

Di seguito è riportato un file advisor di esempio denominato **ADV_sample**.

```

/**
 * ADV_sample: L'advisor HTTP di Load Balancer
 *
 *
 * Questa classe definisce un advisor personalizzato di esempio per Load Balancer.
 * Analogamente a
 * tutti gli advisor, questo advisor personalizzato estende la funzione
 * dell'advisor di base,
 * denominato ADV_Base. L'advisor di base esegue effettivamente
 * la maggior parte delle
 * funzioni dell'advisor, come ad esempio l'invio dei carichi
 * a Load Balancer da utilizzare nell'algoritmo di valutazione di Load Balancer. Inoltre,
 * tale advisor effettua le operazioni di connessione e chiusura del socket e fornisce
 * i metodi di invio e di ricezione
 * all'advisor. L'advisor stesso viene utilizzato
 * esclusivamente per l'invio e la ricezione dei dati a e dalla porta sul server
 * esaminato. I metodi TCP forniti con l'advisor di base sono programmati per calcolare
 * il carico. Se necessario, un'indicatore all'interno del costruttore dell'advisor
 * di base sostituisce il carico esistente con il nuovo carico restituito dall'advisor.
 *
 * Nota: in base al valore impostato nel costruttore, l'advisor di base fornisce
 * il carico all'algoritmo di valutazione a intervalli specifici. Se
 * l'advisor effettivo non è stato completato in modo che restituisca un carico valido,
 * l'advisor di base utilizza il carico precedente.
 *
 * DENOMINAZIONE
 *
 * La convenzione di denominazione è la seguente:
 *
 * - Il file deve trovarsi nella seguente directory Load Balancer:
 *
 * lb/servers/lib/CustomAdvisors/ (lb\servers\lib\CustomAdvisors su Windows)
 *

```

```

* - Il nome Advisor deve essere preceduto da "ADV_". Tuttavia, è possibile
*   avviare l'advisor solo con il nome; ad esempio, l'advisor "ADV_sample"
*   può essere avviato con "sample".
*
* - Il nome dell'advisor deve avere caratteri minuscoli.
*
*   Quindi, tenendo presente quanto riportato sopra, questo esempio viene definito:
*
*       <base directory>/lib/CustomAdvisors/ADV_sample.class
*
* Gli advisors, come tutti i componenti restanti di Load Balancer, devono essere
* compilati con la versione prereq di Java. Per garantire l'accesso alle classi Load Balancer,
* verificare che il file ibmlb.jar (situato nella sottodirectory lib della directory
* di base) sia incluso nel CLASSPATH del sistema.
*
* Metodi forniti da ADV_Base:
*
* - ADV_Base (Costruttore):
*
*   - Parametri
*     - String sName = Nome dell'advisor
*     - String sVersion = Versione dell'advisor
*     - int iDefaultPort = Numero porta predefinita su cui effettuare l'esame
*     - int iInterval = Intervallo durante il quale eseguire l'esame dei server
*     - String sDefaultName = Non utilizzato. Deve essere inviato come "".
*     - boolean replace = True - sostituisce il valore del carico calcolato
*                               dall'advisor di base
*                               False - aggiunge il valore del carico calcolato
*                               dall'advisor di base
*   - Valori di ritorno
*     - I costruttori non hanno valori di ritorno.
*
* Poiché l'advisor di base è basato sul thread, sono disponibili
* altri metodi a cui è possibile fare riferimento utilizzando
* il parametro CALLER inviato in getLoad().
*
* Questi metodi sono:
*
* - send - Invia un pacchetto di informazioni sulla connessione socket stabilita
*         al server sulla porta specificata.
*   - Parametri
*     - String sDataString - I dati da inviare sotto forma di una stringa
*   - Valori di ritorno
*     - int RC - Invio dei dati riuscito o meno: zero indica che
*               i dati sono stati inviati; un valore intero negativo indica un errore.
*
* - receive - Riceve le informazioni dalla connessione socket connection.
*   - Parametri
*     - StringBuffer sbDataBuffer - I dati ricevuti durante la chiamata di ricezione
*   - Valori di ritorno
*     - int RC - Ricezione dei dati riuscita o meno; zero
*               indica che i dati sono stati inviati; un valore intero negativo indica
*               un errore.
*
* Se la funzione fornita dall'advisor di base non è sufficiente,
* è possibile creare la funzione adeguata nell'advisor e
* i metodi forniti dall'advisor di base verranno ignorati.
*
* Una domanda importante sul carico restituito è se applicare
* tale carico a quello generato nell'advisor di base
* oppure se sostituirlo; sono presenti istanze valide di entrambe le situazioni.
*
* Questo esempio corrisponde essenzialmente all'advisor HTTP di Load Balancer. Il funzionamento
* è molto semplice: viene emessa una richiesta di invio--una richiesta head http. Quando viene
* ricevuta la risposta, il metodo getLoad termina, indicando all'advisor
* di base di arrestare la sincronizzazione della richiesta. Il metodo è quindi completo. Le

```



```

* informazioni restituite non vengono analizzate; il carico si basa sul tempo
* necessario per eseguire le operazioni di invio e ricezione.
*/

package CustomAdvisors;
import com.ibm.internet.nd.advisors.*;

public class ADV_sample extends ADV_Base implements ADV_MethodInterface {
    String COPYRIGHT =
        "(C) Copyright IBM Corporation 1997, All Rights Reserved.\n";

    static final String ADV_NAME = "Sample";
    static final int ADV_DEF_ADV_ON_PORT = 80;
    static final int ADV_DEF_INTERVAL = 7;

    // Nota: la maggior parte dei protocolli del server richiede un ritorno a capo ("\r")
    // e un avanzamento riga ("\n") alla fine dei messaggi. In questo caso, includerli
    // nella stringa.
    static final String ADV_SEND_REQUEST =
        "HEAD / HTTP/1.0\r\nAccept: */*\r\nUser-Agent: " +
        "IBM_Load_Balancer_HTTP_Advisor\r\n\r\n";

    /**
     * Costruttore.
     *
     * Parametri: Nessuno ma il costruttore per ADV_Base ha diversi parametri
     * che devono essere inviati.
     */
    public ADV_sample() {
        super( ADV_NAME,
              "2.0.0.0-03.27.98",
              ADV_DEF_ADV_ON_PORT,
              ADV_DEF_INTERVAL,
              "", // non utilizzato
              false);
        super.setAdvisor( this );
    }

    /**
     * ADV_AdvisorInitialize
     *
     * Qualsiasi inizializzazione specifica dell'advisor che deve essere effettuata
     * in seguito all'avvio dell'advisor di base. Questo metodo viene richiamato solo
     * una volta e, generalmente, non viene utilizzato.
     */
    public void ADV_AdvisorInitialize()
    {
        return;
    }

    /**
     * getLoad()
     *
     * Questo metodo viene chiamato dall'advisor di base per completare il funzionamento
     * dell'advisor, in base ai dettagli specifici del protocollo. In questo advisor
     * di esempio, è necessaria solo una singola operazione di invio e di ricezione; in
     * caso di logiche più complesse, è possibile emettere più operazioni di invio e
     * ricezione. Adesempio, una risposta potrebbe essere ricevuta e analizzata. In base alle
     * informazioni apprese, potrebbe essere emessa un'altra operazione di invio e di ricezione.
     *
     * Parametri:
     *
     * - iConnectTime - Il carico corrente poiché fa riferimento al tempo impiegato
     * per completare la connessione al server attraverso

```

```

*          la porta specificata.
*
* - caller - Un riferimento alla classe dell'advisor di base in cui i metodi forniti da Load
*            Balancer devono eseguire richieste TCP semplici,
*            principalmente l'invio e la ricezione.
*
* Risultati:
*
* - Carico - Un valore, espresso in millisecondi, che può essere aggiunto
*            o sostituito al carico esistente, come specificato
*            dall'indicatore "replace" del costruttore.
*
* Più è grande il carico e maggiore sarà il tempo necessario al server per rispondere;
* quindi, il peso all'interno di Load Balancer verrà ridotto.
*
* Se il valore è negativo, potrebbe essersi verificato un errore. Un errore proveniente
* da un advisor indica che il server che sta tentando di raggiungere non
* è accessibile ed è stato individuato come disattivo. Load Balancer
* non tenterà di eseguire il bilanciamento del carico su un server disattivo. Load Balancer
* riprenderà tale operazione quando riceverà un valore positivo da tale server.
*/
public int getLoad(int iConnectTime, ADV_Thread caller) {
    int iRc;
    int iLoad = ADV_HOST_INACCESSIBLE;    // -1

    // Per inviare la richiesta tcp
    iRc = caller.send(ADV_SEND_REQUEST);
    if (iRc >= 0)
    {
        // Per eseguire una ricezione
        StringBuffer sbReceiveData = new StringBuffer("");
        iRc = caller.receive(sbReceiveData);

        /**
         * In modalità advisor normale (l'indicatore "replace" è false), il carico
         * restituito è 0 o 1 a seconda se il server è attivo o meno.
         * Se la ricezione è avvenuta con esito positivo, viene restituito un carico con valore
         * zero che indica che è necessario utilizzare il carico creato nell'advisor di base.
         *
         * Altrimenti (l'indicatore "replace" è true), viene restituito il valore di carico
         * desiderato.
         */

        if (iRc >= 0)
        {
            iLoad = 0;
        }
    }
    return iLoad;
}

} // Fine - ADV_sample

```

Appendice D. Esempio di configurazione di disponibilità elevata a due livelli con Dispatcher, CBR e Caching Proxy

Questa appendice descrive come impostare una configurazione di disponibilità elevata a due livelli combinando le funzioni di due componenti di Load Balancer (il componente Dispatcher e il componente CBR) con Caching Proxy.

Configurazione della macchina server

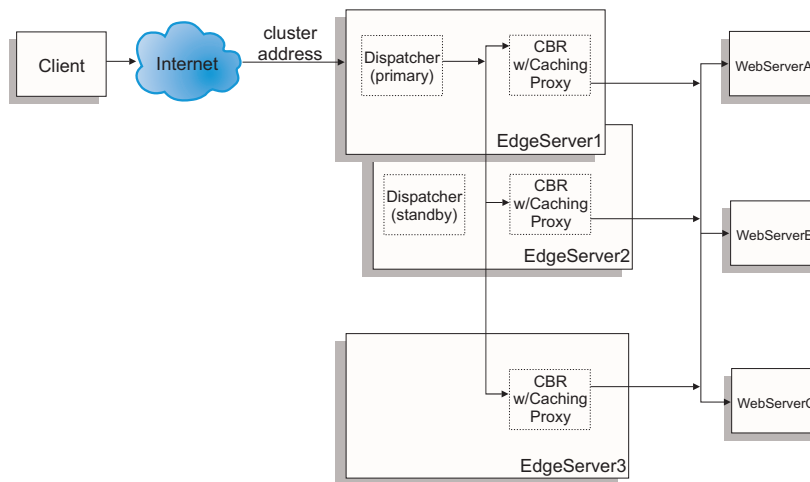


Figura 46. Esempio di configurazione di disponibilità elevata a due livelli con Dispatcher, CBR e Caching Proxy

La configurazione della macchina server per Figura 46 è la seguente:

- EdgeServer1: macchina Dispatcher principale (disponibilità elevata) posizionata con CBR e Caching Proxy che bilancia il carico tra i server Web
- EdgeServer2: macchina Dispatcher in standby (disponibilità elevata) posizionata con CBR e Caching Proxy
- EdgeServer3: macchina CBR e Caching Proxy
- WebServerA, WebServerB, WebServerC: server Web di backend

La Figura 46 mostra una rappresentazione grafica di più server (EdgeServer1, EdgeServer2, EdgeServer3) che eseguono il bilanciamento del carico tra più server Web di backend. Il componente CBR utilizza Caching Proxy per inoltrare le richieste in base al contenuto dell'URL ai server Web di backend. Il componente Dispatcher viene utilizzato per bilanciare il carico dei componenti CBR tra gli EdgeServer. La funzione di disponibilità elevata del componente Dispatcher viene utilizzata per garantire che le richieste del server di backend continuino ad essere elaborate anche se la macchina principale con disponibilità elevata (EdgeServer1) dovesse subire un malfunzionamento.

Linee guida per la configurazione di base:

- Configurare Caching Proxy allo stesso modo su tutti gli EdgeServer. Per migliorare l'accessibilità complessiva alle pagine Web sui server di backend, configurare Caching Proxy in modo da eseguire la memorizzazione nella cache. Ciò consente agli EdgeServer di memorizzare nella cache le pagine Web che

sono richieste più frequentemente. Per ulteriori informazioni sulla configurazione di Caching Proxy, fare riferimento alla *guida all'amministrazione di Caching Proxy*.

- Definire l'indirizzo cluster e le porte sugli stessi valori per i componenti CBR e Dispatcher di Load Balancer.
- Configurare il componente CBR con gli stessi valori in tutti gli EdgeServer. Utilizzare i server Web A, B e C come server sulle porte che si desidera definire per il cluster. Per ulteriori informazioni sulla configurazione del componente CBR, vedere Capitolo 11, "Configurazione di Content Based Routing", a pagina 107.
- Configurare il componente Dispatcher con gli stessi valori su EdgeServer1 e su EdgeServer2. Definire tutti gli EdgeServer come server sulle porte che si desidera definire sul cluster che deve essere sottoposto al bilanciamento del carico da parte di Dispatcher. Per ulteriori informazioni sulla configurazione del componente Dispatcher, vedere Capitolo 7, "Configurazione del Dispatcher", a pagina 61.
- Configurare EdgeServer1 come la macchina principale con disponibilità elevata e EdgeServer2 come la macchina in standby (backup) con disponibilità elevata. Per ulteriori informazioni, vedere "Disponibilità elevata" a pagina 198.

Nota:

1. Per evitare che gli indirizzi dei server di backend vengano visualizzati nell'URL di un client, è necessario impostare la direttiva ReversePass per ciascun indirizzo di server di backend nel file di configurazione di Caching Proxy.
2. Per garantire che la memorizzazione nella cache delle pagine Web sia utilizzata effettivamente, impostare la direttiva "Caching" su "ON" e aumentare la direttiva "CacheMemory" alle dimensioni richieste nel file di configurazione di Caching Proxy.
3. Righe di esempio che si riferiscono alle note 1-2 (sopra):

```
Caching          ON
CacheMemory      128000 K
ReversePass /* http://websrvA.company.com/* http://www.company.com/*
```
4. Ricordarsi di creare l'alias dell'indirizzo cluster sulla scheda di interfaccia di rete per EdgeServer1 e di creare l'alias dell'indirizzo cluster sul dispositivo loopback sugli altri EdgeServer.
5. Se si utilizza la piattaforma Linux per gli EdgeServer, può essere necessario installare una patch al kernel Linux o utilizzare un'alternativa per creare l'alias del dispositivo loopback. Per ulteriori informazioni, vedere "Alternative per l'aggiunta dell'alias loopback Linux quando si utilizza il metodo di inoltro mac di Load Balancer" a pagina 76.
6. Per CBR, l'affinità di porta (tempo di aderenza) non deve essere utilizzata quando si utilizzano le regole di contenuto; in caso contrario, le regole di contenuto non verranno attivate durante l'elaborazione delle richieste ai server Web di backend.

File di configurazione di esempio:

I seguenti file di configurazione di esempio sono analoghi ai file creati quando si imposta la configurazione di Edge Components come mostrato nella Figura 46 a pagina 477. I file di configurazione di esempio rappresentano i file per i componenti Dispatcher e CBR di Load Balancer. Nella configurazione di esempio, viene utilizzato un unico adattatore Ethernet per ciascuna macchina EdgeServer e

tutti gli indirizzi sono rappresentati da una sottorete privata. I file di configurazione di esempio utilizzano i seguenti indirizzi IP per le macchine specificate:

- EdgeServer1 (EdgeServer principale con disponibilità elevata): 192.168.1.10
- EdgeServer2 (EdgeServer di backup con disponibilità elevata): 192.168.1.20
- EdgeServer3 (EdgeServer per la memorizzazione nella cache delle pagine Web): 192.168.1.30
- Indirizzo cluster del sito Web: 192.168.1.11
- WebServersA-C (server Web di backend): 192.168.1.71, 192.168.1.72 e 192.168.1.73

File di configurazione di esempio per il componente Dispatcher sull'EdgeServer principale con disponibilità elevata:

```
dscontrol executor start

dscontrol cluster add 192.168.1.11 primaryhost 192.168.1.10

dscontrol port add 192.168.1.11:80

dscontrol server add 192.168.1.11:80:edgeserver1 address 192.168.1.10
dscontrol server add 192.168.1.11:80:edgeserver2 address 192.168.1.20
dscontrol server add 192.168.1.11:80:edgeserver3 address 192.168.1.30

dscontrol manager start manager.log 10004

dscontrol highavailability heartbeat add 192.168.1.10 192.168.1.20
dscontrol highavailability backup add primary auto 4567
```

File di configurazione di esempio per il componente CBR sugli EdgeServer:

```
cbrcontrol set loglevel 1
cbrcontrol executor start

cbrcontrol cluster add 192.168.1.11

cbrcontrol port add 192.168.1.11:80

cbrcontrol server add 192.168.1.11:80:webserverA address 192.168.1.71
cbrcontrol server add 192.168.1.11:80:webserverB address 192.168.1.72
cbrcontrol server add 192.168.1.11:80:webserverC address 192.168.1.73

cbrcontrol rule add 192.168.1.11:80:webA_rule type content
  pattern (URI=*WSA*)|(URI=*wsA*) priority 21
cbrcontrol rule useserver 192.168.1.11:80:webA_rule webserverA

cbrcontrol rule add 192.168.1.11:80:webB_rule type content
  pattern (URI=/WS_B*) priority 22
cbrcontrol rule useserver 192.168.1.11:80:webB_rule webserverB

cbrcontrol rule add 192.168.1.11:80:webC_rule type content
  pattern URI=*webC* priority 23
cbrcontrol rule useserver 192.168.1.21:80:webC_rule webserverC
```

Appendice E. Avvertenze

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti d'America.

IBM non può offrire in altri paesi i prodotti, i servizi o le funzioni descritti in questo documento. Per le informazioni sui prodotti ed i servizi disponibili al momento nella propria area, rivolgersi al rivenditore IBM locale. Qualunque riferimento relativo a prodotti, programmi o servizi IBM non implica che solo quei prodotti, programmi o servizi IBM possano essere utilizzati. In sostituzione a quelli forniti da IBM, possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino violazione dei diritti di proprietà intellettuale o di altri diritti dell'IBM. È tuttavia responsabilità dell'utente valutare e verificare la funzionalità di tali prodotti, programmi o servizi non IBM.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nel presente documento. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su di essi. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

Per domande sulle licenze relative a informazioni DBCS, contattare IBM Intellectual Property Department nel proprio paese oppure scrivere a:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Il seguente paragrafo non è valido per il Regno Unito o per tutti i paesi le cui leggi nazionali siano in contrasto con le disposizioni in esso contenute:

INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE QUESTA PUBBLICAZIONE NELLO STATO IN CUI SI TROVA SENZA ALCUNA GARANZIA, ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIALIZZABILITÀ ED IDONEITÀ AD UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, quindi, la presente dichiarazione potrebbe non essere a voi applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate su base periodica; tali modifiche verranno incorporate nelle nuove edizioni o nella nuova documentazione. IBM si riserva il diritto di apportare miglioramenti e/o modifiche ai prodotti e/o ai programmi descritti nel manuale in qualsiasi momento e senza preavviso.

Tutti i riferimenti a siti Web non IBM contenuti in questo documento sono forniti solo per consultazione. I materiali contenuti in tali siti Web non fanno parte della documentazione per questo prodotto IBM e il loro utilizzo è a discrezione dell'utente.

IBM può utilizzare o distribuire qualsiasi informazione fornita dall'utente nel modo più appropriato senza incorrere in alcuna obbligazione.

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire: (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a:

IBM Corporation
Attn.: G7IA./503.
P.O. Box 12195
3039 Cornwallis Rd.
Research Triangle Park, N.C. 27709-2195
U.S.A.

Queste informazioni possono essere rese disponibili secondo condizioni contrattuali appropriate, compreso, in alcuni casi, l'addebito di un canone.

Il programma su licenza descritto in queste informazioni e tutto il materiale su licenza ad esso relativo sono forniti da IBM nel rispetto delle condizioni previste dall'accordo IBM International Program License Agreement o da accordi equivalenti.

Tutti i dati relativi alle prestazioni contenuti in questa pubblicazione sono stati determinati in ambiente controllato. Pertanto, i risultati ottenuti in ambienti operativi diversi possono variare in modo considerevole. Alcune misure potrebbero essere state calcolate su sistemi di livelli di sviluppo per cui non si garantisce che queste saranno uguali su tutti i sistemi disponibili. Inoltre, alcune misure potrebbero essere state ricavate mediante estrapolazione. I risultati possono quindi variare. Gli utenti di questa pubblicazione devono verificare che i dati siano applicabili al loro specifico ambiente.

Le informazioni relative a prodotti non IBM sono state ottenute dai fornitori di tali prodotti. IBM non ha verificato tali prodotti e, pertanto, non può garantirne l'accuratezza delle prestazioni o la compatibilità. Eventuali commenti relativi alle prestazioni dei prodotti non IBM devono essere indirizzati ai fornitori di tali prodotti.

Tutte le dichiarazioni riguardanti la futura direzione o le intenzioni di IBM sono soggette a sostituzione o al ritiro senza preavviso e rappresentano unicamente scopi e obiettivi di IBM.

Queste informazioni contengono esempi di dati e report utilizzati quotidianamente nelle operazioni aziendali. Per meglio illustrarli, tali esempi contengono nomi di persone, società, marchi e prodotti. Tutti i nomi contenuti nella guida sono fittizi e ogni riferimento a nomi ed indirizzi reali è puramente casuale.

Se si stanno visualizzando queste informazioni in formato elettronico, le illustrazioni a colori e le foto potrebbero non essere visualizzate.

Marchi

I seguenti termini sono marchi o marchi registrati di IBM Corporation negli Stati Uniti, in altri paesi o in entrambi.

AFS
AIX
DFS
IBM
iSeries
NetView
OS/2
Redbook
RS/6000
SecureWay
ViaVoice
WebSphere
zSeries

Java e tutti i marchi basati su Java sono di Sun Microsystems, Inc. negli Stati Uniti, in altri paesi o in entrambi.

Microsoft, Windows, Windows NT e il logo Windows sono marchi di Microsoft Corporation negli Stati Uniti, in altri paesi o in entrambi.

Intel, Intel Inside (loghi), MMX and Pentium sono marchi di Intel Corporation negli Stati Uniti, in altri paesi o in entrambi.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e in altri paesi.

Linux è un marchio di Linus Torvalds, negli Stati Uniti, in altri paesi o in entrambi.

Altri nomi di società, prodotti o servizi possono essere marchi o marchi di servizi di altre società.

Glossario

A

ACK. Un bit di controllo (riconoscimento) che non occupa spazio nella sequenza e indica che il campo riconoscimento di questo segmento specifica il successivo numero della sequenza che il mittente di questo segmento si aspetta di ricevere, riconoscendo quindi la ricezione di tutti i numeri precedenti della sequenza.

advisor. Gli advisor sono una funzione di Load Balancer. Gli advisor raccolgono e analizzano le informazioni restituite dai singoli server e informano la funzione gestore.

affinità multiporta. È la funzione di affinità (aderenza) allargata a più porte. Vedere anche tempo di aderenza.

agente. (1) Nella gestione dei sistemi, un utente che per una particolare interazione ha assunto il ruolo di un agente. (2) Un'entità che rappresenta uno o più oggetti gestiti (a) emettendo notifiche relative agli oggetti e (b) gestendo richieste provenienti dai gestori relative a operazioni di gestione per modificare o interrogare gli oggetti.

alias. Un nome aggiuntivo attribuito a un server. L'alias rende il server indipendente dal nome della sua macchina host. L'alias deve essere definito nel DNS (Domain Name Server).

alias di loopback. Un indirizzo IP alternativo associato all'interfaccia loopback. L'indirizzo alternativo presenta l'utile effetto secondario di non interferire con un'interfaccia reale.

API. Application Programming Interface. L'interfaccia (convenzioni di chiamata) tramite la quale un'applicazione accede al sistema operativo e ad altri servizi. Le API vengono definite a livello del codice sorgente e forniscono un livello di astrazione tra l'applicazione e il kernel (o altri programmi di utilità privilegiati) per garantire la portabilità del codice.

B

backup. In una configurazione di Dispatcher a disponibilità elevata, il partner della macchina principale. Controlla lo stato della macchina principale e, se necessario, prende il suo posto. Vedere anche disponibilità elevata, principale.

C

Caching Proxy. Un server proxy di memorizzazione nella cache che consente di velocizzare i tempi di risposta agli utenti finali tramite schemi di memorizzazione nella cache molto efficienti. I filtri PICS flessibili consentono agli amministratori di rete di controllare gli accessi alle informazioni basate sul Web da una posizione centrale.

CBR. Content Based Routing. Un componente di Load Balancer. CBR funziona associato al Caching Proxy per bilanciare il carico delle richieste entranti, in base ai contenuti delle pagine Web utilizzando tipi di regole specifiche, sui server HTTP o HTTPS.

cbrcontrol. Fornisce l'interfaccia con il componente Content Based Router di Load Balancer.

cbrserver. Nel componente Content Based Router, gestisce le richieste dalla riga comandi all'executor, al gestore e agli advisor.

cococontrol. Nel componente Controller Cisco CSS, fornisce l'interfaccia con lo switch Cisco CSS.

cocoserver. Nel componente Controller Cisco CSS, gestisce le richieste dalla riga comandi ai consultant.

CGI. Common Gateway Interface. Uno standard per lo scambio di informazioni tra un server Web e un programma esterno. Il programma esterno può essere scritto in qualsiasi linguaggio supportato dal sistema operativo ed eseguire attività che non vengono normalmente eseguite dai server, come ad esempio l'elaborazione dei moduli.

client. Un computer o un processo che richiede un servizio a un altro computer o processo. Ad esempio, una workstation o un personal computer che richiede documenti HTML da un Webserver Go Lotus Domino è un client di quel server.

cluster. Nel Dispatcher, un gruppo di server TCP o UDP utilizzati per lo stesso scopo e identificati tramite un solo nome host. Vedere anche cella.

consultant. Raccoglie le metriche dai server su cui viene eseguito il bilanciamento del carico e invia informazioni sui pesi dei server allo switch che esegue il bilanciamento del carico.

contenuto proprietario. Rappresenta il nome del proprietario e la regola di contenuto di un proprietario, entrambi definiti sul Switch Cisco CSS.

contrassegnare come attivo. Consentire a un server di ricevere nuove connessioni.

contrassegnare come inattivo. Interrompere tutte le connessioni attive a un server e impedire di inviare a tale server nuove connessioni o pacchetti.

controller. Una raccolta di uno o più consultant.

Controller Cisco CSS. Un componente di IBM Load Balancer. Il controller Cisco CSS utilizza la tecnologia di Load Balancer per fornire in tempo reale informazioni di bilanciamento del carico allo switch Cisco Content Services.

Controller Nortel Alteon. Un componente di IBM Load Balancer. Controller Nortel Alteon utilizza la tecnologia di Load Balancer per fornire in tempo reale informazioni di bilanciamento del carico allo Switch Nortel Alteon Web.

D

daemon. Disk And Execution Monitor. Un programma non coinvolto esplicitamente nelle operazioni ma che rimane inattivo in attesa che si verifichi una o più condizioni. Il concetto è che l'esecutore della condizione non dovrebbe essere consapevole dell'esistenza del daemon inattivo (anche se spesso un programma esegue un'azione solo perché è consapevole che quell'azione richiederà implicitamente un daemon).

default. Un valore, un attributo o un'opzione che viene selezionata automaticamente se non ne viene specificata esplicitamente un'altra.

Dispatcher. Un componente di Load Balancer che bilancia in modo efficiente il traffico TCP o UDP tra gruppi di singoli server collegati. La macchina Dispatcher è il server che esegue il codice di Dispatcher.

disponibilità elevata. Una funzionalità di Load Balancer in cui un Load Balancer può assumere le funzioni di un altro, qualora questo diventi non disponibile.

disponibilità elevata reciproca. La disponibilità elevata reciproca consente a due macchine Dispatcher di agire come principale e come backup l'una per l'altra. Vedere anche backup, disponibilità elevata, principale.

domain name server. DNS. Un servizio generico, distribuito e replicato di interrogazione dati, utilizzato principalmente su Internet per tradurre nomi host in indirizzi Internet. Inoltre, lo stile del nome host utilizzato su Internet, per quanto tale nome venga definito più correttamente nome dominio completo. Il DNS può essere configurato per utilizzare una sequenza di server dei nomi, in base ai domini in cui viene ricercato il nome, fino a individuare una corrispondenza.

dscontrol. Fornisce l'interfaccia con il componente Dispatcher di Load Balancer.

dsserver. In Dispatcher, gestisce le richieste dalla riga comandi all'executor, al gestore e agli advisor.

E

Ethernet. Un tipo di rete locale (LAN) standard. Consente a più stazioni di accedere al supporto di trasmissione in qualsiasi momento, senza coordinamento preventivo, previene i conflitti grazie al deferimento e alla sensibilità della portante e risolve i conflitti utilizzando il rilevamento di collisioni e trasmissioni. I protocolli software utilizzati dai sistemi Ethernet possono variare, ma comprendono il TCP/IP.

executor. Una delle diverse funzioni di Load Balancer. L'executor inoltra le richieste ai server TCP o UDP monitorando inoltre il numero di connessioni nuove, attive e terminate, eseguendo anche la raccolta dei dati inutilizzati delle connessioni completate o azzerate. L'executor fornisce le connessioni nuove e attive alla funzione gestore.

F

FIN. Un bit di controllo (fine) che occupa un numero della sequenza e indica che il mittente non invierà ulteriori dati o controlli occupando lo spazio della sequenza.

Firewall. Un computer che collega una rete privata, quale quella di un'azienda, a una rete pubblica, quale Internet. Contiene programmi che limitano l'accesso tra le due reti. Vedere anche *gateway proxy*.

FQDN. Fully Qualified Domain Name. Il nome completo di un sistema, composto dal nome host locale e il nome dominio, compreso un dominio di livello superiore (TLD, Top-Level Domain). Ad esempio, "venera" è un nome host, mentre "venera.isi.edu" è un FQDN. Un FQDN dovrebbe essere sufficiente a determinare un indirizzo Internet univoco per qualsiasi host su Internet. Questo processo, detto "risoluzione dei nomi", utilizza il DNS (Domain Name System).

FTP (File Transfer Protocol). Un protocollo applicativo utilizzato per trasferire file da e verso computer in rete. FTP richiede un ID utente e, talvolta, una password per consentire l'accesso ai file su un sistema host remoto.

G

gateway. Un'unità funzionale che collega due reti di computer con architetture diverse.

gestore. Una delle diverse funzioni di Load Balancer. Il gestore imposta i pesi in base a contatori interni nell'executor e al feedback fornito dagli advisor. L'executor utilizza poi i pesi per eseguire il bilanciamento del carico.

GRE. Generic Routing Encapsulation. Un protocollo che consente di trasmettere un protocollo di rete arbitrario A attraverso qualsiasi altro protocollo di rete arbitrario B, incapsulando i pacchetti di A in pacchetti GRE, che a loro volta sono contenuti nei pacchetti di B.

H

heartbeat. Un pacchetto semplice inviato tra due macchine Load Balancer in modalità a disponibilità elevata, utilizzato da Load Balancer in standby per monitorare lo stato del Load Balancer attivo.

host. Un computer, collegato a una rete, che fornisce un punto di accesso a tale rete. Un host può essere un client, un server o entrambi contemporaneamente.

HTML (Hypertext Markup Language). Il linguaggio utilizzato per creare documenti in formato ipertesto. Gli ipertesti comprendono collegamenti ad altri documenti che aggiungono ulteriori informazioni relative al termine o all'argomento evidenziato. HTML controlla il formato del testo e la posizione delle aree di immissione dei moduli, ad esempio, nonché i link navigabili.

HTTP (Hypertext Transfer Protocol). Il protocollo utilizzato per trasferire e visualizzare documenti in formato ipertesto.

HTTPS (Hypertext Transfer Protocol, Secure). Il protocollo utilizzato per trasferire e visualizzare documenti in formato ipertesto utilizzando SSL.

I

ICMP. Internet Control Message Protocol. Un protocollo di controllo dei messaggi e di segnalazione degli errori tra un server host e un gateway verso Internet.

IMAP. Internet Message Access Protocol. Un protocollo che consente a un client di accedere a messaggi di posta elettronica su un server e di manipolarli. Consente la manipolazione delle cartelle di messaggi remote (caselle postali) in un modo funzionalmente equivalente alle caselle postali locali.

indirizzo. Codice univoco assegnato a ciascun dispositivo o workstation collegato a una rete. Un indirizzo IPv4 standard è un campo indirizzo a 32 bit contenente due parti. La prima parte è l'indirizzo di rete e la seconda parte è il numero dell'host. Un indirizzo IPv6 è un campo indirizzo a 128 bit che supporta un numero molto più elevato di indirizzi rispetto a IPv4. Supporta inoltre opzioni aggiuntive come l'indirizzamento multicast e anycast.

indirizzo cluster. Nel Dispatcher, l'indirizzo al quale si connettono i client.

indirizzo della destinazione accessibile. In disponibilità elevata per Dispatcher, l'indirizzo della destinazione a cui l'advisor deve inviare ping per verificare che la destinazione risponda.

indirizzo del server. Il codice univoco assegnato a ciascun computer che fornisce servizi condivisi ad altri computer su una rete; ad esempio, un server di archiviazione, un server di stampa o un server di posta. L'indirizzo del server può essere l'indirizzo IP o il nome host.

indirizzo destinazione. In una configurazione a disponibilità elevata, l'indirizzo della macchina partner a cui vengono inviati heartbeat e risposte.

indirizzo IP. Indirizzo Internet Protocol. L'indirizzo univoco che specifica l'effettiva posizione di ciascuna unità o stazione di lavoro in una rete. È noto anche come indirizzo Internet.

indirizzo MAC. Indirizzo Media Access Control. L'indirizzo hardware di un dispositivo connesso a un supporto di rete condiviso.

indirizzo metrica. L'indirizzo con cui si collega Metric Server.

indirizzo mittente. Un nome host o un indirizzo IP univoco. È configurato sulla macchina Dispatcher e utilizzato dal Dispatcher come proprio indirizzo di origine durante il bilanciamento del carico delle richieste client al server.

indirizzo origine. Nella funzione di disponibilità elevata per Dispatcher, l'indirizzo della macchina partner a disponibilità elevata che invia gli heartbeat.

inizio intervallo. In un contesto di bilanciamento del carico basato su regole, il valore minimo specificato per una regola. Il valore predefinito dipende dal tipo di regola.

instradamento. Il percorso del traffico di rete dall'origine alla destinazione.

interfaccia loopback. Un'interfaccia che evita funzioni di comunicazione non necessarie quando le informazioni sono indirizzate a un'entità sullo stesso sistema.

Internet. La raccolta mondiale di reti interconnesse che utilizzano la suite di protocolli Internet e consentono accesso pubblico.

intervallo finale. Nel bilanciamento del carico basato su regole, un valore più alto specificato per una regola. L'impostazione predefinita di questo valore dipende dal tipo di regola.

intranet. Una rete privata protetta che integra gli standard e le applicazioni Internet (quali i browser Web) con l'infrastruttura di reti di computer esistente all'interno di un'organizzazione.

IP. Internet Protocol. Un protocollo non dipendente dalla connessione, che instrada i dati attraverso una rete di reti interconnesse. IP agisce da intermediario tra gli strati di protocollo superiori e lo strato fisico.

IPSEC. Internet Protocol Security. Uno standard in via di sviluppo per la sicurezza dello strato di rete o di elaborazione dei pacchetti della comunicazione di rete.

L

LAN. Local Area Network. Una rete di dispositivi collegati e comunicanti all'interno di un'area geografica limitata, che può essere connessa a una rete più grande.

larghezza di banda. La differenza tra la frequenza più alta e più bassa di un canale di trasmissione; la quantità di dati che possono essere trasmessi, al secondo, attraverso un determinato circuito di comunicazione.

M

macchina server. Un server inserito da Dispatcher in un gruppo di server che agisce come un unico server virtuale. Il Dispatcher bilancia il traffico tra le macchine server. Sinonimo di server in cluster.

macchina server TCP. Un server collegato ad altri da Load Balancer per creare un unico server virtuale. Load Balancer bilancia il traffico TCP tra le macchine server TCP. Sinonimo di server in cluster.

maschera subnet. Per IPv4, una maschera a 32 bit utilizzata per identificare i bit dell'indirizzo della sottorete nella parte host di un indirizzo IP.

metrica. Un processo o comando che restituisce un valore numerico, utilizzabile nel bilanciamento del carico sulla rete, ad esempio il numero di utenti attualmente connessi.

Metric Server. Precedentemente noto come SMA (Server Monitor Agent). Metric Server fornisce metriche specifiche del sistema al gestore di Load Balancer.

MIB. (1) Management Information Base. Una raccolta di oggetti accessibili mediante un protocollo di gestione della rete. (2) Una definizione delle informazioni di gestione che specifica le informazioni disponibili da un host o gateway e le operazioni consentite.

N

nalcontrol. Fornisce l'interfaccia con il componente Controller Nortel Alteon di Load Balancer.

nalserver. In Controller Nortel Alteon, gestisce le richieste dalla riga comandi ai Consultant.

netmask. Per IPv4, una maschera a 32 bit utilizzata per identificare i bit dell'indirizzo della sottorete nella parte host di un indirizzo IP.

Network Address Port Translation. NATP, noto anche come mappatura delle porte. Consente di configurare più daemon server all'interno di un singolo server fisico perché siano in ascolto su numeri di porta diversi.

Network Address Translation. NAT, o Network Address Translator, LAN virtuale. Un dispositivo hardware attualmente in via di sviluppo, utilizzato per estendere gli indirizzi Internet già in uso. Consente l'utilizzo di indirizzi IP duplicati all'interno di un'azienda e di indirizzi univoci all'esterno.

NFA (nonforwarding address, indirizzo di non inoltrare). L'indirizzo IP primario della macchina Load Balancer, utilizzato per la gestione e la configurazione.

NIC. Network Interface Card, scheda di rete. Una scheda adattatore installata in un computer per fornire il collegamento fisico a una rete.

NNTP. Network News Transfer Protocol. Un protocollo TCP/IP per il trasferimento di articoli di news.

nodo gestito. Nelle comunicazioni Internet, una stazione di lavoro, un server o un router che contiene un agente di gestione della rete. Nel protocollo Internet (IP), il nodo gestito contiene solitamente un agente SNMP (Simple Network Management Protocol).

nome host. Il nome simbolico assegnato a un host. I nomi host vengono risolti su indirizzi IP mediante un server dei nomi di dominio.

nome sito. Un nome sito è un nome host non risolvibile che viene richiesto dal client. Ad esempio, un sito Web ha 3 server (1.2.3.4, 1.2.3.5 e 1.2.3.6) configurati per il nome sito *www.dnsload.com*. Quando un client richiede questo nome sito, come risoluzione verrà restituito uno degli indirizzi IP dei server associati. Il nome sito deve essere un nome dominio completo, ad esempio: *dnsload.com*. Un nome non completo, ad esempio *dnsload*, non è valido come nome sito.

notazione decimale con punti. La rappresentazione sintattica di un intero a 32 bit, costituita da quattro numeri di 8 bit, scritti in base 10 e separati da punti. Utilizzata per rappresentare gli indirizzi IPv4.

P

pacchetto. L'unità di dati che viene instradata tra un'origine e una destinazione su Internet o altra rete a commutazione di pacchetti.

PICS. Platform for Internet Content Selection. I client che supportano PICS consentono agli utenti di determinare i servizi di restrizione che intendono utilizzare e, per ciascuno di essi, quali restrizioni sono accettabili o meno.

ping. Un comando che invia pacchetti di richiesta echo ICMP (Internet Control Message Protocol) a un host, gateway o router attendendo di riceverne una risposta.

POP3. Post Office Protocol 3. Un protocollo utilizzato per lo scambio di posta in rete e l'accesso alle caselle postali.

porta. Un numero che identifica un'unità di comunicazione astratta. I server Web utilizzano la porta 80 per impostazione predefinita.

posizionamento di indirizzi multipli. Il posizionamento di indirizzi multipli consente al cliente di specificare l'indirizzo del server posizionato in modo che sia diverso dall'indirizzo di non inoltrare (NFA) nella configurazione. Vedere anche **posizionare**.

posizionare. Quando Load Balancer viene installato sulla stessa macchina per la quale sta eseguendo il bilanciamento del carico.

principale. Nella disponibilità elevata per Dispatcher, la macchina avviata come principale, cioè quella che instrada attivamente i pacchetti. Il relativo partner, la macchina di backup, esegue il monitoraggio dello stato della macchina principale e, se necessario, prende il suo posto. Vedere anche **backup**, **disponibilità elevata**.

priorità. Nel bilanciamento del carico basato su regole, il livello di importanza attribuito a una determinata regola. Il Dispatcher valuta le regole a partire dal primo livello di priorità per finire con l'ultimo.

procedura guidata. Una finestra di dialogo all'interno di un'applicazione che utilizza istruzioni passo-passo per guidare un utente durante lo svolgimento di un'attività specifica.

prossimità della rete. La prossimità di due entità in rete, quali un client e un server, determinata da Site Selector mediante il calcolo del round-trip.

protocollo. L'insieme di regole che governano il funzionamento di unità funzionali di un sistema di comunicazione se deve esserci una comunicazione. I protocolli possono determinare dettagli a basso livello delle interfacce tra macchine, quale l'ordine di invio dei bit di un byte, ma anche scambi ad alto livello tra programmi applicativi, quale il trasferimento file.

Q

Quality of Service (QoS). Le proprietà di prestazioni di un servizio di rete, compresa la velocità di trasmissione, il ritardo di transito e la priorità. Alcuni protocolli consentono l'inclusione di requisiti QoS in pacchetti o flussi.

R

reach. In Dispatcher, un advisor che invia ping a una determinata destinazione e notifica se questa risponde o meno.

registrazione binaria. Consente di memorizzare le informazioni relative ai server in file binari. Questi dati vengono quindi elaborati per analizzare le informazioni sui server che sono state raccolte nel corso del tempo.

regola. Nel bilanciamento del carico basato su regole, un meccanismo per raggruppare server in modo che un server possa essere scelto in base a informazioni diverse dall'indirizzo e dalla porta di destinazione.

rete. Sistema di comunicazione hardware e software. Le reti vengono spesso classificate in base alla loro estensione geografica, come LAN (local area network, rete locale), MAN (metropolitan area network, rete cittadina), WAN (wide area network, rete geografica) e anche in base ai protocolli utilizzati.

rete privata. Una rete separata su cui Dispatcher comunica con i server raggruppati in cluster per motivi legati alle prestazioni.

RMI. Remote Method Invocation. Parte della libreria del linguaggio di programmazione Java che consente a un programma Java in esecuzione su un computer di accedere a oggetti e metodi di un altro programma Java, su un altro computer.

router. Un'unità che inoltra pacchetti tra reti. La decisione per l'inoltro si basa sulle informazioni dello stato di rete e sulle tabelle di instradamento, spesso create da prodotti per l'instradamento.

RPM. Red Hat Package Manager, il gestore pacchetti per Red Hat.

S

scalabile. Relativo alla capacità di un sistema di adattarsi rapidamente a un'intensità di uso, volume o domanda maggiore o minore. Ad esempio, un sistema scalabile può adattarsi efficacemente a funzionare con reti più grandi o più piccole, eseguendo attività di complessità variabile.

script CGI. Un programma CGI scritto in un linguaggio script come Perl o REXX che utilizza Common Gateway Interface per eseguire attività che normalmente non vengono eseguite dai server, come ad esempio l'elaborazione dei moduli.

server. Un computer che fornisce servizi condivisi ad altri computer su una rete; ad esempio, un server di archiviazione, un server di stampa o un server di posta.

server in cluster. Un server inserito da Dispatcher in un gruppo di server che agisce come un unico server virtuale. Load Balancer gestisce il bilanciamento del traffico TCP o UDP tra questi server raggruppati in cluster.

servizio. (1) Una funzione fornita da uno più nodi; ad esempio, HTTP, FTP, Telnet. (2) Per il Controller Nortel Alteon, un servizio è la funzione o l'informazione richiesta da un utente finale da un sito. Viene identificato da un indirizzo IP virtuale e da un numero di porta virtuale per la richiesta di un utente finale. Sullo switch, viene identificato da un identificativo server virtuale, costituito da un intero e da un numero di porta virtuale o nome servizio. (3) Per Cisco CSS Consultant, un servizio è una posizione di destinazione su cui è residente fisicamente un contenuto. Ad esempio, un server e una porta, in locale o remoto.

shell. Il software che accetta ed elabora righe comandi da una stazione di lavoro di un utente. La shell bash è una delle diverse shell disponibili per UNIX.

Site Selector. Un componente di bilanciamento del carico di Load Balancer basato su DNS. Site Selector esegue il bilanciamento del carico sui server all'interno di una rete geografica (WAN) utilizzando misurazioni e pesi raccolti dal componente Metric Server in esecuzione su tali server.

SMTP. Simple Mail Transfer Protocol. Nella suite di protocolli Internet, un protocollo applicativo per il trasferimento di posta tra utenti nell'ambiente Internet. SMTP specifica le sequenze di scambio della posta e il formato dei messaggi. Assume il TCP (Transmission Control Protocol) come protocollo sottostante.

SNMP. Simple Network Management Protocol. Il protocollo standard di Internet, definito in STD 15, RFC 1157, sviluppato per la gestione di nodi su una rete IP. SNMP non è limitato al TCP/IP. Può essere utilizzato per gestire e monitorare qualsiasi tipo di dispositivo, tra cui computer, router, hub, toaster e jukeboxe.

sospensione. Interruzione di un processo che attende fino al normale completamento delle sue operazioni.

SPARC. Scalable processor architecture.

sscontrol. Fornisce l'interfaccia con il componente Site Selector di Load Balancer.

SSL. Secure Sockets Layer. Un diffuso schema di sicurezza sviluppato da Netscape Communications Corp. e RSA Data Security Inc. SSL consente al client di autenticare il server e far sì che tutti i dati e le richieste vengano cifrati. L'URL di un server sicuro protetto da SSL inizia con https (anziché HTTP).

ssserver. In Site Selector, gestisce le richieste dalla riga comandi al nome sito, al gestore e agli advisor.

Stato FIN. Lo stato di una transazione completata. Quando una transazione assume lo stato FIN, lo strumento di raccolta dei dati inutilizzati di Load Balancer può ripulire la memoria riservata per la connessione.

stazione di gestione della rete. Nel protocollo SNMP (Simple Network Management Protocol), una stazione che esegue programmi applicativi di gestione per il monitoraggio e il controllo degli elementi della rete.

strategia. Nella disponibilità elevata di Dispatcher, una parola chiave per specificare come viene eseguito il ripristino a seguito del malfunzionamento della macchina attiva.

strumento di raccolta delle metriche. Risiede nel consultant ed è responsabile della raccolta di una o più metriche.

Switch Cisco CSS. Qualsiasi switch della serie Cisco CSS 11000, utilizzato per l'inoltro dei pacchetti e l'instradamento dei contenuti.

Switch Nortel Alteon Web. Gli switch Nortel Alteon ACE Director Series e Nortel Alteon 180 Series del portafoglio switch Web Alteon, utilizzati per l'inoltro dei pacchetti e l'instradamento dei contenuti.

SYN. Un bit di controllo nel segmento in entrata, che occupa un numero in sequenza, utilizzato all'inizio di una connessione, per indicare dove inizia la numerazione della sequenza.

T

TCP. Transmission Control Protocol. Un protocollo di comunicazione utilizzato su Internet. TCP fornisce uno scambio di informazioni affidabile tra host. Utilizza IP come protocollo sottostante.

TCP/IP . Transmission Control Protocol/Internet Protocol. Una suite di protocolli progettata per consentire la comunicazione tra reti a prescindere dalle tecnologie di comunicazione utilizzate in ciascuna di esse.

Telnet. Protocollo emulazione di terminale, un protocollo applicativo TCP/IP per il servizio di connessione remota. Telnet consente a un utente in una sede di accedere a un host remoto come se la sua stazione di lavoro fosse connessa direttamente all'host remoto.

tempo di aderenza. L'intervallo compreso tra la chiusura di una connessione e l'apertura di una nuova connessione, durante il quale un client verrà rinviato allo stesso server utilizzato durante la prima connessione. Dopo questo intervallo, il client potrebbe essere indirizzato a un server diverso dal primo.

timeout. L'intervallo di tempo allocato per lo svolgimento di un'operazione.

tipo di regola. Nel bilanciamento del carico basato su regole, un indicatore delle informazioni da valutare per determinare se una regola è soddisfatta.

TOS. Type Of Service. Un campo da un byte nell'intestazione IP del pacchetto SYN.

TTL. Il TTL (time to live) DNS è il numero di secondi in cui un client può memorizzare nella cache la risposta della risoluzione nome.

U

UDP. User Datagram Protocol. Nella suite di protocolli Internet, un protocollo che fornisce un servizio datagramma non affidabile e indipendente dalla connessione. Consente a un programma applicativo su una macchina o a un processo di inviare un datagramma a un programma applicativo su un'altra macchina o a un altro processo. UDP utilizza IP (Internet Protocol) per la consegna dei datagrammi.

URI. Universal Resource Identifier. L'indirizzo codificato di qualsiasi risorsa sul Web, quale un documento HTML, un'immagine, un videoclip, un programma, e così via.

URL. Uniform Resource Locator. Un metodo standard per specificare la posizione di un oggetto, tipicamente una pagina Web, su Internet. Gli URL sono la forma di indirizzo utilizzata nel World-Wide Web. Vengono utilizzati nei documenti HTML per specificare la destinazione di un collegamento ipertestuale, spesso rappresentata da un altro documento HTML (che può anche essere memorizzato su un altro computer).

utente root. L'autorizzazione illimitata all'accesso e alla modifica di qualsiasi parte del sistema operativo AIX, Red Hat Linux o Solaris, normalmente associata all'utente incaricato di gestire il sistema.

V

VPN. Virtual Private Network, rete privata virtuale. Una rete costituita da uno o più tunnel IP sicuri che connettono due o più reti.

W

WAN. Wide Area Network. Una rete che fornisce servizi di comunicazione a un'area geografica più ampia di quella servita da una LAN o MAN e che può utilizzare o fornire funzionalità di comunicazione pubblica.

WAP. Wireless Application Protocol. Uno standard internazionale aperto per le applicazioni che utilizzano la connessione wireless, ad esempio l'accesso a Internet da un telefono cellulare.

WAS. WebSphere Application Server.

Web. La rete di server HTTP che contengono programmi e file, molti dei quali sono documenti ipertestuali, contenenti collegamenti ad altri documenti su server HTTP. Noto anche come World Wide Web.

WLM. Workload Manager. Un advisor fornito con Dispatcher. È progettato per funzionare solo insieme a server su mainframe OS/390 che eseguono il componente MVS Workload Manager (WLM).

Indice analitico

A

- accessibilità xvii
- add
 - Controller Cisco CSS 420
 - Controller Nortel Alteon 438
- aderenza (affinità)
 - aderenza (ignora affinità di porta) 213
 - affinità multiporta 215, 216
 - cookie attivo 217, 218
 - cookie passivo 217, 219
 - funzionamento 214
 - ignora affinità di porta 213
 - maschera indirizzo affinità 216
 - quiesce now 217
 - stickymask 215, 216
 - stickytime 53
 - tempo di aderenza 214, 215
 - URI 218
- advisor
 - cbrcontrol 339
 - componente CBR
 - advisor ssl2http 185
 - componente Dispatcher 181
 - advisor autonomo 186, 187
 - advisor Caching Proxy 185
 - arresto 342
 - avvio 69, 342
 - avvio/arresto 182
 - elenco di 184, 342
 - intervallo per 183, 342
 - nome di 339
 - nuovi tentativi server 178, 184
 - personalizzazione 188
 - porta per 346
 - report 343
 - report sullo stato di 342
 - rilevamento rapido degli errori 184
 - tentativi server 340
 - timeout connessione server 183, 339, 342
 - timeout report 183, 341
 - timeout ricezione server 183, 340, 342
 - versione di 343
- considerazioni su IPv6 82
- controller 240
 - personalizzazione 242
 - rilevamento rapido degli errori 241
 - tempo di inattività 241
 - tentativi dell'advisor sui server 241
 - timeout di connessione per i server 241
 - timeout di ricezione per i server 241
- dscontrol 339
- elenco di 341
- esempio personalizzato 473
- advisor (*Continua*)
 - file di configurazione di esempio 473
 - limitazione su Solaris 181
 - opzione URL, advisor HTTP 186
 - richiesta/risposta advisor HTTP 186
- Site Selector
 - arresto 394, 395
 - avvio 393, 395
 - elenco di 393, 395
 - intervallo 392
 - intervallo per 395
 - list 392
 - loglevel 392
 - nome di 392
 - nuovi tentativi server 184
 - porta per 339, 392
 - report sullo stato di 393, 395
 - rilevamento rapido degli errori 184
 - tentativi server 393
 - timeout connessione server 183, 392, 395
 - timeout report 394, 396
 - timeout ricezione server 183, 393, 395
 - versione di 394, 396
- sscontrol 392, 399
- advisor, componente Load Balancer
 - avvio 69
- advisor Caching Proxy 185
- advisor DB2 186
- advisor ftp 339, 392
- advisor http 339, 392
- advisor personalizzato 242
- advisor personalizzato (personalizzabile) 188
 - esempio 473
- advisor ssl2http 106, 185
- advisor WAS 186, 189
- advisor Workload Manager (WLM) 193, 247
- affinità (aderente)
 - aderenza (ignora affinità di porta) 213
 - affinità multiporta 215, 216
 - cookie attivo 217, 218
 - cookie passivo 217, 219
 - funzionamento 214
 - ignora affinità di porta 213
 - maschera indirizzo affinità 216
 - opzione regola 217
 - quiesce now 217
 - stickymask 215
 - tempo di aderenza 214, 215
 - URI 218, 220
- affinità (aderenza)
 - ID SSL (inoltre cbr) 53
 - stickymask 216
 - stickytime 53
- affinità (permanente)
 - affinità multiporta 369
- affinità (permanente) (*Continua*)
 - cookie attivo 378
 - cookie passivo 378
 - permanente (ignora affinità di porta) 382
 - quiesce now 364, 367
 - stickymask 370
 - stickytime 370, 378
 - URI 378
- affinità cookie attivo 217, 218, 378
- affinità cookie passivo 217, 219, 378
- affinità multiporta 215, 369
- affinità URI 218, 220, 378
- agenti secondari 257, 261
 - dscontrol 389
- aggiornamento della configurazione in modalità remota 256
- aggiunta
 - cluster 347
 - porta a un cluster 68, 373
 - server a una porta 68, 385, 412
- AIX
 - installazione 30
 - requisiti 29
- alias
 - NIC 67, 114
 - unità loopback 70
- amministrazione basata sul Web 253, 255
 - aggiornamento 256
- amministrazione remota 33, 36, 37, 38
 - amministrazione basata sul Web 253
 - Amministrazione basata sul Web 255
 - RMI 253, 254
- amministrazione remota (basata sul Web)
 - aggiornamento 256
- arresto
 - advisor 342, 394, 395
 - Controller Cisco CSS 269
 - Controller Nortel Alteon 270
 - executor 353
 - gestore 367, 403, 405
- attivo, contrassegnare un server
 - come 385, 411, 412
- avvertenze 481
- avvio
 - advisor 69, 342, 393, 395
 - CBR 98
 - Cisco CSS Controller 136
 - Controller Cisco CSS 269
 - Controller Nortel Alteon 154, 270
 - Dispatcher 45
 - executor 66, 353
 - gestore 69, 367, 402, 404
 - Metric Server 270
 - server 66
 - Site Selector 120, 269
- avvio e arresto
 - CBR 268
 - Dispatcher 260

avvisi
controller 249
Dispatcher, CBR, Site Selector 180

B

backup, disponibilità elevata 57, 357, 427, 445
configurazione 199
bilanciamento del carico basato su regole
connessioni al secondo 376
connessioni attive alla porta 376
contenuto delle richieste 53, 376
indirizzo IP client 375, 380, 408, 410
larghezza di banda condivisa 376, 380
larghezza di banda riservata 376, 380
metricall 408
metricavg 408
ora del giorno 375, 380, 408, 410
porta client 376
sempre true 376, 380, 408, 410
tipo di servizio (TOS, type of service) 376, 380
bilanciamento del carico in base alle regole 205
connessioni al secondo 208
connessioni attive sulla porta 208
contenuto delle richieste 212
indirizzo IP client 207
larghezza di banda condivisa 209
larghezza di banda riservata 209
media metrica 211
metric all 211
opzione di valutazione 213
opzione di valutazione server 213
ora del giorno 207
porta client 207
scelta di regole, per componente 206
sempre true 212
tipo di servizio (TOS, Type of service) 208
binlog
cbrcontrol 344
dscontrol 344
file di log binario, per statistiche server 344

C

Caching Proxy 105
configurazione per CBR 111
CBR
advisor e destinazioni finali
contrassegnano tutti i server come inattivi (Windows) 319
avvio e arresto 268
comando ifconfig 114
comportamento imprevisto della GUI
con schede Matrox AGP 318
con Caching Proxy
advisor ssl2http 106
configurazione 116
connessioni SSL 105
panoramica 104
parola chiave mapport 106

CBR (*Continua*)
configurazione
configurazione della macchina CBR 111
panoramica delle attività 107
creazione dell'alias della NIC 114
determinazione delle funzioni da utilizzare 23
disconnessione dall'host quando si utilizza l'amministrazione Web 318
errore di cbrcontrol 317
errore di cbrcontrol su Solaris 318
errore di lbadm 317
errore di sintassi o di configurazione 318
Errore memoria / thread di Java (HP-UX) 319
esempio di avvio rapido 97
impostazioni di bilanciamento del carico 176
nuovi tentativi dell'advisor sui server 184
mancata esecuzione 317
pianificazione 103
problema nella risoluzione dell'indirizzo IP su un nome host (Windows) 319
richieste non sottoposte a bilanciamento del carico 318
tabella di risoluzione dei problemi 284
utilizzo del componente Dispatcher 53
Visualizzazione di caratteri nazionali Latin-1 corrotti (Windows) 319
CBR (Content Based Routing)
impostazioni di bilanciamento del carico 176
tabella di risoluzione dei problemi 284
uso 268
CBR (Content Based Routing, instradamento basato sul contenuto)
utilizzo del componente Dispatcher 53
cbrserver
avvio 98
ccoserver
avvio 136
mancato avvio 293, 322
chiave privata
per l'autenticazione remota 254
chiave pubblica
per l'autenticazione remota 254
chiavi
lbkeys 192, 245
Cisco CSS Controller
advisor 240
advisor Workload Manager 247
avvisi 249
comando di aggiornamento che non aggiorna la configurazione 324
comportamento imprevisto della GUI
con schede Matrox AGP 323
disconnessione dall'host quando si utilizza l'amministrazione Web 324
errore di connessione consultant 323

Cisco CSS Controller (*Continua*)
Errore memoria / thread di Java (HP-UX) 324
esempio di avvio rapido 135
impostazioni di bilanciamento del carico 238
Metric Server 245
pesi non aggiornati dallo switch 324
registrazione binaria per le statistiche dei server 247
requisiti hardware e software 139
cluster
aggiunta 347
cbrcontrol 345
configurazione dell'indirizzo 67
definizione 67, 347
dscontrol 345
impostazione delle proporzioni 69
jolly 67
proportions 345
rimozione 348, 415
visualizzazione
stato di questo cluster 348
cluster jolly 67, 348
con Caching Proxy per proxy trasparente 230
per bilanciare il carico dei firewall 230
per combinare le configurazioni di server 229
collegamento esplicito 228
collocated (parola chiave) 385
comandi
cbrcontrol
advisor 339
binlog 344
cluster 345
executor 349
file 354
help 356
host 361
logstatus 362
manager 363
metric 368
port 369
rule 375
server 381
set 387
status 388
ccocontrol
consultant 420, 423
file 425
help 426
host 432
metriche 430
prompt 419
server, configurazione 435
Controller Cisco CSS 419
Controller Nortel Alteon 437
dscontrol
advisor 339
agente secondario, configurazione SNMP 389
binlog 344
cluster 345
disponibilità elevata, controllo 357, 445

- comandi (*Continua*)
 - dscontrol (*Continua*)
 - executor 349
 - file 354
 - help 356
 - host 361
 - logstatus 362
 - manager 363
 - metric 368
 - per controllare il gestore 69
 - per controllare l'advisor 69
 - per definire un indirizzo di non inoltro 66, 352
 - per definire un server 68
 - per definire una porta 68
 - port 369
 - prompt 338
 - rule 375
 - server 381
 - set 387
 - status 388
 - ifconfig 68, 224
 - per creare l'alias dell'unità loopback 71
 - instradamento
 - per eliminare un instradamento supplementare 74, 75
 - nalcontrol
 - consultant 438, 441
 - file 443
 - help 444
 - host 452
 - metrica 448
 - prompt 437
 - server, configurazione 450
 - ndcontrol
 - disponibilità elevata, controllo 427
 - netstat
 - per controllare gli indirizzi IP e gli alias 74
 - Site Selector 391
 - sscontrol
 - advisor 392
 - file 397
 - help 399
 - logstatus 400
 - manager 401
 - metric 406
 - nameserver 407
 - rule 408
 - server 411
 - set 413
 - sitename 414
 - status 417
- comandi dscontrol
 - prompt dei comandi 338
- comando cbrcontrol
 - advisor 339
 - binlog 344
 - cluster 345
 - executor 349
 - file 354
 - help 356
 - host 361
 - logstatus 362
 - manager 363
- comando cbrcontrol (*Continua*)
 - metric 368
 - port 369
 - rule 375
 - server 381
 - set 387
 - status 388
- comando ccocontrol
 - consultant 420, 423
 - file 425
 - help 426
 - host 432
 - metriche 430
 - prompt dei comandi 419
 - server 435
- comando dscontrol
 - advisor 69, 339
 - binlog 344
 - cluster 345
 - executor 66, 349
 - file 354
 - gestore 69
 - help 356
 - highavailability 357, 445
 - host 361
 - logstatus 362
 - manager 363
 - metric 368
 - port 369
 - porta 68
 - riduzione parametri comando 338
 - rule 375
 - server 68, 381
 - set 387
 - status 388
 - subagent 389
- comando ifconfig 68, 71, 114, 224
- comando nalcontrol
 - consultant 438, 441
 - file 443
 - help 444
 - host 452
 - metrica 448
 - prompt dei comandi 437
 - server 450
- comando ndcontrol
 - highavailability 427
- comando netstat 74
- comando route 74, 75
- comando sscontrol
 - advisor 392
 - file 397
 - help 399
 - logstatus 400
 - manager 401
 - metric 406
 - nameserver 407
 - rule 408
 - server 411
 - set 413
 - sitename 414
 - status 417
- componente Cisco CSS Controller
 - Visualizzazione di caratteri nazionali Latin-1 corrotti (Windows) 324
- componente Dispatcher
 - avvio 260
- componente Dispatcher (*Continua*)
 - configurazione
 - configurazione della macchina Load Balancer 64
 - impostazione di una rete privata 228
 - panoramica delle attività 61
 - HA (high availability), suggerimenti sulla configurazione 310
 - impostazioni di bilanciamento del carico 176
 - indice di arrotondamento 179
 - intervalli dell'advisor 183
 - intervalli gestore 179
 - nuovi tentativi dell'advisor sui server 178, 184
 - pesi 177
 - proporzione di importanza attribuita alle informazioni sullo stato 176
 - soglia di sensibilità 179
 - timeout dell'advisor per i server 183
 - timeout report dell'advisor 183
 - inoltro MAC 51
 - instradamento basato sul contenuto 53
 - messaggio di avvertenza Java che viene visualizzato quando si installano le fix di servizio 316
 - NAT/NAPT 51
 - pianificazione 49
 - ripristino di un server guasto 178
 - ripristino server inattivi 372
 - ritardo quando si carica la configurazione di Load Balancer 308
 - su Linux, Dispatcher inoltra i pacchetti, ma questi non vengono ricevuti dal server di backend 314
 - su Linux, limitazioni quando si utilizzano server zSeries o S/390 312
 - su Linux, mancanza di memoria quando si utilizzano il gestore e gli advisor 314
 - su Solaris, non è possibile aggiungere i server IPv6 alla configurazione 316
 - su Windows, si verifica un problema con il takeover HA 315
 - supporto IPv6 79
 - uso 259
- Componente Dispatcher
 - advisor e destinazioni finali contrassegnano tutti i server come inattivi (Windows) 304
 - aggiornamento di Java fornito con l'installazione 317
 - alias restituito al posto dell'indirizzo locale 301
 - cdisponibilità elevata onflitto di indirizzi IP quando si utilizza la disponibilità elevata 308
 - comportamento imprevisto con "rmmod ibmlb" 302

Componente Dispatcher (*Continua*)
 comportamento imprevisto della GUI
 con schede Matrox AGP 302
 comportamento imprevisto durante il
 caricamento di un file di
 configurazione di grandi
 dimensioni 300
 connessione a una macchina in
 remoto 296
 disconnessione dall'host quando si
 utilizza l'amministrazione Web 303
 disponibilità elevata nella modalità
 wide area di Load Balancer non
 funziona 299
 errore di dscontrol 296
 errore di lbadmin 296
 Errore memoria / thread di Java
 (HP-UX) 304
 errore quando è installato Caching
 Proxy 297
 font coreani indesiderati su AIX e
 Linux 301
 gli indirizzi IP non vengono risolti
 sulla connessione remota 301
 GUI non avviata correttamente 297
 GUI non visualizzata
 correttamente 298
 Il percorso di Discovery impedisce il
 traffico di ritorno con Load
 Balancer 298
 il server non risponde 294
 impossibile aggiungere heartbeat 295
 impossibile aprire la finestra della
 guida 297
 impossibile inoltrare un frame 298
 indirizzo router non specificato o non
 valido per il metodo della
 porta 307
 instradamenti in eccesso
 (Windows) 295
 interruzione dei processi di Load
 Balancer (Solaris) 308
 lbadmin si scollega dal server dopo
 l'aggiornamento della
 configurazione 301
 le richieste dei client non riescono
 quando si tenta di restituire risposte
 con pagine di grandi
 dimensioni 309
 macchina primaria e di riserva attive
 in una configurazione a disponibilità
 elevata 309
 mancata esecuzione 294
 mancata registrazione dei carichi del
 server 303
 mancato funzionamento degli
 advisor 296
 mancato funzionamento degli advisor
 in un'installazione a disponibilità
 elevata dopo un'interruzione della
 rete (Windows) 306
 mancato funzionamento della
 disponibilità elevata 295
 Mancato funzionamento di MS IIS e
 SSL 296

Componente Dispatcher (*Continua*)
 non utilizzare il comando IP address
 add per creare alias di loopback
 (Linux) 307
 problema nella risoluzione
 dell'indirizzo IP su un nome host
 (Windows) 305
 richieste non bilanciate 294
 scomparsa delle finestre della
 guida 298
 server Web con binding a 0.0.0.0 303
 su Linux, il Dispatcher HA non viene
 sincronizzato 310
 su Windows, viene restituito il
 messaggio "Il server non
 risponde" 309
 tabella di risoluzione dei
 problemi 278
 tempo di risposta eccessivo 302
 Visualizzazione di caratteri nazionali
 Latin-1 corrotti (Windows) 304
 visualizzazione di una schermata blu
 all'avvio dell'executor 298
 componenti prodotto 49
 configurazione
 attività, avanzate 175
 attività, avanzato 195
 avvio del consultant 149, 171
 cbrwizard 110
 componente Dispatcher 61
 Content Based Routing 107
 Controller Cisco CSS 145
 Controller Nortel Alteon 167
 definizione del consultant dello
 switch 170
 disponibilità elevata 171
 Disponibilità elevata 149
 dswizard 64
 file di esempio 467
 metodi
 GUI (CBR) 109
 GUI (Controller Cisco CSS) 147
 GUI (Controller Nortel
 Alteon) 169
 GUI (Dispatcher) 62
 GUI (Site Selector) 129
 procedura guidata (CBR) 110
 procedura guidata
 (Dispatcher) 64
 procedura guidata (Site
 Selector) 129
 riga comandi (CBR) 108
 riga comandi (Controller Cisco
 CSS) 145
 riga comandi (Controller Nortel
 Alteon) 167
 riga comandi (Dispatcher) 62
 riga comandi (Site Selector) 127
 script (CBR) 109
 script (Cisco CSS Controller) 146
 script (Controller Nortel
 Alteon) 168
 script (Dispatcher) 62
 script (Site Selector) 128
 metriche 149, 171
 servizio 170
 Site Selector 127

configurazione (*Continua*)
 sswizard 129
 verifica 75, 150, 172
 connecttimeout
 Site Selector 392
 connessioni, impostazione della
 proporzione di importanza 177, 348
 connessioni SSL
 advisor HTTPS 184
 advisor SSL 185
 configurazione di ibmproxy 105
 per CBR 105, 106
 problemi di abilitazione 296
 consultant
 avvio 149, 171
 ccocontrol 420, 423
 Controller Cisco CSS
 add 420
 binarylog 420
 report 420
 Controller Nortel Alteon
 add 438
 binarylog 438
 report 438
 nalcontrol 438, 441
 consultant dello switch
 definizione 170
 Content Based Routing
 configurazione
 configurazione della macchina
 CBR 111
 panoramica delle attività 107
 pianificazione 103
 contrassegnare un server come
 attivo 385, 411, 412
 inattivo 385, 411, 412
 controller
 advisor personalizzato
 (personalizzabile) 242
 Controller Cisco CSS
 loglevel 421, 423
 logsize 421, 423
 report 423
 set 423
 Controller Nortel Alteon
 loglevel 439, 441
 logsize 439, 441
 report 441
 set 441
 impostazioni di bilanciamento del
 carico
 importanza attribuita alle
 informazioni metriche 238
 pesi 239
 soglia di sensibilità 239
 tempi di inattività 239
 tempi di inattività
 dell'advisor 241
 tentativi dell'advisor sui
 server 241
 timeout dell'advisor per i
 server 241
 peso fisso 239
 Controller Cisco CSS
 avvio 269
 avvio e arresto 269
 comandi 419

Controller Cisco CSS (*Continua*)

- configurazione
 - configurazione della macchina CSS 148
 - esempio 15
 - panoramica delle attività 145
- determinazione delle funzioni da utilizzare 27
- disponibilità elevata 235
- errore di ccocontrol 322
- errore di lbadmim 322
- impossibile creare il registro sulla porta 13099 323
- mancato avvio 322
- pianificazione 139
- posizionare 235
- report
 - controller 423
- tabella di risoluzione dei problemi 287
- uso 269

Controller Nortel Alteon

- advisor 240
- advisor Workload Manager 247
- avvio e arresto 270
- avvisi 249
- comandi 437
- comando di aggiornamento che non aggiorna la configurazione 326
- comportamento imprevisto della GUI con schede Matrox AGP 326
- configurazione
 - configurazione della macchina Controller Nortel Alteon 170
 - panoramica delle attività 167
- disconnessione dall'host quando si utilizza l'amministrazione Web 326
- disponibilità elevata 235
- errore di connessione consultant 326
- errore di lbadmim 325
- errore di nalcontrol 325
- Errore memoria / thread di Java (HP-UX) 327
- esempio di avvio rapido 153
- impossibile creare il registro sulla porta 14099 325
- impostazioni di bilanciamento del carico 238
- mancato avvio 325
- Metric Server 245
- pesi non aggiornati dallo switch 326
- pianificazione 157
- posizionare 235
- registrazione binaria per le statistiche dei server 247
- report
 - controller 441
- requisiti hardware e software 157
- tabella di risoluzione dei problemi 288
- uso 270
- visualizzazione di caratteri nazionali Latin-1 corrotti (Windows) 327

definizione

- cluster 347
- indirizzo di non inoltrare 66, 352
- porta a un cluster 68, 373
- server a una porta 68, 385, 412

diagnosi dei problemi

- advisor e destinazioni finali
 - contrassegnano tutti i server come inattivi (Windows) 304, 319, 322
- aggiornamento di Java fornito con l'installazione 317
- alias restituito al posto dell'indirizzo locale 301
- cdisponibilità elevata onflitto di indirizzi IP quando si utilizza la disponibilità elevata 308
- comando di aggiornamento che non aggiorna la configurazione 324, 326
- comportamento imprevisto con "rmmod ibmlb" 302
- comportamento imprevisto della GUI con schede Matrox AGP 302, 318, 321, 323, 326
- comportamento imprevisto durante il caricamento di un file di configurazione di grandi dimensioni 300
- disconnessione dall'host quando si utilizza l'amministrazione Web 303, 318, 321, 324, 326
- Dispatcher, Microsoft IIS e SSL non funzionano 296
- Dispatcher e il server non rispondono 294
- disponibilità elevata nella modalità wide area di Load Balancer non funziona 299
- errore dei comandi cbrcontrol o lbadmim 317
- errore dei comandi ccocontrol o lbadmim 322
- errore dei comandi dscontrol o lbadmim 296
- errore dei comandi nalcontrol o lbadmim 325
- errore dei comandi sscontrol o lbadmim 320
- errore di cbrcontrol su Solaris 318
- errore di connessione consultant 323, 326
- Errore di sintassi o di configurazione 318
- errore durante l'esecuzione di Dispatcher con Caching Proxy installato 297
- Errore memoria / thread di Java (HP-UX) 304, 319, 322, 324, 327
- font coreani indesiderati su AIX e Linux 301
- gli indirizzi IP non vengono risolti sulla connessione remota 301
- GUI non avviata correttamente 297
- GUI non visualizzata correttamente 298
- HA (high availability), suggerimenti sulla configurazione 310

diagnosi dei problemi (*Continua*)

- Il percorso di Discovery impedisce il traffico di ritorno con Load Balancer 298
- il valore della metrica restituisce -1 dopo l'avvio di Metric Server 331
- Impossibile aggiungere heartbeat 295
- impossibile creare il registro sulla porta 13099 323
- impossibile creare il registro sulla porta 14099 325
- impostazione di metric server in una configurazione a due livelli 328
- indirizzo router non specificato o non valido per il metodo della porta 307
- instradamenti in eccesso 295
- interruzione dei processi di Load Balancer (Solaris) 308
- lbadmim si scollega dal server dopo l'aggiornamento della configurazione 301
- le richieste dei client non riescono quando si tenta di restituire risposte con pagine di grandi dimensioni 309
- Load Balancer non può elaborare e inoltrare un frame 298
- macchina primaria e di riserva attive in una configurazione a disponibilità elevata 309
- mancata esecuzione di CBR 317
- Mancata esecuzione di Dispatcher 294
- Mancata esecuzione di Site Selector 320
- mancata registrazione dei carichi del server 303
- mancato avvio di ccoserver 322
- Mancato avvio di nalserver 325
- mancato avvio di sserver su Windows 321
- mancato funzionamento degli advisor 296
- mancato funzionamento degli advisor in un'installazione a disponibilità elevata dopo un'interruzione della rete (Windows) 306
- mancato funzionamento della disponibilità elevata di Dispatcher 295
- messaggio di avvertenza Java che viene visualizzato quando si installano le fix di servizio 316
- messaggio di errore quando si tenta di visualizzare la guida in linea 297
- Metric Server IOException su Windows 327
- Metric Server non notifica i carichi 327
- nel log di Metric Server è riportato "La firma è necessaria per l'accesso all'agente" 328
- non utilizzare il comando IP address add per creare alias di loopback (Linux) 307

D

default.cfg 66, 113, 130

diagnosi dei problemi (*Continua*)

- numeri di porta utilizzati da CBR 291
- numeri di porta utilizzati da Cisco CSS Controller 293
- numeri di porta utilizzati da Controller Nortel Alteon 293
- numeri di porta utilizzati da Dispatcher 290
- numeri di porta utilizzati da Site Selector 292
- pesi non aggiornati dallo switch 324, 326
- problema nella risoluzione dell'indirizzo IP su un nome host (Windows) 305, 319
- problemi comuni e soluzioni 294, 296, 317, 320, 322, 325, 327
- Richieste di Dispatcher non inoltrate 294
- richieste non sottoposte a bilanciamento del carico 318
- ritardo quando si carica la configurazione di Load Balancer 308
- scomparsa dei pannelli di aiuto 298
- server Web con binding a 0.0.0.0 303
- Site Selector non esegue correttamente il bilanciamento del carico 321
- Site Selector non esegue il round-robin (Solaris) 320
- su AIX, l'output del comando ps -vg risulta corrotto 328
- su Linux, Dispatcher inoltra i pacchetti, ma questi non vengono ricevuti dal server di backend 314
- su Linux, il Dispatcher HA non viene sincronizzato 310
- su Linux, limitazioni quando si utilizzano server zSeries o S/390 312
- su Linux, si verifica una mancanza di memoria quando si utilizza il gestore e gli advisor 314
- su sistemi Linux, non è possibile richiamare i valori da metric server 330
- su Solaris, gli script producono messaggi console indesiderati 329
- su Solaris, non è possibile aggiungere i server IPv6 alla configurazione 316
- su Windows, si verifica un problema con il takeover HA 315
- su Windows, viene restituito il messaggio "Il server non risponde" 309
- tempo di risposta eccessivo 302
- visualizzazione di caratteri nazionali Latin-1 corrotti (Windows) 327
- Visualizzazione di caratteri nazionali Latin-1 corrotti (Windows) 304, 319, 321, 324
- visualizzazione di una schermata blu all'avvio dell'executor di Load Balancer 298

diagrammi della sintassi

- esempi 335
- lettura 335
- parametri 335
- punteggiatura 335
- simboli 335

disattivazione di un server 217, 364, 366, 367

disinstallazione

- in AIX 30
- in Linux 35
- in Solaris 37
- in Windows 38
- su HP-UX 34

Dispatcher

- configurazione
 - configurazione di server backend 70
 - determinazione delle funzioni da utilizzare 19
- disponibilità elevata 57
 - configurazione 171
 - considerazioni su IPv6 83
 - Controller Cisco CSS 235
 - Controller Nortel Alteon 235
 - dscontrol 357, 445
 - primaryhost 347, 348
 - reciproca 58, 347, 348, 359
- Disponibilità elevata 5, 6
 - configurazione 149
 - ndcontrol 427
- disponibilità elevata reciproca 58, 199, 200
 - primaryhost 347, 348
 - script 203
 - takeover 202
- DPID2 262
- dsserver
 - avvio 45

E

eliminazione

- cluster 348, 415
- instradamento supplementare 74
- porta da un cluster 373
- server da una porta 385, 411, 412

esempi

- avvio rapido
 - CBR 97
 - Cisco CSS Controller 135
 - Controller Nortel Alteon 153
 - Site Selector 119
- gestione dei server locali 10, 11, 12, 14, 15
- rapida 43

esempio di avvio rapido

- CBR 97
- Cisco CSS Controller 135
- Controller Nortel Alteon 153
- Site Selector 119

esempio rapido 43

executor

- arresto 353
- avvio 353
- cbrcontrol 349
- dscontrol 349

F

file

- cbrcontrol 109, 354
- ccocontrol 425
- dscontrol 62, 354
- nalcontrol 443
- sscontrol 128, 397

file di configurazione di esempio 467

- advisor 473
- componente Dispatcher (AIX) 467
- componente Dispatcher (Windows) 470

file mappatura indirizzo

- esempio di 229

Firewall (limitazioni) 38

funzionamento di Load Balancer 253

G

gestione di Load Balancer 253

gestore

- arresto 367, 403, 405
- avvio 69, 367, 402, 404
- peso fisso 178
- proporzioni 176
- versione di 367, 403, 405

goActive 203

goIdle 204

goInOp 203

goStandby 203

GRE (Generic Routing Encapsulation)

- Linux 227
- OS/390 227
- supporto rete geografica 227

guasto, contrassegnare un server

- come 385, 411, 412

GUI

- CBR 109
- Controller Cisco CSS 147
- Controller Nortel Alteon 169
- Dispatcher 63
- istruzioni generali 455
- risoluzione 298
- Site Selector 129

H

help

- cbrcontrol 356
- ccocontrol 426
- dscontrol 356
- nalcontrol 444

High Availability (HA) 198

- configurazione 199
- inoltro nat 203
- Linux per S/390 204
- reciproca 200
- script 202
 - goActive 203
 - goIdle 204
 - goInOp 203
 - goStandby 203
 - highavailChange 204

highavailChange 204

host

- cbrcontrol 361

host (*Continua*)

- cococontrol 432
- dscontrol 361
- nalcontrol 452

hostprincipale 200

HP-UX

- comando arp publish 68
- installazione 33
- requisiti 33

I

IBM Firewall (limitazioni) 38

ibmlb.conf

- configurazione per Solaris 65

ibmproxy 105, 111

ignora affinità di porta

- server 213, 382, 385

impostazione

- dimensione massima del log

 - per il gestore 366, 401, 403

 - per l'advisor 257, 342, 393, 395

- frequenza con cui il gestore richiede le

 - informazioni all'executor 179, 366

- indice di arrotondamento 180, 367,

 - 402, 404

- indirizzo cluster 68

- indirizzo di non inoltro 64

- intervallo

 - l'advisor richiede informazioni ai

 - server 342, 395

 - per il gestore per aggiornare

 - l'executor 179, 366, 401, 403

- Livello di registrazione

 - per il gestore 401

 - per l'advisor 257, 342, 395

- nome del file di log 394

 - per il gestore 402

- peso massimo

 - per i server su una porta

 - specifica 177, 373

- peso per un server 366, 367, 385, 411

- proporzione di importanza nel

 - bilanciamento del carico 348

- sensibilità per l'aggiornamento dei

 - pesi 179, 367, 402, 404

impostazioni, visualizzazione di tutti i

- valori globali

 - per il gestore 367, 403, 404

 - per un advisor 343, 394, 395

impostazioni di bilanciamento del carico

- (ottimizzazione) 176, 238

indice di arrotondamento,

- impostazione 180, 367, 402, 404

indirizzo di non inoltro

- definizione 66

- impostazione 352

informazioni, raccolta 273

installazione

- in AIX 30

- in Linux 35

- in Solaris 36

- in Windows 38

- Load Balancer 29

- su HP-UX 33

instradamenti, rimozione

- supplementari 74

instradamenti, supplementari 74

instradamenti supplementari 74

Instradamento basato sul contenuto 5

interfaccia utente grafica (GUI)

- CBR 109

- Cisco CSS Controller 147

- Controller Nortel Alteon 169

- Dispatcher 62

- istruzioni generali 455

- Site Selector 129

intervallo, impostazione della frequenza

- il gestore aggiorna i pesi

 - sull'executor 179, 366, 401, 403

- il gestore richiede informazioni

 - all'executor 179, 366

- l'advisor richiede informazioni ai

 - server 342, 395

K

keys

- lbkeys 254

L

lbkeys 192, 246, 254

lbwebaccess 255, 256

Linux

- Disponibilità elevata su S/390 204

- installazione 35

- requisiti 34

Load Balancer

- attività di configurazione,

 - avanzate 175

- attività di configurazione,

 - avanzato 195

- configurazione

 - CBR 107

 - componente Dispatcher 64, 111,

 - 130

 - Controller Cisco CSS 145

 - Controller Nortel Alteon 167

 - Site Selector 127

- considerazioni sulla

 - pianificazione 49, 123

- esempio di avvio rapido

 - CBR 97

 - Cisco CSS Controller 135

 - Controller Nortel Alteon 153

 - Site Selector 119

- esempio rapido 43

 - funzionamento e gestione 253, 269,

 - 270

 - funzioni 3, 9

 - installazione 29

 - panoramica 3, 9

 - risoluzione dei problemi 273

 - supporto IPv6 79

 - vantaggi 4

Load Balancer per IPv4 e IPv6 79

- abilitazione dei pacchetti IPv6 85

- advisor, uso 82

- autoconf6, AIX 85

- comandi dscontrol 90

- considerazioni sulla

 - configurazione 81

Load Balancer per IPv4 e IPv6 (*Continua*)

- creazione dell'alias del dispositivo

 - loopback 86

- differenze di sintassi dei comandi 89

- disponibilità elevata 83

- dsconfig 86

- funzioni non supportate 82

- ifconfig 86

- indirizzo locale di collegamento 81

- ip addr 86

- Metric Server 84

- modprobe, Linux 85

- posizionamento 83

- supporto piattaforme 80

log

- binario, per statistiche server 233

- dimensioni, impostazione

 - per il consultant 258

 - per il gestore 257, 366, 401, 403

 - per il server 257, 258

 - per l'advisor 257, 342, 393, 395

 - per l'agente secondario 257, 258

- file, configurazione del nome di

 - per il gestore 402

 - per l'advisor 394

- livello, impostazione

 - per il consultant 258

 - per il gestore 257, 401

 - per il server 257, 258

 - per l'advisor 257, 342, 395

 - per l'agente secondario 257

- uso dei log di CBR 269

- uso dei log di Controller Cisco

 - CSS 270

- uso dei log di Load Balancer 257

- uso dei log di Metric Server 271

- uso dei log di Site Selector 269

logstatus

- cbrcontrol 362

- dscontrol 362

- sscontrol 400

loopback

- alternative per aggiungere l'alias per

 - Linux 76

M

manager

- cbrcontrol 363

- dscontrol 363

- sscontrol 401

marchi 483

maschera indirizzo affinità 216, 370

metodo di inoltro

- cbr 53, 54

- mac 51, 52

- mac, nat o cbr 54, 371

- nat 54

- NAT 51

metodo di inoltro cbr 53, 54

- stickytime 53

metodo di inoltro nat 54

metodo di inoltro NAT 51

metodo di instradamento mac 51

metodo inoltro NAT

- script disponibilità elevata 203

- metric
 - cbrcontrol 368
 - dscontrol 368
 - sscontrol 406
- Metric Server
 - avvio e arresto 270
 - considerazioni su IPv6 84
 - il valore della metrica restituisce -1
 - dopo l'avvio di Metric Server 331
 - impostazione di metric server in una
 - configurazione a due livelli 328
 - Metric Server IOException su
 - Windows 327
 - Metric Server non notifica i
 - carichi 327
 - nel log di Metric Server è riportato
 - "La firma è necessaria per l'accesso all'agente" 328
 - panoramica 191, 245
 - su AIX, l'output del comando ps -vg
 - risulta corrotto 328
 - su sistemi Linux, non è possibile
 - richiamare i valori da metric server 330
 - su Solaris, gli script producono
 - messaggi console indesiderati 329
 - tabella di risoluzione dei
 - problemi 289
 - uso 270
- metrica
 - nalcontrol 448
- metriche
 - cococontrol 430
 - configurazione 149, 171
- metriche del sistema
 - configurazione 430
 - impostazione della proporzione di
 - importanza 177, 238
- metriche di sistema
 - configurazione 448
 - configure 368, 406
 - impostazione della proporzione di
 - importanza 345, 346
- migrazione 29

N

- nalserver
 - avvio 154
 - mancato avvio 325
- nameserver
 - sscontrol 407
- NAPT (Network Address Port
 - Translation) 51
- NAT (Network Address Translation) 51
- nat, posizionamento server con 197
- NIC
 - alias 67
 - ethernet (per Solaris) 65
 - mappatura (per Windows) 67
- NIC Ethernet
 - ibmlb.conf
 - configurazione per Solaris 65
- Nortel Alteon Consultant
 - determinazione delle funzioni da
 - utilizzare 28

- nuove connessioni, impostazione della
 - proporzione di importanza 176, 346
- nuove funzioni, V6.1
 - advisor SIP 7
 - configurazione client posizionata 7
 - supporto per HP-UX Itanium
 - 64-bit 6
 - supporto per il browser Firefox 7
 - supporto per Linux zSeries 64-bit 7
 - supporto senza kernel 6
 - supporto spazio utente 6

O

- opzione del menu Monitor 261
- opzioni di prossimità 126
- OS/390
 - supporto GRE 227

P

- panoramica
 - configurazione del componente
 - Dispatcher 61
 - configurazione di CBR 107
 - configurazione di Controller Cisco
 - CSS 145
 - configurazione di Controller Nortel
 - Alteon 167
 - configurazione di Site Selector 127
- permanente (affinità)
 - affinità multiporta 369
 - cookie attivo 378
 - cookie passivo 378
 - permanente (ignora affinità di
 - porta) 382
 - quiesce now 364, 367
 - stickymask 370
 - stickytime 370, 378
 - URI 378
- peso
 - come il gestore imposta 178
 - controller 239
 - impostazione
 - limite per tutti i server su una
 - porta 177, 373
 - per un server 385, 411
- peso massimo, impostazione
 - per i server su una porta
 - specifica 177, 373
- pianificazione
 - CBR 103
 - componente Dispatcher 49
 - Controller Cisco CSS 139
 - Controller Nortel Alteon 157
 - Site Selector 123
- pianificazione dell'installazione 3, 9, 49, 123
- port
 - cbrcontrol 369
 - dscontrol 369
 - porta jolly 68, 373
 - advisor ping 185
 - per indirizzare il traffico per una
 - porta non configurata 231
 - per la gestione del traffico FTP 231

- porte
 - aggiunta 373
 - definizione di un cluster 68, 373
 - impostazione del peso massimo 177, 373
 - jolly 68
 - per gli advisor 339, 392
 - rimozione 373
 - visualizzazione
 - stato dei server su questa
 - porta 373
- posiziona con nat 197
- posizionamento con più indirizzi 69
- posizionare
 - considerazioni su IPv6 83
 - Controller Cisco CSS 235
 - Controller Nortel Alteon 235
- posizionare, Load Balancer e client 234
- posizionare, Load Balancer e server 64, 69, 196, 224, 382, 385
- posizionato (parola chiave) 197
- primaryhost 348
- procedura guidata, configurazione
 - CBR 110
 - Dispatcher 64
 - Site Selector 129
- proporzione di importanza per il
 - bilanciamento del carico,
 - impostazione 176, 348
- prossimità della rete 126

R

- raccolta delle informazioni 273
- registrazione binaria per le statistiche dei
 - server 233, 258, 259
 - controller 247
- regola contenuto 53, 212
- remove
 - cluster 348, 415
 - instradamento supplementare 74
 - porta da un cluster 373
 - server da una porta 385, 411, 412
- report
 - Controller Cisco CSS 423
 - Controller Nortel Alteon 441
- report istantanea delle statistiche,
 - visualizzazione 366, 402, 403
- requisiti
 - AIX 29
 - HP-UX 33
 - Linux 34
 - Solaris 36
 - Windows 38
- requisiti hardware
 - Cisco CSS Controller 139
 - Controller Nortel Alteon 157
- requisiti software
 - Cisco CSS Controller 139
 - Controller Nortel Alteon 157
- rete privata, uso di Dispatcher 228
- riavviare tutti i server con i pesi
 - normalizzati 366, 402, 404
- ricerca
 - instradamento supplementare 74
- referimenti sui comandi
 - come leggere 335

- riga comandi
 - esempio di configurazione
 - CBR 98
 - Cisco CSS Controller 136
 - Controller Nortel Alteon 154
 - Dispatcher 45
 - Site Selector 120
 - Send command (GUI) 460
- Rilevamento attacco di tipo Denial of service 231
 - halfopenaddressreport 373
 - maxhalfopen 372
- risoluzione, GUI 298
- risoluzione dei problemi 273
 - advisor e destinazioni finali
 - contrassegnano tutti i server come inattivi (Windows) 304, 319, 322
 - aggiornamento di Java fornito con l'installazione 317
 - alias restituito al posto dell'indirizzo locale 301
 - cdisponibilità elevata onflitto di indirizzi IP quando si utilizza la disponibilità elevata 308
 - comando di aggiornamento che non aggiorna la configurazione 324, 326
 - comportamento imprevisto con "rmmod ibmlb" 302
 - comportamento imprevisto della GUI con schede Matrox AGP 302, 318, 321, 323, 326
 - comportamento imprevisto durante il caricamento di un file di configurazione di grandi dimensioni 300
 - disconnessione dall'host quando si utilizza l'amministrazione Web 303, 318, 321, 324, 326
 - Dispatcher, Microsoft IIS e SSL non funzionano 296
 - Dispatcher e il server non rispondono 294
 - disponibilità elevata nella modalità wide area di Load Balancer non funziona 299
 - errore dei comandi cbrcontrol o lbadmim 317
 - errore dei comandi ccocontrol o lbadmim 322
 - errore dei comandi dscontrol o lbadmim 296
 - errore dei comandi nalcontrol o lbadmim 325
 - errore dei comandi sscontrol o lbadmim 320
 - errore di cbrcontrol su Solaris 318
 - errore di connessione consultant 323, 326
 - Errore di sintassi o di configurazione 318
 - errore durante l'esecuzione di Dispatcher con Caching Proxy installato 297
 - Errore memoria / thread di Java (HP-UX) 304, 319, 322, 324, 327
 - font coreani indesiderati su AIX e Linux 301
- risoluzione dei problemi (*Continua*)
 - gli indirizzi IP non vengono risolti sulla connessione remota 301
 - GUI non avviata correttamente 297
 - GUI non visualizzata correttamente 298
 - HA (high availability), suggerimenti sulla configurazione 310
 - Il percorso di Discovery impedisce il traffico di ritorno con Load Balancer 298
 - il valore della metrica restituisce -1 dopo l'avvio di Metric Server 331
 - Impossibile aggiungere heartbeat 295
 - impossibile creare il registro sulla porta 13099 323
 - impossibile creare il registro sulla porta 14099 325
 - impostazione di metric server in una configurazione a due livelli 328
 - indirizzo router non specificato o non valido per il metodo della porta 307
 - instradamenti in eccesso 295
 - interruzione dei processi di Load Balancer (Solaris) 308
 - lbadmim si scollega dal server dopo l'aggiornamento della configurazione 301
 - le richieste dei client non riescono quando si tenta di restituire risposte con pagine di grandi dimensioni 309
 - Load Balancer non può elaborare e inoltrare un frame 298
 - macchina primaria e di riserva attive in una configurazione a disponibilità elevata 309
 - mancata esecuzione di CBR 317
 - Mancata esecuzione di Dispatcher 294
 - Mancata esecuzione di Site Selector 320
 - mancata registrazione dei carichi del server 303
 - mancato avvio di ccserver 322
 - Mancato avvio di nalservice 325
 - mancato avvio di ssservice su Windows 321
 - mancato funzionamento degli advisor 296
 - mancato funzionamento degli advisor in un'installazione a disponibilità elevata dopo un'interruzione della rete (Windows) 306
 - mancato funzionamento della disponibilità elevata di Dispatcher 295
 - messaggio di avvertenza Java che viene visualizzato quando si installano le fix di servizio 316
 - messaggio di errore quando si tenta di visualizzare la guida in linea 297
 - Metric Server IOException su Windows 327
 - Metric Server non notifica i carichi 327
- risoluzione dei problemi (*Continua*)
 - nel log di Metric Server è riportato "La firma è necessaria per l'accesso all'agente" 328
 - non utilizzare il comando IP address add per creare alias di loopback (Linux) 307
 - numeri di porta utilizzati da CBR 291
 - numeri di porta utilizzati da Cisco CSS Controller 293
 - numeri di porta utilizzati da Controller Nortel Alteon 293
 - numeri di porta utilizzati da Dispatcher 290
 - numeri di porta utilizzati da Site Selector 292
 - pesi non aggiornati dallo switch 324, 326
 - problema nella risoluzione dell'indirizzo IP su un nome host (Windows) 305, 319
 - problemi comuni e soluzioni 294, 296, 317, 320, 322, 325, 327
 - Richieste di Dispatcher non inoltrate 294
 - richieste non sottoposte a bilanciamento del carico 318
 - ritardo quando si carica la configurazione di Load Balancer 308
 - scomparsa dei pannelli di aiuto 298
 - server Web con binding a 0.0.0.0 303
 - Site Selector non esegue correttamente il bilanciamento del carico 321
 - Site Selector non esegue il round-robin (Solaris) 320
 - su AIX, l'output del comando ps -vg risulta corrotto 328
 - su Linux, Dispatcher inoltra i pacchetti, ma questi non vengono ricevuti dal server di backend 314
 - su Linux, il Dispatcher HA non viene sincronizzato 310
 - su Linux, limitazioni quando si utilizzano server zSeries o S/390 312
 - su Linux, si verifica una mancanza di memoria quando si utilizza il gestore e gli advisor 314
 - su sistemi Linux, non è possibile richiamare i valori da metric server 330
 - su Solaris, gli script producono messaggi console indesiderati 329
 - su Solaris, non è possibile aggiungere i server IPv6 alla configurazione 316
 - su Windows, si verifica un problema con il takeover HA 315
 - su Windows, viene restituito il messaggio "Il server non risponde" 309
 - tempo di risposta eccessivo 302
 - visualizzazione di caratteri nazionali Latin-1 corrotti (Windows) 327

- risoluzione dei problemi (*Continua*)
 - Visualizzazione di caratteri nazionali
 - Latin-1 corrotti (Windows) 304, 319, 321, 324
 - visualizzazione di una schermata blu all'avvio dell'executor di Load Balancer 298
- RMI (Remote Method Invocation) 33, 36, 37, 38, 253, 254
- rule
 - cbrcontrol 375
 - dscontrol 375
 - sscontrol 408

S

- script 202
 - ccoserverdown 249
 - goActive 203
 - goldle 204
 - goInOp 203
 - goStandby 203
 - highavailChange 204
 - uscita utente 180, 249
- script di uscita utente 180, 249
 - ccoallserversdown 249
 - ccoserverdown 249
 - ccoserverup 249
 - managerAlert 180
 - managerClear 180
 - nalallserversdown 249
 - naloserverup 249
 - nalserverdown 249
 - rilevamento denial of service 232
 - serverDown 180
 - serverUp 180
- sensibilità per l'aggiornamento dei pesi, impostazione 179, 367, 402, 404
- server
 - address 381
 - advisorrequest 384
 - advisorresponse 384
 - aggiunta 385, 412
 - attivazione 367
 - cbrcontrol 381
 - ccocontrol 435
 - collocated 382, 385
 - contrassegnare come attivo 385, 411, 412
 - contrassegnare come inattivo 385, 411, 412
 - cookievalue 382
 - definizione di una porta 68, 385, 412
 - disattivazione 217, 364, 366, 367
 - dscontrol 381
 - fisico 55
 - fixedweight 382
 - impostazione del peso 385, 411
 - logico 55
 - mapport 106, 383
 - nalcontrol 450
 - non permanente (ignora affinità di porta) 382, 385
 - posizionato con nat 197
 - protocol 383
 - returnaddress 383
- server (*Continua*)
 - riavvio di tutti i server con i pesi normalizzati 366, 402, 404
 - rimozione 385, 411, 412
 - ripristino di un server guasto 178
 - router 383
 - sscontrol 411
 - suddivisione in partizioni 55
 - weight 382
- server specifici del collegamento 68, 69, 181
- server specifico del collegamento 224
- servizio
 - configurazione 170
- set
 - cbrcontrol 387
 - dscontrol 387
 - sscontrol 413
- Site Selector
 - advisor e destinazioni finali
 - contrassegnano tutti i server come inattivi (Windows) 322
 - avvio e arresto 269
 - bilanciamento del carico dei Dispatcher in disponibilità
 - elevata 204
 - comandi 391
 - comportamento imprevisto della GUI con schede Matrox AGP 321
 - configurazione
 - configurazione della macchina 130
 - panoramica delle attività 127
 - determinazione delle funzioni da utilizzare 25
 - disconnessione dall'host quando si utilizza l'amministrazione Web 321
 - errore di lbadmim 320
 - errore di sscontrol 320
 - Errore memoria / thread di Java (HP-UX) 322
 - errori di bilanciamento del carico in presenza di instradamenti duplicati 321
 - esempio di avvio rapido 119
 - esempio di configurazione 14
 - impostazioni di bilanciamento del carico 176
 - nuovi tentativi dell'advisor sui server 184
 - timeout dell'advisor per i server 183
 - mancata esecuzione 320
 - mancata esecuzione del round-robin del traffico dai client Solaris 320
 - mancato avvio di ssserver su Windows 321
 - panoramica 13
 - pianificazione 123
 - tabella di risoluzione dei problemi 285
 - uso 269
 - Visualizzazione di caratteri nazionali
 - Latin-1 corrotti (Windows) 321
- sitename
 - sscontrol 414
- SNMP 257, 261

- SNMP (Simple Network Management Protocol) 261
- soglia di sensibilità 239
- Solaris
 - comando arp publish 68
 - configurazione della macchina
 - Dispatcher 65
 - installazione 36
 - requisiti 36
- specifico del cluster
 - proportions 414
- SSL 68
- SSL (Secure Sockets Layer) 68
- ssserver
 - avvio 120
- stato, visualizzazione
 - server su una porta specifica 373
- status
 - cbrcontrol 388
 - dscontrol 388
- supporto IPv6 79
 - abilitazione dei pacchetti IPv6 85
- advisor, uso 82
- autoconf6, AIX 85
- comandi dscontrol 90
- considerazioni sulla
 - configurazione 81
- creazione dell'alias della NIC 86
- differenze di sintassi dei comandi 89
- disponibilità elevata 83
- dsconfig 86
- funzioni non supportate 82
- ifconfig 86
- indirizzo locale di collegamento 81
- ip addr 86
- Metric Server 84
- modprobe, Linux 85
- posizionamento 83
- supporto piattaforme 80
- supporto rete geografica 221
 - esempio di configurazione 225
- Linux 227
- uso di Dispatcher remoto 222
- utilizzo di advisor remoti 223
- utilizzo di GRE 227
- supporto senza kernel 80
- supporto spazio utente 80

T

- tabelle di risoluzione dei problemi
 - CBR 284
 - Componente Dispatcher 278
 - Controller Cisco CSS 287
 - Controller Nortel Alteon 288
 - Metric Server 289
 - Site Selector 285
- timeout inattività 260, 347, 350, 371

U

- unità loopback
 - alias 70

V

- verifica
 - configurazione 150, 172
- versione, visualizzazione
 - advisor 343, 394, 396
 - gestore 367, 403, 405
- visualizzazione
 - contatori interni 352
 - elenco di
 - advisor che attualmente forniscono le metriche 342, 395
 - numero versione
 - del gestore 367, 403, 405
 - dell'advisor 343, 394, 396
 - report delle statistiche 366, 402, 403
 - report sullo stato di un advisor 342, 393, 395
 - stato di
 - server su una porta 373
 - un cluster o tutti i cluster 348
 - valori globali e impostazioni predefinite
 - per il gestore 367, 403, 404
 - per un advisor 343, 394, 395

W

- WAS (WebSphere Application Server)
 - advisor WAS 186, 189
- Windows
 - comando executor configure 67
 - configurazione della macchina
 - Dispatcher 65
 - installazione 38
 - requisiti 38



Printed in Denmark by IBM Danmark A/S

GC13-3365-02



Spine information:



WebSphere Application Server

Guida alla gestione per Load Balancer

Versione 6.1

GC13-3365-02